

# IS CASH STILL KING? REVIEWING THE RISE OF MOBILE PAYMENTS

---

## HEARING BEFORE THE TASK FORCE ON FINANCIAL TECHNOLOGY OF THE COMMITTEE ON FINANCIAL SERVICES U.S. HOUSE OF REPRESENTATIVES ONE HUNDRED SIXTEENTH CONGRESS SECOND SESSION

---

JANUARY 30, 2020

---

Printed for the use of the Committee on Financial Services

**Serial No. 116–80**



---

U.S. GOVERNMENT PUBLISHING OFFICE

42–795 PDF

WASHINGTON : 2021

## HOUSE COMMITTEE ON FINANCIAL SERVICES

MAXINE WATERS, California, *Chairwoman*

CAROLYN B. MALONEY, New York	PATRICK McHENRY, North Carolina,
NYDIA M. VELAZQUEZ, New York	<i>Ranking Member</i>
BRAD SHERMAN, California	ANN WAGNER, Missouri
GREGORY W. MEEKS, New York	PETER T. KING, New York
WM. LACY CLAY, Missouri	FRANK D. LUCAS, Oklahoma
DAVID SCOTT, Georgia	BILL POSEY, Florida
AL GREEN, Texas	BLAINE LUETKEMEYER, Missouri
EMANUEL CLEAVER, Missouri	BILL HUIZENGA, Michigan
ED PERLMUTTER, Colorado	STEVE STIVERS, Ohio
JIM A. HIMES, Connecticut	ANDY BARR, Kentucky
BILL FOSTER, Illinois	SCOTT TIPTON, Colorado
JOYCE BEATTY, Ohio	ROGER WILLIAMS, Texas
DENNY HECK, Washington	FRENCH HILL, Arkansas
JUAN VARGAS, California	TOM EMMER, Minnesota
JOSH GOTTHEIMER, New Jersey	LEE M. ZELDIN, New York
VICENTE GONZALEZ, Texas	BARRY LOUDERMILK, Georgia
AL LAWSON, Florida	ALEXANDER X. MOONEY, West Virginia
MICHAEL SAN NICOLAS, Guam	WARREN DAVIDSON, Ohio
RASHIDA TLAIB, Michigan	TED BUDD, North Carolina
KATIE PORTER, California	DAVID KUSTOFF, Tennessee
CINDY AXNE, Iowa	TREY HOLLINGSWORTH, Indiana
SEAN CASTEN, Illinois	ANTHONY GONZALEZ, Ohio
AYANNA PRESSLEY, Massachusetts	JOHN ROSE, Tennessee
BEN McADAMS, Utah	BRYAN STEIL, Wisconsin
ALEXANDRIA OCASIO-CORTEZ, New York	LANCE GOODEN, Texas
JENNIFER WEXTON, Virginia	DENVER RIGGLEMAN, Virginia
STEPHEN F. LYNCH, Massachusetts	WILLIAM TIMMONS, South Carolina
TULSI GABBARD, Hawaii	VAN TAYLOR, Texas
ALMA ADAMS, North Carolina	
MADELEINE DEAN, Pennsylvania	
JESUS "CHUY" GARCIA, Illinois	
SYLVIA GARCIA, Texas	
DEAN PHILLIPS, Minnesota	

CHARLA OUERTATANI, *Staff Director*

TASK FORCE ON FINANCIAL TECHNOLOGY

STEPHEN F. LYNCH, Massachusetts, *Chairman*

DAVID SCOTT, Georgia  
JOSH GOTTHEIMER, New Jersey  
AL LAWSON, Florida  
CINDY AXNE, Iowa  
BEN McADAMS, Utah  
JENNIFER WEXTON, Virginia

TOM EMMER, Minnesota, *Ranking Member*  
BLAINE LUETKEMEYER, Missouri  
FRENCH HILL, Arkansas  
WARREN DAVIDSON, Ohio  
BRYAN STEIL, Wisconsin





# CONTENTS

	Page
Hearing held on:	
January 30, 2020 .....	1
Appendix:	
January 30, 2020 .....	33

## WITNESSES

THURSDAY, JANUARY 30, 2020

Ahmed, Usman, Head of Global Public Policy, PayPal Inc. ....	6
Del Rio, Deyanira, Co-Director, New Economy Project .....	4
Ford, Kim, Executive Director, U.S. Faster Payments Council (FPC) .....	11
Klein, Aaron, Fellow, Economic Studies, and Policy Director, Center on Regulation and Markets, Brookings Institution .....	7
Tetreault, Christina, Senior Policy Counsel, Consumer Reports .....	9

## APPENDIX

Prepared statements:	
Payne, Hon. Donald M. ....	34
Ahmed, Usman .....	37
Del Rio, Deyanira .....	47
Ford, Kim .....	55
Klein, Aaron .....	65
Tetreault, Christina .....	76

## ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Lynch, Hon. Stephen F.:	
Written statement of Americans for Common Cents .....	88
Written statement of Cardtronics .....	94
Written statement of Coinstar .....	102
Written statement of the Electronic Payments Coalition .....	105
Written statement of the Electronic Transactions Association .....	108
Written statement of FMI-The Food Industry Association .....	111
Written statement of the Innovative Payments Association .....	118
Javelin Advisory Services report entitled, “Growing P2P Adoption” .....	126
Written statement of the Merchant Advisory Group .....	146
Written statement of the Modern Money Network .....	150
Written statement of the Money Services Business Association .....	154
Written statement of Nacha .....	158
Written statement of the National Association of Convenience Stores .....	160
Written statement of the National Grocers Association .....	162
Written statement of the Payment Card Industry Security Standards Council .....	164
Written statement of The Pew Charitable Trusts .....	171
RPGC Group Investigative White Paper entitled, “Payment Insecurity—How Visa and Mastercard Use Standard-Setting to Restrict Competition and Thwart Payment Innovation” .....	179
Written statement of the Secure Payments Partnership .....	247



## IS CASH STILL KING? REVIEWING THE RISE OF MOBILE PAYMENTS

---

Thursday, January 30, 2020

U.S. HOUSE OF REPRESENTATIVES,  
TASK FORCE ON FINANCIAL TECHNOLOGY,  
COMMITTEE ON FINANCIAL SERVICES,  
*Washington, D.C.*

The task force met, pursuant to notice, at 9:34 a.m., in room 2128, Rayburn House Office Building, Hon. Stephen F. Lynch [chairman of the task force] presiding.

Members present: Representatives Lynch, Scott, Gottheimer, Axne, McAdams; Emmer, Luetkemeyer, Hill, Davidson, and Steil.

Ex officio present: Representatives Waters and McHenry.

Also present: Representatives Himes, Payne, Hollingsworth, and Gonzalez of Ohio.

Chairman LYNCH. The Task Force on Financial Technology will now come to order.

Good morning. Without objection, the Chair is authorized to declare a recess of the task force at any time. Also, without objection, members of the full Financial Services Committee who are not members of this task force are authorized to participate in today's hearing.

And without objection, Representative Donald Payne of New Jersey may also participate in today's hearing and be recognized by the Chair to question witnesses under the 5-minute rule, so long as all members of the Committee on Financial Services who are present have been recognized for that round of questioning.

Today's hearing is entitled, "Is Cash Still King? Reviewing the Rise of Mobile Payments." I now recognize myself for 4 minutes to give an opening statement.

Again, welcome, everyone. Good morning, and thank you for attending this hearing of the task force, and thank you for joining us today. We are here to discuss the future of payments in America. Over the past few years, we have heard anecdotal but growing evidence that retailers and consumers are moving toward a cashless society, a society where consumers don't carry cash and retailers don't accept it, instead using either plastic or mobile forms of payment. A truly cashless future is not imminent, but the rise is real, and today's conversation is to help our committee better understand the implications of that rise for financial inclusion, consumer privacy, and costs to both business and consumers.

New payment methods, the theory goes, speed up transactions to give consumers more control over their money, and make operating a business cheaper and safer. A consumer can swipe a card or tap

their phone instead of making change at the register. That transition is then instantaneously documented with her financial institution, automatically adding it to her ledger which tracks spending and available balances, and the business gets to avoid the time and expense of accounting for safely storing and moving physical currency.

However, the use of physical cash is still a major part of our retail economy. Research shows that cash payments make up 42 percent of transactions under \$25, and 49 percent of transactions under \$10. These transactions disproportionately involve disadvantaged and working-class Americans.

Cashless payments typically require that consumers have access to a bank account to back their payment method. Despite improvements over the past few years, the most recent FDIC survey showed that roughly 14 million adults, 6½ percent of America's households, lack bank account access. If we don't solve the problem of banking access before transitioning to a cashless society, we will be preventing families across the country from accessing many of the basic goods and services they need to survive.

Further, high-profile data breaches have been a regular fixture in the news over the past few years. This has left consumers rightly concerned about the security of their financial data. Cash transactions involve no consumer data being collected, while non-cash payments require at least some data to be exchanged.

More than a quarter of all malware attacks in 2018 were directed at banks and financial organizations. As the amount of personally identifiable information (PII) stored by financial services firms grows, we will continue to see a rise in the attacks on these groups. And while our financial institutions continue to combat these attacks, some consumers choose to manage their finances in cash. A cashless future would not give these Americans that choice.

We need to continue to promote innovation and payment technology, inclusion, and security. I hope that today's hearing will focus on the ways we can develop our payment system to reflect these needs. The ubiquity of mobile payments is on the rise in Europe and Asia, and our competitors there will also continue to develop their own technology. We must learn from their experience and focus on meeting the needs of all of our consumers here at home.

So I look forward to today's discussion, and to hearing from our witnesses. With that, I now recognize my friend, and the new ranking member of the task force, Mr. Emmer, for 5 minutes for an opening statement.

Mr. EMMER. Thank you, Mr. Chairman, and thank you for convening this hearing on mobile payments.

I want to take a moment to acknowledge the concerns that some of our witnesses will offer in their testimony, some of which you just shared. There are serious public policy challenges to address, and I look forward to working through them with you and everybody on this task force. However, I may differ in tone today because I would like to look at the many positive changes and innovations we have in mobile payments.

We have tremendous innovation occurring in the mobile payment space. The term, "mobile payments," is so broad that it even fails

to capture all of the improvements in ease and convenience of payment as well as the growing methods of payment.

We can't be afraid of innovation and change. Ignoring, or even suppressing innovation, will not make it go away. Innovation can actually be a key driver in lowering costs to individuals and creating new ways to enhance consumer protection.

We have so many ways to pay today using our digital devices. This past holiday season, Americans spent more than \$50 billion just using their phones. Apple Pay, Venmo, Zelle, Square Cash, and even Bitcoin are now household names. Some of the most successful mobile payment applications include Uber and Lyft, or I can open my favorite merchant mobile app, select items to purchase, see what coupons and rewards are available, and in one click, pay for my items.

This hearing is titled, "Is Cash Still King?" While we have differing opinions among our witnesses and among task force members, is this really the right question to ask? Regardless of the dominant form of payments, shouldn't we be asking, how can we make access to commerce easier and more fair? How do we ensure financial inclusion in an evolving world? How can new forms of payment facilitate access to services and uplift struggling Americans?

Cash is undoubtedly still with us, and will remain that way for the foreseeable future, but this is the Financial Technology Task Force, and I hope we spend some time trying to learn about and better understand the changes taking place in our society. And I hope we discuss ways that mobile payments can include everyone and enable access to capital and financial services in ways that were previously impossible.

I would also like to acknowledge former Ranking Member French Hill for his efforts in this space. Representative Hill led a letter to the Federal Reserve supporting further research into the concept of a digital dollar. This concept could both speed up transactions and provide convenience for consumers, but it could also extend access to those previously excluded, and help bring more people into our increasingly digital world.

In advance, I thank the witnesses for their time and insights on these topics. I look forward to the discussion today, and I yield back.

Chairman LYNCH. The gentleman yields back.

The Chair now recognizes Mr. Scott from Georgia for 1 minute.

Mr. SCOTT. Thank you very much, Chairman Lynch. I look forward to today's hearing on financial inclusion, how we can work on that, on how payments innovation can improve access and convenience for underbanked customers. Also, security in our financial system, and how an increase in online transactions impact transparency and fraud.

And also, Mr. Chairman, our task force has been critically engaged in the ways that cutting-edge technology can benefit consumers and small businesses. I look forward to our distinguished panelists. And thank you, Mr. Chairman.

Chairman LYNCH. The gentleman yields back.

Today, we welcome the testimony of a distinguished and accomplished panel of witnesses: Ms. Deyanira Del Rio, the co-executive

director of the New Economy Project, an organization built to support community-controlled development and produce safe and healthy communities; Mr. Usman Ahmed, head of global public policy at PayPal, a leading company in digital payments technology, and owner of the peer-to-peer payments company, Venmo, which I use to continually send money to my daughter in college, at Elon University in North Carolina—she appreciates your service; Mr. Aaron Klein, a fellow in economic studies, and the policy director for the Center on Regulation and Markets at the Brookings Institution. Mr. Cline has also served as Deputy Assistant Secretary for Economic Policy at the Treasury Department, and as the Chief Economist for the Senate Banking Committee.

Next, Ms. Christina Tetreault, senior policy counsel at Consumer Reports, a nonprofit consisting of policy and legal experts who advocate for pro-consumer policies and financial services; and Ms. Kim Ford, executive director of the U.S. Faster Payments Council, an industry trade organization dedicated to modernizing the U.S. payment system.

Thank you all for being here, and for helping the task force with its work. Witnesses are reminded that your oral testimony will be limited to 5 minutes. And without objection, your written statements will be made a part of the record.

Ms. Del Rio, you are now recognized for 5 minutes to give an oral presentation of your testimony.

**STATEMENT OF DEYANIRA DEL RIO, CO-DIRECTOR, NEW ECONOMY PROJECT**

Ms. DEL RIO. Thank you. Chairman Lynch, Ranking Member Emmer, and members of the Task Force on Financial Technology, thank you for the invitation to testify at today's hearing. I am here on behalf of the New Economy Project, an economic justice center in New York City that, for more than 25 years, has worked with low-income New Yorkers and community-based organizations to challenge systemic discrimination in our financial system, and to advance fair lending, financial inclusion, and reinvestment as a matter of racial justice, and to ensure the tools are available for equitable neighborhood development.

I am pleased to share our perspectives on some of the issues being discussed at today's hearing, focusing on bank redlining, and continued impediments to banking access for too many Americans, as well as the growth of cashless businesses and disparities in financial services access as they play out in low-income neighborhoods and communities of color.

I have attached to my testimony several maps that just paint a bit of the landscape in New York City and show the vast disparities in terms of where bank branches even locate based on the racial composition of neighborhoods. And you will see that on the maps, they show that there is fewer than one bank branch per 10,000 residents in communities that are predominantly Black or Latino, and that compares to 3½ branches in predominantly white neighborhoods. It is just one indicator that shows the different kind of financial services landscape that people encounter in their daily lives, not only in New York City but throughout the country, where those patterns play out consistently.

I want to emphasize a few things in my verbal testimony. One is that the issues addressed in today's hearing, we believe, are systemic in nature and deeply entrenched. They call for bold, systemic solutions, including strong regulation. Too often, discussions about financial access disparities, including the use of cash versus credit or debit, focus on choices or behaviors of individuals or on the need to design so-called alternative products, rather than on addressing the continued structural barriers that block millions of people, including poor people, immigrants, low-wage workers, and many others from accessing mainstream and strongly-regulated institutions, products, and systems.

As this committee knows, there are multiple impediments, and some of them include the high cost of maintaining bank accounts; persistent redlining, as I mentioned; and prohibitive identification requirements, which all create barriers to entry for millions of people.

Through our legal assistance hotline which assists thousands of people every year, we have, in fact, seen a very clear and growing pattern of mainstream banks actually pushing low-income people out of the banking system and out of regulated services in a myriad of ways.

One example is the way that banks typically will close people's accounts if they experience fraud, or at the end of the month, if they have incurred high and hidden overdraft fees and are unable to pay those overdraft fees back, which can easily total in the hundreds of dollars. Not only do banks close people's accounts in those instances, but they report those customers' information to ChexSystems and other consumer reporting databases shared by the bank, and it effectively blacklists people from opening accounts elsewhere. And so, the conversation about access to finance and how that can facilitate mobile payments needs to look at some of the continued predatory practices in our system.

I want to point out a few things. One is that while we believe that eliminating barriers to access is important, at the same time, we have to recognize that financial products and technology are not a solution to these deeply systemic problems. They aren't solving poverty or income inequality. Too often, we hear industry and policymakers tout different products and services as being the solution to deeply entrenched problems that require bolder solutions.

We also believe that we must challenge the rhetoric and the sort of alleged benefits around financial innovation and fintech, which, in the experience of low-income people and communities that we work with, just simply fail to match reality too often.

For decades, companies have invoked innovation as a smoke-screen, frankly, to evade strong regulation and to peddle inferior high-cost, or even outright predatory products, from subprime lending to payday loans to fee-riddled prepaid debit cards and payroll cards that are often marketed to low-wage workers or that employers force workers to receive their payments on, essentially transferring the cost of managing payroll from the employer to the low-wage worker.

And I just want to emphasize that the term, "fintech," obviously is very broad, and is used in many ways. It can refer to a range of companies and technologies. We recognize that appropriate and

safe technology can, of course, benefit people. But too often, we see these companies claiming to be eliminating banking deserts and supporting and empowering communities when they are, in fact, perpetuating segregation in our banking system.

One example is how fintech companies in New York are routinely seeking to circumvent strong State consumer protection laws, including our State usury laws, which have effectively kept out payday and other exploitive usurious lending from our State. The Administration's efforts currently to exempt fintech companies from critical consumer protection rules only exacerbates the serious risks.

Thank you so much for your time, and I look forward to addressing the other topics during the Q&A.

[The prepared statement of Ms. Del Rio can be found on page 47 of the appendix.]

Chairman LYNCH. Thank you, Ms. Del Rio.

Mr. Ahmed, you are now recognized for 5 minutes.

**STATEMENT OF USMAN AHMED, HEAD OF GLOBAL PUBLIC POLICY, PAYPAL INC.**

Mr. AHMED. Thank you, Chairman Lynch, Ranking Member Emmer, Chairwoman Waters, Ranking Member McHenry, and members of the task force. I would like to thank you all for giving PayPal the opportunity to testify today on the important topic of mobile payments.

Since 1998, PayPal has been at the forefront of mobile payments. PayPal operates an open, secure, and technology-agnostic digital payments platform that gives our over 300 million active account holders the confidence to connect and transact in new and powerful ways, whether they are online, in app, or in person.

Through a combination of technological innovation and strategic partnerships, PayPal creates better ways to manage and move money. We offer people and businesses choice and flexibility when they send and receive payments. Whether sending and receiving money with friends and family through apps like PayPal, Venmo, and Zoom, or engaging in e-commerce, more and more people are using their smartphones to make purchases, receive payments, and manage their accounts. Our technology is giving more people and businesses access to the global market, and the ability to use financial services tailored to their specific needs.

The mobile phone has transformed nearly every aspect of our lives. We use it to communicate with friends and family, watch our favorite shows, order a cab, change the temperature at home, and engage in payments. The growth of smartphones, over the past decade, has been incredible. In 2011, only 35 percent of Americans had access to a smartphone. The percentage grew to 81 percent by 2019. At PayPal, we have witnessed how the rise of mobile devices has transformed payments. In Q4 of 2019, 44 percent of the \$199 billion of total payment volume we processed was made on a mobile device.

The advancement of mobile payments has important implications for unbanked, underbanked, and financially unhealthy individuals and communities. For example, giving people access to money instantly via mobile device can help in reducing fees and late pay-



ments. Sending remittances using a mobile device is about half the cost of a traditional remittance, and can save over an hour of time for both the sender and the receiver. Mobile payments can also provide a baseline for credit underwriting, which can enable consumer finance during cash-flow challenges.

Mobile payments can also benefit small businesses due to the lower costs of acceptance as well as payments data being leveraged to help fill the gap in small business working capital, in particular for women- and minority-owned businesses.

Security has been front and center throughout the development of mobile payments, leading to the adoption of tokenization technology, which reduces the number of entities that have access to sensitive financial data. PayPal is a pioneer of tokenization technology. Tokenization substitutes sensitive financial information with a series of non-sensitive numbers that confirm to a business that a payment is authentic, but minimizes the likelihood of data breaches and reduces fraud. Mobile payment information is sensitive, and PayPal leverages payment data for fraud reduction and service improvement.

Cash is an ubiquitous form of payment. But while it may appear costless to transfer, there are costs associated with cash. Cash is deeply implicated in tax evasion, which costs the U.S. Federal Government some \$500 billion a year in revenue. When Mexican drug lord El Chapo was arrested, there was more than \$200 million in cash found on the premises, and the global drug trade is estimated at \$600 billion.

And finally, 20 percent of unbanked consumers report having cash lost or stolen. In a study of low-income Los Angeles area households, the finding was that the average unbanked consumer lost the equivalent of nearly 2 weeks of household expenses when cash was lost or stolen.

Mobile payments present a tremendous opportunity to reduce many of these costs associated with cash. While we don't predict the death of cash in the next decade or two, and we believe that consumers should have a choice in what payments options they choose, at PayPal, we are working diligently to make sure that the value proposition of digital payments vastly exceeds the value proposition of cash for every member of society.

Thank you, again, for the opportunity to address the task force on this important and timely topic, and I look forward to answering any questions.

[The prepared statement of Mr. Ahmed can be found on page 34 of the appendix.]

Chairman LYNCH. Thank you, Mr. Ahmed.

Mr. Klein, you are now recognized for 5 minutes.

**STATEMENT OF AARON KLEIN, FELLOW, ECONOMIC STUDIES,  
AND POLICY DIRECTOR, CENTER ON REGULATION AND  
MARKETS, BROOKINGS INSTITUTION**

Mr. KLEIN. Thank you, Chairman Lynch, Ranking Member Emmer, Chairwoman Waters, Ranking Member McHenry, and members of the task force, for the opportunity to testify on the critically important issue of the future of cash and the rise of digital wallets.

Let me start by answering the question the hearing poses. Yes, cash is still king. In fact, cash is used by a diverse set of people who defy traditional political or geographic boundaries. False narratives abound that cash is dying or a cashless society is the future or that millennials don't use cash. In fact, millennials and their grandparents have cash in common. Both generations use it more than those between ages 30 and 60.

In a sample of mostly small business transactions, Iowa and Wisconsin, two of the more cash-intensive States, have a lot more in common with the Bronx and Staten Island, while Utah and Virginia, two of the more card-intensive States, are much more similar to Brooklyn and Manhattan. Nationally, racial minorities and rural Americans both use cash more frequently, and it has been stated that cash is the most common way people pay for things under \$25.

While cash is still king, there is no denying that an increasingly large number of goods and services are moving onto digital payment platforms that do not accept cash. As the economy digitizes, those without access to low-cost, reliable digital payments are increasingly unable to participate and share in the benefits.

Prior concerns about a digital divide were centered around the question of access. Smartphones have successfully bridged this divide. However, online access alone is insufficient. Without a means to purchase the goods or services being offered, the benefits of the app, gig, or online economy fail to convey.

Access to digital payments has become the new digital divide. Online and app-based goods and services lower costs for everything from ordering groceries to hailing a cab. However, the economics of many digital services simply assume users will always have funds to cover recurring or periodic expenses, and expect the ability to tap into a consumer's bank account to get paid. Given the high cost of overdraft fees, growing income volatility, and our nation's anachronistically slow payment system, the reality for people living paycheck to paycheck is a far more expensive system than for those on the other side of the divide.

For consumers to truly benefit from the digital economy, cheap and reliable digital payments are necessary. Yet, our existing system provides them freely to those with money, and charges a lot to those without. It may require government policy and resources and strong rules to fix this problem.

A corollary to the policy that businesses continue to accept cash is that consumers have access to digital payments, and that needs to be facilitated. My written testimony goes into significant detail regarding the high and often hidden costs of existing banking products like overdraft fees that create an effectively different cost structure for people living paycheck to paycheck. It highlights multiple policies to solve some of these problems, and reduce the demand for expensive ways to access cash, like check-cashing. The key is to require immediate funds availability for consumers, which most of rest of the world developed decades ago through real-time payments.

Waiting for the Federal Reserve to follow through on its announcement to build a system sometime this decade is not enough. Policymakers could solve this problem today if they wanted to, by regulation or legislation. In fact, tomorrow is the 31st. A lot of peo-

ple will get paid that day and will struggle to come up with the amount of money available in their bank account to meet their payments on the first of the month the next day.

I want to conclude by noting that America once led the world in payment technology. Fifty years ago, America pioneered the new payment technology that would come to dominate the world, magnetic stripe plastic cards, but technology alone was not enough. It required robust consumer protection legislation from Congress, such as the Electronic Funds Transfer Act, to successfully create an environment where cards flourished.

Today, China has leapfrogged cards. China's new system is built on digital wallets, and QR codes, and runs through their own big tech firms. China's system largely disintermediates banks, and creates an alternative payment ecosystem with different incentives between merchants, consumers, and payment system providers. It challenges the longstanding placement of payments on the side of banking as opposed to commerce.

China's system is unlikely to catch on in America precisely because it is more efficient. Because it does not take large sums of money from merchants at the register, it will not be able to compete with the growing high-end credit cards that come to line America's wealthy with thousands of tax-free dollars in rewards. Ironically, the inefficiency in America's payment system that has turned it into a reverse Robin Hood that contributes income equality will block adoption of alternative technology.

This committee is wise to consider the rise of mobile wallets, and policymakers should devote more time and attention and resources to figure out how to create a more fair, efficient, and inclusive payment system.

I thank the chairman and the ranking member and the rest of the task force, and I look forward to your questions.

[The prepared statement of Mr. Klein can be found on page 65 of the appendix.]

Chairman LYNCH. Thank you, Mr. Klein.

Ms. Tetreault, you are now recognized for 5 minutes,

#### **STATEMENT OF CHRISTINA TETREAU, SENIOR POLICY COUNSEL, CONSUMER REPORTS**

Ms. TETREAU. Chairwoman Waters, Ranking Member McHenry, Chairman Lynch, Ranking Member Emmer, and members of the Financial Technology Task Force, thank you for the opportunity to be here today. I am Christina Tetreault, senior policy counsel for Consumer Reports (CR). CR is an expert, independent, non-profit organization whose mission is to work for a fair, safe, and just marketplace for all.

My CR colleague, Suzanne Martindale, testified before this committee in 2012 regarding the future of money and the rise of mobile payments. She noted that consumer privacy concerns inhibited mobile payments adoption and that fragmentation in payments law creates uncertainty for consumers. Eight years later, I will make these same points today.

American adoption of mobile payments continues to lag that of other countries. Americans still love cash, and as compared to mobile, they love cards. It is important to note that mobile is a plat-

form and not a new payment type. Beneath the modern veneer of mobile payments is mostly technology built in the early 1970s. New payments rails including faster payments and cryptocurrency are, in the case of faster payments, or should be, in the case of cryptocurrency, covered by existing laws.

Unfortunately, payments law is an irrational mess. Under current law, credit card holders have the strongest protections. Debit card, bank transfer, and prepaid accounts have weaker protections. Gift cards and direct to carrier building have almost none. Congress can fix the mess in payments law making every way safe to pay. They can do this by establishing a strong floor of uniform protections for all non-cash, non-check payments.

Now, when it comes to mobile payments, unfortunately, consumers do not understand their rights and obligations. When we asked a focus group of mobile payments users what they thought would happen if something went wrong with the payment, they uniformly said that they expected that the company whose name was on the app or wallet would fix the problem and make them whole. This is not necessarily the case. In some instances, users may, in fact, be obligated to contact their bank or card issuer for help. Other problems fall outside the scope of current law. For example, when a consumer is tricked into sending money to a scammer, they will find that these transactions have essentially the same level of protection as cash.

Now, many claims have been made about how mobile will increase financial inclusion. The reality is quite different. Americans without checking and savings accounts are less likely than bank consumers to use mobile payments and are far more cash-reliant than other Americans. Unbanked consumers are more likely to suspend or cancel their cell service because of the cost of maintaining coverage, making regular use of mobile financial services nearly impossible. No act fixes the structural issues that lock out too many Americans.

Cryptocurrency has also been proposed as a fix for financial inclusion. If the legal mess in traditional payments is bad, the legal mess in cryptocurrency is worse. The few consumer protections that cryptocurrency payments have are largely found in State money transmitter laws and are seriously lacking.

Cryptocurrency, and for that matter, any emerging financial service should not be tested on consumers with the least cushion in their financial lives. The best way to ensure consumer access to faster and safer electronic payments is to support the Federal Reserve's proposal to build the FedNow faster payment system, and not by empowering untested, unregulated corporate schemes such as Facebook's Libra.

There is another shadow over mobile payments. The current protections for mobile payments made with stored value, for example, the money held in Venmo accounts, are threatened by the PayPal lawsuit seeking to invalidate the Consumer Financial Protection Bureau's (CFPB's) prepaid rule. Before the rule, consumers had to rely on the inadequate protections provided by State money transmitter laws. Billions of dollars and millions of consumer accounts are at risk if this rule is invalidated.

Privacy concerns exist alongside legal concerns in mobile payments. So while mobile payments and even some additional financial services are free to consumers, users are not the customers of these services. They are, in fact, the product. The potential for users' information to be weaponized against them is particularly acute when payments are combined with platforms.

We need strong privacy legislation that creates a Federal floor of protections, a law that requires data minimization, clear information about provider practices, and strong data security standards. This law must also have vigorous enforcement tools and tools to ensure accountability.

I thank you for the opportunity to be here today, and I look forward to your questions.

[The prepared statement of Ms. Tetreault can be found on page 76 of the appendix.

Chairman LYNCH. Thank you, Ms. Tetreault.

And Ms. Ford, you are now recognized for 5 minutes.

**STATEMENT OF KIM FORD, EXECUTIVE DIRECTOR, U.S.  
FASTER PAYMENTS COUNCIL (FPC)**

Ms. FORD. Good morning, Chairman Lynch, Ranking Member Emmer, and distinguished members of the task force. Thank you for the invitation to be here today. My name is Kim Ford, and I am executive director of the U.S. Faster Payments Council (FPC). The FPC is a membership organization that is leading the industry effort to modernize the U.S. payment system. We were formed from the work of the Federal Reserve's Faster Payments Task Force, which brought the industry together to start to figure out how to make the U.S. payment system faster, more secure, and more efficient. I am grateful for the opportunity to be with you today as we examine consumers' payment preferences, and look to what the future may hold for the U.S. payment system as a result.

As you know, the payments landscape is in the midst of unprecedented change. When I entered this industry in 2004, the headline at that time was that checks were just starting to lose ground to debit and credit cards, and now, we are talking about things like mobile payments, biometrics, machine learning, artificial intelligence, cryptocurrency, and more. Clearly, we have transitioned in this country from an environment dominated by paper checks and cash to one dominated by electronic payments. And we are seeing that cash is being used less and less for some of the major payment categories it once led.

For example, historically, cash has been used for low value payments below \$25, but we are seeing card use grow in this area as well. And as we think about why that is, two themes come across most clearly: consumers' desire for convenience; and consumers' desire for security. Take electronic payment cards. They are accepted at retailers across the globe. They enable convenient tracking of transactions, provide budgeting options, and provide consumers with protections against loss and fraud. And while cash may also be convenient, easy to carry, and widely accepted, it can be easily lost or stolen, and there are no measures in place for consumers to recoup such funds.

For these reasons, among others, electronic payments have climbed the ranks to become a preferred payment option for U.S. consumers. Moreover, as Americans incorporate their smartphones into so many aspects of their lives, they also expect that on-demand functionality to transact with their friends, family, businesses, employers, and even the government.

This has translated to an increase in the use of smartphones for things like internet banking, e-commerce transactions, and the use of mobile payment apps. One study by payment provider TSYS reported that over the last 3 years of their consumer payment research, survey respondents consistently rated the most attractive features of mobile payments as: one, the ability to immediately stop a fraudulent transaction; two, the ability to instantly view their transactions; and three, the ability to use their phone to turn their payment card on or off to prevent unauthorized usage. These findings underscore so many Americans' increasing reliance on electronic payments to solve for convenience and added security.

But of course, the popularity of mobile phones and access to the internet are not enough to increase financial inclusion, and certainly, it is appropriate to ensure that people can actually benefit from digital financial services. And this, of course, requires a well-developed payment system, reliable and accessible infrastructure, and a robust regulatory framework with consumer protection safeguards. And while we haven't completely solved the access issue in the U.S., financial inclusion is getting better, due in part to new types of financial services that are accessed through mobile phones and the internet.

But challenging our system to be better isn't limited to plastic cards and mobile phones. At the FPC, we believe that the next evolution of our payment system is a more real-time, safe, and efficient system that anyone can access at any time, anyhow, and anywhere. We believe that faster payments have the potential to build on the benefits of current electronic payment mechanisms, and further improve money management, remove costly paper processes, minimize settlement risks, and encourage global competitiveness.

Our members believe it so much that they created an organization to bring all the payment industry stakeholders segments together to identify barriers to faster payments adoption and then work shoulder to shoulder to solve those problems.

For example, we are examining the regulatory landscape for faster payments, studying fraud best practices and trends, promoting transparency for consumer and business end users, assessing directory models, and helping our members understand how to develop and implement a faster payment strategy.

Yes, we support electronic payments, but we also support an environment in which payment choice is preserved, whether that be paying with cash, writing a check, sending a wire ACH, or using a credit, debit, or prepaid card. I am also proud of the fact that we are demonstrating that it is possible to get a widely diverse group of industry stakeholders together, representing consumer groups, merchants, tech providers, financial institutions, and more, to tackle complex problems in a fair, inclusive, and transparent manner with an end goal on which we all agree, which is driving universal

access to a faster payment system that delivers a high quality and secure user experience for all.

Thank you for the opportunity to present to you, and I look forward to answering your questions.

[The prepared statement of Ms. Ford can be found on page 55 of the appendix.]

Chairman LYNCH. Thank you, Ms. Ford. I now yield myself 5 minutes for questions.

Mr. Klein, you illustrate a good point where if you look at young people and their consumer preferences, you know, our two girls, I don't think, have ever been in a bank except for maybe getting travelers' checks or something like that. Probably less than 5 times in their lifetime, compared to how I grew up, where on payday, you would go down there and stand in line with everybody else.

So this is a trend that is really overtaking us, and it is being driven by consumer preference. I don't think it is necessarily some cabal or diabolical plan. I think it is just easier, and people want to do it. The problem is that not everybody has that opportunity.

You have an interesting background in terms of looking at international payment systems and things like that. Are there models out there that would sort of address what we are trying to get at? We know this is much cheaper, and in many ways, more efficient and safer in some instances. Are there systems out there that do a better job than we have right now in terms of the payment systems that are out there?

Mr. KLEIN. Yes. Chairman Lynch, it pains me to say this, but China's system is much more efficient, much faster, and has reached a level of universal adoption that is somewhat mind boggling. You have 2 services that started less than 5 years ago, and they each have a billion monthly users.

Chairman LYNCH. Yes.

Mr. KLEIN. And they were able to do it, in part—one of the fascinating things about the Chinese experience is this is a country that had, by some estimates, 7 million debit cards, but only 20 million to 40 million card readers. You could not take a card—go around China and try and do something with your magnetic stripe card, and they look at you like you are from a century ago.

It is all on codes and digital wallets. Now, the problems with the Chinese system—I am not advocating that we move there, particularly because of some of the commercial concerns involved in bringing the banking system—the payment system outside of banking. And our legal and regulatory framework completely assumes that payments are part of a banking system. As Ms. Tetreault's testimony points out, everything is tied to this being in banking. When you legally look at the cleft between banking and commerce in the United States, there is nothing that ties payments onto the banking side.

Chairman LYNCH. Thank you.

And Ms. Tetreault, I want to ask you—we raised the China model. So right now, if banking goes the way of the internet where they just collect all of our information, not what they need to, but everything they can get their hands on, and then they screen scrape and sell personal data, personal financial data—I know that you have written extensively on privacy. Do we need a new archi-

ture, with respect to financial data than we—we have given it away in terms of our personal data on the information side, on the internet side. Do we need a new architecture to be more covetous and protective of our financial data, or can we overlay this on the existing system?

Ms. TETREAULT. I think there are two solutions to the problem. The first is provider practices, so enabling tools for consumers to be able to really see what information is being collected and then make choices, and there are efforts out there. I know that the Financial Data Exchange was here before the committee previously, and they are creating those tools, and those tools are very helpful and more supportive of that effort.

The other aspect, though, is strong, a Federal privacy floor that actually includes curbs on data collection and sharing. The Gramm-Leach-Bliley Act (GLBA) is often touted as a privacy law, but it is not, in fact, privacy protected in those ways, so it is time for a new approach.

Chairman LYNCH. Right. Thank you.

Mr. Ahmed, speaking for Venmo and for the industry in terms of what you have come up with, are there mechanisms or models that you identify that might address the concerns that we have raised here?

Mr. AHMED. Certainly. I want to acknowledge something Mr. Klein raised about merchant acceptance. In China, a lot of the reason why there has been success there in moving to mobile payments was getting all of the businesses to accept these small QR codes. And I agree with Mr. Klein that maybe it is that model, or maybe it is something else. But I just want to stress that when we are talking about consumer adoption, low- and moderate-income consumers, rural consumers, if the places where they go don't accept mobile payments, then they won't switch. It is a chicken-and-egg problem, and we also have to include a focus on the merchant side of the equation.

Chairman LYNCH. That is great. Thank you very much. My time has expired.

I now recognize the gentleman from Minnesota, our ranking member, Mr. Emmer, for 5 minutes.

Mr. EMMER. Thank you, Mr. Chairman, and thank you to the witnesses for your testimony and for being here today. It is interesting. More than one of you this morning was critical in different respects to the promise that the innovation, that new technologies provide. In fact, I think one of you even referred to the rhetoric that gets used about how this is going to benefit consumers in society.

I could focus on several, but in my short time, Ms. Tetreault, I was particularly concerned by some provisions in your written testimony that you have submitted that criticize cryptocurrency, although you only mention Libra which is not, in itself, a cryptocurrency. I would hope that you more fully explored these innovations, or if you haven't, that you will be in the opportunities that they provide to both build a financial future for individuals, but also to empower individuals to control the value of their own assets separate from government control. Have you done any of that?



Ms. TETREAULT. We have looked at cryptocurrency, and I made remarks almost, what, 6 or 7 years ago, that the original promise of cryptocurrency was returning power to consumers. And what, in fact, has happened in the intervening years is that—what we have seen is an infrastructure that is built up, that is largely acting as an intermediary, that consumers are not truly empowered to “be their own bank.” And that these intermediaries are often under-regulated, and undersupervised, that there aren’t clear rules of the road, and so the promise of cryptocurrency in many ways has been lost.

There are any number of needs, not the least of which is to fold them into payments law in a more rational way, and to rationalize payments law overall.

Mr. EMMER. Right. As defined by you or someone else what is rational. Seriously. It is your definition of what is rational, because there is a whole environment out there, brilliant, genius young people who are coming up with new ways to transfer value every single day, and I worry that we are going to crush that entrepreneurial spirit and that advancement. Obviously, you and I, we have heard of Bitcoin. We have heard of Ethereum. Are you familiar with XRP and the efforts of Ripple?

Ms. TETREAULT. With the distributed ledger technology for their payments?

Mr. EMMER. Yes. And you are familiar with Eos?

Ms. TETREAULT. No.

Mr. EMMER. What about privacy coins like Monero or Zcash?

Ms. TETREAULT. I had a footnote. If I understood the aim of this hearing, it was that I was not going to approach the privacy concerns. There are any number of different privacy technologies around cryptocurrencies. Some are concerning, some are very promising, and it really is very item-specific. So I don’t have a lot to say on that, only that you are right. I agree with you that there are definitely some interesting things going on there.

Mr. EMMER. How about Zero Pay and Algorand? What about Stellar, which is facilitating cross-border transfers? Are you familiar with that one?

Ms. TETREAULT. No.

Mr. EMMER. I could keep going through these, but it is amazing, the things that are happening out there, and it concerns me when we are talking about mobile payment systems, and we draw in any one of you, cryptocurrency or these new innovations and suggest that it is a negative. Because, by the way, major companies like IBM are doing work on this too. The Plastic Bank is a pilot program that has proven to be successful in Haiti, where a digital asset is provided in return for cleaning up plastic waste, amazing things. Are you familiar with M-Pesa?

Ms. TETREAULT. Yes.

Mr. EMMER. We should talk because somebody used the term, “rhetoric.” “M” stands for mobile. “Pesa” is Swahili for money. This is a mobile phone-based money transfer, financing, and micro-financing service launched in 2007 by Vodaphone, the largest mobile network operator in Kenya and Tanzania. By 2012, it had 17 million accounts. This service has been credited with giving mil-

lions of people access to the formal financial system and for reducing crime in the otherwise largely cash-based society.

Again, I think we have to take a deeper look at this and learn more about these innovations. It is not black and white. And the really interesting developments come when you start to get into the details and differences in the technology. So I would appreciate it, as we talk about mobile payments and move forward, if we could be more inclusive about the technologies instead of fearing something that we don't know enough about. Thank you.

Chairman LYNCH. The gentleman yields back. The Chair now recognizes the gentleman from Georgia, Mr. Scott, for 5 minutes.

Mr. SCOTT. Thank you very much, Mr. Chairman. Ladies and gentlemen, first, let me say that each of your testimonies were very, very informative, and opened our eyes, I am sure, to much of what we were only dimly aware of. However, this whole issue is sort of bringing us into the new frontier for our entire financial services industry. It is very important.

I have been spending quite a bit of my time dealing with an issue that I want to present to this committee, which is, are we doing enough to make sure we address this fundamental problem? According to the most recent statistics, there are 58 million unbanked and underbanked folks out there. What is most startling is that most of these are unbanked, meaning they don't have a savings account, not mama, not daddy, sister, brother. Nobody in the household has a savings account or a checking account.

Mr. Ahmed, let me start with you. How do we address this to make sure that we are providing the transparency, the affordability, the convenience for these consumers, but access to electronic payment systems have traditionally required a savings account, or a checking account, which presents challenges here. How are you all at PayPal, which has certainly been a forerunner in all of this, addressing this issue to make sure we bring everybody along with us as we make this technology jump?

Mr. AHMED. Thank you for the question, Mr. Scott. I think it has to be done in partnership. PayPal is a technology company, but there are all sorts of entities that are on the ground in the communities, in the places where you are talking about. I think of retailers, 7-Eleven, Walmart. I think of a remittance provider like ARIAS, where we can partner with those entities, enable cash to be offered up at the point of sale, and then digitize it on the back end.

So I think it is really in getting on the ground in the communities and the places where these people are and providing them a service, as I mentioned in my testimony, that is actually more valuable than just a cash-based service. Because until and unless we create a value proposition that really can respond to the challenges and the issues that they are facing, then there won't be a reason to move into this ecosystem.

Mr. SCOTT. Are you confident that we will not leave these unbanked and underbanked folks behind?

Mr. AHMED. I would say at PayPal, we are making very, very strong efforts to do that, and I think it is going to be about everyone in this room working together, a public-private partnership,

and intentionality behind the efforts in order to prevent that from happening.

Mr. SCOTT. Do you think there are costs associated with accepting cash for small businesses?

Mr. SMITH. Certainly. I think a typical small business, when they are accepting cash, they assume that it is a costless transaction. But actually, when it comes to simple things like accounting for that cash, doing payouts to employees, doing payouts to vendors, providing security for the cash, there are actually a number of costs associated with that. My mom was a small business owner, and I remember the challenges of trying to account for everything. And so, digital kinds of transactions can really help to simplify a lot of those processes and reduce some of those transaction costs.

Mr. SCOTT. Ms. Ford, you have been working very much in this area throughout your career. What are your thoughts on this?

Ms. FORD. I think that we have to recognize that, obviously, there are limitations that financial institutions have because there is a regulatory framework in which they have to operate. But I think when we look at the experience in the U.S. as well as globally, I think that is one reason we have seen the rise of non-bank fintechs who are saying, okay, we have this great technology out there. We want to try to be some sort of a link to consumers. So if we can be that intermediary and try to get somebody who is unbanked to be more comfortable, maybe it starts with a gift card or some sort of prepaid card they can load with cash. Then, that gets them slowly into the financial services system, and they can become banked. That is obviously where we want to move things.

So I think that we are making progress, but I agree with you that the unbanked issue is very real. It is one reason that at the FPC, we have a whole consumer segment who are constantly asking, how are we going to make this as inclusive as possible? But I do think we have to acknowledge that financial institutions are constrained by certain regulations as well.

Mr. SCOTT. Thank you very much.

Thank you, Mr. Chairman.

Chairman LYNCH. The gentleman yields back.

The Chair now recognizes the gentleman from Missouri, Mr. Luetkemeyer, for 5 minutes.

Mr. LUETKEMEYER. Thank you, Mr. Chairman.

Mr. Klein, you made my day today when you said a while ago that the seniors and the millennials have something in common with regard to cash. Seniors don't have anything in common with millennials, so thank you.

Mr. KLEIN. You are welcome.

Mr. LUETKEMEYER. Also, one of the attributes and one of the benefits, I guess, of being a little older and having been through the mill a little bit here is the fact I remember when credit cards came out. Yes, I am that old. Moses and I, we came down the mountain together. And I remember everybody said, well, that is the end of the checks. No more checks. Credit cards are going to take over. Checks are gone.

But as of today, the latest Federal Reserve report from the Federal Reserve Bank of St. Louis said we actually have twice as much cash in the system now as we did 10 years ago. We still have as

many checks issued today as we did 40 years ago, or whenever credit cards—50 years ago when credit cards came out, and now, we have all different sorts of payment systems out there. If I was forming a new business today, I would have all of these kinds of payments, because it enhances the ability for me to be a new business, to transact business, to attract everybody in, and enable them to make the transaction.

So when people get exercised here about this is going to happen, that is going to happen, everybody should take a deep breath and step back. This is just an alternative, another way of doing this.

I come from the point of view of, okay, how can we do this in a safe fashion? I think Ms. Ford made some really good closing comments in her testimony a minute ago. I think Ms. Tetreault made some comments with regards to Libra and cryptocurrencies, and that, quite frankly, is now the preferred way of money laundering with cryptocurrencies for all of our nefarious folks out there.

I look at the security of the data, how you can improve the convenience for people, and how you can minimize the use of enabling people to do fraud and launder money. So to me, this is where we need to be focusing, to enhance the ability of the mobile phones and the different types of payment transactions.

Ms. Ford, I would like for you to elaborate just a little bit on your final comments about how we can make a faster system and a safer system and be more inclusive.

Ms. FORD. Absolutely. Again, one of the elements that is driving this whole conversation around faster payments, besides the fact that a lot of other countries have implemented faster payment systems, is that we have better technology out there. And I think, as we look to, for instance, the experience in the card space as it relates to security, we have seen some great innovations around encryption and tokenization where the idea is that—I think the mindset used to be, how do we protect our sensitive information from being subject to unauthorized usage?

Now, I think we know how sophisticated the criminals are, so the conversation has shifted to, how do we devalue the data, because it is likely that there is going to be some sort of a breach somewhere.

So I think those are the kinds of things that we are looking at in the context of faster payments as well, which is, how can we continue to leverage these types of innovations? For instance, if you look at fraud prevention practices historically in payments, a lot of that was very manual processes, individuals actually sitting in front of a monitor trying to look at these transactions. Now, we can think about, okay, how can we leverage artificial intelligence, for instance, or machine learning. Obviously, there can be biases in those as well, but I think there are some opportunities to be able to leverage this technology to add security components.

Mr. LUETKEMEYER. Thank you for that.

Ms. Del Rio, you talked a little bit about some of the concerns with folks who can't work with a bank because of the costs that are involved there, and they have to go to a strictly cash way of living. Have you found that because the banks charge for cashing checks or for having an account or for a minimum amount that you have

to have in there before you get free checking, is that the kind of problems that you see?

Ms. DEL RIO. Yes. Those are some examples. And just to clarify, not only are people being pushed out of the banking system and being forced to rely on cash, but then in the vacuum that banks leave in these neighborhoods is where you see the pawn shops, rent-to-own stores, and so on.

Mr. LUETKEMEYER. Why do you think that the banks are having to charge those fees?

Ms. DEL RIO. I think that the banks have made pretty clear—well, first of all, there has been a wave of deregulation of the banks, and there is a weakening of the Consumer Financial Protection Bureau and other rules that govern banks. We think the banks have made pretty clear they are not very interested in serving low-income people. We see that in a myriad of ways.

And yes, the minimum balances that banks require to avoid fees is one impediment. Identification requirements that actually go far beyond what regulations require are another impediment for millions of Americans.

Mr. LUETKEMEYER. Have you talked to any banks and asked them what it costs to maintain an account?

Ms. DEL RIO. Absolutely. I am actually the board chair of a community-based credit union, and so we are very aware of the cost of implementing—

Mr. LUETKEMEYER. It is difficult to give a service for free unless you can find another way to subsidize that within your institution, right?

Ms. DEL RIO. I think one of the problems is that in terms of checking accounts, it is low-income people, through overdraft fees, who are subsidizing the free checking of more affluent people. And so, yes, we believe there are costs, and there are ways to manage the costs, but right now, the costs are not being borne fairly among banks' customers. You can look at who pays overdraft fees. It is a very small percentage of people, and it is the lower-income segment.

Mr. LUETKEMEYER. Those are loans, by the way. Thank you very much.

Chairman LYNCH. The gentleman yields back.

The Chair now recognizes the gentlewoman from Iowa, Mrs. Axne, for 5 minutes.

Mrs. AXNE. Thank you, Mr. Chairman. And thank you to the witnesses for being here today. I really appreciate it.

Obviously, we are hearing a lot of discussion about the benefits that mobile payments can provide. As the co-owner with my husband of a digital design firm, who uses PayPal literally every day, nationally and internationally, for payments, I am certainly familiar with the benefits. And I think there is absolutely so much opportunity to help people with better services, and, hopefully, we will see more of that down the road.

However, I am concerned that we are leaving some people behind. We have been talking about it today with smartphone and internet access. People can't use these wonderful services, as we well know, and the FCC estimates that approximately 20 million

Americans lack broadband service, and I certainly know that in the State of Iowa.

Also, due to the issues with mapping, we know that that number is probably far greater than just 20 million. In fact, Microsoft estimated that 150 million Americans aren't actually using the internet at broadband speeds, which they would need to be able to perform these functions, and a lot of these people are, unfortunately, in my district. That kind of difficulty is why Iowa is one of the top five States, as Mr. Klein pointed out, in terms of use of cash.

So, Mr. Klein, I am worried that moving too quickly to mobile payments will risk exacerbating what we are already seeing with rural communities absolutely being left behind. I am trying to fight to keep them getting the opportunities that we need. Are you seeing that moving to mobile too quickly and risking the opportunities for rural communities is something that your research shows to be a problem?

Mr. KLEIN. Yes, Congresswoman. It is very important to appreciate that, as the economy digitizes, there are huge benefits, and those benefits then are not accessible to people without the ability to transact in that.

I think a lot of the conversation about preference for cash that we have seen, if you dig into the data, what you really see is a rise in online purchases, particularly for that age category between 30 and 60.

Now, whether that is consumer preference or choice, or whether that is just the changing nature of our economy, because you can get these goods better, cheaper, faster, can be debated. But what does that mean for people who don't have the ability either to access that material online and to have the ability to make payment online in a convenient and low-cost fashion?

If you risk an overdraft to buy something that is \$5 cheaper online, it may end up costing you \$30 more, and part of the problem why there are so many overdrafts is, "I don't know when my paycheck has cleared." If I get paid tomorrow on the 31st of the month—10 percent of Americans get paid monthly; 38 percent get paid biweekly. A lot of people get paid tomorrow.

Do not mistake direct deposit for immediate deposit. You are not certain if your payment is going to be available for your funds the very next day, and this makes life incredibly challenging for people in rural America and for people who are living paycheck to paycheck.

The sad reality is we had the tools to fix that 10, 15, 20 years ago. The United Kingdom went to real-time payments in 2008, and Mexico in 2004.

And so I think for your constituents in rural America, you are facing a double whammy: You have this access problem, and you have a means-of-payment problem, and, particularly for those living paycheck to paycheck—and older people, for example, who may be relying on Social Security—it becomes incredibly challenging for consumers to be empowered enough to be able to solve these problems and access all of these online benefits.

Mrs. AXNE. Thank you for that. I appreciate that. And, as the State who has the fourth-oldest population in the country, I appre-

ciate your concern for them being able to get their Social Security that they need.

Moving on, Mr. Ahmed, you mentioned in your opening statement that PayPal is committed to serving every American, or something to that effect. Bringing broadband access to all Iowans is a major priority for me. As a matter of fact, I'm on the Whip's Rural Broadband Task Force. We want to make this happen. And I think it needs to be really a priority for all of the American economy, or we will leave parts of this country behind.

So I want to ask you specifically, since you work for PayPal, and I'm really asking all of the mobile payment community to get behind this priority so that everyone can actually benefit from what you have to offer. As a recipient of your product that I know works well, we need everybody to have access to this. My small business owners in Iowa need to be able to utilize services like yours.

Are there steps you are able to take to help us spread the access more quickly than we are doing right now?

Mr. AHMED. I think we can be supportive, of course, of your efforts, and I think we can also add in kind of our perspective on the benefits that access provides in terms of increased growth and increased payments, and I would also point out that you highlight access as such a key issue, but it is also cost and kind of driving down the cost for individuals, in particular, in rural areas and making sure that the data is not so expensive that, yes, you have access, but you can't actually use it.

And so, I think we can be supportive of your efforts, and I would love to kind of partner with you on that and figure out how we can be helpful.

Mrs. AXNE. We will be in contact, because we need your help. I yield back. Thank you.

Chairman LYNCH. The gentlelady yields back. The Chair now recognizes the gentleman from Arkansas, Mr. Hill, for 5 minutes.

Mr. HILL. Thank you, Chairman Lynch.

It's great to be here with you, and it's great to have a broad payments hearing today. Thank you for making those arrangements. We are having a great discussion. I have enjoyed hearing everybody's presentation.

Mr. Ahmed, I was interested in your testimony that 40 million users and 28 percent of PayPal's total volume is Venmo. I take it from looking at your—and I, too, like my friend from Massachusetts, have a regular Venmo user in my family.

My question for you is, of those 40 million people, how many of those users have an account balance with Venmo or PayPal, meaning there is cash left in their name out on the system, would you guess?

Mr. AHMED. I don't have the exact number, but I would be happy to follow up in writing and—

Mr. HILL. I would be interested in that exact number and what the average balance is because, of course, everybody knows those are not FDIC-insured deposits, and it reminds me of the old American Express traveler's checks, from the 1960s, where you have this money that PayPal gets to use, but people may or may know they have it. So, if you would follow up with me on that, I would appreciate it.

Mr. AHMED. Okay.

Mr. HILL. Also, I was pleased to read about your being involved in the Faster ID Alliance, and I assume, Ms. Ford, you are also involved in the Faster ID Alliance?

Ms. FORD. I am not, personally. Some of our members are, yes.

Mr. HILL. Yes. I think that's important because, in this Fintech Task Force, we have talked about these foundational building blocks of a digital future. Authentication is fundamental to get away from name and password, and so, if you could send me some follow-up information on that, who the members are, and what is being done there, that would be of interest.

I want to turn to tokenization, and you referenced that, and also ask Ms. Ford first on that, this idea that banks and nonbanks have a payment rail out there in the payment system—we have wire transfers, we have ACH, we have SWIFT, we have cash, obviously, we have MasterCard Direct. We have all of these different methodologies, and my question is, can we have an approved regulatory payment rail that is blockchain-based that is available to banks and nonbanks equally, where someone could propose a blockchain effort, and what does that look like from a regulatory point of view, that rail?

So, it is not a debit rail. It is not a credit rail. It is a blockchain-available digital rail, whether there is a cryptocurrency involved or not. Be neutral on that.

What are your thoughts, Ms. Ford, on that?

Ms. FORD. I am not sure how authorized I am to speak on that issue. I am not an expert on that type of technology, but I would say that I don't think it would be a limitation of technology being able to support that rail. I think it would actually come down to whatever policy implications there are, and I think Christina has alluded to some of this as well, that I think there is an inconsistency in the way that blockchain or distributed ledger is regulated today. It seems to be happening mainly at the State level, and so that kind of inconsistency with the regulatory environment might be one of the limitations that could exist.

Mr. HILL. Right.

Mr. Ahmed, do you want to comment on that?

Mr. AHMED. I would just note that, for the kind of core banking architecture, I think there would probably be some changes needed in terms of the Federal Reserve System, but for smaller-valuation or smaller-amount payments, I think you already are seeing some blockchain-based systems being created that enable the movement of money, and so I think there are examples out there—we talked about XRP or others—that kind of offer this.

Mr. HILL. Mr. Klein, for 40 years, I have been in and out of the banking business, small banks and larger ones, and I couldn't agree more with your testimony about access to available funds and the timeliness of that. We thought we were going to get there in 2004, obviously, and this is a huge frustration to people, and it leads to higher overdraft usage because of that 2- or 3-day gap.

I think we do have a financial literacy issue there, too, and Dr. Foster and I have worked a lot on that. I think people don't know they can schedule their payments around their payday by just simply calling the 1-800 number and doing it, and so they are juggling



when they could move everything given that, but what should the Fed do about making—you suggested up to \$5,000 be available if it is—I get complaints about this from my constituents.

Mr. KLEIN. Under the Expedited Funds Availability Act, that's where it requires the first \$100, as you well know, to be made available immediately, and the Federal Reserve has all the legal authority—

Mr. HILL. To change that number.

Mr. KLEIN. —to change that number and to change the amount of time, up to \$5,000 for customers of more than 6 months.

Mr. HILL. Yes. Thank you for that. We will talk more about that. I yield back, Mr. Chairman.

Chairman LYNCH. The gentleman yields back.

The Chair now recognizes the gentleman from Ohio, Mr. Davidson, for 5 minutes.

Mr. DAVIDSON. I thank the chairman, and I thank our guests. Thanks for your expertise in this field. It's safe to say we don't all agree on all of the issues here, but I am encouraged by the shared consensus that privacy is such a foundational principle for sound payment systems.

Data breaches and data arbitrage pose inherent and under-appreciated risk to consumers, and we do need a new architecture to protect personally identifiable information, and Congress needs to set clear parameters on what data can be collected or transferred. We also need to preserve what has worked so well for so long with the U.S. dollar.

Cash is an incredibly important tool, and the features of it were alluded to by Mr. French Hill when he was talking about a system that could work for banks and for individuals. The U.S. dollar, if I exchange it, I don't have to go to a bank. I can transfer it between any one person. It is recognized as legal tender throughout the United States. And I don't necessarily have to share all kinds of personally identifiable information when I get it. Some people hate that.

But the reality is, when you go to a bank, our system of laws requires the bank to know all sorts of things, and, frankly, to spy on all their customers in order to continue to be permitted to operate, and they do that largely to keep us safe and to protect us from crimes and things like that, but there is this system of cash that is still permissible for peer-to-peer.

So, as we talked about blockchain in a—I don't think everyone would agree in terms of where we are at with blockchain or crypto-based assets, but I think it is largely a matter of whether it is understood or rightly understood, in my opinion, because there is a fear that there is all this abuse. There has been some fraud in the cryptospace, and the solution isn't to just avoid that space altogether. It is the exact opposite. It is to provide regulatory certainty and legislative clarity that does not exist currently.

Blockchain broadly protects personally identifiable information, and, done correctly, it eliminates or can eliminate intermediaries, true distributed ledger technology.

So how could we do this? It is not a partisan issue, as I said. I have cosponsors for legislation that include people who support Bernie Sanders, and cosponsors who support Donald Trump, co-

sponsors from the North, South, East, and West, Republicans and Democrats. The real issue is whether we will confront the innovator's dilemma. Will we continue the broken status quo that protects incumbents at all costs, or will we embrace innovation that will inherently disrupt the current system?

When confronted with this opportunity in the 1990s, Congress got it right, and the internet flourished. Congress did not try to understand everything about the architecture of the internet, and, clearly, any time there is a hearing on the topic, Congress still does not understand everything about the internet. In fact, no one has yet envisioned all the use cases for the internet or internet technology.

How does all this relate to payments? Innovators and payment systems are flourishing, but, unfortunately, they are often launching projects outside of the United States, not to avoid our regulations, but to find legislative clarity in places like Switzerland or Singapore.

So, will we unleash the power of our innovative economy? Will we provide legislative certainty where it is absent with bills like the bipartisan Token Taxonomy Act? Will we finally address the foundational problem of privacy? And, finally, will we allow all Americans to interact freely and privately without intermediaries that collect, monetize, and often compromise our data? They slow the payment system, charge fees, and do make banking less accessible to some people.

So I think, if we are talking about this—and, Mr. Ahmed, perhaps as the bridge between the old economy and the new economy, what are your thoughts on the framework that I have laid out here?

Mr. AHMED. I completely understand the framework, and I understand the need for anonymity, and I think it is the cryptography aspect of cryptocurrencies or payment solutions that leverage the blockchain that really enables that, and I think you see that in varying degrees, as I mentioned, with tokenization technology, reducing the amount of actors that have access to sensitive financial information.

So I think it is certainly is something that people demand. I think it is certainly something that there are technological fixes for, but, as you also acknowledge, there are real concerns from a government perspective about terrorist financing and money laundering and figuring out a balance between those two and how to resolve those, I think is the key question that you are raising.

Mr. DAVIDSON. Yes. Good points, and I think I am encouraged by things like the technology on a distributed ledger that lets you follow it, so you do have privacy, but you don't truly have secrecy. You have a much more transparent system with a distributed ledger than you have with cash. And, so far, I haven't heard calls to eliminate cash, thankfully.

My time has expired. Thank you, all.

Chairman LYNCH. The gentleman yields back.

The Chair now recognizes the gentleman from Ohio, Mr. Gonzalez, for 5 minutes.

Mr. GONZALEZ OF OHIO. Thank you, Mr. Chairman, and thank you to our panel today. I, too, have thoroughly enjoyed this discus-

sion. We kind of have a lot of different perspectives and opinions on this, which I think reflects, frankly, some of the challenges that we have legislatively. It has always seemed to me that, with respect to fintech, we are not quite sure where we want to go. We think we kind of have a destination in mind, but how we get there is always different.

Ms. Del Rio, I want to start with you. I just want to kind of try to summarize part of your testimony, and just give me a yes or no as to whether you think I kind of got it.

I saw a lot of claims that seem to be that fintech is primarily or more about jargon that ultimately is exclusionary in its application as opposed to providing real innovation that expands access. Is that a fair characterization?

Ms. DEL RIO. Sort of.

Mr. GONZALEZ OF OHIO. Okay. Can you clean it up for me?

Ms. DEL RIO. Sure. So, again, it is not to malign innovation or technology. They are not intrinsically bad or good, and that is the point. I think my point is that there has been a lot of sort of reifying of technology as a solution, and so it was going to solve the problem of the unbanked and solve inequality and all of these deeply-entrenched problems that we have talked about today and that your committee is well aware of, and so I think that my point was to sort of—this is the Task Force on FinTech—underscore that our experience and those of other advocates, community groups, financial institutions as well that work with low-income people, with immigrants, with these marginalized communities that don't experience these benefits of fintech yet, and, in fact, it is often the reverse, where they promise that this is a stepping stone to greater access and to a greater opportunity, when it is not.

Mr. GONZALEZ OF OHIO. Okay.

Ms. DEL RIO. It is reinforcing the segregation.

Mr. GONZALEZ OF OHIO. Thank you.

I want to turn to Mr. Ahmed. Can you talk specifically about the work that you all have been able to do by being in the digital payment space specifically with respect to expanding access to affordable credit for small businesses, minority businesses? I hear about this from folks in my district, frankly, that they love products like yours because now they have the ability to access credit in a way that they otherwise would not have.

Mr. AHMED. Certainly. Thank you for the opportunity.

We have a product called PayPal Working Capital, and it leverages the merchant payments data that we secure. We partner with a bank and then offer a loan, and what we find is that 70 percent of these loans are going to the counties that lost 10 or more banks, as Ms. Del Rio mentioned, since the financial crisis. So, kind of going and filling in that gap, we found that 32 percent of these loans go to women-owned businesses whereas, in traditional financial institutions, it is 16 percent. And, actually, in the U.S. statistics, women-owned businesses are 32 percent of the economy.

So it is the ability to offer that loan to the individual who needs it anywhere in the country very, very quickly, in a secure manner and in a convenient manner that I think is really the distinctive part of the product.

Mr. GONZALEZ OF OHIO. And of course it is because you have access to that proprietary data for those businesses, right? You can see dollars coming in and out, and that allows you to price credit more effectively?

Ms. DEL RIO. Absolutely, yes.

Mr. GONZALEZ OF OHIO. Great. So in your experience, at least with that product, the innovation has been working? It has been expanding opportunity, which completely mirrors the feedback that I get. I am sensitive to the comments of Ms. Del Rio. I think it is absolutely legitimate that we need to, as we are thinking through the regulatory environment, making sure that access is a central component of what we are doing, right?

Ms. DEL RIO. Yes.

Mr. GONZALEZ OF OHIO. But I do think, if we are in a world where we are going to try to stop all innovation in advance because of a fear of something that may or may not happen, I think that is a dangerous place to be.

And then, with respect to—you also mentioned—we have 50 seconds—AML/BSA compliance. As we transition or potentially hopefully transition to more of a blockchain system, that is one concern that everybody raises.

Can you just provide your perspective on that? Is that a tech challenge? Is that a regulatory challenge? How can we be comfortable in that world?

Mr. AHMED. I think, as we heard, there are technological solutions to be able to track transactions even with cryptography, depending on the type of cryptography, and it is quite a prism and quite a range depending on what the solution is that is being offered, and then there is a regulatory challenge of how you actually go after the types of things that you are worried about, but ensure that legitimate transactions are getting through, so I think it is probably a little bit of both.

Mr. GONZALEZ OF OHIO. Great. Thank you.

And I yield back.

Chairman LYNCH. The gentleman yields back.

The Chair now recognizes the gentleman from New Jersey, Mr. Payne, for 5 minutes.

Mr. PAYNE. Thank you, Mr. Chairman, and let me thank you for allowing me to sit in today with the task force.

Being a guest here, and allowing the members on the task force to go before me, my thunder kind of gets stolen, but I would just like to associate myself with the comments Mr. Davidson of Ohio made in terms of cash.

For me, it is about choice, and I will ask Ms. Del Rio and Mr. Klein: What happens to that segment of the country that does not come along with this move towards other currencies? What happens to the grandmother who just can't learn all of this rigamarole on the phone? What happens to the child that their dad gives a dollar to go get candy?

What, you have to carry a card now, or say, "Here, son, here is a credit card; go get yourself a lollipop?" It is about choice, and that is—when the issue is raised, is cash still king, I don't know if it is king or not, but in the United States of America, there should

be a choice, and there are underserved, underbanked communities that are not going to ride.

I still, unfortunately, don't use PayPal because I have not learned to use it yet, and I would consider myself fairly—well, fairly savvy, but there are just communities that I am concerned about that I represent that are just not going to ride this change.

And privacy issues. Cash is still the only way that you have total privacy in this country. Wawa, the convenience store, was just hacked several days ago; 30 million people's information—30 million Americans' information. Forget about Target several years ago.

So, cash is really America. It is the American way—a legal dollar, George Washington's face on the dollar, and we are talking about doing away with that. You are doing away with a segment of the country. The statistics are right behind you: 34 percent of African Americans use cash. That is a major segment of the country.

What do you say to making sure that there is a choice in this country? That is what this nation was built on, having a choice. Not that we aren't going down that road, but to not have a choice in the matter is my concern.

Ms. Del Rio?

Ms. DEL RIO. Yes. Thank you.

I appreciate your comments very much. I want to say that I have been doing this work since the mid-1990s, and, at that point, I remember people were predicting the demise of cash, and there were going to be no more bank branches anywhere. Everything was digital and technology-based, and that hasn't borne out.

So I appreciate your comments, and I just want to note also that, in New York City, our city council, just last week, passed a ban on cashless businesses for all the sort of reasons you outlined, the impact that would have, the racially-exclusionary impact it would have of keeping people out of certain storefronts, which is just fundamentally problematic.

When I started doing this work is when public benefits were starting to be transferred to electronic benefits cards. And, at that point, our organization and many others raised some of the concerns that you are mentioning. How would that impact people who don't have easy access to bank branches or ATMs in order to access their food stamps? And what we have warned about and have seen bear out is that people end up paying huge amounts of their public benefits in fees to access their cash benefit, or publicly-subsidized benefits. They have to take buses to use their benefits cards and things like that. That is just one small example, but it bears out in many other ways.

So I think we absolutely agree, and I think this panel agrees that cash shouldn't disappear, that people should have their choice preserved and protected, and that stronger action by Congress to make sure that people are protected no matter what choice they make, these are just fundamentally key things if we are going to build infrastructure that allows for greater options for people.

Mr. PAYNE. Thank you, and I see my time is up.

I yield back.

Chairman LYNCH. The gentleman yields back, and the Chair now recognizes the gentleman from Wisconsin, Mr. Steil, for 5 minutes.

Mr. STEIL. Thank you very much.

Thank you, Mr. Chairman, for holding today's hearing.

I think we have heard a lot of discussion today that is focused on the idea that innovation and the adoption of mobile payment technology can lead to financial exclusion. There are people in this country who are unbanked and lack access to smartphones, but we should be working, I think, to ensure that the public policy creates an environment where everybody benefits from innovation that we are creating.

I think there is an opportunity here to talk a little bit about how we can use this technology to improve financial inclusion. I look to Mr. Ahmed, and I think, for us, it is important to step back maybe and just put a little bit of context to this. And so, if I can, I dug up some numbers from Pugh research: 96 percent of Americans own a cell phone. Ten years ago, it was about 85 percent. The same study found that 81 percent of adults owned a smartphone. Back in 2011, it was about 35 percent. The numbers for smartphone ownership rates by White, Black, and Hispanic adults, this study found, was nearly identical: 82, 80, and 79 percent respectively, reasonably identical rates.

And, while lower-income adults are less likely than those with higher incomes to own a smartphone, the overwhelming majority of respondents earning less than \$50,000 per year did own a smartphone. Some interesting data: 71 percent of those earning less than \$30,000 have a smartphone; 78 percent of those earning between \$30,000 and \$50,000 do. And we are seeing this trend not only in the United States, but globally: 60 percent of adults in Brazil, 52 percent in Mexico, and 41 percent in Kenya have smartphones, and the numbers are continuing to rise at a very aggressive rate.

And so, given the adoption of smartphones and the near total market penetration, I think we should be having a conversation about how mobile payments can foster financial inclusion rather than simply identify the risks of financial exclusion. We should identify the risks, but I think we should spend some more time on how this could actually help us moving forward and how technology can actually help those who are unbanked.

Mr. Ahmed, in your testimony, you mentioned that the most significant barrier to mobile payments for underbanked consumers is their poor compatibility with the way in which unbanked consumers often earn and use money.

Can you elaborate on that comment just a bit?

Mr. AHMED. Certainly. So, if your employer pays you in cash and then if you are living in a community where most of the options available for you to get your groceries or to take transportation—if the common method of acceptance or the preferred method of acceptance is going to be cash, then it makes a lot of sense for you to be using cash.

But I appreciate you highlighting the point about financial inclusion in the way that we are thinking about it—PayPal is really about financial health—can we create value propositions using the full suite of financial services to say, actually, there is a better option here if the digital payment is accepted by the merchant, whether you are offering credit to the merchant as an incentive or

lower cost, or on the consumer side. So that is really where we are trying to focus, and to do it in partnership with a lot of the entities on the ground.

Mr. STEIL. Thank you. And, as we go back and look at the widespread adoption of smartphones and the continuing trend lines across the United States and across different demographic groups, can you comment on how that is allowing PayPal to serve some of these individuals who were previously unbanked?

Mr. AHMED. We are riding a very strong trend in this space, in the mobile access space, and we are seeing mobile payments grow as a result of that, so certainly a lot of the core focus of our company, whether it is in Venmo or in our core PayPal product, is to create better and more experiences using the mobile device for people to be able to use, again, everywhere they go.

Mr. STEIL. I appreciate your comments. And I appreciate your time here today. I do think, as we spent a lot of time today identifying some of the risks, I think it is important that we also identify a lot of the positives in how some of these mobile-payment technologies can assist those who are currently unbanked in our system.

Thank you very much. I yield back.

Chairman LYNCH. The gentleman yields back. The Chair will now recognize the ranking member for 5 minutes for closing remarks.

Mr. EMMER. Thank you, Mr. Chairman, and, again, thank you to the panel for this interesting discussion.

I really appreciate my colleague from Wisconsin, I think, pushing the reset button and getting us to refocus, because a lot of what I hear when we talk about technology reminds me of what humans have dealt with since the beginning of time: We fear what we don't understand.

And by acting before we really understand what we are dealing with, we have a tendency to drive innovation and, more importantly, the entrepreneurs responsible for the great science, everything else, out. We should lead when it comes to these technology advances.

Frankly, I was listening to the comment by—when you said that we banned cashless businesses. That is actually kind of sad, because—and the next follow-up was, we need government to give us more solutions. If you think back to 2007, I believe we had roughly 9,000 community banks on Main Streets across this country. We had roughly 9,000 credit unions like the one that you Chair.

A year later, after the crash, we still had roughly—between 2008 to 2010 or 2011, we still had roughly 9,000 of each. And then Congress rushed in to help, like Congress did with the savings and loan crisis and every other crisis, because the government has to save us from ourselves.

And, ever since, it has accelerated the pressures on small community banks and credit unions to the extent that we now have roughly, I think, less than 6,000 of each, and we are losing more every day, rather than trying to create an environment where we are creating more Main Street banking opportunities.

So the idea that government is going to solve it by banning it, I just want to give you something, because I think it is funny when

I hear from even one of my own colleagues that crypto is the preferred method of laundering money. Well, my colleague, Mr. Payne, just pointed out the only truly private thing left is cash. We can identify people on the internet. You can't necessarily identify somebody who is carrying around suitcases of cash, and I think the comment was that El Chapo had \$200 million in cash on his property. I had my guys check. I don't think he had any cryptocurrency, by the way. His son might have, but he didn't.

I would suggest to anybody who is interested, again, because I think the rhetoric really is, this is dangerous, technology is going to disenfranchise because we don't learn it. And, by the way, to my colleague who says: What about the grandmother who doesn't know, or the child? I agree with him, but I am one of those people that, when I go through the checkout line in the grocery store and they say, "Sir, the self-serve is open." No, no. I'm going to the person. I want to talk to somebody. The young people are going through—besides, if I go through the self-serve, I want the employee discount, because I am doing the job, right? I should get the discount.

But I think, while we should be concerned always, and I respect and am very sensitive to the fact that we are all thinking, I hope, in the same vein: We want people to have access. We want people to be empowered and to grow and be able to lift themselves up. We just look at it a little differently. I suggest, if you haven't, to take a look at the book, "The Age of Cryptocurrency."

This book begins with a story of Afghani women who are typically excluded and shunned from partaking in finances. It is a cultural issue. These Afghani women were using bitcoin to build up a financial livelihood and to store value that is solely theirs. This is the kind of empowerment that is not something that I think we should just be tossing aside, again, because we can't see all the things out on the horizon. We have to make sure we are very careful, and this institution, in particular, has to start moving a little quicker with the certainty questions that we talked about in the marketplace because, at the end of the day, that is where we are going.

And I think people need to be very clear. We can either help facilitate this technology advancement, or it is going to happen without us, and God forbid it happens somewhere else where we don't have any say.

So, again, thank you to the witnesses.

And, Mr. Chairman, thank you very much for having this hearing today.

Chairman LYNCH. Absolutely. Thank you. Thank you for your remarks as well.

In closing, I do want to point out the difficulty here that we face. I was in Somalia last week. We did a codel there to the Horn of Africa, and I am keenly aware of the need within Somalia for a secure banking apparatus to help that country recover. All of the big banks have left, because of the threat of reputational damage due to the control of al-Shabaab and terrorist elements in that country, but you do see the need for a value-transfer system that is secure and that will allow that country to recover. So, clearly, there are



some advantages to be had in a digital system that is secure. It is a very different circumstance, but I clearly see the benefits.

But I also see the benefits that our regulatory system has secured. Most of our regulatory system on the financial side, the traditional system, has been created as a result of responses to calamities in this country, right? We had 9,000 bank failures during the Depression—9,000. So Congress, in coordination with the SEC and others, created the Federal Deposit Insurance Corporation (FDIC). So, we have the Federal Deposit Insurance Corporation, and even though we had a major catastrophe in the recession in 2007, 2008, we didn't see all the banks closing down like we did before. So, there are advantages to having those intermediaries.

And now, I am a bit concerned about the push for blockchain and a system that eliminates the intermediaries. It is peer-to-peer ledger. So we go around the Federal Reserve because it is peer-to-peer. We go around the SEC. We go around Treasury and the Financial Crimes Enforcement Network (FinCEN). We go around all these intermediaries that allow us to rebalance and correct some of the inequities.

So it is a big challenge, but it is extremely interesting. And I agree; we have to try to tackle this and get the best out of a system like that while protecting against the worst aspects of what some of this new, untested technology might present.

I want to thank you all for the wonderful testimony. All of you brought your "A game" here today and really helped us work through some of these issues that are extremely complicated, but we want to understand how this affects everyone. The banking industry has tended to gravitate toward the needs of the wealthy, right?

I remember when I was an ironworker. I was an ironworker for 20 years, and I became union president, and we had accounts so that the men and women on the jobs could go cash their checks at the end of the workday, and I remember a bank, a big bank, still around, who told me as union president that they didn't want to do business with my workers anymore because the amount of money they were making on their transactions didn't cover the cleaning of the rug, because my guys and gals were coming in with muddy boots.

So, that type of elitist attitude that we want to take care of the rich folks and not the workers so much, and that is where the money is on the high end of this spectrum. We have to be careful. We have to be careful when we are designing a system, that it is inclusive of everyone, and I think we can do it. I think we can accomplish the goals that have been articulated up here. We just have just to be smarter about it.

Part of it is the way we engineer this, and part of it is the way that we not only engineer the architecture, but also regulate it on behalf of the American people because we are the only group who can really intercede on behalf of those people in our economic system and our legal system.

So, thank you very much for your testimony.

Without objection, the following letters will be submitted for the record: letters from Americans for Common Cents, C-E-N-T-S; Coinstar; the Electronic Payments Coalition; Nacha; the Electronic

Transactions Association; the Money Services Business Association; the National Association of Convenience Stores; the National Association of Federally-Insured Credit Unions; the payment card industry; the Payment Card Industry Security Standards Council; Square; the American Bankers Association; Javelin Advisor Services, and the Honorable Donald Payne, Jr.

Thank you.

The Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

This hearing is now adjourned. Thank you.

[Whereupon, at 11:15 a.m., the hearing was adjourned.]

# **A P P E N D I X**

January 30, 2020

Statement of Congressman Donald M. Payne, Jr. (NJ-10) before the  
U.S. House Committee on Financial Services Subcommittee Task Force on Financial Technology  
**“Is Cash Still King? Reviewing the Rise of Mobile Payments”**  
January 30, 2020

Chairman Lynch, Ranking Member Emmer, and distinguished members of the Subcommittee, thank you for the opportunity to come before this Subcommittee to discuss an alarming concern that is rising not only across the country but around the world. The subject of this hearing – “Is Cash Still King? Reviewing the Rise of Mobile Payments” is a question that deserves exploration and significant attention.

**Problem**

The Federal Deposit Insurance Corporation, better known as the FDIC, has reported that in 2017, 6.5 percent of United States households were “unbanked,” which in simple terms means that no one, not one adult, had a checking and/or savings account. 8.4 million U.S. households, made up of 14.1 million adults and 6.4 million people under the age of eighteen, were unbanked in 2017.

In addition, the FDIC reported that 18.7 percent of U.S. households were “underbanked” in 2017, translating to 24.2 million households composed of 48.9 million adults and 15.4 million people under the age of eighteen. Underbanked means that the household had an account at an insured institution but also obtained financial products or services outside of the banking system.

Simply stated, a household is underbanked if it has a checking or savings account and uses alternative financial services in the preceding 12 months. For instance, money orders, check cashing institutions, international remittances, payday loans, refund anticipation loans, rent-to-own services, pawn shop loans, or auto title loans are all alternative financial services. These numbers should strike your ears with true alarm. Many hard-working people across this country are on the verge of being unable to purchase goods and necessities because of the growing cashless movement. Millions of people are at risk of being left behind. We cannot allow that on our watch.

There are millions of Americans who truly rely on cash to ensure that they budget properly. There are some with physical and mental health concerns who find using financial technology services extremely difficult.

The cashless trend particularly discriminates against low-income residents and people of color, as communities of color are unbanked at higher percentages.

The Civil Rights Act of 1964 states that all persons shall be entitled to the full and equal enjoyment of the goods, services, facilities; and privileges, advantages, and accommodations of any place of public accommodation without discrimination or segregation on the ground of race, color, religion, or national origin. Whether they know it or not, proponents of cashless establishments are further excluding hardworking people. This is not acceptable. Is their money not also green?

#### Solution

Since Congress passed the Coinage Act of 1792 and the United States created the dollar as the country's standard unit of currency and furthermore established the United States Mint, cash has been an extremely important part of this nation.

I believe that cash still has and deserves a prominent place in our country's day to day commerce and I furthermore believe that it should remain so.

Between 1978 and 2019, ten states and six cities across this great country, including, Connecticut, New Hampshire, Massachusetts, Illinois, New Jersey, New York, Oregon, Rhode Island, Vermont, Wisconsin; New York City, Philadelphia, San Francisco, St. Louis, West Hollywood, and Washington, D.C., have thoughtfully and legislatively taken the FDIC's alarming data into consideration and moved towards passing legislation or enacting laws that bans cashless and card only merchants from excluding those hardworking people who may only have cash to purchase goods or services.

Last week, the New York City Council passed its bill which bans cashless businesses. The bill was sent to Mayor Bill de Blasio for his review and signature.

I am proud to say that in March of 2019, in my home state, where I represent the Tenth Congressional District of New Jersey became the second state to pass a bill which prohibits a person from selling or offering for sale any goods or services at retail if the person requires the buyer to pay with credit or prohibits the buyer from paying with cash.

Cash must continue to be the dominant form of purchasing power in America to ensure that all people can access it.

Americans should not have to purchase a gift card or prepaid credit card in order to spend their hard-earned money.

I do recognize some potential benefits for going cashless which could include the reduction of robberies of stores and individuals, armored truck logistics, large banking fees, and reducing the possibility of human accounting errors.

However, cashless policies disproportionately harm seniors, minorities, immigrants, low-income populations, and working-class communities.

We must also be aware that some of the largest retail stores in this country have recently been hacked, with bad actors siphoning millions of people's private information to the black market with which to darken and manipulate their financial health and privacy.

Cash continuing to reign supreme in this country is not about stifling or slowing entrepreneurship or innovation. The ability for people to be able to use cash at all stores is about inclusion not exclusivity.

#### Payment Choice Act of 2019, H.R. 2650

As a strong advocate for consumer choice, I introduced H.R. 2650, the Payment Choice Act of 2019. This bill would prohibit retail businesses from refusing cash payment and provides relief to consumers affected by this exclusionary practice. Rep. Chris Smith of New Jersey is the Republican co-lead of this bill.

The bill includes **exemptions** for any goods or services purchased by telephone, mail or the internet.

And, the bill carries **civil penalties**, via the court system, in the form of fines with violations including:

- 1) persons will be liable for actual damages
- 2) persons will be fined up to \$2,500 for the first offense
- 3) persons will be fined up to \$5,000 for the second and subsequent offenses.

Currently, this bipartisan bill has 34 cosponsors. It would not prohibit businesses from accepting credit or debit cards, it simply guarantees consumers the choice to use cash as a form of payment.

Every consumer should have the legal protection of payment choice and businesses should no longer be able to deny consumers their civil liberty to pay with cash.

#### Conclusion

In conclusion, Chairman Lynch, Ranking Member Emmer, and distinguished members of the Subcommittee, thank you again for this opportunity to discuss this significantly dangerous trend sweeping across our country and my bipartisan legislation to combat purchase power exclusion. I look forward to answering any questions you might have on this subject matter.

**37**

**TESTIMONY OF**

**Usman Ahmed**

**Head of Global Public Policy**

**PayPal Inc.**

**BEFORE THE**

**United States House of Representatives**

**Committee on Financial Services**

**Taskforce on Financial Technology**

**Is Cash Still King? The Rise of Mobile Payments**

**PRESENTED**

**Rayburn House Office Building, Room 2128**

**January 30, 2020**

**9:30 AM**

### Introduction – Who is PayPal

Chairwoman Waters, Ranking Member McHenry, Chairman Lynch, Ranking Member Emmer, and members of the Task Force, I would like to thank you all for giving PayPal Inc. the opportunity to testify today on the important topic of mobile payments. Since 1998, PayPal has been at the forefront of innovation in mobile payments. PayPal operates an open, secure and technology-agnostic digital payments platform that gives our over 300 million active account holders the confidence to connect and transact in new and powerful ways, whether they are online, on a mobile device, in an app, or in person.

Through a combination of technological innovation and strategic partnerships, PayPal creates better ways to manage and move money. We offer people and businesses choice and flexibility when they send payments and receive payments. Whether sending money to friends and family through apps like PayPal, Venmo, and Xoom, or engaging in e-commerce, more and more people are using their smartphones to make purchases, receive payments and manage their accounts. Our technology is giving more people and businesses access to the global market, and financial services tailored to their specific needs.

We enable peer-to-peer, or P2P, payments via PayPal, Venmo and Xoom. In Q3 of 2019, our collective P2P volume was \$51B and represented 28% of our total payment volume. In particular, Venmo has seen enormous growth since it launched in 2009 as a fee-free, digital way to move money between friends in the US.<sup>i</sup> As of August 2019, Venmo had 40 million users.<sup>ii</sup> Venmo's contribution to PayPal's total payment volume stood at 14%. According to a survey done in 2017, of the 65% of young Americans that did use payment apps, more than two-thirds — 68% — said they used Venmo most often.<sup>iii</sup>

The Venmo app pioneered the idea of social payments by allowing users to post memos and emojis attached to transactions where you can see friends paying one another for a meal out, or roommates sending money to each other for utilities and rent. While this social aspect is what makes Venmo unique, it is imperative to note that users can determine their privacy settings and have the option to make transactions “private” so that they appear only to the sender and the recipient. Being able to send secure and easy P2P payments across the country via a few taps on the phone is an important improvement in people's lives. And, what began as a fun way to pay friends back for everyday expenses has now become an option to pay at millions of retailers.

The ability to use Venmo is not solely limited to purchases and payments within the e-commerce ecosystem. The Venmo Card enables users to spend their Venmo balance in-store and online anywhere that Mastercard is accepted in the U.S. The card is ATM friendly. Venmo's functionality offers tools to make people's lives easier. The app includes a tool that automatically calculates suggested tip amounts, so there's no need to crunch the numbers on a calculator or worry about over or under tipping. Also, users can easily split and share the payment with friends in the Venmo app on a single purchase such as dinner at a restaurant.

Xoom is a pioneer in international digital remittances, and a fast and secure way to send money, pay bills and reload phones for loved ones globally. It allows consumers to use a mobile device



or PC to send money to recipients for cash pickup or directly into their bank accounts, typically in minutes, to more than 160 countries globally. Xoom users can also save their family the trouble of carrying cash and waiting in line, by taking care of the bill payments. Most bills will be paid typically within minutes. These remittances serve as a lifeline for many people around the world and are used to pay for everyday needs like utility bills, healthcare, mobile reload, and education costs, as well as emergencies. The largely cash-based system of sending money across borders is full of paperwork, high fees, standing in line and an ever-present uncertainty of when, and if, the money will arrive. By providing fast and more secure payment options for customers to seamlessly and securely send money across borders by going online or using a mobile device, PayPal and Xoom are helping to expand and improve the financial health of millions of people worldwide.

In November 2019, Xoom announced an expansion of its services to give customers in the United States the ability to send money to recipients within the U.S.—for the first time. Through collaborations with Walmart and Ria, people in the U.S. can now use Xoom to send money fast for cash pick-up typically in minutes at nearly 5,000 store locations across the country.

As the economy digitizes, PayPal as a two-sided network, will continue to drive consumer adoption and merchant acceptance of mobile payments. PayPal's mobile app is localized in over 100 markets and 26 languages. We also help merchants, particularly small merchants, optimize their checkout pages for mobile access.

Finally, we can utilize data from mobile payments, in partnership with a financial institution, to underwrite working capital loans for small businesses. This access to finance is key to the growth of small businesses. 70% of PayPal Working Capital loans go to the 10% of counties in the US that have lost 10 or more banks since the financial crisis. Moreover, 32% of PayPal Working Capital loans go to women owned businesses, whereas the average from traditional financial institutions is just 16%.

By leveraging technology to make financial services and commerce more convenient, affordable, and secure, the PayPal platform is empowering over 300 million consumers and merchants in more than 200 markets to join and thrive in the global economy. In Q3 of 2019, 43% of the \$179 billion total payment volume we processed were made on a mobile device.

#### **The Power of Mobile Payments**

The mobile phone has transformed nearly every aspect of our lives. We use it to communicate with family, to read the news, order a cab, find a hotel, and engage in payments. The growth of smartphones over the past decade has been incredible. In 2011, only 35% of Americans owned a smartphone; the percentage grew to 81% by 2019.<sup>iv</sup>

Payment technologies have evolved throughout history – checks and bills of exchange were the innovation of 1750s, credit cards were the innovation of the 1950s, ACH in the 1960s, and debit cards in the 1970s. Since the dawn of the Internet revolution in the 1990s, online and mobile payments have transformed the payments industry.

At the end of 2018, 3.6 billion people were connected to the mobile internet; which means almost half of the world's population are mobile internet users.<sup>v</sup> The ubiquity of smartphones has made it an ideal platform over which robust payment solutions are offered. While money is a complex and very personal aspect of our lives, essentially every dollar earned or spent in every country follows the same pattern: it is acquired, it is managed, and it is sent.

For most of history, acquiring, managing, and sending money were interconnected in concept but disparate in reality. We took different actions, used different services, and visited different places, depending on where we were in the process and what funding instruments were used. However, mobile has the power to bring them together and make them available at our fingers, along with the power of customization and freedom. It is now possible to receive, manage, and send money using apps on a single mobile device, consolidating and simplifying disparate tasks that have historically been costly, in terms of money, time, and mental bandwidth.

Mobile payments offer an unprecedented level of seamlessness and convenience. The PayPal One Touch technology enables businesses to provide a quick and easy checkout method for customers. Users can transact without pop-up windows, redirection or having to type or retype a username, password or 16-digit credit card number, all in a secure manner. In addition to enabling remote transactions, mobile payments can also be a more convenient option for in-person transactions, relative to cash. Mobile devices can be used for payments at the point of sale through a simple touch.

Mobile payments have been growing rapidly in importance for everyday payments. 17% of businesses earn the majority (more than 50%) of their revenue through the mobile channel today. 32% of businesses expect mobile to represent at least half of their total revenue by 2020.<sup>vi</sup>

Mobile devices are the new hardware foundation upon which a full suite of financial services can be offered. There are countless opportunities to improve financial services like bill payment, government disbursement, consumer credit, and small business financing through the data derived through mobile payments.

At PayPal, we regard fighting cybercrime as a strategic business priority, and we invest heavily in keeping our sites and services as safe and secure as possible. PayPal's philosophy on cybersecurity has a strong focus on customer data protection. Everything we do around security is focused on our commitment as the "secure way to pay and be paid." It is important to approach security across the industry, helping providers to keep their systems secure by analyzing data in real-time to understand behavior alongside static data to help verify identity and protect consumers.

Security has been front and center throughout the development of mobile payments, leading to adoption of innovations such as the tokenization technology, which reduces the number of entities that have access to sensitive financial data. PayPal has been a pioneer of tokenization technology. Tokenization substitutes a person's sensitive financial information with a series of non-sensitive numbers that confirm to the business that a payment is authentic, helping to minimize the likelihood and impact of data breaches as well as reduce fraud.

Service providers can also leverage key information from the mobile device to improve identification, authentication, and fraud reduction. PayPal is a founding member of the Fast Identity Online (FIDO) Alliance whose mission is to find new methods of authentication that move away from passwords and towards biometrics (fingerprint, etc.). Moreover, with a PayPal transaction, should something go wrong with a purchase, e.g. an item doesn't arrive, or it doesn't appear significantly the way it was described, then PayPal covers them under Purchase Protection or Free Return Shipping for eligible purchases. These services are made possible in large part due to mobile payments data that we use for fraud and risk management services.

PayPal also engages and partners with law enforcement proactively and reactively to help stop illegal activities that leverage mobile payments, while also catching the bad actors that have committed crimes and are under investigation. This ability to leverage the mobile payment system to stop illicit payments is a marked distinction from a payments system that is predominantly cash based.

Finally, mobile payments hold the power and promise to improve people's financial health. Tasks that many take for granted like cashing a check, paying a bill, and sending money to a loved one are inconvenient, expensive, unsafe—and sometimes impossible. The advancement of mobile payments has important implications for unbanked, underbanked, and financially unhealthy individuals and communities.

The 2017 FDIC survey of unbanked and underbanked households found that about 8.4 million households are unbanked.<sup>vii</sup> According to research from Pew, the majority of the unbanked have a smartphone.<sup>viii</sup> The reason for the failure to use mobile payments is not necessarily lack of access. The most significant barrier to mobile payments for unbanked consumers is their poor compatibility with the way in which unbanked consumers often earn and use money.<sup>ix</sup>

Nearly 25 million US households are underbanked, meaning they use alternative financial services like payday lenders and check cashers alongside their formal financial services.<sup>x</sup> To manage their financial lives, the underbanked use instruments such as money orders, check cashing, international remittances, payday loans, refund anticipation loans, rent-to-own services, pawn shop loans, or auto title loans.<sup>xi</sup> Professor Lisa Servon's research has shown that the underbanked use these instruments because they are often more timely, more immediate, lower cost, and more convenient than traditional products.<sup>xii</sup>

Regardless of banking status, a large portion of the U.S. population is financially unhealthy. Nearly 70% of Americans have less than \$1,000 in savings.<sup>xiii</sup> Four in five Americans say they live paycheck to paycheck.<sup>xiv</sup> Faced with a \$400 emergency expense, 40% of all Americans would not be able to pay, and would need to sell something or rely on credit.<sup>xv</sup> And countless hours have been wasted just for low- and moderate-income individuals to pay their bills.

Mobile payments technology allows customers to make online and point-of-sale purchases, pay bills, and send or receive money from their smartphones via web browsers, apps, or text messages. Mobile payments offer a low cost, safe, fast, and convenient way of managing and moving money, and that has the potential to improve the financial health of consumers who are underserved by the traditional financial system. For example, giving people access to their

money instantly via mobile can actually help quite a bit in reducing fees and late payments. Access to credit during cash flow challenges is another area where mobile payments can make a big difference. Finally, remittances and P2P payments at a distance can be made far more efficient and lower cost.

Xoom's services potentially benefit more than 44 million foreign-born people in the U.S. who send remittances to family and friends in their home countries.<sup>xvi</sup> Sending money overseas with Xoom/PayPal costs on average less than half the cost of traditional remittances.<sup>xvii</sup> Our analysis suggests that digital remittances are well on the way to achieving the UN Sustainable Development Goal of lowering remittances costs to less than 3%.<sup>xviii</sup> Moreover, mobile payments can greatly reduce the time cost of sending a remittance, which typically takes over 30 minutes on average to send.<sup>xix</sup> When sending a digital remittance through Xoom by depositing money to a bank account, it typically takes less than 3 minutes. That is 27 minutes saved on average every time someone sends a remittance, around 10 days given back to that person over the course of their life, nearly 300 million hours and almost \$5 billion in time-cost in aggregate that could be put to better use.

By harnessing the power of mobility to bring the financial institutions to the consumer, mobile technologies can serve as a tool for improving financial health. Access to institutions and funds, as well as clarity of account information, can disproportionately impact poorer individuals. By offering a more convenient and less expensive way for managing and moving money, without the constraints of geography and hours, mobile technologies like digital wallets and person-to-person (P2P) payments can help the underbanked take more control of their financial lives.<sup>xx</sup> For example, consumers can easily utilize different payment options, which is important for managing costs at the margins. Moreover, one of the features of mobile payments is automatically tracking and displaying a clear record of how a user is spending money, thereby enabling better decision-making.

There is also an opportunity for mobile payments to form a baseline architecture upon which other value-added financial services can be offered in an innovative and prudent manner. PayPal has built successful products and partnerships for peer-to-peer, remittances, credit, savings goals and wealth management. PayPal has partnered with several players to provide U.S. consumers with access to affordable and convenient financial solutions for the underserved. The PayPal Cash Mastercard allows unbanked and underbanked customers to pay bills and shop anywhere that Mastercard is accepted without monthly fees. "Direct Deposit" allows customers to load all or part of their paychecks directly into PayPal. "Money Pools" help groups using PayPal to collectively pool funds for shared items or activities. "Goals" help people plan ahead and organize their funds for future spending. Integration with Acorns allows customers to easily transfer funds from their PayPal to their Acorns account and track investment performance. These products leverage technology to lower costs, increase access, enhance security, maximize convenience, and improve financial health of our customers. Because of the proliferation of mobile technology and the digitization of financial transactions, we have entered into a period where financial services can be transformed at an unprecedented pace and scale.

Digital payments are not made in silos. Partnerships across the industry, platforms and networks serve as electronic paths and highways that connect customers in ways that benefit them. For example, our partnership with Citi allows institutional clients of Citi to make payments into their customers' PayPal digital wallets. Also, we partner with Visa for a more seamless payment experience for Visa cardholders and will offer greater choice for how consumers pay with PayPal and Venmo wallets. And we count several major technology companies as partners.

In order to modernize and make inclusive the mobile payments system, we work together with both traditional financial services and startups to enable businesses and consumers to benefit from lower cost and more efficient services. As PayPal has evolved, our biggest shift has come by realizing that payments itself is a trillion-dollar industry and financial services is far bigger; no one company should or will ever own that whole market. Therefore, PayPal has fully embraced an ecosystem partnership strategy. We believe that fintech is not about disruption; it is about value creation for everyone in the expanding digital economy, by enabling consumers, merchants, traditional financial leaders and technology leaders to participate in the global movement to the digital mobile economy. And, we believe that this value creation comes through partnership. While mobile has created completely new avenues and channels to democratize finance, it is only through partnership that we can more fully maximize those opportunities.

## Cash

Although use of non-cash payments, including mobile, has been growing in recent years, cash still remains a major portion of the payments ecosystem in the United States. The 5<sup>th</sup> Federal Reserve Diary of Consumer Payment Choice conducted in 2019 found that consumers used cash in 26 percent of transactions. The share of cash use among individuals under 25 years old is the highest of any age group. Cash continues to be used extensively for small-value purchases, representing nearly 50 percent of all payments under \$10, and 42 percent of payments less than \$25. In contrast, cash is used for approximately 10 percent of payments \$25 and higher.<sup>xxi</sup>

Cash is a ubiquitous form of payment, but while it may appear costless to transfer, there are high costs associated with cash usage. Sixty-five percent of the unbanked earn less than \$25,000 a year, and these low-income consumers incur additional costs and risks because they lack access to mainstream banking services. For example, 20 percent of unbanked consumers reported having cash lost or stolen.<sup>xxii</sup> A study of low-income Los Angeles area households found that the average unbanked consumer lost the equivalent of nearly two weeks of household expenses when cash was lost or stolen.<sup>xxiii</sup>

Professor Kenneth Rogoff of Harvard University authored a book entitled "The Curse of Cash" in which he documented several costs associated with cash.<sup>xxiv</sup> Cash is deeply implicated in tax evasion, which costs the US federal government some \$500 billion a year in revenue. The drug trade, bribes, human trafficking, and terrorism are all fueled by cash payments. When Mexican drug lord El Chapo was arrested more than \$200 million in cash was found on the premises; the drug trade globally is estimated at \$600 billion. Cash can also be used to facilitate corruption; the scale of bribes is estimated at \$2 trillion annually. Cash is the currency of choice to fund terrorism; the official currency of ISIS is the US dollar and the organization has annual

expenditures of between \$1 and 2 billion per year. Counterfeiting, though a small problem in the grand scheme, nevertheless exists and results in harm.

Mobile payments present a tremendous opportunity to reduce reliance many of the costs associated with cash. We don't predict the death of cash over the next decade or two and we believe that consumers should have choice in their payment options. We are working diligently to make sure that the value proposition of digital payments vastly exceeds the value proposition of cash for every member of society.

### **The Role of Policy**

To reflect the move towards mobile, payments policy will need to continue to evolve.

We urge policymakers to collaborate with industry to ensure regulation of mobile payments meets the goals of consumer protection, security, and healthy industry innovation. Responsible innovation can and ought to develop with consumer protection, security and safety at the core.

The key is to put in place regulations that are smart and technology-neutral, such that regulations are created based on performance rather than the type of technology. Regulations are most successful if they consider divergent risks posed by new offerings and tailor requirements that are proportionate to the risk being posed. Not every innovation is inherently riskier, and sometimes innovation can lower risks.

Moreover, from the perspective of security, mobile payments may be considered a good tool for reducing reliance on the use of anonymous cash. Mobile payments can aid in reducing Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) risks due to improved transaction monitoring and restrictions. Mobile payments can be enabled via effective and proportionate applications of AML/CFT regulatory frameworks.

We also urge policymakers to consider the connection between broadband and mobile broadband deployment and its impact on access to mobile payments for members of the unbanked, underbanked, and financially unhealthy individuals and communities. While many unbanked and underbanked families have access to the Internet, maintaining phone service is often a financial hardship for this population. The unbanked are nearly twice as likely as banked consumers to suspend or cancel their cellphone plans because they were too expensive. Among smartphone owners with limited data plans, nearly half of unbanked consumers reach their data limits most or some months, which indicates a high amount of use. About 7 percent of U.S. consumers rely exclusively on their smartphones for accessing the Internet.<sup>xxv</sup>

Households with incomes under \$30,000 annually, which include about 60 percent of unbanked consumers, are almost twice as likely as the general population to be smartphone- dependent. Unless smartphone owners with limited data plans can access a Wi-Fi network or purchase additional data at an affordable rate, they are unable to use mobile payments technology regularly. As a result, mobile payments use is significantly lower among the unbanked: About 39 percent of unbanked smartphone owners have ever made a purchase, paid bills, or sent or received funds using mobile payments technology compared with 64 percent of banked

smartphone owners.<sup>xxvi</sup> Since a majority of the unbanked population in America has a smartphone, that represents tremendous opportunity to reach out to these unbanked customers through digital tools.

Policy can also play a role in helping to improve the mobile payment use cases for unbanked and underbanked consumers. Government payments can be disbursed directly into electronic formats. Government bill payments can incentivize electronic payment acceptance. Micro-entrepreneurs in low-income neighborhoods can be incentivized to move towards electronic and mobile payments, which would create a virtuous cycle for consumer adoption of mobile payments. All of these incentives can be created in partnership with the private sector to enable greater reach and a balanced equitable solution set.

### **Conclusion**

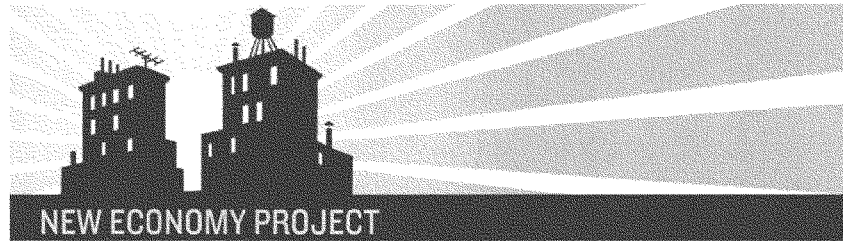
Fueled by a fundamental belief that having access to financial services creates opportunity, PayPal is committed to democratizing financial services and empowering people and businesses to join and thrive in the global economy. We believe that individuals, families, small businesses and communities are going to be the economic winners from the continued melding of mobile technology and payments as well as increased competition.

Thank you again for the opportunity to address the Task Force on this important and timely topic. I look forward to answering your questions.

## References

- <sup>i</sup> <https://www.fastcompany.com/40400786/how-peer-to-peer-payment-pioneer-venmo-grew-up-and-got-serious>
- <sup>ii</sup> <https://www.cnbc.com/2019/04/24/venmo-has-40-million-users-paypal-reveals-for-first-time.html>
- <sup>iii</sup> <https://bankinnovation.net/allposts/biz-lines/payments/for-most-millennials-its-still-venmo-or-nothing/>
- <sup>iv</sup> <https://www.pewresearch.org/internet/fact-sheet/mobile/>
- <sup>v</sup> <https://www.gsma.com/r/mobileeconomy/>
- <sup>vi</sup> <https://www.kount.com/blog-against-fraud/measuring-mobile-payments-fraud-kounts-2018-report-is-here/>
- <sup>vii</sup> <https://www.fdic.gov/householdsurvey/2017/2017execsumm.pdf>
- <sup>viii</sup> <https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2016/06/what-do-consumers-without-bank-accounts-think-about-mobile-payments>
- <sup>ix</sup> <https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2016/06/what-do-consumers-without-bank-accounts-think-about-mobile-payments>
- <sup>x</sup> <https://publicpolicy.wharton.upenn.edu/issue-brief/v5n4.php>
- <sup>xi</sup> <https://www.fdic.gov/householdsurvey/2017/2017report.pdf>
- <sup>xii</sup> <https://www.lisaservon.com/books>
- <sup>xiii</sup> <https://www.gobankingrates.com/saving-money/savings-advice/americans-have-less-than-1000-in-savings/>
- <sup>xiv</sup> <https://www.cnbc.com/2019/01/09/shutdown-highlights-that-4-in-5-us-workers-live-paycheck-to-paycheck.html>
- <sup>xv</sup> <https://www.federalreserve.gov/publications/files/2017-report-economic-well-being-us-households-201805.pdf>
- <sup>xvi</sup> <https://news.xoom.com/s/article/xoom-rolls-out-domestic-money-transfer-services-in-the-u-s>
- <sup>xvii</sup> [https://publicpolicy.paypal-corp.com/sites/default/files/policy/PayPal-Policy-Paper\\_Digital-Remittances.pdf](https://publicpolicy.paypal-corp.com/sites/default/files/policy/PayPal-Policy-Paper_Digital-Remittances.pdf)
- <sup>xviii</sup> [https://publicpolicy.paypal-corp.com/sites/default/files/policy/PayPal-Policy-Paper\\_Digital-Remittances.pdf](https://publicpolicy.paypal-corp.com/sites/default/files/policy/PayPal-Policy-Paper_Digital-Remittances.pdf)
- <sup>xix</sup> <https://publicpolicy.paypal-corp.com/sites/default/files/policy/Time%20is%20Money%20Xoom%20Report.pdf>
- <sup>xx</sup> <https://publicpolicy.paypal-corp.com/issues/mobile-payments>
- <sup>xxi</sup> <https://www.frbsf.org/cash/publications/fed-notes/2019/june/2019-findings-from-the-diary-of-consumer-payment-choice/>
- <sup>xxii</sup> <https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2016/06/what-do-consumers-without-bank-accounts-think-about-mobile-payments>
- <sup>xxiii</sup> [http://www.pewtrusts.org/~media/legacy/uploadedfiles/wwwpewtrustsorg/reports/safe\\_banking\\_opportunities\\_project/slipping20behindpdf.pdf](http://www.pewtrusts.org/~media/legacy/uploadedfiles/wwwpewtrustsorg/reports/safe_banking_opportunities_project/slipping20behindpdf.pdf)
- <sup>xxiv</sup> <https://press.princeton.edu/books/hardcover/9780691172132/the-curse-of-cash>
- <sup>xxv</sup> <https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2016/06/what-do-consumers-without-bank-accounts-think-about-mobile-payments>
- <sup>xxvi</sup> <https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2016/06/what-do-consumers-without-bank-accounts-think-about-mobile-payments>





TESTIMONY OF DEYANIRA DEL RIO  
CO-DIRECTOR, NEW ECONOMY PROJECT  
BEFORE THE U.S. HOUSE COMMITTEE ON FINANCIAL SERVICES  
TASK FORCE ON FINANCIAL TECHNOLOGY

“Is Cash Still King? Reviewing the Rise of Mobile Payments”

January 30, 2020

Chairman Lynch and Ranking Member Emmer, and Members of the Task Force on Financial Technology, thank you for the invitation to testify at today’s hearing on behalf of New Economy Project, an economic justice center based in New York City. For 25 years, our organization has led local efforts to press for fair lending, community reinvestment, and financial inclusion, as a matter of racial justice and equitable neighborhood development. We believe fundamental change is necessary to creating an economy that works for all. I am pleased to share our perspectives on bank redlining, the growth of cashless businesses, and disparities in financial services access that serve to perpetuate inequality and poverty in our city and nationally.

My testimony today is informed by more than two decades of work with low-income New Yorkers and community groups to challenge systemic discrimination by Wall Street banks and other financial corporations, and to support responsible, cooperative, and community development finance. New Economy Project’s many accomplishments include keeping payday lending debt traps out of New York, through vigorous defense of New York State’s 25% usury cap and other consumer protections; ending in NYC an insidious form of employment discrimination based on a job applicant’s credit history; and winning strong state regulations to curb discriminatory and abusive debt collection.<sup>1</sup> We provide direct legal assistance to thousands of low-income New Yorkers and recently settled a groundbreaking class action

---

<sup>1</sup> *Rogue Democrats Could Be Trying to Open New York Up to Payday Lenders*, at [bit.ly/2uMQMjB](https://bit.ly/2uMQMjB); *New York City Just Outlawed Running Credit Checks on Job Applicants*, at [bit.ly/3aOJKvo](https://bit.ly/3aOJKvo); *And Now for Some Good News*, at [bit.ly/2RCMHrx](https://bit.ly/2RCMHrx)

lawsuit we brought against a debt buyer network, resulting in a \$59 million monetary award and the vacating of almost \$800 million in debt collection default judgments.<sup>2</sup>

My comments are additionally informed by my service as a board member of the Lower East Side People’s Federal Credit Union, a regulated, not-for-profit community development financial institution that serves a majority low-income and immigrant membership in New York City.

I would like to focus our testimony on the following points:

**First, the financial justice issues addressed in today’s hearing are systemic in nature, and call for bold, systemic solutions.** Too often, discussions about financial access disparities focus on the choices and behaviors of individuals, or on the need to design “alternative products,” rather than on structural barriers that block poor people, immigrants, and people of color from mainstream financial institutions and systems. As this committee knows, the high cost of maintaining bank accounts, persistent redlining of neighborhoods of color, and prohibitive identification requirements all create real entry barriers for millions of people across the country.<sup>3</sup> Through our legal assistance hotline, we have in fact seen a clear, growing pattern in which mainstream banks are actively pushing low-income people out of the banking mainstream. Banks typically close people’s accounts and report their information to ChexSystems and other consumer reporting databases, for example, when they are unable to pay exorbitant, often hidden overdraft fees – effectively blacklisting people from opening accounts elsewhere.<sup>4</sup>

The sheer absence of bank branches in communities of color speaks volumes. Attached to my testimony are maps that illustrate extreme disparities in bank branch service based on the income and race composition of neighborhoods in NYC – patterns you see in cities throughout the U.S. In NYC neighborhoods of color, there is just one bank branch, on average, for every 10,000 residents – compared to almost 3.5 branches for majority white neighborhoods. The maps also show what happens when banks fail to serve neighborhoods adequately – or at all: high-cost, fringe financial services like check cashers and pawn shops fill the vacuum. Nationally, as a result of the persistent bank redlining and other structural inequities in our

---

<sup>2</sup> *Victims of Debt Collection Scheme in New York Win \$59 Million in Settlement*, at [nyti.ms/2UcPSb7](https://nyti.ms/2UcPSb7)

<sup>3</sup> *How Neighborhoods Help New Yorkers Get Ahead*, at [bit.ly/2vwXtH7](https://bit.ly/2vwXtH7); *Access to Financial Services, Savings, and Assets Among the Poor*, at [bit.ly/2O9Ucnp](https://bit.ly/2O9Ucnp); *Immigrant Financial Services Study*, at [on.nyc.gov/38R050C](https://on.nyc.gov/38R050C)

<sup>4</sup> *Where Are the Unbanked and Underbanked in New York City?*, at [urbn.is/37Ea21x](https://urbn.is/37Ea21x); *Bank Clients Might Be Unfairly Denied Accounts*, at [nyti.ms/2U3INdT](https://nyti.ms/2U3INdT)

economy, approximately 17% of black households and 14% of Latino households don't have a bank account, compared to 3% of white households.<sup>5</sup>

**Eliminating barriers to fair banking and financial inclusion is a critical step to ensuring economic opportunity and justice.** As in other parts of our economy, poor people pay more for basic, too often inferior, financial services. Lack of a banking or credit history, in turn, can unfairly block people from housing, affordable insurance and other vital economic opportunities, as growing numbers of landlords, employers, insurance companies and others consider people's credit histories, leading to wholesale discrimination.<sup>6</sup> Indeed, in communities across New York and around the country, unequal access to credit has long fueled housing segregation, racial disparities in homeownership and small business-ownership, and vast and deepening racial wealth inequality.<sup>7</sup>

**At the same time, financial products and technology are not a solution to poverty or income inequality.** Policymakers frequently ask us what kinds of products and services are needed to address the glaring disparities we see throughout our financial system. Simply put, we are not going to "product-design" our way out of deeply entrenched, racially-unjust structures and institutions. Too often we hear industry – and policymakers – tout products and services that are "less predatory," or better than nothing, though these products and services are still exploitative and inferior in nature. Exploitative financial services and credit can worsen racial inequities, as we saw with "subprime" mortgages that led to the foreclosure crisis and wiped out hard-won homeownership gains among families of color and devastated entire communities. We see this with payday loan debt traps that claim to serve – but in fact exploit – working poor Americans struggling to make ends meet, and who would benefit from living wage laws and other affirmative measures to address root causes of economic insecurity.

**As we work to eliminate barriers, we must challenge the rhetoric and alleged benefits of "financial innovation" and "fintech."** We strongly urge this Task Force and Committee to scrutinize oft-cited industry tropes, which simply fail to match reality, particularly for low-income people and communities. For decades, companies have invoked "innovation" as a smokescreen to evade regulation and peddle inferior, high-cost, or outright predatory products – from "subprime" and payday loans to fee-ridden prepaid debit cards – to low-wage workers, immigrants, and people of color. To be sure, the term "fintech" is itself broad, and encapsulates a range of companies and technologies, not all of which fall within today's hearing topic. And appropriate and safe technology can of course benefit underserved people and communities.

<sup>5</sup> 2017 FDIC National Survey of Unbanked and Underbanked Households, at [bit.ly/2RAaaJG](https://bit.ly/2RAaaJG)

<sup>6</sup> Data Point: Credit Invisibles, at [bit.ly/2O3GUsl](https://bit.ly/2O3GUsl); Background On: Credit Scoring, at [bit.ly/2RXTbjA](https://bit.ly/2RXTbjA)

<sup>7</sup> Access to Credit, at [bit.ly/3aRrYaT](https://bit.ly/3aRrYaT)

Too often, however, companies identifying as “fintechs” claim to “eliminate banking deserts” or “empower communities” redlined by banks, when in fact they are exploiting communities’ unmet needs and perpetuating inequality in our banking system.<sup>8</sup>

Fintech companies routinely seek to circumvent state consumer protection laws, such as New York State’s strong usury law, through “sham” partnerships with national and out-of-state banks; engage in risky securitization of loans; rely on broad and invasive data collection; employ racially-biased loan underwriting algorithms; and have been the subject of numerous state and federal enforcement actions. We should be extremely concerned by the fintech industry’s invasive data collection – and the privacy, data breach, and surveillance risks – to which these companies expose all of us.<sup>9</sup>

The Trump administration’s efforts to exempt fintech companies from critical consumer protection rules only exacerbates these serious risks. CFPB’s creation of a “regulatory sandbox,” for example, would offer a safe haven to unscrupulous lenders – flying in the face of the Bureau’s statutory mandate to protect consumers from unfair, deceptive, abusive, and discriminatory acts and practices. Similarly, the Office of the Comptroller of the Currency’s national fintech charter, and proposal that would encourage “rent-a-bank” schemes, threaten to confer broad powers to fintechs to avoid state interest rate caps, other state protections, and state oversight.<sup>10</sup>

Combined with the administration’s takeover of the Consumer Financial Protection Bureau – as well as dangerous proposals to gut the Community Reinvestment Act<sup>11</sup> and Fair Housing Act – the financial services industry has received the green light to unleash new waves of predatory and extractive products and practices. These actions are guaranteed, if not intended, to exacerbate racial disparities, and will inevitably lead to new crises.

**In this context, I would like to comment on the growth of cashless businesses, which reinforce inequities in our financial system and economy at large.** Just last week, the NYC Council passed a local law similar to H.R. 2650, the “Payment Choice Act of 2019,” requiring

<sup>8</sup> *UniRush LLC and Mastercard International Incorporated*, at [bit.ly/2RZ5Y59](https://bit.ly/2RZ5Y59); *FTC Charges Prepaid Card Company Deceptively Marketed Reloadable Debit Card*, at [bit.ly/2S0rA15](https://bit.ly/2S0rA15)

<sup>9</sup> *Fintech and Consumer Protection: A Snapshot*, at [bit.ly/3aQgQel](https://bit.ly/3aQgQel)

<sup>10</sup> New York State’s Department of Financial Services has forcefully cracked down on abusive practices by online lenders and taken outspoken positions on fintech. See *Online Lending Report* at [on.ny.gov/208LwQ2](https://on.ny.gov/208LwQ2). New Economy Project joined 246 consumer, civil rights, and community groups in opposing the OCC’s new nonbank charter. See *Comment letter to the OCC*, January 13, 2017 at <https://bit.ly/2u15g4m>.

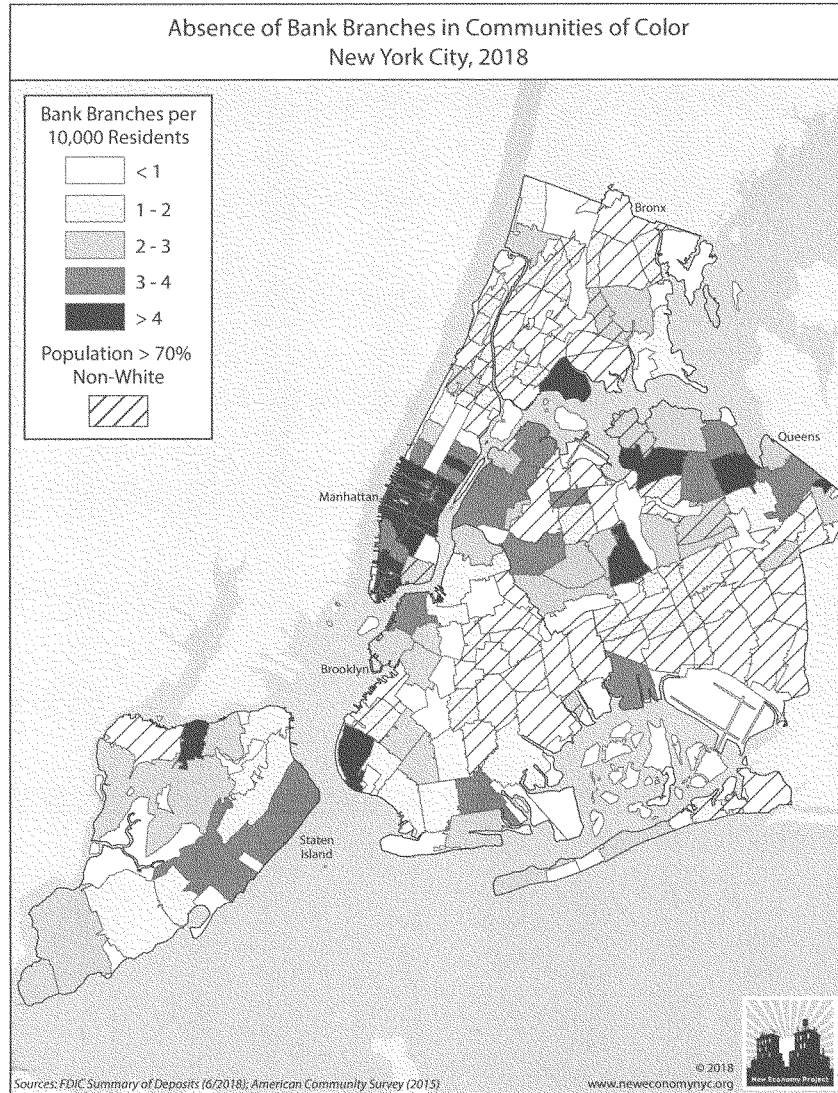
<sup>11</sup> *Statement On FDIC, OCC Notice Of Proposed Rulemaking For Community Reinvestment Act*, at [bit.ly/2UhaFFN](https://bit.ly/2UhaFFN); *Trump Pulls Back Efforts to Enforce Housing Desegregation*, at [nyti.ms/2GuILtG](https://nyti.ms/2GuILtG); *FDIC/OCC Proposal Would Encourage Rent-a-Bank Predatory Lending*, at [bit.ly/2uFaYEa](https://bit.ly/2uFaYEa); *Trump’s Bank Regulators Open the Door to More Predatory Lending*, at <https://bit.ly/2GuMeRN>

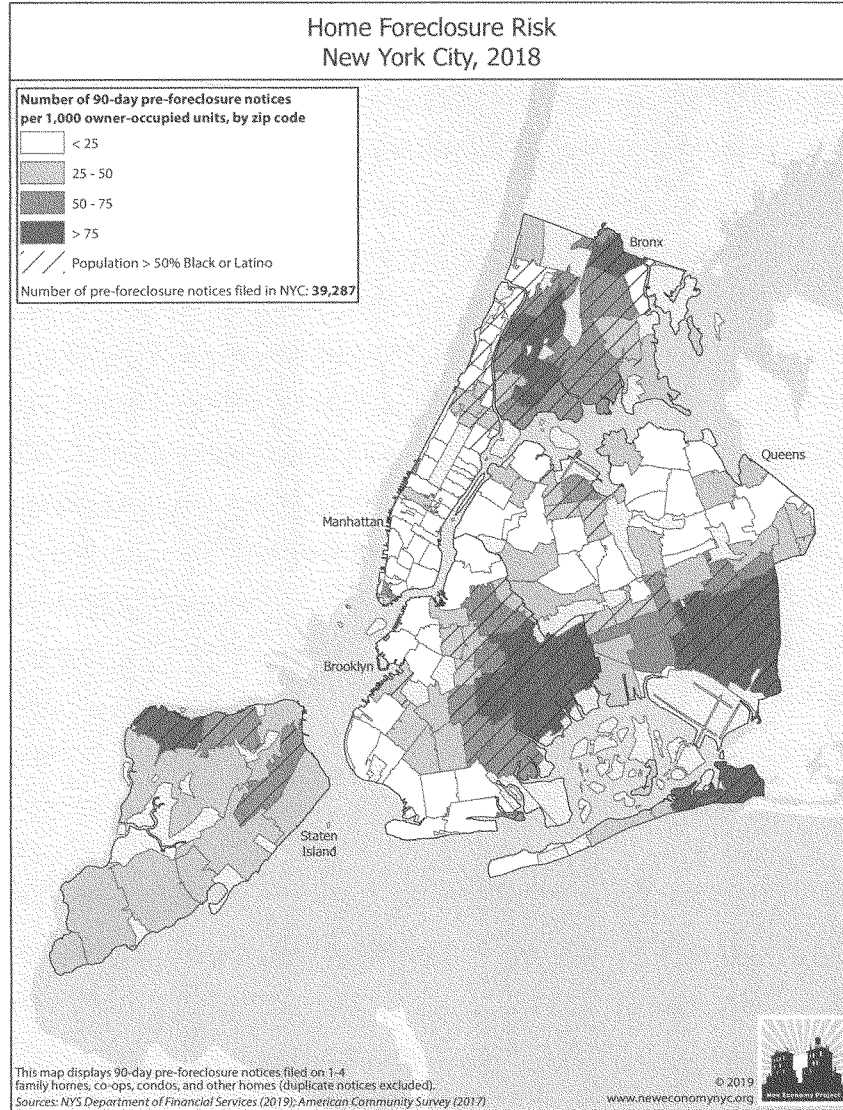
stores and restaurants in NYC to accept cash payments. Like H.R. 2650, the NYC law will also prohibit charging people more if they pay with cash. The NYC Council passed the bill because of the discriminatory effect cashless businesses have on low-income people, people of color, and immigrants, who face longstanding, systemic barriers to fair banking access – as banks continue to redline neighborhoods throughout the country, neighborhoods continue to reel from the foreclosure crisis, and the Administration continues to dangerously roll back financial services regulation and oversight, notably in the areas of consumer protection, fair lending, and community reinvestment.

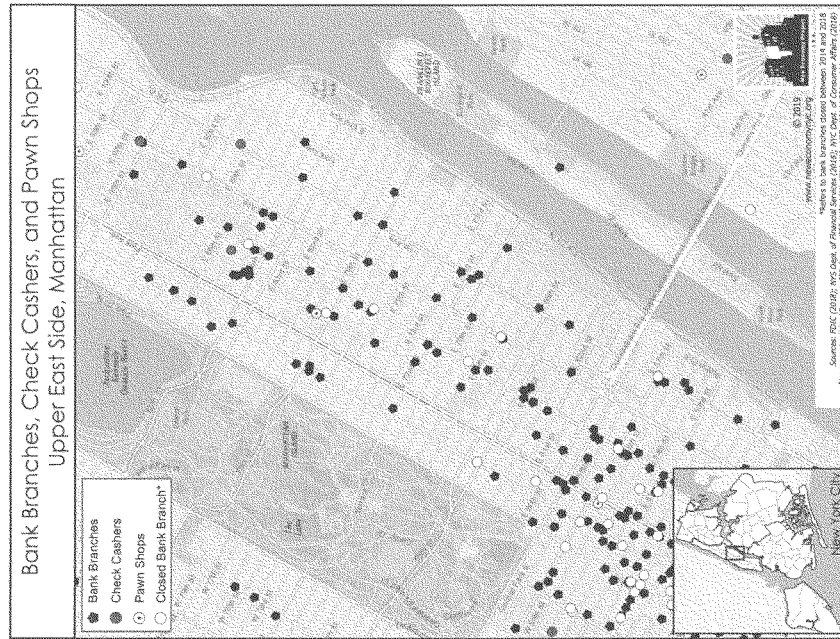
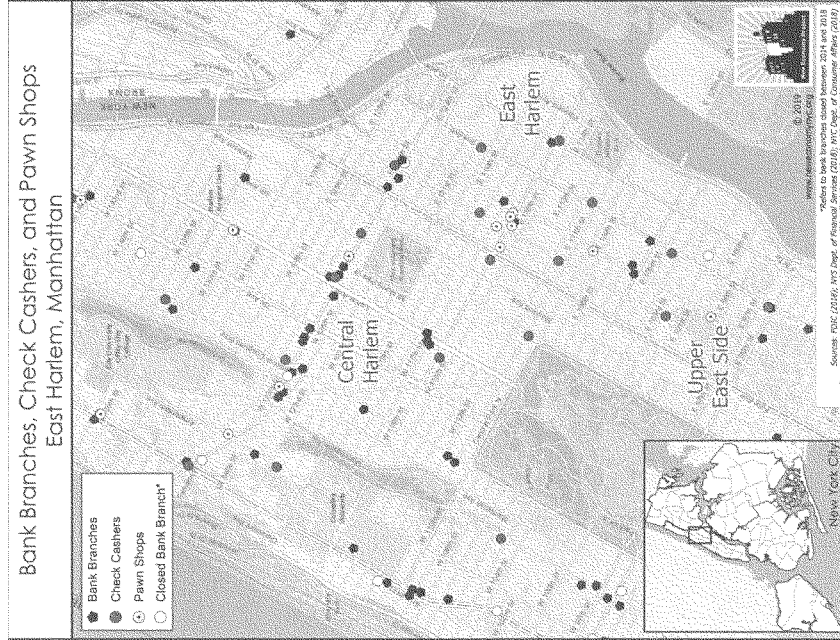
**Credit card and fintech companies, businesses, and others tout the benefits of a cashless economy without addressing the economic and racial injustice it perpetuates.** Permitting stores and restaurants to be cashless also promotes a shift to inferior and poorly-regulated digital payment, prepaid cards, and other non-bank services – depriving people of the strong federal consumer protections that apply to all bank and credit union accounts, in some cases, and requiring people to cede ever more personal information to large companies.

**We need bold solutions to address our two-tiered financial system.** In New York, we are working to advance bold, affirmative solutions that move us toward a just financial system and economy. These include public banking – common in other countries, and on the rise across the U.S.; community land trusts and non-speculative housing; cooperative and community development financial institutions; and strong state and local agencies action in the absence of federal regulation and enforcement. Congress should support efforts to democratize our economy, working with and for communities that have been exploited and excluded from the mainstream financial system for decades.

Thank you for the opportunity to testify on behalf of New Economy Project. We would welcome the opportunity to share case examples and discuss these issues in greater depth.









55

Written Testimony of

**Kim Ford**  
**Executive Director**  
**U.S. Faster Payments Council**

Before the Task Force on Financial Banking Technology of the House Financial  
Services Committee

**“Is Cash Still King? Reviewing the Rise of Mobile Payments”**

**Thursday, January 30, 2020**  
**9:30 am**  
**2128 Rayburn House Office Building**

Chairman Lynch, Ranking Member Emmer, and distinguished members of the Task Force on Financial Technology of the House Financial Service Committee, thank you for this opportunity to testify before you today at this hearing on “Is Cash Still King? Reviewing the Rise of Mobile Payments.” My name is Kim Ford, and I am the Executive Director of the Faster Payments Council (FPC), an industry trade association born out of the efforts of the Federal Reserve and the collective payments industry to modernize the U.S. payments system. Today, the FPC serves as an inclusive and representative membership organization whose mission is to facilitate ubiquitous faster payments in the U.S. Our membership represents every facet of the payments industry, including business end-users, consumer organizations, financial institutions, payment network operators, technology providers, associations and other interested stakeholders such as individuals representing academic institutions and industry consultants.

The FPC works to achieve its mission through:

1. Education - The FPC spearheads educational initiatives to foster better understanding of faster payments and confidence among providers and end users to increase adoption.
2. Problem-Solving - The FPC tackles the tough issues that inhibit adoption of faster payments so that end users can pay and be paid in seamless and transparent ways. The FPC provides safe forums for dialogue, encouraging honest contributions, and honoring differing views to enable the ideas and solutions that will drive progress.
3. Industry Guidance - The FPC identifies and evaluates practices, principles, and guidelines that enhance safety, security, and transparency, and enable opportunities and access.

Prior to my role at the FPC, I was employed at First Data for 15 years, most recently serving as senior vice president and head of global government affairs. I’ve also held a number of industry leadership positions, including serving as Chair of the Legislative and Regulatory Council for the Electronic Funds Transfer Association; Co-Chair of the Government Relations Council at the Electronic Transaction Association; Past Chair of the Board of Directors for the National Card Coalition; and Board Member for the Innovative Payments Association.

My current and past industry roles have allowed me to develop a deep subject-matter expertise on a broad range of payments topics, particularly electronic/digital payments (of which mobile payments are a component). Thus, I am grateful for this opportunity to share with you details on how consumers pay,

the growing use of electronic payments as a preferred payment choice, the role faster payments can play in furthering electronic payments, and some of our organization's efforts to ensure we foster a secure, efficient, and accessible digital payments future for U.S. consumers.

#### **I. Background: Payments Landscape**

The payments landscape is rapidly evolving. With a plethora of mobile payment offerings, the advent of faster payments, and the availability of new technologies such as artificial intelligence and machine learning, we are transitioning from an environment dominated by paper checks and cash to a digitally-based payments system where electronic transactions serve as a primary form of payment and constitute nearly \$100 trillion of the value of payments overall.<sup>1</sup> According to the Federal Reserve's 2019 Diary of Consumer Payments Choice<sup>2</sup>, electronic payments surpassed cash as the preferred method of payment for the first time in 2018. According to the study, consumers used cash in only 26 percent of transactions, while debit cards were cited as the most frequently used payment instrument, accounting for 28 percent of payments.<sup>3</sup>

With respect to checks, 2018 served as the first year that automated clearinghouse (ACH) transactions outnumbered check payments. According to the Federal Reserve's 2019 Payments Study, there were 16.6 billion ACH debit transfers compared to 14.5 billion check payments. In contrast, in 2000, the number of ACH debit transfers stood at 2.1 billion compared to 42.6 billion check payments.<sup>4</sup>

#### **II. How Consumers Pay and Why**

##### **Consumers' Payment Use: Choice Matters**

While evidence points to consumers' growing desire to use electronic payment formats, they still use a wide variety of payment options, such as cash, check, ACH, debit and credit cards, demonstrating a strong desire for payment choice. While choice rings through as a theme, the trend towards electronic

<sup>1</sup> 2019 Federal Reserve Payments Study at <https://www.federalreserve.gov/paymentsystems/2019-December-The-Federal-Reserve-Payments-Study.htm>

<sup>2</sup> 2019 Diary of Consumer Payment Choice at <https://www.frbsf.org/cash/publications/fed-notes/2019/june/2019-findings-from-the-diary-of-consumer-payment-choice/>

<sup>3</sup> 2019 Diary of Consumer Payment Choice at <https://www.frbsf.org/cash/publications/fed-notes/2019/june/2019-findings-from-the-diary-of-consumer-payment-choice/>

<sup>4</sup> 2019 Federal Reserve Payments Study at <https://www.federalreserve.gov/paymentsystems/2019-December-The-Federal-Reserve-Payments-Study.htm>

payments cannot be ignored. The 2019 Diary of Consumer Payments Choice also showed that electronic payments—specifically, debit cards—were the most frequently used payment option in 2018, experiencing a growth of 2 percent from 2017. In fact, use of all major electronic payment methods experienced growth from 2017 to 2018. And while cash is still a widely preferred payment option, usage is decreasing, as its share of payments dropped 4 percent from 2017 to 2018.<sup>5</sup>

Not only is cash use decreasing overall, but it is being used less and less for the major payment categories it once dominated. Historically, cash has been used for low-value payments below \$25. But 2018 numbers show that electronic payments are beginning to take hold as a way to conduct small-value transactions. 2018 marks the first year that cash was not used for the majority of transactions for purchases under \$10 (decreasing from 56 percent to 49 percent) and in the \$10-\$24.99 payment range, debit cards and cash now stand nearly identical in terms of use.<sup>6</sup>

Even in other types of categories, such as in-person payments and gifts/person-to-person (P2P) transfers, where cash has historically reigned supreme, electronic payments have gained ground. While cash remains the most used payment instrument for in-person payments at 35 percent, in-person credit card usage grew 5 percent over the last three years, cutting into cash's share, while cash use declined 5 percent. Additionally, 2018 represented the first year that both debit and credit cards were used for gifts and transfers, reflecting the growing trend towards use of digital payments apps for these types of transactions. And even when looking at the other major payment categories, such as government and nonprofit; auto and vehicle related; food and personal care payments; medical, education and personal service; general merchandise; entertainment and transportation and housing related, cash use declined in every category from 2017 to 2018.<sup>7</sup>

#### **Types of Consumers and Payment Use**

When looking at various age groups, cash is a universal payment type that is still used among all segments. Individuals under 25 and over 45 represent the segments that use cash the most, while consumers age 25 to 44 remain the segment using cash least. But even within these segments, cash use

<sup>5</sup> 2019 Diary of Consumer Payment Choice at <https://www.frbsf.org/cash/publications/fed-notes/2019/june/2019-findings-from-the-diary-of-consumer-payment-choice/>

<sup>6</sup> 2019 Diary of Consumer Payment Choice at <https://www.frbsf.org/cash/publications/fed-notes/2019/june/2019-findings-from-the-diary-of-consumer-payment-choice/>

<sup>7</sup> Ibid.

is declining. And more often than not, age segments that are showing a decline in cash use are replacing this payment option for electronic options, such as debit and credit cards.<sup>8</sup>

When considering income level, cash is used among all segments regardless of income, and consumers make about the same number of cash transactions each month. Those making under \$25,000 represent the largest users of cash payments. In all other income segments, credit and debit card use outnumbers cash.<sup>9</sup>

#### **Consumers' Preferred Payment Method and Rationale**

Various Federal Reserve and other industry studies report that while cash is a universal payment type, electronic payments rank highest among consumer segments as the *preferred* way to pay. Both the 2019 Diary and other studies on consumer payment mechanisms, such as Tsys's 2018 Consumer Payments Study, show that debit cards are the most preferred payment method among the surveyed individuals.<sup>10</sup> Credit cards generally rank second, and cash third.<sup>11</sup>

Today's payment preferences are driven by a number of factors, dominated by a desire for convenience and security. According to the most recent PSCU Eye on Payments study, 60 percent of consumers reported convenience and ease of use as the main drivers behind their choice in payment. And nearly 40 percent cited safety as a factor influencing payment choice.<sup>12</sup>

Almost 80 percent of consumers own a debit or credit card.<sup>13</sup> And both of these instruments are widely accepted at retailers across the globe. Electronic transactions are traceable. They enable convenient logging and tracking of transactions. Electronic payments, particularly debit cards, also allow consumers

<sup>8</sup> 2019 Diary of Consumer Payment Choice at <https://www.frbsf.org/cash/publications/fed-notes/2019/june/2019-findings-from-the-diary-of-consumer-payment-choice/>

<sup>9</sup> 2018 Diary of Consumer Payment Choice at <https://www.frbsf.org/cash/publications/fed-notes/2018/november/2018-findings-from-the-diary-of-consumer-payment-choice/>

<sup>10</sup> Tsys 2018 Consumer Payments Study at [https://www.tsys.com/Assets/TSYS/downloads/rs\\_2018-us-consumer-payment-study.pdf](https://www.tsys.com/Assets/TSYS/downloads/rs_2018-us-consumer-payment-study.pdf)

<sup>11</sup> 2019 Diary of Consumer Payment Choice at <https://www.frbsf.org/cash/publications/fed-notes/2019/june/2019-findings-from-the-diary-of-consumer-payment-choice/>

<sup>12</sup> 2019 Eye on Payments at <http://www.pscu.com/PDF/Whitepapers/2019%20Eye%20On%20Payments.pdf>

<sup>13</sup> The 2018 Survey of Consumer Payment Choice at <https://www.frbatlanta.org/-/media/documents/banking/consumer-payments/survey-of-consumer-payment-choice/2018/2018-survey-of-consumer-payment-choice.pdf>

to efficiently manage their money. Additionally, electronic payments provide consumers with protections against loss and fraud.

While cash may be convenient, easy-to-carry, and widely accepted, it can be easily lost or stolen, and there are no measures in place for consumers to recoup such funds. For these reasons, among others, electronic payments have climbed the ranks to become a dominant payment option for U.S. consumers.

#### **Mobile Payments Use**

In the U.S., mobile payment use is also on the rise. Much of the growth of mobile payments can be attributed to the proliferation of smartphone ownership and the availability of mobile payment apps. Almost nine in 10 U.S. households own a smartphone, making it the second-most owned technology device after television sets<sup>14</sup>, and 30 percent of smartphone owners used a mobile payment app in 2019, representing an increase of 9.1 percent over the previous year.<sup>15</sup> Even more, nearly 30 percent of U.S. consumers have indicated a desire to pay with their smartphone all the time.<sup>16</sup> As consumers increasingly spend time on their smartphones and integrate them into all aspects of their lives, it's understandable that consumers want to incorporate payments into their mobile phone experience as well.

Tsys's 2018 study also showed that over the last three years of their research, survey respondents consistently rated the most attractive mobile features as the ability to immediately stop a fraudulent transaction, the ability to instantly view their transactions, and the ability to use their phone to turn their payment card on or off to prevent unauthorized usage.<sup>17</sup> These findings underscore the population's increasing reliance on electronic payments to solve for convenience and added security.

The significance of this growing mobile use is that more often than not, the funding mechanism behind mobile transactions is an electronic payment option, typically a credit or debit card. Thus, as electronic

<sup>14</sup> "5 Trends Driving Growth of Digital Wallets" at <https://www.paymentsource.com/list/5-trends-driving-growth-of-digital-wallets>

<sup>15</sup> "ApplePay Overtakes Starbucks as Top Mobile Payment App in the US" at <https://www.emarketer.com/content/apple-pay-overtakes-starbucks-as-top-mobile-payment-app-in-the-us>

<sup>16</sup> Statista at <https://www.statista.com/topics/982/mobile-payments/>

<sup>17</sup> Tsys 2018 Consumer Payments Study at [https://www.tsys.com/Assets/TSYS/downloads/rs\\_2018-us-consumer-payment-study.pdf](https://www.tsys.com/Assets/TSYS/downloads/rs_2018-us-consumer-payment-study.pdf)

payment usage continues to grow and access to the Internet becomes more widespread, we can expect a commensurate increase in mobile payment usage.

#### **Financial Inclusion**

The FPC is driven by values of inclusivity and transparency, and we take seriously the desire of our member organizations to provide access to a safe and efficient payments system for as many end users as possible. Across the globe, financial inclusion is getting better, and various studies credit smart phones and digital payments as factors. For example, the 2017 Global Findex report created by the World Bank in partnership with the Bill and Melinda Gates Foundation states that recent progress in financial inclusion “has been driven by digital payments, government policies, and a new generation of financial services accessed through mobile phones and the Internet.”<sup>18</sup>

The report goes on to state that the benefits of digital financial services are wide ranging. For example, mobile money services can help improve individuals’ income earning potential and thus reduce poverty, and digital financial services can help individuals manage financial risk, can lower the cost of receiving payments, and can also help people accumulate savings and increase spending on necessities.

Similar findings were uncovered at a 2018 conference, *FinTech Financial Inclusion – and the Potential to Transform Financial Services*, hosted by the Boston Federal Reserve and the Aspen Institute’s Financial Security Program. The discussions from that conference highlighted that “established and emerging FinTech solutions offer real potential to give unbanked people new access to financial services and impact their financial lives” and pointed to mobile devices as the starting point for providing the unbanked with access to financial services.<sup>19</sup>

### **III. The Faster Payments Opportunity**

#### **Benefits of Faster Payments in an Electronic Environment**

The growing and preferred use of electronic payment options across all US demographics presents a substantial opportunity for faster payments. Faster payments has been defined differently in countries

---

<sup>18</sup> The Global Findex Database 2017, <https://globalfindex.worldbank.org/>

<sup>19</sup> The Boston Federal Reserve Bank, “Can FinTech Close the Gap Between ‘Unbanked’ Populations and Financial Services?” <https://www.bostonfed.org/news-and-events/news/2018/fintech-and-financial-inclusion.aspx>

around the world, but according to the Faster Payments Playbook, a joint project between Nacha and the FPC, the term “faster payments” is broadly used in the U.S. payments industry to indicate that increased speed, convenience and accessibility are essential features for the future of the payment and settlement system.”<sup>20</sup>

As such, in an environment in the U.S. where electronic payments are a preferred payment method, faster payments can provide for the following:

1. Improved visibility and financial management – Faster electronic payments allow for easier cash flow management with accurate and timely insight into account activities. Faster payments reduce the chance for end users to make unintentional overdrafts and help them avoid costly fees or the need for short-term financing.
2. Improve payments system efficiency – Faster electronic payments decrease the reliance on infrastructure needed to support paper-based payments, like checks and cash, reducing costs and resources necessary to operate and maintain such infrastructure.
3. Minimize payments risk – Faster electronic payments help reduce many of the risks in the current payments system by shortening the delay between payment initiation, clearing, and settlement. Timely confirmation of good funds and payment finality can provide certainty of payment for consumers.
4. Encourage global competitiveness – Faster electronic payments could foster greater global competitiveness and the potential for faster and easier global transactions. Indeed, faster payments solutions with global interoperability could eventually help to facilitate faster and more transparent cross-border payments.

#### **IV. FPC Efforts**

##### **Regulatory, Fraud and Transparency-Related Efforts**

State and federal regulators, along with certain payments industry participants, have established a robust framework of statutes, regulations, and industry standards that protect consumers, promote a

---

<sup>20</sup> The Faster Payments Playbook, <https://fasterpaymentsplaybook.org/>



reliable and consistent user experience, and help maintain a healthy, efficient, and safe financial market with respect to payments.

As FPC members collectively prepare for a U.S. payments system that enables broad adoption of faster payments solutions, the FPC has established a Regulatory Work Group to identify and analyze laws and regulations that may impact faster payments and consider options as to how to support and accelerate the adoption of faster payments. The Work Group is currently conducting a comprehensive review of laws, regulations and regulatory guidance that apply to faster payments, including UCC Article 4A, the Electronic Funds Transfer Act, the Bank Secrecy Act, FFIEC guidance, and more. These requirements are being categorized and examined so that organizations that want to incorporate faster payments into their suite of solutions can arm their legal and compliance teams with a better understanding of the regulatory landscape.

As electronic transactions become increasingly widespread, continued work to safeguard the data surrounding them remains a focus of the payments industry. Our efforts in assessing today's robust regulatory infrastructure extend to evaluating data security as well. Payments stakeholders rely on key data points to combat and reduce fraud and to safeguard transactions, and at the same time, are working diligently to ensure the robust consumer protections in place today continue to meet their customers' needs. As the payments system speeds up, the FPC's collective efforts will focus on striking that right balance, enabled by input from all facets of the industry.

In addition, to support the security of transactions, the FPC recognizes the need to exchange data related to fraud in an effort to protect the payments system from all threats, whether they be cyber threats or other fraud threats. To that end, the FPC established the Fraud Information Sharing Work Group. Today, it is working to develop a publicly accessible white paper addressing the following three areas of fraud prevention as they pertain to faster payments: 1) fraud prevention best practices, 2) fraud themes and trends, and 3) fraud prevention solutions and channels.

The FPC believes that this paper will serve as a comprehensive resource to help the industry mitigate the potential for fraud in a faster payments environment.

And we are also working diligently to ensure consumers are informed of and prepared for faster payments. The FPC's End-User Transparency Work Group recently released *Faster Payments Transparency Guidelines for Payment Services Providers*. The resource is designed to help providers of

faster payments anticipate and answer a wide variety of consumer questions that may surface about certain characteristics, associated fees, and protections related to their faster payment offering. Solution providers are presented with questions such as “How long does the enrollment process take?, Is there a limit on the amount of a single transaction?, What is the process for disputing a payment?,” and more. By outlining these questions for solution providers, the FPC believes that they will be better prepared to educate their customers while also creating a safe and positive user experience.

#### **Global Effort Considerations**

Many countries outside of the U.S. are making significant advancements towards a faster, more cashless payments environment. While the U.S. is moving in that direction with the launch of new real-time payments systems, including The Clearing House’s Real-Time Payment (RTP) network and the recently announced FedNow™ system, we are still generally behind many other countries in the adoption of faster payments systems. These countries can provide some instructive lessons learned for the U.S. and the future of payments. Because of this, the FPC recently announced plans to establish a Cross-Border Payments Work Group, which is expected to, among other things, examine the payments environments of other countries to assemble helpful tips and information to support our efforts to modernize the payments system in the U.S. Our goal with this work will be to draw out key lessons learned and identify areas of opportunity for the U.S. in moving into a more digital, faster payments environment.

#### **V. Conclusion**

In conclusion, it is clear that Americans continue to embrace a more digital society, given the advent of real-time payments systems and the growing use of electronic payments. With that said, our payments system has evolved over time to support many different payment mechanisms, driven by individuals’ desire to pay how they want, where they want, when they want. Ultimately, the FPC supports an environment in which payment choice is preserved, while also allowing the flexibility to enable a faster, more digital payments environment enables that delivers an array of benefits and protections for consumers, businesses and government end-users. We are dedicated to working with all of the stakeholders across the payments ecosystem to ensure that together we can achieve the ideal faster, more efficient, and more secure payments environment of the future.

Again, thank you for the opportunity to testify today. I look forward to answering any questions you may have.

**Testimony of Aaron Klein, Fellow, Economic Studies, Brookings Institution  
U.S. House Committee on Financial Services Task Force on Financial Technology  
“Is Cash Still King? Reviewing the Rise of Mobile Payments”  
January 30, 2020**

Chairman Lynch, Ranking Member Emmer, members of the Task Force, thank you for the opportunity to testify on the critically important issue of the future of cash. Participation in our economy requires the ability to make safe, secure, and speedy payments. Despite their critical importance, how Americans pay for things and the associated cost of those payments are often assumed to be far less costly than they are. In reality, how American consumers and businesses send and receive payments is quite complicated, costly, and slow compared to other nations. The payment system’s gap between those with money and access to new payment technology, and those without money and access is growing. The ramifications of exclusion from the world of digital payments can be severe. The fault lines developing are a mixture of traditional ones and some new ones. Congressional inquiry into this issue is needed and I applaud the Task Force for prioritizing the issue.

My testimony will focus on five main points.

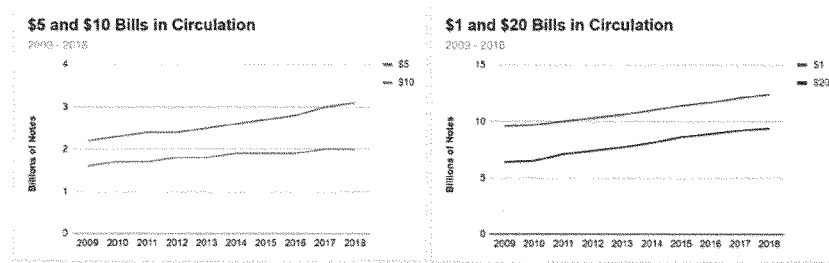
1. Cash is still king. Those who are more likely to use cash represent an unusual cross-section of Americans that defy traditional grouping such as elderly rural Americans and young African Americans.
2. America’s payment system has broadly become an engine of income inequality, charging the poor more, giving to the rich, and benefiting large businesses relative to small businesses.
3. As the economy digitizes, those without access to low cost, reliable digital payments are increasingly unable to participate and share in the benefits.
4. America’s payment system has become a global laggard in payment technology. Having invented the payment system of the past fifty years does not automatically mean we will have the system of the future.
5. Policy makers have the tools to modernize our payment system, empower consumers, small businesses, and engender equitable and broad access to mobile payments. The question is if, when, and how policymakers will use them.

From this analysis, several policy recommendations come forth. Businesses conducting in-person sales, particularly small dollar sales of core consumer goods, should as a general matter, with some exceptions, be required to accept cash. Banks and credit unions should be required to make consumer’s funds available immediately, subject to the existing anti-fraud provisions in the Expedited Funds Availability Act. Research is needed to develop comprehensive recommendations for how the future of America’s retail payment system, including how to ensure universal access to low cost, secure digital wallets.

### I. Cash is King (still)

Despite rumors of its demise, the amount of cash in circulation continues to grow. Demand for small dollar notes proves cash's reign is alive, and demand for smaller dollar transactions remains. Over this decade: the number of one-dollar notes has grown by almost 30 percent, and the number of five-dollar notes has grown by over 40 percent.<sup>1</sup> Similar growth in ten- and twenty- dollar notes in circulation can be seen in Figure 1 below. This rate of growth is evidence of continued usage and underlying demand for cash, and decidedly unlike the penny, which is produced by the government and which, more often than not, ends up in a jar.<sup>2</sup>

Figure 1: Currency in Circulation



Data from the Federal Reserve

Data on cash transactions are difficult to come by. It is inherently harder to track cash than electronic payments. The Federal Reserve's Diary of Consumer Payment Choice<sup>3</sup> survey asks a representative sample of Americans to track how they purchase goods in the month of October, which is then used to extrapolate annual and national trends. The survey's data has several consistent findings:

- Cash usage is inversely correlated to the size of the transaction. Cash is the most common way to pay for transactions under \$25. It is unusual to use cash for transactions over \$100 (only 6 percent of all transactions over \$100 report using cash).

<sup>1</sup> Data from the Federal Reserve's currency in circulation. Time frame is 12/31/2009 through 12/31/2018. "Federal Reserve Board - Currency in Circulation."

<sup>2</sup> Gadsby, J., *Future of the Penny*, Federal, United States General Accounting Office, July 1996.

<sup>3</sup> Federal Reserve Bank of San Francisco. "2019 Findings from the Diary of Consumer Payment Choice." Accessed January 28, 2020. <https://www.frbsf.org/cash/publications/fed-notes/2019/june/2019-findings-from-the-diary-of-consumer-payment-choice/>.

- Cash is more popular among low-income households, those under 25, those over 65, and those in rural areas. This is contrary to a popular narrative that young people never use cash.<sup>4</sup> Skepticism regarding anecdotal reporting regarding payment usage is recommended, given the high correlation between income and payment type.
- There has been a small decline in cash usage in the survey – falling from 31 percent of transactions in 2016 to 26 percent in 2018. This decline is driven by changes in the composition of purchases, which is related to but separate from many of the underlying reasons why cash is king. Specifically, a ten percent decline in the number of small dollar purchases (under \$25) and a five percent increase in the number of purchases over \$100 result in total reduction in cash usage. The decline of purchases not made in person (presumably made on-line) has increased by four percent, further reducing the potential for cash transactions.

Additional data sources show that African Americans are significantly more likely to use cash, and a small increase in the likelihood of cash usage among Latinx households.<sup>5</sup> The case of Square, a digital payments provider, is particularly interesting. Square analyzed data for small businesses that use their cash register product and found 37 percent of all transactions were in cash, a figure higher than the Federal Reserve’s survey found as a national average for all consumer payments. This indicates that small businesses are maybe more likely to receive cash, or that the Square businesses maybe dealt in disproportionately smaller dollar transactions, or possibly both. Square found substantial variation between states, although, in every state, at least one out of three transactions used cash. The five states in which cash was used as often as cards were (50/50) Wisconsin, Delaware, Iowa, West Virginia, and Hawaii.<sup>6</sup> Higher cash rates in states with large rural populations is consistent with the San Francisco Federal Reserve Bank’s finding that “Rural areas are more likely to make cash payments than urban areas. Credit card usage in urban areas is twice that of rural areas.”<sup>7</sup>

That said, within urban areas cash usage varies significantly. Square looked in-depth within New York City and found significant variation by borough. The Bronx and Staten Island had

<sup>4</sup> Tsosie, Claire. “Millennials Checked Out on Using Cash.” NerdWallet, November 14, 2014.

<https://www.nerdwallet.com/blog/credit-cards/millennials-cash-credit-mobile-banking/>.

<sup>5</sup> Perrin, Andrew. “More Americans Are Making No Weekly Purchases with Cash.” Pew Research Center, December 12, 2018. <https://www.pewresearch.org/fact-tank/2018/12/12/more-americans-are-making-no-weekly-purchases-with-cash/>.

<sup>6</sup> “Making Change: Payments, Perspectives, and Politics.” Accessed January 28, 2020.

<https://squareup.com/us/en/making-change>.

<sup>7</sup> Flannigan, Tom. “Annual Fed Report Indicates Increase in Demand for Cash despite Slight Decline in Usage by Consumers.” Federal Reserve Bank of San Francisco. Federal Reserve Bank of San Francisco, July 10, 2019. <https://www.frbsf.org/our-district/press/news-releases/2019/annual-fed-report-indicates-increase-in-demand-for-cash-despite-slight-decline-in-usage-by-consumers/>.

significantly greater usage of cash as compared to card (approaching 50/50) than Manhattan (25/75) or Brooklyn (30/70). Queens was roughly in the middle (43/57). Expanding the geographical scope, substantial payment differences within a city, between states, and between urban and rural areas indicate that multiple factors are at play determining payment usage. Additional data and research are necessary to refine our understanding of the use of cash. What is clear is that people who disproportionately use cash are an unusual coalition of the very young and old, rural and urban, and racial minorities. The usage of cash is greatest for the daily necessities of life, smaller dollar purchases, and transactions in person.

## **II. Payments Are a Reverse Robin Hood.**

America's payment system segregates people into different means of payment. This is by design. To explore this, start at the bottom rung of the income ladder. Lower income families are more likely to use cash as documented earlier. In addition to cash, pre-paid cards have exploded in usage over the past fifteen years, accounting for over 13 billion transactions worth \$300 billion in 2017 according to the Federal Reserve.<sup>8</sup> For every three credit card swipes there is roughly one prepaid card swipe.

The users of prepaid cards are more likely to be low-income, African-American and property renters (rather than property owners), according to the Pew Charitable Trusts.<sup>9</sup> Pew's survey demonstrated that most pre-paid card holders have checking accounts and consequently have debit card alternatives. Prepaid card holders reported using the prepaid cards as opposed to debit cards, in part, to avoid one of the most expensive elements of the banking system for working families: overdraft fees.

Debit cards are the most common form of card payment, with over 80 billion transactions. They are the most common form of payment for the middle of the middle class. Notably with debit cards, if you always have money in your bank account they are basically free for consumers. However, if you occasionally hit the zero lower bound of your bank account, any purchase on a debit card could trigger an overdraft. Overdrafts are typically \$35 per transaction, which, for a \$3.50 cup of coffee, is the equivalent of a 1,000% immediate fee. One estimate put total overdrafts at \$34 billion in 2015.<sup>10</sup>

<sup>8</sup> "The Federal Reserve Payments Study: 2018 Annual Supplement." The Federal Reserve, December 2018.

<sup>9</sup> "Why Americans Use Prepaid Cards: A Survey of Cardholders' Motivations and Views." The Pew Charitable Trusts, February 2014.

<sup>10</sup> Other estimates differ but magnitudes are all substantial. Theresa Schmall, and Eva Wolkowitz. 2016. "2016 Financially Underserved Market Size Study." Center for Financial Services Innovation. [https://cfsinnovation.org/wp-content/uploads/2016/11/2016-Financially-Underserved-Market-Size-Study\\_Center-for-Financial-Services-Innovation.pdf](https://cfsinnovation.org/wp-content/uploads/2016/11/2016-Financially-Underserved-Market-Size-Study_Center-for-Financial-Services-Innovation.pdf).

The Consumer Financial Protection Bureau's study of overdraft revealed that a whopping 27% of bank accounts tracked in their study year had an overdraft. Among those accounts, the average overdraft and related fees totaled \$225, with some banks having average total fees for accounts that overdraft in excess of \$400.<sup>11</sup>

Overdrafts are common for a combination of reasons. First, many Americans live paycheck to paycheck. Income volatility is rising<sup>12</sup> particularly among lower income households.<sup>13</sup> Second, America's slow and outdated payment system disempowers people from being able to know their actual balance in real-time. Payments can be processed anytime from the same day to five to six calendar days later, depending on a myriad of factors far beyond a person's control. Without knowing when their funds are available, consumers living on the margin are left guessing whether they have enough to cover their purchase.

Debit cards are functionally free for those who always have a cushion in their bank account. However, for those whose incomes are volatile and who occasionally or frequently approach the zero lower bound of their bank account, debit cards can become expensive payment mechanisms. Compounding the problem, the lack of real-time payments results in consumers fundamentally not knowing whether they can or cannot use their debit card without triggering an overdraft. These uncertainties explain both the rise in prepaid card usage and the continued advantages of using cash. Accessing cash is not always free, however ATM fees are required to be posted by federal law<sup>14</sup> and while those fees can be a substantial proportion of a small dollar withdrawal and are often higher for non-bank ATMs located in lower income communities, they are substantially lower than a single overdraft.

At the top of the payment ladder are credit cards. Within credit card offerings there are substantial differences in terms. Subprime credit cards bear little resemblance in features and cost structures to high-end cards. For the purpose of this testimony and to complete the trip through the payment spectrum, it is important to focus on prime, high-end high reward cards. High rewards credit cards are designed for wealthy consumers who typically do not carry a balance but spend a lot. These cards offer substantial rewards, often two percent or more in cash or equivalent value (e.g. frequent flier miles, hotel reward points, and so on). These rewards are worth more to consumers because they are considered rebates and not income, and hence are not subject to federal, state, or local taxation. Thus, for the wealthy families they

---

<sup>11</sup> "CFPB Study of Overdraft Programs." Consumer Financial Protection Bureau, June 2013.

<sup>12</sup> "How Income Volatility Interacts With American Families' Financial Security." The Pew Charitable Trusts, March 2017.

<sup>13</sup> Farrell, Diana, and Fiona Greig. "Paychecks, Paydays, and the Online Platform Economy: Big Data on Income Volatility." JP Morgan & Chase Co. Institute, February 2016.

<sup>14</sup> Electronic Funds Transfer Act, 15 U.S. C. § 1693.

are designed for, the true value of these rewards can approach or pass five percent of pre-tax income for all purchases made.

These rewards add up, too. Consider a wealthy family that spends \$250,000 a year on a credit card with two and a half percent cash back. They receive \$6,250 in tax-free rewards, which is worth more than \$10,000 in pre-tax income.<sup>15</sup> Meanwhile, families using cash or debit cards get nothing.

Here is where the economics of cross-subsidization are revealed. Merchants are bound by contract and consumer expectations to charge the same price to all customers. Because businesses cannot charge more to those who use high-end credit cards, even though merchants often pay higher fees on those cards, they must adjust prices. The result is that lower income workers who use cash and debit end up cross-subsidizing wealthier rewards card holders. If merchants could pass along their full cost of processing, then consumers who use more expensive cards to process, would pay higher prices.

The Supreme Court's recent decision to side with American Express over Ohio (and 16 other states) compounds this problem.<sup>16</sup> As a result of the Court's five to four verdict, state governments are not able to enact legislation to empower merchants to decide whether to accept certain high cost cards. In effect, if you take one Visa credit card you must now take them all. This verdict is bad for most consumers and will allow high end reward cards to continue to grow, accruing more benefits to the wealthy at the expense of the middle and working class and merchants.<sup>17</sup>

This is particularly hard for smaller businesses who have less bargaining power in negotiating card fees. The growth in card usage and fees is an issue of concern for small businesses precisely because they lack the scale to either develop alternative payment forms like the Starbucks app (which, for many years, was the largest payment app in America), or negotiate lower swipe fees. Small coffee shops throughout America are at an economic disadvantage versus the big chains because they pay significantly more in swipe fees, which can often be 10 percent or more of the price of a cup of coffee. Future exploration of the impact of the payment system on small business is warranted.

### **III. Payments are the New Digital Divide**

<sup>15</sup> Klein, Aaron. "Opinion: How Credit Card Companies Reward the Rich and Punish the Rest of Us." Los Angeles Times, December 20, 2019. <https://www.latimes.com/opinion/story/2019-12-20/opinion-how-credit-card-companies-reward-the-rich-and-punish-the-rest-of-us>.

<sup>16</sup> *Ohio et al. v. American Express co. et al.*, 585 U.S. (2018)

<sup>17</sup> Klein, Aaron. "Why the Supreme Court's Decision in Ohio v. AmEx Will Fatten the Wealthy's Wallet (at the Expense of the Middle Class)." Brookings Institute, June 25, 2018.



While cash is still king, there is no denying that an increasingly large number of goods and services are moving onto digital platforms that do not except cash. As online and mobile apps transform the economy, consumers who are dependent on cash or prepaid cards are increasingly left behind.

Prior concerns about a digital divide were incorrectly centered around questions of internet access.<sup>18</sup> Smart phones have successfully bridged much of the divide in terms of access.<sup>19</sup> However, access alone is insufficient. Without a means to purchase the goods or services being offered, the benefits of the app-,gig-, or online-economy fail to convey and the ability to access digital payment systems are creating a practical digital divide.

The ramifications of this divide are greater than fully appreciated. The growth in online and app-based goods and services have brought significant savings to consumers with lower costs for everything from ordering groceries to hailing a taxi. However, people cannot access those savings without access to low cost or free digital payment mechanisms. This is clearly a problem for the one in fifteen households in America that are un-banked.<sup>20</sup> Without access to a bank account, debit or credit card, there is often no way to make a digital payment. Some combination of prepaid cards can provide that for some services. However, that is not always available, can be cumbersome, requires pre-positioning scarce dollars, and is often quite expensive given high costs and fees embedded in debit products.

The problem is also evident for those who are under-banked (roughly one in six Americans) and those who live paycheck to paycheck.<sup>21</sup> Regarding this latter group, some estimates characterize almost half of Americans as living paycheck to paycheck.<sup>22</sup> The economics of many app-based digital services simply assume that the user will always have funds to cover recurring or periodic expenses and expect the ability to tap into that consumer's bank account to receive funds. Given the high cost of overdraft, income volatility, and payment delays, the result for consumers living on the razor's edge can be a far more expensive.

---

<sup>18</sup> Lohr, Steve. "Digital Divide Is Wider Than We Think, Study Says." The New York Times, December 4, 2018, sec. Technology. <https://www.nytimes.com/2018/12/04/technology/digital-divide-us-fcc-microsoft.html>.

<sup>19</sup> There remain areas where concerns about access as a barrier are significant, including rural areas, Native lands, and even in urban areas, concerns about the cost of data and data access for lower income smart phone users. However, broadly speaking the prior century's concerns about access being the primary divide have turned out not to be the case.

<sup>20</sup> FDIC National Survey of Unbanked and Underbanked Households, 2017  
<https://www.fdic.gov/householdsurvey/2017/2017report.pdf>

<sup>21</sup> Ibid

<sup>22</sup> GOBankingRates. "49% of Americans Are Living Paycheck to Paycheck," August 20, 2019.  
<https://www.gobankingrates.com/saving-money/budgeting/americans-living-paycheck-paycheck/>.

The impact of this payments divide extends beyond financial services. Consider the potential health benefits available to a series of new transportation applications, such as bike sharing or healthy food delivery through food- or farm-shares. These technologies hold the promise to reduce costs of some of the largest budget items a family face: food and transportation. They offer better, cheaper ways to meet existing needs that in turn provide significant opportunities to live a healthier lifestyle – eventually reducing societal healthcare costs and improving quality of life. However, neither allow for cash. Both require access to digital payment. One may have a pay as you go system, the other a recurring regular charge. Each may be cheaper than the alternative (grocery store or taxi/public transportation), but those cost savings are built around the assumption of no payment frictions. Once a single overdraft fee is charged, the entire cost savings disappear, and the application is now a money loser for the user.

For lower income consumers, in particular (importantly not just the un-banked, but the underbanked as well), to truly benefit from the digital economy, cheap and reliable digital payments are a necessity. This is a significant and growing problem. It may require government policies that provide resources and set stronger rules mandating different options and availability for Americans of all financial levels. It is a corollary to the policy requirement that cash continue to be accepted, the digital access to payments will also need to be facilitated.

#### **IV. America Once a Global Leader Now a Global Laggard**

Fifty years ago America pioneered the new payment technology that would come to dominate high end payments: magnetic striped plastic cards.<sup>23</sup> This technology, coupled with robust consumer protection legislation from Congress, such as the Electronic Funds Transfer Act, created the environment for this new technology to take off.<sup>24</sup> These cards, and the corresponding terminals to read them, allowed a small plastic card to replace cash and checkbooks for billions of consumers and merchants and process trillions of transactions. These cards achieved such ubiquity in the developed Western world that most consumers and international travelers take their presence for granted. They have continued to grow, providing the backbone for e-commerce and new methods of digital payments.

New methods to utilize card-based payments accounts have grown. Devices can now turn smartphones into credit card processors (such as the case of Square, mentioned above) and transactions can be securely conveyed online (such as the case of PayPal). However, the underlying payment networks in America remain a bank-based system. Do not be fooled into thinking that digital representations of magnetic striped cards, such as Apple Pay, or digital

<sup>23</sup> IEEE Spectrum: Technology, Engineering, and Science News. "Full Page Reload." Accessed January 28, 2020. <https://spectrum.ieee.org/computing/hardware/the-long-life-and-imminent-death-of-the-magstripe-card>.

<sup>24</sup> Much of this section draws from my paper: Is China's new payment system the future. Klein, Aaron. "Is China's New Payment System the Future?" Brookings Institute, June 2019.

wallets that draw and relay funds to bank-based accounts for settlement, are themselves new payment systems. They are simply different ways to use the existing bank-based system more efficiently. In fact, it is still quite anachronistic that the main security feature for standard plastic cards is a signature after a swipe, which seems to be highly ineffective and time consuming, while accessing a phone to use a digital representation can be done with biometric data or a pin, both of which are far more secure and fraud resistant.

While America spent the past decade upgrading its bank-based magnetic striped cards with chips, China experienced a retail payment revolution. Leapfrogging the card-based system, two new payment systems have come to dominate person-to-person, retail, and many business transactions. China's new system is built on digital wallets, QR codes, and runs through their own big tech firms: Alipay running through Alibaba (China's version of Amazon) and WeChat Pay running through Tencent (China's version of Facebook). China's system largely disintermediates banks from payment transactions robbing banks of an important and long-standing source of revenue. It creates an alternative payment ecosystem with different incentives between merchants, consumers, and payment system providers. It challenges the long-standing placement of payments on the side of banking as opposed to commerce. In doing so, this system creates new incentives that could realign existing business models and relationships between merchants, banks, and technology providers.

China's new payment system exploded in under a decade, growing from inception to dominance. With over a billion users on each platform, the power of network incentives has been unleashed. The new payment system has replaced cards and cash at registers, how families give gifts, and even how beggars ask for money, with QR codes replacing tin cups. These and other indicators tell us that China's new payment system is here to stay. It will continue to grow domestically and globally, following Chinese travelers and consumers abroad. China's experience makes clear that new technology allows payment systems to move from banking to follow technology and social networking companies. Those firms have other sources of data on which to base financial decisions such as providing credit.

America legally separates banking and commerce in unique ways. The payment system has historically existed on the banking side of that divide. However, the legal separation does not require that alignment. Payments could move away from banking, in theory, in the U.S., and the incentives created by moving the payment system from banking to technology firms are substantial and potentially concerning. The potential for anti-competitive behavior and privacy concerns by tech platforms by using the payment system and data generated from it is real. It is not clear whether these concerns can and would be remedied by effective regulation. It is also not clear what the departure of the payment system would mean for the health and stability of the financial system.

I do not believe the Chinese system is likely to catch on in America. America's existing system has multiple impediments to the Chinese model, or a similar one, taking over. As discussed early, wealthier consumers benefit more from substantial rewards linked to the current

payment system. Merchants may have difficulty transitioning and generating substantial savings from a new system. Consumer behavior is sticky. America's existing regulatory systems provide substantial consumer protection through the bank-based system that may be lost in a non-bank payment system.

#### V. Rethinking our Payment System

The American legal and regulatory framework is not well prepared should payments move out of the banking system. As financial technology provides greater ability to underwrite and provide credit as part of payment services, our legal framework will be further tested. Financial regulators and policy makers need to revisit the consumer protection and payment laws passed twenty to fifty years ago, and regulations adopting them, to incorporate new technology.

An example of this approach was the CFPB's original prepaid card rule,<sup>25</sup> whereby the protections afforded debit cards under EFTA<sup>26</sup> were expanded to include digital wallets. This type of data driven approach to extend a legal and regulatory framework that helped debit cards become the largest electronic payment system would work well for prepaid cards and digital wallets. All financial regulators should proactively explore how their rules and regulations can be extended to incorporate new payment technology.

An example of a mistake was the Federal Reserve's failure to utilize its longstanding legal authority to require consumers to have immediate access to their own funds. Despite rapid widespread adoption of check truncation, the Fed maintains its multiday hold periods. The result is billions of dollars in unnecessary costs for millions of lower income Americans. Congress did its part in passing the Check-21 Act in 2004<sup>27</sup> to allow for digital check processing. The Fed failed to do its job to require the funds to move faster to consumers. As a result, millions of American families will get paid tomorrow, Friday January 31<sup>st</sup>, but will be unable to access their own money until Monday, February 3<sup>rd</sup>, or in some cases Wednesday, February 5<sup>th</sup>. How are those families who live paycheck to paycheck supposed to pay their bills due the first of the month, put food on the table, and make it through the three to five days when their own money is sitting in there, not accessible to them? The sad reality is that payday lenders, check cashers, and bank overdraft fees will be the costly answer. The payment system is one reason why it is very expensive to be poor.

This problem, and many others could be solved by widespread adoption of real-time payments. Americans should not have to wait to reap the benefits of real time payments until the Federal Reserve's proposed system is built and operational, which best case will be almost twenty years after similar technology was deployed in the United Kingdom, Mexico, and Brazil. Instead, the Fed can and should use their regulatory authority to require existing bank customers to have

---

<sup>25</sup> 12 C.F.R. § 1005.2016.

<sup>26</sup> 15 U.S.C. § 1693.

<sup>27</sup> Check Clearing for the 21<sup>st</sup> Century Act, Pub. L. No. 108-100, 117 Stat. 1177 (2003).

access to the first \$5,000 of any deposit immediately. Banks can choose to use an existing real-time payment provider or continue to clear that payment through the Fed's slow and outdated ACH system and give up the float. If the Fed will not use its regulatory authority as Congress instructed until it modernizes its own operating system, then Congress should. Doing so is one of the best levers to reduce income inequality in America without raising taxes. Creating real-time electronic funds availability would likely reduce the demand for cash. After all, one of the biggest benefits of cash as a payment form is immediate clearing.

#### **Final Thought**

In conclusion, cash continues to play a vital role in America and is likely to for many years. The existing payment system does not serve the needs of working American families very well. Instead the payment system has become a reverse Robin Hood, imposing large, direct and indirect costs, on those with less and providing growing rewards to wealthy families. The growth of financial technology, particularly cashless digital wallets, is an opportunity to fix these problems. More research and strategic thinking are necessary to ensure universal access to future payment systems. The new digital divide is increasingly not about being able to get on-line, it is about being able to pay electronically.



United States House of Representatives Financial Services Committee

Task Force on Financial Technology

Is Cash Still King? Reviewing the Rise of Mobile Payments

Testimony of Christina Tetreault

Senior Policy Counsel

Consumer Reports

January 30, 2020

## Introduction

Chairman Lynch and Ranking Member Emmer and Members of the Financial Technology Task Force, thank you for the invitation to appear today. I am Christina Tetreault, senior policy counsel on Consumer Reports' financial services policy team. Consumer Reports is an expert, independent, non-profit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. Consumers Reports works for pro-consumer policies in the areas of financial services and marketplace practices, antitrust and competition policy, privacy and data security, food and product safety, telecommunications and technology, travel, and other consumer issues in Washington, DC, in the states, and in the marketplace. Consumer Reports is the world's largest independent product-testing organization, using its dozens of labs, auto test center, and survey research department to rate thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

Consumer Reports (CR) has a long history of working to improve payments protections for consumers. In 2008, the then-leader of CR's financial services policy team, Gail Hillebrand, published a comprehensive overview of and proposed solutions for "the mess" in payments law that she saw would be exacerbated by the rise of mobile.<sup>1</sup> In 2011, CR published its first report on mobile payments, Michelle Jun's *Mobile Pay or Mobile Mess: Closing the Gap Between Mobile Payment Systems and Consumer Protections*.<sup>2</sup> From 2015 - 2018, CR staff served on the steering committees of the Federal Reserve's Faster and Secure Payments Task Forces, working with industry, retailers, regulators and other consumer groups to ensure safer payments modernization. In 2018, Consumer Reports rated peer-to-peer payment services, including Apple, Square's Cash app and Venmo.<sup>3</sup> With the launch of CR's Digital Lab in 2019, Consumer Reports continues to make digital privacy and security, including for financial services, an essential part of our work for a fair, just and safe marketplace. I appreciate the opportunity to share our expertise here today, and thank the Committee for calling attention to the consumer implications of the rise of mobile payments.

Consumer problems with mobile payments reflect problems in payments and the digital ecosystem: current law irrationally applies different consumer protections to different payment methods, and electronic payments have inherent privacy and security issues. These issues are intensified by the mobile environment. Congress can fix these problems by creating uniform payments protections for all payment types, and establishing a strong federal floor of privacy protections with curbs on data collection and sharing, empowered watchdogs to ensure compliance, and real consequences for those companies that fail to meet their obligations.

---

<sup>1</sup> Gail Hillebrand, *Before the Grand Rethinking: Five Things to Do Today with Payments Law and Ten Principles to Guide New Payments Products and New Payments Law*, <https://advocacy.consumerreports.org/wp-content/uploads/2013/04/WhereisMyMoney08.pdf>. The specific reference to mobile is at 786.

<sup>2</sup> <https://advocacy.consumerreports.org/wp-content/uploads/2013/02/Mobile-Pay-or-Mobile-Mess.pdf>

<sup>3</sup> <https://www.consumerreports.org/digital-payments/mobile-p2p-payment-services-review/>

I. **Mobile is a platform, not a payment type.**

**A mobile payment is a payment made from a mobile device using an app or a wallet, and funded by a linked funding mechanism.**

Mobile payments allow consumers to make purchases or transfer money with a few taps on a mobile device. The most common method for making a mobile payment in the United States is to use a mobile payments application, either one that is downloaded to a mobile device, such as Venmo, or one that is integrated into the mobile device's operating system, such as Apple Pay. Mobile payments include payments made at the point of sale, online and in apps, and person-to-person money transfers. To make an online or in-app payment, the user simply taps a few commands on their mobile device. At the point of sale, a user may tap their phone to pay, or flash a QR code that is read by the register. Less common are mobile payments via text message, which are charged to the payee's mobile carrier bill. For example, during the 2019 fires in Sonoma County, people could text REDCROSS to 90999 to make a \$10 donation; the \$10 appeared on the donor's phone bill.<sup>4</sup> With the exception of direct-to-carrier billing, users must link a funding source to the app to fund the payment. Funding sources include credit, debit, gift or prepaid cards, or a bank account. After a wallet is funded, some services allow users to transact with stored value, funds held in the user's digital account by the service provider.

While the user interfaces of mobile wallets and payment apps make it appear that money moves instantly, it does not. Beneath the modern veneer of mobile payments is technology older than the oldest Millennials. Money moving as a result of a mobile payment ultimately moves the same way money moves with a bank transfer or payment card: along rails built in the early 1970s.<sup>5</sup> Cryptocurrency, rarely used for consumer payments,<sup>6</sup> relies on new technology to move money, as does The Clearing House's Real Time Payments (RTP) rail. However, these technologies are quite different. Private cryptocurrencies, as discussed in more detail below, create more consumer problems than they solve, and raise questions about applicable law. RTP moves money at the speed of information, but RTP payments are still electronic funds transfers, and are, as leadership from The Clearing House has said, covered by existing payments law.<sup>7</sup> Regardless of the underlying technology, however, mobile is a platform, not a new payment type.

<sup>4</sup> <https://abc7news.com/5659200/>

<sup>5</sup> Behind the scenes, mobile payments move money on the Automated Clearing House, launched in 1974, (<https://www.nacha.org/content/history-nacha-and-ach-network>) and the card networks. These are also from the early 70s. See for example, Visa, <https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/visa-net-booklet.pdf>

<sup>6</sup> <https://www.reuters.com/article/us-crypto-currencies-payments-analysis/bitcoin-for-payments-a-distant-dream-as-usage-dries-up-idUSKCN1NP1D8>

<sup>7</sup> The Clearing House, RTP, Increasing Payment Efficiency, Weil, Gotshal & Manges Roundtable, at slide 9, [https://ccl.yale.edu/sites/default/files/files/Hunter\\_Rob\\_Presentation.pdf](https://ccl.yale.edu/sites/default/files/files/Hunter_Rob_Presentation.pdf)



## II. Mobile payments expose the contradictions and inconsistencies in payments law.

### Consumer protections for mobile payments follow the underlying payment type.

What types of protections a mobile payment has depends on what the underlying funding mechanism is.<sup>8</sup> In most mobile payment applications, users can draw on a host of payment types to make purchases. With the exception of direct-to-carrier billing, these payments look pretty much the same to consumers. However, they each provide different levels of protection to consumers.

The type of consumer protections a payment type has depends on the laws and regulations that apply to it. Mobile payments linked to credit cards have the strongest protections. Mobile payments funded by debit cards or bank accounts are second best. Mobile payments linked to gift cards have few protections, and payments charged to a mobile phone bill fewer still.<sup>9</sup> The most pronounced differences among payments protections are the caps on liability for errors and fraud, and the right to withhold payment when there is a dispute.

### Payment protections by payment type:

**Credit cards:**<sup>10</sup> Consumer liability for unauthorized credit card charges resulting from a lost or stolen credit card, which in mobile payments can include the phone itself, a chip in the phone or a sticker on the phone, is limited to \$50. If a billing error appears on a consumer's credit card statement, there is no liability as long as the consumer reports the error within 60 days. Credit cards also have a chargeback right, the right to reverse a charge if the goods or services were not delivered as agreed, including non-delivery, defect, or delivery of the wrong item.

**Debit cards (includes stored value and funds drawn from a linked bank account):**<sup>11</sup> This includes a growing set of products, from debit cards to services such as Venmo and Paypal that store value for consumers. For these products, consumer liability for unauthorized transactions is limited to \$50 if the consumer notifies the financial institution within two business days after learning of the loss or theft of the access device. If the consumer fails to notify the financial institution within two business days after learning of the loss or theft of the access device but notifies the bank within 60 days, liability can be up to \$500. If notice to the issuer exceeds 60 days, losses may be unlimited. Consumers have the right to be re-credited missing funds from unauthorized

<sup>8</sup> Michelle Jun, *Mobile Pay or Mobile Mess*,

<https://advocacy.consumerreports.org/wp-content/uploads/2013/02/Mobile-Pay-or-Mobile-Mess.pdf>.

<sup>9</sup> For a thorough discussion of direct to carrier billing, see Michelle Jun, *Mobile Pay or Mobile Mess*, <https://advocacy.consumerreports.org/wp-content/uploads/2013/02/Mobile-Pay-or-Mobile-Mess.pdf>. As noted by Professor Mark Budnitz in *The Legal Framework of Mobile Payments: Gaps, Ambiguities and Overlaps*, the FCC took steps to address the issue of "cramming," unauthorized charges added to mobile carrier bills, after the publication of *Mobile Pay or Mobile Mess*, but large gaps remain: [https://www.pewtrusts.org/-/media/assets/2016/02/legal\\_framework\\_of\\_mobile\\_payments\\_white\\_paper.pdf](https://www.pewtrusts.org/-/media/assets/2016/02/legal_framework_of_mobile_payments_white_paper.pdf) at 35 and 42.

<sup>10</sup> Rules governing credit cards are found in the implementing Regulation Z, Truth in Lending, 12 CFR Part 1026.

<sup>11</sup> Rules governing these transactions are found in the implementing Regulation E governing electronic funds transfers 12 CFR Part 1005.

transactions within 10 business days. Debit cards and stored value do not have a chargeback right.

**Gift cards:**<sup>12</sup> Consumers have no legal protections that limit liability in the case of unauthorized transactions or other errors for gift cards. Consumers who link mobile payments to gift cards will not likely be able to recover lost funds in the event of fraud or error.

**Direct to carrier billing:** Consumers whose mobile payments are charged to their phone bills have unclear legal protections. Interstate and international telephone services are regulated by the Federal Communications Commission (FCC). FCC truth-in-billing requirements are meant to ensure that a consumer's bill contains necessary information in a fashion that consumers can understand.<sup>13</sup> The rules prohibit carriers from putting unauthorized charges on consumers' bills, but they do not contain clear liability limits, rights of recredit or chargeback rights. There may be some protections for consumers in state laws or public utility agency rules, but these vary from state-to-state.

**Consumers do not understand their rights and obligations when using mobile payments, and may find they have trouble resolving mobile payments problems.**

While mobile payment providers may think of themselves as a mere "trusted intermediary" to whom consumers entrust their payment credentials,<sup>14</sup> consumers don't think of these companies that way. Users in CR's 2017 focus groups of peer-to-peer (P2P) services told CR that the company with whom they interacted—Facebook, Square, PayPal, etc.—would help fix any problems and make them whole. CR research found this is not necessarily the case.<sup>15</sup> Research by Pew found that consumers find mobile payments problems unusually difficult to resolve.<sup>16</sup> CR's research shows that providers make help relatively difficult to find in the wallet or app,<sup>17</sup> and few make telephone contact numbers publicly available.<sup>18</sup> These practices are out of alignment with the consumer expectation expressed in CR's focus groups.

<sup>12</sup> Rules governing gift cards are contained in Regulation E, and are found at 12 CFR § 1005.20

<sup>13</sup> 47 CFR Y §64.2400-2401, Truth-in-Billing Requirements for Common Carriers. For a more complete discussion see Budnitz, The Legal Framework of Mobile Payments: Gaps, Ambiguities and Overlaps, [https://www.pewtrusts.org/-/media/assets/2016/02/legal\\_framework\\_of\\_mobile\\_payments\\_white\\_paper.pdf](https://www.pewtrusts.org/-/media/assets/2016/02/legal_framework_of_mobile_payments_white_paper.pdf) ¶ 42.

<sup>14</sup> *PayPal v Consumer Financial Protection Bureau* complaint at 14.

<sup>15</sup> Why Apple Pay Is the Highest-Rated Mobile P2P Payment Service, <https://www.consumerreports.org/digital-payments/mobile-p2p-payment-services-review/>.

<sup>16</sup> Pew, Are Americans Embracing Mobile Payments? Survey of consumer experiences finds greater trust in credit, debit cards, <https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2019/10/are-americans-embracing-mobile-payments>.

<sup>17</sup> Consumer Reports, Peer-to-Peer Payments Are Generally Safe, But Consumers Must Be Aware of Risks, <https://www.consumerreports.org/digital-payments/peer-to-peer-payments-are-generally-safe-but-consumers-must-be-aware-of-risks/>.

<sup>18</sup> Social media is filled with pleas from consumers that are some variation on, "Can't I just call you to resolve this?" See for example, <https://twitter.com/VictorMavika/status/1218295784405266432?s=20> and <https://twitter.com/Kittieb3/status/1217931828071366657?s=20>.

The gap between consumer expectations and provider practices would not be worrying if problems were extremely rare, but they are not. There are numerous media reports of consumers being scammed into sending money via mobile payment apps, only to discover too late that these transactions have essentially the same level of protections as cash.<sup>19</sup> The law covering electronic funds transfers considers a transfer “authorized” by the account holder even if the account holder was induced to send those funds by fraud.<sup>20</sup> We have called on the Consumer Financial Protection Bureau to extend legal protections to fraud victims.<sup>21</sup> The need for consumers to have a right to be made whole in these instances will only become more urgent as faster payments become more common.

CR’s research also shows that P2P users sometimes mistakenly send money to the wrong person, and, as noted above, service providers often tell users that they are on their own to get it back.<sup>22</sup> We think that in instances of misdirected payments, service providers have a legal responsibility to assist users transacting with stored value. The rules covering electronic funds transfers, found in Regulation E, include a definition of error: “An incorrect electronic fund transfer to or from the consumer’s account.”<sup>23</sup> While we believe that Regulation E is clear on this point already and that no regulatory changes are needed, we have called on the Consumer Financial Protection Bureau to clarify procedures to remove any uncertainty.<sup>24</sup>

---

<sup>19</sup> These scams vary, and occur with many different payment apps. See for example, Consumer Reports, Peer-to-Peer Payments Are Generally Safe, But Consumers Must Be Aware of Risks, , <https://www.consumerreports.org/scams-fraud/how-to-protect-yourself-from-p2p-payment-scams/>; Venmo texting scam: Here’s what you need to know about the new con, <https://www.foxbusiness.com/technology/venmo-texting-scam-what-to-know/>; Scammers are targeting Cash App users hoping for free money, <https://www.zdnet.com/article/scammers-are-targeting-cash-app-users-hoping-for-free-money/>; How cyber crooks target bank accounts via payment apps like PayPal, <https://www.freep.com/story/money/personal-finance/susan-tompori/2019/05/08/payment-apps-scams-venmo-paypal/3661254002/>; Instant fraud: Consumers see funds disappear in Zelle account scam The digital payment service embedded in banking apps has made it easier for thieves to access funds in personal checking and savings accounts, experts say, <https://www.nbcnews.com/business/consumer/instant-fraud-consumers-see-funds-disappear-zelle-account-scam-n1015736>.

<sup>20</sup> 12 CFR 1005.2(m) “Unauthorized electronic fund transfer” means an electronic fund transfer from a consumer’s account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit.”

<sup>21</sup> Consumer Reports comment on the Consumer Financial Protection Bureau’s Inherited Regulations and Inherited Rulemaking Authorities, <https://www.regulations.gov/document?D=CFPB-2018-0012-0039>.

<sup>22</sup> Consumer Reports, Peer-to-Peer Payments Are Generally Safe, But Consumers Must Be Aware of Risks, <https://www.consumerreports.org/digital-payments/peer-to-peer-payments-are-generally-safe-but-consumers-must-be-aware-of-risks/>

<sup>23</sup> 12 CFR § 1005.11(a)(1)(ii)

<sup>24</sup> Consumer Reports comment on the Consumer Financial Protection Bureau’s Inherited Regulations and Inherited Rulemaking Authorities, <https://www.regulations.gov/document?D=CFPB-2018-0012-0039>.

**Consumers worry about mobile payments security, and mobile payments providers could do more to secure user accounts.**

Consumers worry about the security of mobile payments, according to Pew research.<sup>25</sup> There is reason for concern. Both the Consumer Financial Protection Bureau and the Federal Trade Commission have sued mobile payments providers over security practices.<sup>26</sup> Additionally, CR research shows providers can and should do more to keep users safe. In particular, they could design their apps to “default” to the highest security settings, meaning users would have to actively choose to opt out. In our 2018 research, several payment apps, including Venmo, Square’s Cash App, and Facebook Payments in Messenger, failed to require a password, PIN, or fingerprint for repeat access to the app or to initiate a transaction when their default security settings are in place.<sup>27</sup> Media reports appear with some regularity in which scammers ask to borrow a person’s phone then use the victim’s payment apps to transfer significant sums out.<sup>28</sup> If access or transfers required user authentication every time, scammers could not do this.

**Many Americans remain adverse to mobile payments.**

American adoption of mobile payments has lagged behind that of other countries and analysts’ expectations.<sup>29</sup> That may in part be because Americans still love cash: cash is the most frequently used payment instrument, representing 30 percent of all transactions and 55 percent of transactions under \$10.<sup>30</sup> As compared to mobile, consumers prefer card payments, and are skeptical of mobile payments safety and security, a skepticism that crosses generations.<sup>31</sup> So

<sup>25</sup> Pew, Are Americans Embracing Mobile Payments? Survey of consumer experiences finds greater trust in credit, debit cards, <https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2019/10/are-americans-embracing-mobile-payments>

<sup>26</sup> PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act, <https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information> and CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices <https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/>

<sup>27</sup> Consumer Reports, Peer-to-Peer Payments Are Generally Safe, But Consumers Must Be Aware of Risks, <https://www.consumerreports.org/digital-payments/peer-to-peer-payments-are-generally-safe-but-consumers-must-be-aware-of-risks/>

<sup>28</sup> See eg. Criminals are asking to use your phone, then sending cash to themselves, police say, <https://www.wncn.com/article/news/crime/criminals-are-asking-to-use-your-phone-then-sending-cash-to-themselves-police-say/275-603972444>

<sup>29</sup> The Economist explains Why Americans are warming to mobile payments, They are finally being weaned off their cheque books, <https://www.economist.com/the-economist-explains/2018/06/26/why-americans-are-warming-to-mobile-payments>

<sup>30</sup> <https://www.frbst.org/cash/publications/fed-notes/2018/november/2018-findings-from-the-diary-of-consumer-payment-choice/>

<sup>31</sup> Pew, Are Americans Embracing Mobile Payments? Survey of consumer experiences finds greater trust in credit, debit cards, <https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2019/10/are-americans-embracing-mobile-payments>

while seemingly every year is going to be “the year of mobile payments,”<sup>32</sup> 2020 is probably not going to be that year.

**PayPal's lawsuit to overturn the CFPB Prepaid Rule threatens mobile payment protections.**

Current protections for mobile payments made with stored value, imperfect as they are, are threatened by the PayPal lawsuit seeking to invalidate the Consumer Financial Protection Bureau's Prepaid rule. The rule essentially extends the protections that apply to bank account transfers and debit card transactions to stored value.<sup>33</sup> Before the prepaid rule, consumers had to rely on what few protections state money transmitter laws have to cover their use of prepaid accounts.<sup>34</sup> These laws lack the error resolution rights<sup>35</sup> and right of recredit that apply to prepaid cards now that they are covered by the prepaid rule.

PayPal's lawsuit argues that the prepaid rule was meant to apply to physical general purpose reloadable prepaid cards and not to digital wallets. This misunderstands prepaid's history, and the history of the rule. Prepaid is not and never was simply a plastic card. Early prepaid users adopted prepaid accounts to shop online or otherwise where cash is not accepted.<sup>36</sup> Prepaid users were among the first to send money person-to-person via text. And as an example of how the rule was never meant simply to apply to plastic cards, CR sought to have it extended to cryptocurrency wallets.<sup>37</sup>

A lot of money will be at risk if the rule goes away. Today, Venmo has 40 million users. These consumers are responsible for more than \$100 billion in transactions.<sup>38</sup> Even if only a small fraction of that is stored value, consumer funds in Venmo are likely in the billions. And Venmo is but one example of a digital account covered by the prepaid rule. Millions of Bluebird, Walmart

<sup>32</sup> Tony Danova, Mobile Is Poised To Upend The Payments Industry [2013] <https://www.businessinsider.com/the-mobile-payments-moment-2013-12>; Ryan Rommann, Cash Is Trash: The Future of Mobile Payment [2014], <https://www.forbes.com/sites/teconomy/2014/01/23/cash-is-trash-the-future-of-mobile-payment/#1997b6a61596>; Alix Murphy, The Year Of Mobile Payments [2015], <https://techcrunch.com/2015/04/19/the-year-of-mobile-payments/>.

<sup>33</sup> The Consumer Financial Protection Bureau, Rules Concerning Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z), <https://www.consumerfinance.gov/policy-compliance/rulemaking/final-rules/rules-concerning-prepaid-accounts-under-electronic-fund-transfer-act-regulation-e-and-truth-in-lending-act-regulation-z/>

<sup>34</sup> Pew Issue Brief, Imperfect Protection, Using Money Transmitter Laws to Insure Prepaid Cards, [https://www.pewtrusts.org/-/media/legacy/uploadedfiles/pes\\_assets/2013/pewprepaidmoneytransmitterpdf.pdf](https://www.pewtrusts.org/-/media/legacy/uploadedfiles/pes_assets/2013/pewprepaidmoneytransmitterpdf.pdf).

<sup>35</sup> Professor Mark E. Budnitz, The Legal Framework of Mobile Payments, Gaps, ambiguities, and overlap, at 14 and 33, [https://www.pewtrusts.org/-/media/assets/2016/02/legal\\_framework\\_of\\_mobile\\_payments\\_white\\_paper.pdf](https://www.pewtrusts.org/-/media/assets/2016/02/legal_framework_of_mobile_payments_white_paper.pdf).

<sup>36</sup> Pew, Why Americans Use Prepaid Cards, [https://www.pewtrusts.org/-/media/legacy/uploadedfiles/pes\\_assets/2014/prepaidcardssurveyreportpdf.pdf](https://www.pewtrusts.org/-/media/legacy/uploadedfiles/pes_assets/2014/prepaidcardssurveyreportpdf.pdf) at 13.

<sup>37</sup> <https://advocacy.consumerreports.org/wp-content/uploads/2015/03/signed-final-CU-CFPB-proposed-prepaid-rules-comment.pdf>

<sup>38</sup> <https://www.cnn.com/2019/04/25/venmo-discloses-huge-digital-user-base-but-no-plan-to-profit-from-it.html>

Money Card and Serve accounts - all virtually indistinguishable from online bank accounts under the prepaid rule - will lack protections if the prepaid rule is invalidated.

### **III. Mobile payments multiply privacy concerns inherent in non-cash payments.**

#### **Mobile payments' providers privacy practices are wanting.**

Mobile payments cannot be made anonymously.<sup>39</sup> Electronic payments require the involvement of multiple parties and therefore have many eyes on them. For example, a credit card payment implicates at minimum a merchant, two banks and a payments processor.<sup>40</sup> The number of eyes grows when a mobile device, telecom or internet service provider, and third party app are in the mix. Some data collection is necessary and appropriate, but often digital financial data collection far exceeds this baseline.

Mobile payments services are often touted as "free." Users are not the customers of these services, they are the product. Mobile payment providers justify all-encompassing surveillance of users in the name of "analytics" or "product improvement." Providers also reserve broad rights to use your data for unrelated purposes, including targeted advertising, and share user data outside what a user would reasonably expect. The potential for users' information to be weaponized against them is particularly acute when payments are combined with platforms such as Facebook, Uber and Amazon.

Privacy is a fundamental human right. As CR's Director of Consumer Privacy and Technology Policy Justin Brookman has written, surveillance is a privacy harm, and consumers have a privacy interest in controlling commercial collection of their personal information.<sup>41</sup> Consumers must have options to avoid the always watching eyes of their bank, credit card company or payments provider. That means cash use should continue to be an option for consumers. And it also means there needs to be meaningful curbs on data collection and sharing. People should be able to shop without our every move being tracked, recorded, and shared.

Providers can do more to give consumers control over information collected about them. Consumers deserve easy, standardized tools that give them control over their information and allow them to stop companies from using their data for extraneous purposes. These best practices and more are outlined in The Digital Standard, an open-source digital privacy and security standard, which companies should adopt.<sup>42</sup> Wherever possible, consumers should be able to make choices about multiple companies at once. CR supports and is working on efforts to make these types of controls the industry standard in financial services.<sup>43</sup> However, consumers shouldn't bear the entire burden of protecting their privacy through settings and controls. Laws are necessary to ensure that the cost of access to financial services is not constant surveillance.

<sup>39</sup> Cryptocurrency enthusiasts argue otherwise, but that is not a topic I'm addressing here.

<sup>40</sup> Susan Herbst-Murphy, Clearing and Settlement of Interbank Card Transactions: A MasterCard Tutorial for Federal Reserve Payments Analysts, at 22, <https://www.philadelphiafed.org/-/media/consumer-finance-institute/payment-cards-center/publications/discussion-papers/2013/D-2013-October-Clearing-Settlement.pdf>.

<sup>41</sup> Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, FUTURE OF PRIVACY FORUM BIG DATA & PRIVACY WORKSHOP PAPER COLLECTION (2013), <https://fpf.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf>.

<sup>42</sup> <https://www.thedigitalstandard.org/>

<sup>43</sup> CR recently joined the Financial Data Exchange, <https://financialdataexchange.org/>.

#### IV. Cryptocurrency in its current forms creates more consumer problems while solving none.

Many claims have been made about how mobile financial services, and mobile payments in particular, increase financial inclusion. The entire Libra project, for example, is justified by Facebook with the dubious claim that it will “empower billions of people.”<sup>44</sup> The reality is that the reasons consumers are outside the financial mainstream in the United States are largely structural.<sup>45</sup> Nothing about cryptocurrency fixes this, nor will any app or digital wallet.

Unbanked consumers - people without checking or savings accounts, are less likely than banked consumers to use mobile payments,<sup>46</sup> and are far more cash reliant than other Americans.<sup>47</sup> The reasons consumers rely on cash are many, but unbanked consumers cite not having enough money to keep in account as a primary reason they are unbanked.<sup>48</sup> Unbanked consumers are more likely to suspend or cancel their cell phone plans because of the cost of maintaining coverage, therefore making regular use of mobile financial services is nearly impossible for unbanked consumers.<sup>49</sup>

If the legal mess in traditional payments, as described above, is bad, the legal mess in cryptocurrency is worse. Right now and in the absence of action from either Congress or Consumer Financial Protection Bureau, the few consumer protections that cryptocurrency users have are mostly found in state money transmitter laws. As noted above, these state laws lack the types of payments protection found in federal law. To date, the Consumer Financial Protection Bureau has declined to opine on whether Reg E applies to cryptocurrency wallets. Similarly, there is no federal deposit insurance for cryptocurrency. Cryptocurrency scams and fraud are rampant, and hacking of wallets and exchanges, where virtual currencies are stored, is common.<sup>50</sup> These products and services should not be tested on consumers with the least

<sup>44</sup> <https://libra.org/en-US/white-paper/#introduction>

<sup>45</sup> Unbanked Americans, when asked cite the costs associated with banking, and - first and foremost - not having enough money to keep in account as the main reasons for not having a bank account. <https://www.fdic.gov/householdsurvey/2017/2017execsumm.pdf> at 4.

<sup>46</sup> Pew, What Do Consumers Without Bank Accounts Think About Mobile Payments? <https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2016/06/what-do-consumers-without-bank-accounts-think-about-mobile-payments>

<sup>47</sup> Federal Deposit Insurance Corporation, 2017 FDIC National Survey of Unbanked and Underbanked Households Executive Summary, at 12, <https://www.fdic.gov/householdsurvey/2017/2017execsumm.pdf>.

<sup>48</sup> *Id.* at 4.

<sup>49</sup> Pew, What Do Consumers Without Bank Accounts Think About Mobile Payments? <https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2016/06/what-do-consumers-without-bank-accounts-think-about-mobile-payments>

<sup>50</sup> Olivia Solon, Bitcoin, titcoin, ponzi coin: jokes and scams fuel a cryptocurrency gold rush, *The Guardian* (Feb. 2, 2018),

<https://www.theguardian.com/technology/2018/feb/02/bitcoin-bananacoin-prodeum-cryptocurrencies>; Shane Shifflett and Coulter Jones, Buyer Beware: Hundreds of Bitcoin Wannabes Show Hallmarks of Fraud, *A Wall Street Journal analysis of 1,450 cryptocurrency offerings reveals rampant plagiarism, identity theft and promises of improbable returns*, (May 17, 2018), <https://www.wsj.com/articles/buyer-beware-hundreds-of-bitcoin-wannabes-show-hallmarks-of-fraud-1526573115>; Kate Rooney, \$1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do, *CNBC* (June 7, 2018), <https://www.cnn.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-d>

cushion in their financial lives. The best way to ensure consumer access to faster and safer electronic payments is to support the Federal Reserve's proposal to build the FedNow faster payments system, not by empowering new fangled, untested, unregulated corporate schemes.

## V. Recommendations

### **Congress should create a strong federal floor of consumer payments protections.**

Congress can make every way safe to pay with a few updates to existing laws, as CR's Gail Hillebrand advised in 2008.<sup>51</sup> It remains the case that there is little that consumers can do on their own to ensure their safety,<sup>52</sup> a situation compounded by the mobile environment in which consumers have little understanding of their rights and obligations. Congress can ensure that all payment types have the same baseline protections for consumers.

Congress should amend the Electronic Fund Transfer Act (EFTA) to provide equal, strong loss caps and a guaranteed recredit time periods after unauthorized use for all non-cash, non-check payments. Congress should also update the EFTA to provide a chargeback right for all non-cash, non-check payment types. Congress should also extend the chargeback right in the Fair Credit Billing Act to cover direct-to-carrier billing. These changes would go a long way to ensuring that mobile payments have a strong baseline of protections.

### **Congress should pass strong privacy legislation, including curbs on data collection.**

The Gramm-Leach-Bliley Act (GLBA) makes a distinction between financial and other types of data. When the name of your first pet can be the key to account access, and money can be sent using only a phone number, the line between sensitive financial data and everything else is either already meaningless or well on its way to becoming so.

The Gramm-Leach-Bliley Act should not be mistaken for a privacy law. GLBA requires financial services providers to explain their information-sharing practices to their customers and to protect sensitive data.<sup>53</sup> The disclosures required by GLBA, which are intended to give consumers the opportunity to opt-out of the sharing of nonpublic personal information with third parties and to outline the company's data use practices, are so confusing that consumers are unlikely to exercise their rights. Moreover, GLBA does nothing to curb data collection in excess of what is reasonably necessary. Its incentives to protect consumer data from unauthorized disclosure remain inadequate. Still, banks and financial services providers seek and get broad exemptions from state privacy laws by claiming that GLBA protects consumer privacy.<sup>54</sup> The GLBA regime does no such thing and it is time for Congress to act.

Every person by dint of their humanity has a right to privacy. As noted above, CR urges providers to adopt the tools and practices in the Digital Standard. But legal action is also

[o.html](#).

<sup>51</sup> Gail Hillebrand, *Before the Grand Rethinking: Five Things to Do Today with Payments Law and Ten Principles to Guide New Payments Products and New Payments Law*, <https://consumersunion.org/pdf/WhereisMyMoney08.pdf>

<sup>52</sup> *Id.*

<sup>53</sup> Pub. L. 106-102

<sup>54</sup> For a discussion of the gaps and ambiguities in the California Consumer Privacy Act created by the GLBA exemption, see *The 2018 California Consumer Privacy Act: Understanding Its Implications and Ambiguities*, [https://www.frbsf.org/banking/files/Fintech-Edge-Special-Report\\_CCPA.pdf](https://www.frbsf.org/banking/files/Fintech-Edge-Special-Report_CCPA.pdf) at 5.



needed. Consumer Reports urges Congress to adopt national privacy legislation that creates a strong floor of protections for consumers and requires data minimization, clear information about data practices, strong data security practices. A national privacy law should provide consumers with easy access to their information, and strong enforcement tools to ensure accountability.

#### **Conclusion**

Consumers remain skeptical of mobile payments. This skepticism is not unfounded, given the documented legal mess in payments, and the gaps in privacy and security attendant to mobile payments. Mobile payments problems reflect the fact that current law applies different consumer protections to different payment methods, even though those payment methods are more or less the same. Privacy and data security concerns about mobile payments are issues that transcend payments. Congress can help fix these problems by creating uniform payments protections for all payment types, and establishing a strong federal floor of privacy protections with strong curbs on data collection and sharing, empowered watchdogs to ensure compliance, and real consequences for those companies that fail to meet their obligations.



STATEMENT OF

MARK WELLER

EXECUTIVE DIRECTOR  
AMERICANS FOR COMMON CENTS

ON THE QUESTION OF  
“IS CASH STILL KING? REVIEWING THE RISE OF MOBILE  
PAYMENTS”  
BEFORE THE  
HOUSE FINANCIAL SERVICES TASK FORCE ON FINANCIAL  
TECHNOLOGY

UNITED STATES HOUSE OF REPRESENTATIVES

JANUARY 30, 2020

1401 Eye Street, N.W., Suite 800, Washington, D.C. 20005  
ph (202) 626-8363

[www.pennies.org](http://www.pennies.org)

Chairman Lynch, Ranking Member Emmer, and Members of the Task Force, my name is Mark W. Weller and I am Executive Director of Americans for Common Cents (ACC). I am pleased to submit testimony today concerning the one-cent coin, its importance to the American economy and culture, and more broadly about the key role that cash still plays in our economy, despite growth in the use of credit and debit cards and mobile payments.

By way of background, ACC was established in 1990 to conduct research and educate Congress on the need to retain the penny. Our organization is broad-based and comprised of, and endorsed by, many of the nation's leading coin and numismatic organizations, charitable organizations that benefit from penny donations, and companies involved in the manufacturing and transport of the penny.

There are three primary points I want to share with you today about cash and digital payment technology:

1. **Cash safeguards our privacy.** All electronic payment transactions are traceable and by their nature subject to surveillance and control. If third-party financial institutions must be part of all transactions, then they will be privy to the intimate details of everyone's financial life. The House Financial Services Committee and other policy makers have rightfully raised concerns about privacy and how this data is used.
2. **Cash acts as a public good.** Cash is acceptable to everyone. A move to cashless payments means financial and social exclusion for those who are precluded from participation in a digital society, particularly the young, elderly and minorities who use cash more frequently than individuals with higher incomes.
3. **Cash ensures economic stability.** Digital payment systems are vulnerable to blackouts, technical glitches, and cyberattacks. These vulnerabilities endanger individuals and society to the risk of immediate economic collapse. Cash cannot be hacked. Cash also serves as a fallback solution in times of financial calamity.

The facts above, which are discussed in more detail below, require that we maintain our country's cash infrastructure. ACC is *not* anti-technology. Indeed, we support consumers having several ways to make payments be that in cash, with credit and debit cards, or via contactless payments. But cash must continue to be a payment

option within this landscape of contemporary payments and U.S. policy must protect consumers' right to use cash. For some people, often the most vulnerable populations, cash is their only payment option.

Often lost in the discussion about monetary technologies is the fact that the majority of payments worldwide are still made in cash. Here in the U.S., according to the Federal Reserve, cash is the most used payment instrument for in-person transactions, which is where almost three-quarters of all payments take place and where nearly 90% of non-bill payments are conducted.<sup>1</sup> For these in-person payments, cash accounted for 39% of the volume.<sup>2</sup> Also of note, cash remains the most popular payment method for small value transactions, with almost half of payments under \$10 being made with cash.<sup>3</sup> In addition, when considering payment preferences, cash remains a preferred secondary payment choice regardless of what payment instrument consumers prefer to use primarily.<sup>4</sup> Although the 2019 Federal Reserve study marks the first time cash was not the most used payment instrument, it continues to be used widely across myriad demographic groups.

Even as new payment methods continue to emerge, cash is still king for now. The following expands upon the several important policy reasons informing the need to maintain our cash infrastructure.

#### **CASH SAFEGUARDS OUR PRIVACY**

All electronic payment transactions are traceable. Placing control of our currency in the hands of digital payment companies threatens individuals' privacy as information about one's political and religious affiliation, sexual orientation, health conditions and personal relationships is available. More concerning is the threat that without cash as a payment option, credit card and other private companies could eventually come to decide what constitutes a socially acceptable or allowable purchase.<sup>5</sup>

---

<sup>1</sup> Raynil Kumar and Shaun O'Brien, "2019 Findings from the Diary of Consumer Payment Choice," Federal Reserve Bank of San Francisco, June 2019, found at <https://www.frbsf.org/cash/publications/fed-notes/2019/june/2019-findings-from-the-diary-of-consumer-payment-choice/>

<sup>2</sup> Kumar and O'Brien, *Ibid.*

<sup>3</sup> Kumar and O'Brien, *Ibid.*

<sup>4</sup> Kumar and O'Brien, *Ibid.*

<sup>5</sup> Melissa Quin, "VISA CEO: Company Will Keep Handling Firearms Purchases," Washington Examiner, August 8, 2019 found at <https://www.washingtonexaminer.com/news/visa-ceo-company-will-keep-handling-firearms-purchases>

According to a November 19, 2019 Pew Research Report, the majority of Americans are concerned about the collection and use of their data.<sup>6</sup> Intermediated transactions are by their nature subject to surveillance and control. People's purchasing and credit histories, as well as their online browsing and search behaviors, create user data profiles that are in turn used for targeted ads or to create risk profiles. Beyond the propriety of these activities, the more troubling question becomes what happens if cash is no longer an option – what happens if we lose our financial infrastructure to support cash?

Without cash, all transactions must be necessarily intermediated by financial institutions. If third-party financial institutions must be part of all transactions, then they will be privy to the intimate details of everyone's financial life. They can also choose to disallow certain transactions and potentially even certain persons from transacting.<sup>7</sup> Better is a country where cash remains legal tender for all purchases.

### **CASH ACTS AS A PUBLIC GOOD**

Cash is accessible to all and can be used free of charge once in circulation. I want to elaborate on these two important points for the Task Force.

First, as legal tender, cash is universally accepted and equally accessible to all consumers.<sup>8</sup> In contrast, a move to cashless payments means financial and social exclusion for those who are precluded from participation in a digital society, particularly the young, elderly and minorities who use cash more frequently than individuals with higher incomes. About 25% of US households are either "unbanked" or "underbanked,"<sup>9</sup> typically those with low incomes who lack the minimum balance to open checking and savings accounts. Moves to cashless retail limits the places where the poor and communities of color can access goods and services.

Strong concerns about restaurants and other businesses refusing to accept cash has led to introduction of bipartisan legislation which lies within this Committee's jurisdiction, H.R. 2650, the *Payment Choice Act*. This bill recognizes that cash is a public

<sup>6</sup> Brooke Auxier and Lee Rainie, "Key Takeaways on Americans' Views About Privacy, Surveillance and Data Sharing," Pew Research Fact Tank, November 15, 2019

<sup>7</sup> Jerry Brito, "Case for Electronic Payment, Why Private Peer-to-Peer Payments are Essential to an Open Society," Coin Center, February 2019.

<sup>8</sup> Ursula Dalinghaus, "Virtually Irreplaceable, Cash as Public Infrastructure," Cash Matters White Paper, August 1, 2019, p. 11

<sup>9</sup> "FDIC National Survey of Unbanked and Underbanked Households," Federal Deposit Insurance Corporation, October 2018, found at <https://www.fdic.gov/householdsurvey/2017/2017report.pdf>

good and also the importance of ensuring its continued existence alongside electronic and innovative payment options.

Second, cash is used free of charge once it is in circulation. Paying in cash does not incur any costs for consumers. In contrast, all digital payments firms require a third party intermediary. Indeed, various parties are trying to capture a piece of the lucrative payment market.<sup>10</sup> When paying with a credit card via PayPal or a smartphone app, the card networks, banks, and payment providers are all charging a fee.”<sup>11</sup>

Cash does not discriminate and it doesn’t preclude use by anybody. Cash also sustains transfers free of charge since it is the only method of payment not controlled by a private entity.

### **CASH ENSURES ECONOMIC STABILITY**

Digital payment systems are vulnerable to blackouts, technical glitches, and cyberattacks. These vulnerabilities endanger individuals and society to the risk of immediate economic collapse. Cash cannot be hacked. Cash also serves as a fallback solution in times of financial calamity. These advantages illustrate why we should not lose the infrastructure supporting the economic stability of cash.

The recent tensions over the killing of Quds Force leader Qasem Soleimani highlighted the tangible threat that Iran may employ its cyberwarfare prowess in retaliation. A cyber response is especially worrisome, as Iran has previously demonstrated its ability to conduct cyberattacks crashing US bank’s websites in 2012.<sup>12</sup> As this Committee is well aware, following the imposition of economic sanctions on Iran, customers of 46 large banks were unable to view their accounts or make transactions after being targeted with denial of service attacks linked to the Iranian government. Current cyberterrorism threats highlight vulnerabilities of the US banking and payment system.

Further threats to our economy result when we lose our cash infrastructure. It is increasingly difficult in some European countries for consumers to access their own

<sup>10</sup> Dalinghaus, *ibid*.

<sup>11</sup> Dalinghaus, *ibid*, p. 14

<sup>12</sup> Joseph Marks, “The Cybersecurity 202: Here’s How Iran Disrupted U.S. Businesses the Last Time It Launched Major Cyberattacks,” *The Washington Post*, June 25, 2019, found at <https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/06/25/the-cybersecurity-202-here-s-how-iran-disrupted-u-s-businesses-the-last-time-it-launched-major-cyberattacks/5d1107dea7a0a47d87c56e27/>.

cash. For example, Sweden is a virtually cashless country, with fewer than 20% of payment transactions being made in cash.<sup>13</sup> Half of the country's 1,400 bank branches no longer accept cash deposits, according to the European Consumer Organization.<sup>14</sup> As a result, the country relies heavily on Visa and MasterCard to process its transactions.

As the number of ATMs and bank branches steadily decrease, countries run the risk of losing their cash infrastructure<sup>15</sup>, thus making them even more vulnerable to economic disruption from technology glitches, system power failure and cyberattacks. Indeed, cash's "low tech" useability and capacity to function off the grid makes it a safe backup plan in the face of threats to our banking system, including cyberattacks. Cash's security and reliability reminds us of the importance of cash remaining a payment option.

## CONCLUSION

Our one-cent coin is a vital component of a larger cash infrastructure that must be maintained for the reasons described above.

Cash is convenient, private, and free to use. Cash is also the safest payment method, which is why cash demand skyrockets during crises, be they man-made or a natural disaster. Cash is our most resilient and reliable payment option, and it is imperative that we maintain our cash infrastructure even as consumers utilize other digital technology payment options.

<sup>13</sup> Sweden-The First Cashless Society?, "Swedish Institute, found at <https://sweden.se/business/cashless-society/>

<sup>14</sup> Jean Allix and Farid Aliyev, Cash Versus Cashless: Consumers Need a Right to Use Cash, The European Consumer Organization, September 25, 2019, found at [https://www.beuc.eu/publications/beuc-x-2019-052\\_cash\\_versus\\_cashless.pdf](https://www.beuc.eu/publications/beuc-x-2019-052_cash_versus_cashless.pdf)

<sup>15</sup> Allix and Aliyev, Ibid.

**Statement for the Record of Paul Wilmore**

**Chief Marketing Officer, Cardtronics**

Before the United States House Committee on Financial Services Task Force on  
Financial Technology

**Hearing entitled “Is Cash Still King? Reviewing the Rise of Mobile Payments”**

January 30, 2020  
Rayburn House Office Building, Room 2128

Chairman Lynch, Ranking Member Emmer, and Members of the Task Force on Financial Technology, thank you for the opportunity to submit this statement for the record about the vital role that cash plays in our evolving payments ecosystem and broader U.S. economy.

I am the Chief Marketing Officer for Cardtronics, the largest ATM operator in the world. Cardtronics connects people to cash in 10 countries, across four continents in North America, Europe, Africa, and Australia. Through our partnerships with financial institutions and retailers, Cardtronics operates 290,000 ATMs globally, including more than 200,000 ATMs in the U.S.

Our Allpoint network is the largest free-to-use retail ATM network in the United States. With over 40,000 ATMs nationwide, located in top retail locations, the Allpoint network allows over 2,000 financial institutions, community banks, and credit unions to provide their customers with convenient, surcharge-free access to our ubiquitous ATM network nationwide. Roughly 83% of the U.S. population resides within five miles of a Cardtronics ATM.<sup>1</sup>

As bank branches continue to close in the U.S.--with more than 5,700 branch closures over the past three years<sup>2</sup>--Cardtronics also is investing in high-functioning, cash accepting ATMs here in the U.S., to deliver full-service solutions to credit unions, banks, and other financial services providers for their customers.

We also continue to invest in other technologies, such as our mobile API, which enables cardless transactions, a feature of particular importance to Financial Technology (FinTech) companies who realize that there are times when their customers want to pay with cash and desire fee-free ATM access.

---

<sup>1</sup> <http://ir.cardtronics.com/static-files/4a1187df-38bf-4b95-9d96-e05cf2947c7f>

<sup>2</sup> <https://www.orionprop.com/topfive/bank-branch-closures-are-increasing-but-alternative-tenants-may-take-over-vacated-spaces/>



Our ATMs enable customers not only to convert digital cash into physical cash, but also to convert physical cash to digital cash. As the bridge connecting the worlds of both physical and digital cash, Cardtronics champions the increasing number of innovative payment choices that consumers have: credit, debit, mobile, and digital. Underlying all these payment options is cash—*held in a transactional account*.

While cash usage declined for the first time in 2018,<sup>3</sup> it remains the most widely accepted, durable, and private payment method. Cash is a substantial and important part of the U.S. payments landscape. Anyone can use cash and receive it without prior authorization or credit check for “all debts public and private,” as stated on every U.S. paper denomination.

With the rise of payment innovation that we do support, Cardtronics also has serious concerns an increasing national and global effort by some, to *eliminate* cash as a form of payment.

Numerous brick-and-mortar retailers,<sup>4</sup> restaurants,<sup>5</sup> sports stadiums (Utah Jazz Arena,<sup>6</sup> Mercedes-Benz Stadium, and Tropicana Field<sup>7</sup>) and municipal mass transit systems<sup>8</sup> are implementing cashless-only payment acceptance policies that bar cash-paying customers who have money in their wallets from engaging in commerce. The majority of U.S. airlines do not accept cash on flights.<sup>9</sup>

Americans should have the right to pay with cash, our U.S. currency, particularly financially disadvantaged populations who, in many instances, may have no choice but cash to spend.

Cashless payment accept policies established by businesses are especially confounding when one considers that *cash is the only payment method produced, issued, and backed by the federal government*. Cash provides a public way for all people and businesses to sell and buy goods and services. Consequently, merchants should be required to accept cash and not be required to accept other payment methods issued by private companies.

<sup>3</sup> <https://www.frbsf.org/cash/files/2019-Findings-from-the-Diary-of-Consumer-Payment-Choice-June2019.pdf>

<sup>4</sup> <https://www.usatoday.com/story/money/2018/11/28/holiday-shopping-more-retailers-just-saying-no-cash/2063747002/>

<sup>5</sup> <https://www.tendergreens.com/blog/cashless>

<sup>6</sup> <https://www.thestadiumbusiness.com/2020/01/16/utah-jazz-arena-goes-fully-cashless/>

<sup>7</sup> <https://www.cnbc.com/2019/03/03/arthur-blanks-next-stadium-revolution-going-cashless.html>

<sup>8</sup> [https://www.washingtonpost.com/express/2018/10/01/metro-is-considering-cashless-bus-routes-critics-worry-change-will-disproportionately-affect-poor/?utm\\_term=.efbdf569002f](https://www.washingtonpost.com/express/2018/10/01/metro-is-considering-cashless-bus-routes-critics-worry-change-will-disproportionately-affect-poor/?utm_term=.efbdf569002f)

<sup>9</sup> <https://www.eturbonews.com/539139/cashless-sky-majority-of-airlines-go-cash-free/>

When a business chooses to accept various electronic payment methods, that business must enter contractual agreements with private companies and pay fees on each transaction, which reduces their profits. There are no fees or contracts imposed on merchants or businesses when they accept cash.

Yet, there is no federal law prohibiting businesses from not accepting cash as payment for goods and/or services. The Coinage Act of 1965, specifically Section 31 U.S.C. 5103, entitled Legal tender, states: "United States coins and currency are legal tender for all debts, public charges, taxes, and dues." According to the U.S. Department of Treasury, private businesses are free to develop their own policies on acceptance or refusal of cash, unless a state law prohibits it.<sup>10</sup>

In response to the rise in cashless retail, 14 cities and states, and the United States Congress have introduced legislation that protects cash as a payment choice. Since 2018, the District of Columbia,<sup>11</sup> Connecticut,<sup>12</sup> New Hampshire,<sup>13</sup> New York City,<sup>14</sup> New York,<sup>15</sup> Michigan,<sup>16</sup> Oregon,<sup>17</sup> St. Louis,<sup>18</sup> Vermont,<sup>19</sup> West Hollywood<sup>20</sup>, and Wisconsin<sup>21</sup> introduced bills to prohibit merchants from discriminating against cash-paying customers for in-person transactions. In 1978, Massachusetts<sup>22</sup> became the first state in the union to enact a law that prohibits businesses from not accepting cash. In

<sup>10</sup> <https://www.treasury.gov/resource-center/faqs/Currency/Pages/legal-tender.aspx>

<sup>11</sup> <https://static1.squarespace.com/static/528921f4e4b089ab61d013d3/t/5c59b45824a694fb4c1923a1/1549382745438/Cashless+Retailers+Prohibition+Act+of+2019.pdf>

<sup>12</sup> <https://www.cga.ct.gov/2019/BA/pdf/2019HB-05703-R010931-BA.pdf>

<sup>13</sup> [http://www.gencourt.state.nh.us/bill\\_status/billText.aspx?id=1304&txtFormat=html&sy=2020](http://www.gencourt.state.nh.us/bill_status/billText.aspx?id=1304&txtFormat=html&sy=2020)

<sup>14</sup> <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3763665&GUID=7800AFC9-D8B1-41FD-9C31-172565712686&Options=ID%7CText%7C&Search=cashless>

<sup>15</sup> <https://legislation.nysenate.gov/pdf/bills/2019/S4574>

<sup>16</sup> <http://www.legislature.mi.gov/documents/2019-2020/billintroduced/Senate/pdf/2019-SIB-0310.pdf>

<sup>17</sup> <https://olis.leg.state.or.us/liz/2019R1/Measures/Overview/SB716>

<sup>18</sup> <https://www.stlouis-mo.gov/internal-apps/legislative/upload/boardbill/BB47-wd13.pdf>

<sup>19</sup> <https://legislature.vermont.gov/Documents/2020/Docs/BILLS/H-0902/H-0902%20As%20Introduced.pdf>

<sup>20</sup> <https://www.weho.org/Home/ShowDocument?id=41637>

<sup>21</sup> <http://docs.legis.wisconsin.gov/2019/related/proposals/ab364>

<sup>22</sup> <https://malegislature.gov/laws/generallaws/partiii/titleiv/chapter255d/section10a>

2019, New Jersey,<sup>23</sup> Philadelphia,<sup>24</sup> Rhode Island,<sup>25</sup> and San Francisco<sup>26</sup> enacted similar laws, banning businesses from not accepting cash for brick-and-mortar purchases.

Recognizing the threat of ‘cashless creep’ on our nation, in the 116<sup>th</sup> Congress, Representative Donald Payne (D-NJ) introduced the Payment Choice Act (HR 2650)<sup>27</sup> with co-sponsor, Representative Chris Smith (R-NJ). The bill, which has received wide bi-partisan support, would impose a Federal ban on cashless brick-and-mortar retail establishments. Notably, a recent survey conducted by Square found that 51% of small business owners would also support a regulatory requirement that they accept cash.<sup>28</sup>

All levels of government are working assiduously to ensure that consumers have the right to choose cash for brick-and-mortar retail purchases.

As we discuss the rise in digital payments in the U.S. and debate their impact on cash, **we must also address why cash matters to consumers, the economy, and America’s national security.**

When merchants mandate cashless payment policies for whatever reason, they are picking and choosing which customers they want to serve, effectively engaging in payment discrimination. The message is clear: they don’t care about John or Jane Doe who wants to pay with cash. “Neither you, nor your cash is welcome here.”

This is wrong. And the practice is especially harmful to marginalized, unbanked and underbanked Americans.

According to the *2017 FDIC National Survey of Unbanked and Underbanked Households*:

8.4 million U.S. households were ‘unbanked,’ meaning no one in the household had a checking or savings account. And 66% of unbanked consumers used ONLY cash to pay monthly bills. Another 24.2 million households were ‘underbanked,’ meaning that the household had a checking account; but also relied on other financial services. Nearly one in four underbanked households used *only* cash to pay monthly bills.

Americans also pay with cash, not because they are engaged in nefarious activities, but for privacy in making legitimate purchases. Consumers do not have to share any personal

<sup>23</sup> <https://www.philly.com/business/new-jersey-cashless-store-ban-amazon-philadelphia-20190318.html>

<sup>24</sup> <https://phila.legistar.com/LegislationDetail.aspx?ID=3710586&GUID=FD85947F-8151-4DB5-9949-AF6FEF14A9C9&Options=ID%7CText%7C&Search=180943>

<sup>25</sup> <http://webserver.rilin.state.ri.us/BillText/BillText19/HouseText19/H5116A.pdf>

<sup>26</sup> <https://sfbos.org/sites/default/files/o0100-19.pdf>

<sup>27</sup> <https://www.congress.gov/bill/116th-congress/house-bill/2650/cosponsors>

<sup>28</sup> <https://squareup.com/us/en/making-change>

information (date of birth, Social Security number, or credit card number) with a third party to use cash for a transaction.

Cash can't be hacked or tracked. The cost of online data breaches in the U.S., where consumers' personal information was stolen, reached an astonishing \$2.1 trillion *globally* in 2019.<sup>29</sup>

Cash is a 'censorship-resistant' currency<sup>30</sup> whose use cannot be monitored, controlled, approved, or denied by a third-party or government.

Further, cash is an equal opportunity payment option—meaning anyone, regardless of age, race, or income can use cash. Cash is also durable in an emergency, or when a payment system or electricity shuts down.

Ultimately, cash is freedom—the freedom to lawfully choose what, when, where, and from whom we can buy something, without any entity arbitrating that transaction. When consumers pay with cash, they are in control of their purchases. When consumers use electronic payments, a private company not only dictates the terms and conditions of how they use that payment tool, but also may profit from selling the consumer's personal transaction data.

Today, consumers use cash for 80% of payments under \$25 because cash is convenient and a frictionless, easy way to pay. While there's a misconception that only older people pay with cash, the opposite is true. Younger Americans prefer to pay with cash at a higher rate than any other group. According to the *Federal Reserve's 2018 Diary of Consumer Payment Choice*, individuals aged 18 to 25 pay with cash for 34% of purchases, followed by those 65 and older, who report using cash for 33% of purchases.<sup>31</sup>

Accepting cash won't harm or burden businesses anymore than it harms businesses to accept card or mobile payments. In fact, a 2011 study conducted by economist Anne Layne-Farrar found that even when including costs like point-of-sale transaction time, back office costs, counterfeit costs, and fraud prevention, ***cash was cheaper than debit in terms of cost per \$100 of sales***. Cash cost retailers \$0.53 per \$100 of sales, compared to \$1.12 for signature debit and \$0.81 for PIN debit. The study did not include credit cards.<sup>32</sup>

<sup>29</sup> <https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion>

<sup>30</sup> <https://coincenter.org/files/2019-02/the-case-for-electronic-cash-coin-center.pdf>

<sup>31</sup> <https://www.frbsf.org/cash/files/2019-Findings-from-the-Diary-of-Consumer-Payment-Choice-June2019.pdf>

<sup>32</sup> <https://www.frbsf.org/cash/publications/fed-notes/2019/august/cash-me-if-you-can-impacts-of-cashless-businesses-on-retailers-consumers-cash-use/>

In 2019, there was an estimated \$1.76 trillion of cash in circulation, close to the highest level in roughly 36 years.<sup>33</sup>

Cash directly impacts federal government revenues. In its recent May 10, 2019 report, *Long Live Cash: The Potential Decline of Cash Usage and Related Implications*, Congressional Research Service warned that if demand for cash were to decline, the income that the government receives from seigniorage and Federal Reserve remittances to the Treasury could decrease substantially.<sup>34</sup>

*Seigniorage* is the profit generated by the difference in the value of the physical currency produced by the government and what it cost the government to produce it.

The report notes:

“For example, a \$100 bill costs about 14 cents to print, generating revenues \$99.86 greater than cost. The profit generated by this difference is called seigniorage, and this income would decrease if demand for cash were to fall. In FY2017, the U.S. Mint generated \$391.5 million in net income from circulating coins and the profit generated by the U.S. Bureau of Engraving and Printing generated revenues \$693 million greater than expenses.”<sup>35</sup>

Cash-revenue from remittances that the Fed transfers to the Treasury would also drastically drop if there is less demand for cash. *Remittances* is money that the Fed earns after paying expenses and dividends to member banks. Financial institutions deposit their cash at a Federal Reserve Bank. When consumer demand for cash increases, a bank orders cash, and the Federal Reserve deducts that amount from the bank’s account. The more cash in circulation, the less interest the Fed pays to banks and the more remittance revenue it has to give to Treasury. In 2017, the Fed transferred \$80.6 billion in 2017 to Treasury.<sup>36</sup>

“In January 2019, there was approximately \$1.7 trillion of currency in circulation, and the Fed (as of this publication) paid an annual interest rate of 2.4% on reserve balances. By these measures, if all currency were instead bank reserve balances held at the Fed, it could increase Fed expenses (and thus reduce government revenues) by more than \$40 billion a year. If interest rates on reserves (which change when the Fed alters monetary policy) rose or fell, then expenses would increase or decrease, respectively, in this scenario,” noted the Congressional Research Service.<sup>37</sup>

<sup>33</sup> <https://www.latimes.com/business/story/2019-10-27/cash-is-more-popular-than-ever>

<sup>34</sup> <https://fas.org/sgp/crs/misc/R45716.pdf>

<sup>35</sup> *Id.*

<sup>36</sup> *Id.*

<sup>37</sup> *Id.*

Proponents of doing away with cash have proffered ‘What’s the big deal, if a nation becomes cashless? Electronic payments are more convenient and make it easier to surveille and monitor a population . . . to root out the bad guys.’

Well, we need look no further to China and Sweden to see the risks that emerge when a nation turns its back on cash.

***China is on a crusade to eliminate cash in order to control its citizens.*** Using data from digital payment platforms, the Chinese government builds *Social Credit* scores on citizens as a means to deny them access to certain goods and services, should they make purchases that the Chinese government deems “socially or politically unacceptable.”

***Sweden is a virtually cashless state.*** Most banks have no *krona* on hand. Only 2% of transactions in Sweden are now made with cash. The country relies heavily on major card networks to process nearly all of its banking transactions, leaving Sweden vulnerable to cyber espionage by a foreign government. A parliamentary committee is currently studying the impact that declining cash use will have on the country, particularly in the event of a hacking or power failure.

Conversely, Germany, unlike China and Sweden is on a mission to protect cash in order to preserve individual freedom and privacy. Roughly 80% of all transactions in Germany are conducted in cash. And while some merchants in the U.S. are moving away from accepting cash, most businesses and restaurants in Germany accept only cash.<sup>38</sup>

Max Otte, a German economist who leads Save Our Cash, a national campaign that opposes restrictions on cash, explained in an interview with Bloomberg that:

“Cash, to me, is an important public good by which you measure the transparency and legal order of a society, and also the respect for the individual and the private sphere. ‘Why do Germans like cash?’ is the wrong question . . . Why have others shifted to a cashless society so quickly?”<sup>39</sup>

How other nations are dealing with cash raises important issues for U.S. policymakers to consider in evaluating the positive and negative impact declining cash use will have on our nation. *Cardtronics’ position is not to advocate one payment method over another.* All payment types can and must coexist for the consumer’s benefit, especially when it comes to financial inclusion. There are times that people want to pay with cash, and other instances where they may choose a card or digital wallet. Consumers should have all these choices readily available (and widely accepted) at their fingertips.

As financial services companies continue to innovate beyond our imagination, even more payment options are on the horizon for consumers to access and enjoy. This is good;

<sup>38</sup> <https://www.bloomberg.com/news/features/2018-02-06/germany-is-still-obsessed-with-cash>

<sup>39</sup> *Id.*

however, the rise of digital payments should not mean the demise of cash. America has too much to lose if cash, the nation's currency, upon which America and her ideals was founded, is eliminated.



**United State House Financial Services Committee Task Force on Financial Technology**

**"Is Cash Still King? Reviewing the Rise of Mobile Payments"**

January 30, 2020

Chairman Lynch, Ranking Member Emmer and members of the Task Force, thank you for the opportunity to share our thoughts on the importance of paper currencies to today's modern economy. Technological advancements have made possible tremendous innovations in the financial services industry, but Congress should continue to implement public policy to promote further innovation while preserving paper currency options.

By way of background, Coinstar operates machines across the U.S. that provide consumers a convenient way to exchange loose coins for paper currency, donations or gift cards.

This testimony highlights three advantages of paper currencies over their electronic alternatives.

- **Privacy.** Paper currencies, as opposed electronic and online alternatives, present the surest option to guard against cyber threats and unwanted data sharing.
- **Financial Inclusion.** Although beneficial for some, financial innovations run the risk of leaving certain consumers, particularly rural individuals, behind.
- **Face Value.** Paper currencies present the most straightforward and cheapest method of conducting transactions. Given the costs associated with online and electronic payment systems, lower-income individuals must pay a greater share of their income to use these options.

**Privacy**

Lawmakers have been drafting privacy legislation for years and have yet to pass any comprehensive measures. With many questions left unresolved, enactment of such legislation could be years away, potentially leaving consumers exposed to unwanted sharing of financial information to third parties, who may be the subject of successful cyber-attacks.

We agree with Task Force Chairman Lynch, who said in a hearing last November that "consumers rightly expect their financial data to be kept secure by institutions and applications they use but unfortunately their expectations don't always match reality."<sup>1</sup> In other words, online alternatives to paper currencies, despite the benefits they offer, pose risks that were not present before their introduction into the marketplace.

---

<sup>1</sup> United States. Cong. House. Committee on Financial Service Task Force on Financial Technology. *Banking on Your Data: The Role of Big Data in Financial Services*. Nov. 21, 2019. 116th Cong. 1st sess. (Statement of Rep. Stephen F. Lynch, D-Mass.).



For consumers concerned about the privacy and security of their transactions and financial assets, paper currencies offer an alternative bad actors are unable to penetrate or track online. In other words, paper currencies are unhackable.

Kenneth Rogoff, a professor of economics and public policy at Harvard University, explains the benefit of paper currencies as a means of guarding against cybersecurity risks. In his paper *Costs and Benefits to Phasing Out Paper Currency*, he explains that paper currencies encourage "diversity of technologies and not to become overly dependent on an electronic grid that may one day turn out to be very vulnerable."<sup>2</sup>

In short, transactions carried out with paper currencies are inherently more secure and private than their online alternatives. These protections should be preserved for consumers in a world that has become increasingly vulnerable to lax data privacy practices and cyber-attacks.

### Financial Inclusion

Unlike their electronic alternatives, paper currencies do not marginalize certain communities. Paper currencies require no internet connection or expensive electronic devices, and are therefore inherently more inclusive by comparison.

One substantial barrier to universal use of online payment systems is lack of access to reliable internet connection. In 2018, Pew Charitable Trusts estimated that 24 million Americans lacked broadband connectivity.<sup>3</sup> For these consumers, the inability to use paper currencies to pay bills or make simple transactions would make ordinary life needlessly complex. According to the Congressional Research Service, "if the United States were to move toward becoming a cashless society that required consumers to use noncash, electronic payment services, it could present difficulties for those segments of the population who lack access to the financial system or to an electronic network."<sup>4</sup>

Similar to the data privacy legislation efforts, Congress and the Federal Communications Commission are attempting to bridge the digital divide. Despite their best efforts, many Americans remain without reliable internet access. If they are required to use online methods to make payments, they run a very real risk of falling behind in the modern economy. Congress should not let this happen.

### Face Value

Additionally, mobile payment systems almost always require users pay user fees that are necessarily more expensive for lower-income individuals in terms of percentage of income. By removing the option to use paper currencies, Congress would be directly disadvantaging lower-income individuals. To put it simply: "the basic cost of me handing you a \$100 bill? Zero. Only

<sup>2</sup> Kenneth S. Rogoff, *Costs and Benefits to Phasing Out Paper Currency*, National Bureau of Economic Research, Working Paper no. 20126, May 2014.

<sup>3</sup> Pew Charitable Trusts. (2018). *24 Million Americans Still Lack Broadband Connectivity*. Pew Charitable Trusts: <https://www.pewtrusts.org/-/media/assets/2018/07/broadbandresearchinitiative.pdf>

<sup>4</sup> Perkins, David W. (2019) *Long Live Cash: The Potential Decline of Cash Usage and Related Implications* (CRS Report No. R45716). Retrieved from Congressional Research Service website: <https://fas.org/sgp/crs/misc/R45716.pdf>

the energy to extend my hand. It is 100% free to transfer from one party to another in the simplest sense."<sup>5</sup>

If paper currencies are removed from circulation or no longer accepted by certain places of business, taxpayers without access to online banking services or payment methods will be left behind, unable to participate in the modern economy. Rather than prohibit them from participating, these are precisely the individuals Congress needs to help the most. We urge Congress to reject efforts to reduce the inclusivity of the current financial system. Public policy is meant to lift all boats, not sink the most vulnerable among us.

### Conclusion

Rogoff explains a harmful effect of completely removing paper currencies from circulation when he said an "eliminating a core symbol of the monetary regime could disrupt common social conventions for using money, possibly in unexpected ways. [...] This need not happen."<sup>6</sup>

Coinstar stands ready to work with Congress to enact legislation aimed at promoting financial privacy and inclusion for all Americans.

Thank you for your attention to this important matter.

---

<sup>5</sup> Glory. (2018). *Electronic Payments – Not As Cheap As You Think* [White paper]. Glory: [https://www.glory-global.com/-/media/Global/Downloads/EN\\_US/Whitepapers\\_EN\\_US/NEW-Glory-Electronic-Payments-are-Not-Cheap-White-Paper-US-V1-0.pdf](https://www.glory-global.com/-/media/Global/Downloads/EN_US/Whitepapers_EN_US/NEW-Glory-Electronic-Payments-are-Not-Cheap-White-Paper-US-V1-0.pdf)

<sup>6</sup> Kenneth S. Rogoff, *Costs and Benefits to Phasing Out Paper Currency*, National Bureau of Economic Research, Working Paper no. 20126, May 2014.



## Statement of the Electronic Payments Coalition

The Task Force on Financial Technology Hearing  
*Is Cash Still King? Reviewing the Rise of Mobile Payments*  
 January 30, 2020

As consumers increasingly rely on the electronic payments system to make purchases while keeping their personal data safe, it is critical that all stakeholders with a hand in any transaction continue to innovate and invest in technology to responsibly protect consumers. Consumers appreciate the electronic payments system because of its ease and safety, and merchants continue to accept electronic payments in part because of the high cost of accepting cash. However, the [Electronic Payments Coalition \(EPC\)](#) does not believe that the best solution is to legally mandate that merchants accept certain forms of payment, whether payment cards or cash.

The rise in electronic payments has positively impacted those that are unbanked, too. Some claim that as many as 1 in 4 Americans don't have access to electronic payments, but that claim does not appear to be accurate. The FDIC estimates that 6.5 percent<sup>1</sup> do not have a checking or savings account, and the Congressional Research Service also cites this number in its financial inclusion report.<sup>2</sup> Underbanked consumers may have access to electronic payments but may still engage in transactions outside of the financial system.

Nonetheless, the issue of financial inclusion must be addressed. Innovations by the financial industry are increasing access to banking and electronic payments. For example, in countries with a high unbanked population, many unbanked consumers still have mobile phones. The availability of new, secure mobile payments technologies has the potential to increase inclusion among unbanked and underbanked populations.

Despite growth in the popularity of electronic payments and trust in financial institutions, retailers continue to blur the facts when it comes to payments and security. In fact, mandating types of payments and specific security features may lead to lower costs for retailers, while at the same time decreasing security and choice for consumers (please see the discussion of PIN mandates below). When complaining about the cost of accepting credit and debit cards due to interchange fees, merchants fail to acknowledge the alternative, which is the cost of handling cash, and in the period leading up to the Durbin debit price controls and for years later vigorously asserted that cash had no cost, asserting in Congressional testimony that debit should clear at par.<sup>3</sup> Economic reality has now forced an abrupt reversal upon retailers. Cash requires more resources to accept. This includes everything from the time spent having to count change to paying armored vehicles for cash transport to prevent theft.

Retailers' own studies estimate the average cost of handling cash at about 9 percent, but it can be as high as 15 percent depending on the retail segment. Their research also found the cost of cash handling activities to merchants is \$96 billion in the U.S. and Canada.<sup>4</sup> In fact, 77 percent of small businesses self-report that their cost of accepting electronic payments is lower than the cost of accepting cash<sup>5</sup>. Electronic payments are less expensive to retailers than cash, costing them between 2 and 3.5 percent of the total purchase — and they are getting even

<sup>1</sup> "FDIC National Survey of Unbanked and Underbanked Household." FDIC. 2017.

<sup>2</sup> "Financial Inclusion and Credit Access Policy Issues." CRS. October 2019.

<sup>3</sup> House Committee on Financial Services Hearing on HR 2382, October 8, 2009. "Now, if I may, I'd like to raise one issue that NRF is very concerned about that's outside the Welch bill, and that is debit cards. Cash and check pass at par, that's face value. The Federal Reserve says that in return for a \$100 check, a bank must give you \$100 in exchange. Yet \$100 on a debit card is subject to interchange fees. But what is a debit card other than a plastic check? There's no loan, they're even called 'check cards.' It's time for Congress to demand the Fed to do for plastic checks what they've long insisted on for paper."

<sup>4</sup> "Cash Multipliers — How reducing the costs of cash handling can enable retail sales and profit growth." Enterprise. January 2018.

<sup>5</sup> "2019 Small Business Payments and Banking Survey, Report 2." Mercator Advisory Group. October 2019.

cheaper.<sup>6</sup> According to Verisk, the average fee that merchants pay to accept credit cards —the “merchant discount rate” — decreased from 2.33 percent in 2011 to 2.14 percent in 2019.<sup>7</sup>

Further, the value that U.S. merchants receive when they accept credit cards (+8.5%) and debit cards (4.5%) far exceeds what they pay for accepting credit and debit (-3.5% and -1.4%, respectively). This value, which includes increased sales (i.e., “ticket lift”), reduced cost of cash, faster transaction times, additional retail channels (e.g., e-stores), and prompt guaranteed payments, is ultimately what matters in determining whether the interchange fees merchants pay are “worth it.” Based on the data, it is clear that the value proposition is highly positive for merchants to accept electronic payments. With this evidence, it is impossible not to call into question the motivation of merchants when they resist adopting technology and security measures that improve the electronic payments system.

EPC does not support mandating merchants to take any type of payments. Competition fuels innovation and retailers have many options when it comes to payments, including credit cards, charge cards, prepaid cards, private label cards, debit cards, cash, and checks. This plethora of options incentivizes financial institutions to compete to offer the best rates and consumer protections. It is worth noting that consumers—and merchants — have repeatedly proven their preference for credit and debit cards. Today, most consumers own at least one credit card, including nearly two-thirds of those earning less than \$40,000 per year. And for those that do own a credit card, 87 percent of those consumers own a rewards card, including nearly three-fourths of consumers who earn less than \$20,000 per year.<sup>8</sup> The prevalence of consumer credit cards demonstrates the critical need for a reliable payment system that consumers can be confident in, whether making purchases online or at a brick-and-mortar store.

In today’s electronic payments system, tech companies, card networks, card-issuing banks, and credit unions work in concert to protect consumers, using 21st-century technologies like artificial intelligence and biometrics to detect fraud and secure accounts. U.S. card issuers have continued to innovate by developing and implementing these new technologies that help protect consumer data regardless of where the purchase occurs.

But the payment system that retailers have repeatedly argued for would leave consumers vulnerable to fraud. Retailers’ continued push for outdated technology, like a PIN mandate, would put these advances at risk. PIN is a fifty-year old technology, created in 1967, and is only effective at deterring lost or stolen card fraud—a small and diminishing share of overall fraud. The costs of converting to this standard would dwarf the expected benefits: a 2016 study suggests it would cost retailers \$4 billion over a five-year period to fully implement PIN, while eliminate just \$850 million in fraud.<sup>9</sup> A PIN mandate would have no impact in protecting against card-not-present (CNP) fraud, the largest and fastest-growing fraud component, as consumers increasingly shop online.

Reducing electronic payments card fraud is an important goal that the EPC strongly supports, which is why the industry remains laser-focused on developing and implementing technologies that address the two largest types of fraud (which together comprise nearly 90 percent of U.S. card fraud): counterfeit fraud and card-not-present fraud. Regarding counterfeiting, the transition to EMV technology has helped reduce counterfeit fraud by 87 percent in March 2019 compared to September 2015, a remarkable turnaround after years of steady growth in fraud levels.<sup>10</sup>

In the modern card-not-present payment environment, fraud “solutions” like PIN mandates that fail to guard against counterfeiting or protect transactions in the digital marketplace fall far short of what is needed. To stay ahead of highly sophisticated criminals today means investing in the latest 21<sup>st</sup>-century advancements and supporting meaningful federal data legislation that addresses the legitimate problems that foster electronic

<sup>6</sup> Based on data from Peter T. Dunn & Company LLC (2018). <http://capitalpolicyanalytics.com/2018/11/costs-benefits-interchange>

<sup>7</sup> Verisk Financial Research, 2019.

<sup>8</sup> “2016 Credit Card Monitor Report,” Phoenix Marketing International, April 2016.

<sup>9</sup> “Chip Cards in the United States: The PIN, PINless, Debit, Credit Conundrum,” Alite Group, July 2016.

<sup>10</sup> “Visa EMV Chip Cards Help Reduce Counterfeit Fraud by 87 Percent,” Visa, June 2019.

payments fraud. Mandating one technology over another will divert resources away from investing in the critical protections that have recently developed, and it would keep the payments system stuck in the 1960s. A combination of dynamic authentication technologies including EMV, tokenization, and end-to-end encryption delivers results and has proven to be the best way forward.

Financial institutions have repeatedly stepped up and led the adoption of innovative technology, like EMV. EMVCo, the specification-setting body for electronic transactions, works with stakeholders across the electronic payment system to facilitate adoption of secure technologies. In addition to chip cards, EMVCo promotes secure mobile and online transaction practices, creating a worldwide defense against payment fraud. Chip technology has overwhelmingly worked, too, as the 87 percent reduction in counterfeit fraud over the last four years illustrates.<sup>11</sup> Retailers adopted EMV with some reticence, but it has proven successful in greatly reducing point of sale fraud while eliminating liability for those who did adopt.

Retailers frequently fail to acknowledge the benefits they receive from the current electronic payment system. Card payments reduce check-out times, resulting in transactions that are twice as fast as cash and many times faster than paper checks. With electronic payments, retailers also have the option to expand their businesses to online and mobile commerce, likely reaching more consumers.

In addition, customers who pay via card spend nearly twice as much as those who pay with cash. On average, debit card users spend \$44 per transaction, while cash users pay just \$21.<sup>12</sup> Consumers should have a voice in their payment choices, and they have repeatedly shown that they prefer cards. Eighty-six percent of consumers are satisfied with credit cards' ease of use, and 84 percent are satisfied with credit card processing speed.<sup>13</sup>

As hackers get more sophisticated in fraud, it is imperative that lawmakers, retailers, and financial institutions do their part to protect consumers. The electronic payments system requires significant investment and resources to maintain and develop safeguards for consumers and merchants, which financial institutions have repeatedly proven they're willing to make. Merchants benefit from the system greatly and must do their part to maintain it, and they should not be pushing for mandates that will artificially control how people make purchases or how their data is secured.

**Jeffrey Tassey**  
Chairman of the Board  
Electronic Payments Coalition

The Electronic Payments Coalition | 202-627-0544 | [info@electronicpaymentscoalition.org](mailto:info@electronicpaymentscoalition.org)

<sup>11</sup> "Visa EMV Chip Cards Help Reduce Counterfeit Fraud by 87 Percent," Visa, June 2019.

<sup>12</sup> "Cash Continues to Play a Key Role in Consumer Spending; Evidence from the Diary of Consumer Payment Choice," Federal Reserve Bank of San Francisco, April 2014.

<sup>13</sup> "New Data Shows Consumers Want Innovative Options to Stay Protected at the Register," Electronic Payments Coalition, February 2016.



1620 I. Street NW, Suite 1020  
Washington, DC 20036

202.828.2635  
electra.org

January 30, 2020

The Honorable Stephen Lynch  
Chairman  
Task Force on Financial Technology  
Committee on Financial Services  
United States House of Representatives  
Washington, DC 20515

The Honorable Tom Emmer  
Ranking Member  
Task Force on Financial Technology  
Committee on Financial Services  
United States House of Representatives  
Washington, DC 20515

Dear Chairman Lynch, Ranking Member Emmer, and Members of the Task Force:

The Electronic Transactions Association ("ETA") appreciates the opportunity to submit this statement for the Task Force on Financial Technology hearing on "Is Cash Still King? Reviewing the Rise of Mobile Payments."

ETA is the leading trade association for the payments industry, representing over 500 companies that offer electronic transaction processing products and services. ETA's members include financial institutions, mobile payment service providers, mobile wallet providers, and non-bank online lenders that make commercial loans, primarily to small businesses, either directly or in partnership with other lenders. ETA member companies are creating innovative offerings in financial services, revolutionizing the way commerce is conducted with safe, convenient, and rewarding payment solutions and lending alternatives.

#### Hearing

The focus of this hearing – security and financial inclusion – mirrors ETA's 2020 policy priorities to fight fraud and ensure all consumers, including the underserved, have access to safe, convenient, and affordable payment options and other financial services. Consumers continue to benefit from a robust credit card payment system that provides nearly universal payment access and strong consumer fraud protections.

We appreciate the opportunity below to highlight how ETA members are working to innovate and strengthen the payments industry.

#### ETA Priorities for 2020

ETAs three major policy themes during 2020 are:

- **Helping the Underserved:** ETA members, through the introduction of new products and services have expanded, and are continuing to expand, financial opportunities for underserved consumers.
- **Innovation:** ETA supports the development and deployment of products and services that represents the future of financial services.
- **Payments Security:** ETA supports industry's on-going efforts to keep the payments industry secure. Fighting fraud is a top priority for ETA and its members.



1620 L Street NW, Suite 1020  
Washington, DC 20036

202.628.2635  
electra.org

What follows is a discussion of these themes.

#### Helping the Underserved

One of the goals of ETA members is to provide high quality, secure, and affordable financial services for the broadest possible set of consumers. An inclusive financial system is one that provides consumers and businesses with access to a variety of financial products and services. Example of these include; prepaid products; mobile banking services; peer-to-peer payments; online small business lending; and financial literacy programs.

Both of the two other policy themes- innovation and payments security- expand accessibility for consumers and small businesses, lower costs, empower financial management, help the underserved, and drive a more secure payments ecosystem.

ETA annually produces an annual white paper<sup>1</sup> that catalogues the emphasis how the technologies, products, and services that the financial institutions, payments companies, and FinTech companies are implementing help the underserved. ETA's annual white paper explores how ETA members are working diligently to expand consumer access to payment options, credit, and other financial services to all.

#### Innovation

ETA member companies are creating innovative offerings, revolutionizing the way commerce is conducted with safe, responsible, convenient, and rewarding payment solutions and lending alternatives that are available to a broader set of consumers. This transforming marketplace through the integration of current and new technologies expands accessibility for consumers and small businesses, lowers costs, empowers financial management, helps the underserved, and drives a more secure payments ecosystem.

By bringing together traditional players and new participants, ETA members are constantly developing and deploying new products and services while touching, enriching, and improving the lives of underserved consumers while making the global flow of commerce possible. A goal of ETA member companies is to continually enhance the electronic payments and financial ecosystem so that it is accessible for all consumers, while ensuring their transactions can be completed securely, efficiently, and ubiquitously.

#### Payments Security

ETA member companies take seriously their affirmative and continuing obligation to protect the confidentiality and security of their customers' information. Our payments systems are built to detect and prevent fraud -- and to insulate consumers from any liability. As evidence of this fact, the payments industry assigns consumers in the United States zero liability for fraud. The cost of fraud is borne by payments companies. Considering this financial responsibility and a desire to preserve consumer confidence in the security of electronic transactions, ETA members have a strong interest in making sure fraud does not occur. Towards that end, payments technology businesses are bolstered by robust compliance practices -- whether their own in-house policies, or ETA's own carefully crafted industry Guidelines, which establish underwriting practices to help payments companies detect and eliminate fraud.

<sup>1</sup> Electronic Transactions Association (2020). *How FinTech is Addressing the Needs of the Underserved*.



1620 I. Street NW, Suite 1020  
Washington, DC 20036

202.828.2635  
electra.org

Examples:

- EMV: ETA has long championed the adoption of EMV enabled chip cards. EMV is one part of the overall, multi-layered solution to protecting data, consumers, and the payments system.
- Tokenization: Removes sensitive information from a transaction by replacing customer data with a unique identifier that cannot be mathematically reversed. Tokenization is designed to work when a consumer pays with plastic in person, online, or with a mobile phone. If a thief steals the tokenized identifier, it is useless to them.
- Encryption: ETA member companies use of point-to-point encryption. It is advanced risk management tool where card data is encoded from the moment the card is dipped, swiped or tapped, all the way to authorization. This technology minimizes opportunities for hackers and criminals to access data during a purchase.
- Artificial Intelligence: Payment companies use advanced artificial intelligence and machine learning systems that monitor transactions and data patterns to detect unusual activity that may indicate an account has been hacked or a card lost or stolen.
- Mobile Payments: Using a mobile device to initiate a transaction will soon be as common as swiping a card. Mobile devices provide enhanced security, including passcode protection for the phone, biometrics security like a fingerprint, secure chip technology, and geo-locational information to assist with verification.

ETA and its members encourage policymakers to support these efforts through policies that encourage innovation, security and the use of technology to improve financial inclusion for all consumers. ETA advocates that policymakers remain thoughtful and forward-thinking in how to best support the industry's ongoing efforts to provide opportunities for all consumers and small businesses to access and benefit from innovative financial products and services.

ETA would like to thank the Task Force for this opportunity to provide this statement for the record on this important topic and we appreciate your leadership on this important issue. If you have any questions, please feel free to contact me directly at [stalbott@electra.org](mailto:stalbott@electra.org).

Sincerely,

Scott Talbott  
Senior Vice President of Government Affairs  
Electronic Transactions Association

Attachment: ETA's *How FinTech is Addressing the Needs of the Underserved* White Paper





February 5, 2020

Chairman Stephen Lynch  
House Financial Services Committee,  
Fintech Task Force  
2109 Rayburn House Office Building  
Washington, DC 20515

Ranking Member Tom Emmer  
House Financial Services Committee,  
Fintech Task Force  
315 Cannon House Office Building  
Washington, DC 20515

Dear Chairman Lynch and Ranking Member Emmer,

FMI<sup>1</sup> - The Food Industry Association watched the Task Force's hearing, "Is Cash Still King? Reviewing the Rise of Mobile Payments," with great interest and respectfully requests to have this letter entered into the hearing record. FMI has long engaged on payments issues on behalf of our retail members, from the metallic content of coinage and check acceptance policy to the transition from paper food stamps to electronic benefits. With this long history and experience, it is our pleasure to share the grocery industry's insights into the U.S. payments ecosystem and areas where we see a need for improvement.

Every year, FMI publishes the "Food Retailing Industry Speaks"<sup>2</sup> survey. In this survey, FMI gains insights into what is happening in the food retail marketplace, and we are pleased to have the opportunity to share some of these with you. As the title of the hearing questions, "is cash still king?" we would like to share some insights into the use of cash and other tender forms in our members' stores. In our 2019 "Speaks" report, FMI reported that fifteen of every one hundred dollars spent in our members' stores is paid for with cash. Below is a chart with a total tender breakdown.

<sup>1</sup> As the food industry association, FMI works with and on behalf of the entire industry to advance a safer, healthier and more efficient consumer food supply chain. FMI brings together a wide range of members across the value chain — from retailers that sell to consumers, to producers that supply food and other products, as well as the wide-variety of companies providing critical services — to amplify the collective work of the industry. [www.FMI.org](http://www.FMI.org)

<sup>2</sup> Food Marketing Institute, Food Retailing Industry Speaks 2019, (Arlington, VA) 2019





TABLE 27 PAYMENT METHODS AS A PERCENTAGE OF TOTAL SALES

Q21: WHAT WAS YOUR BREAKDOWN OF SALES AMONG THE FOLLOWING PAYMENT METHODS IN 2018?

AVERAGE   WEIGHTED	n	CREDIT	DEBIT	CASH	CHECK	EBT	GIFT CARDS	OTHER
ALL RESPONDENTS	78	35%	38%	15%	3%	5%	1%	4%
COMPANY SIZE								
1-10 STORES	41	42%	32%	15%	4%	5%	1%	1%
11-100	23	39%	35%	13%	4%	4%	1%	3%
>100	16	35%	38%	16%	2%	5%	1%	4%

As the chart demonstrates, grocery customers use a wide variety of tender types, and our members are, as they always have, responding to customer demand. However, as customer choice continues to shift toward electronic payment forms, FMI members find themselves faced with both opportunities to enhance the customer shopping experience but also challenges of accepting different payment forms.

Each payment form comes with its own "rules of the road" that FMI members must abide by. In some areas, retailers have had great success in collaborating with stakeholders to ensure a payments system works for all involved. A great example of that was the Supplemental Nutrition Assistance Program (SNAP) transition from paper to electronic benefits (EBT). As the private partner in SNAP, serving as the main point of redemption of benefits, FMI members had a vested interest in ensuring the EBT systems worked for all parties. FMI and our members participated in a multi-year-long project with all stakeholders to write and implement uniform standards, acceptance policies and security tools. Today, the EBT system operates at a low and transparent cost, and one could argue more securely than many commercial transactions as a customer must authenticate every purchase by entering a personal identification number (PIN), a practice that has been proven to prevent fraud. Importantly, while PIN is used today, FMI and our members are working with USDA to explore new and emerging technologies to verify a customer is indeed authorized to use the EBT card they present for payment.

Additionally, as of this week, FMI members are now piloting online SNAP sales in the states of New York and Washington, with other states coming on board in the coming





months. The SNAP online pilot is another example of collaboration among all stakeholders to find safe ways to better serve all our customers who may face mobility or food access issues.

Unfortunately, there is a lack of open collaboration and transparency on the commercial side of payments, which FMI firmly believes is putting our members at a competitive disadvantage in the global market and making the entire system less secure and efficient. Unlike the government benefits space, commercial payment card security standards are set by a closed body, with only one sector of the ecosystem having the ability to affect outcomes. A recent paper published by the Secure Payments Partnership (SPP)<sup>3</sup> highlights the serious challenges grocery retailers and other payment industry stakeholders are facing with the lack of collaboration and competition making our electronic payments more secure. Today, EMVCo, who acts as the standard setting body, is owned and operated solely by the global card brands, including the four U.S.-based brands (Visa, Mastercard, American Express and Discover) as well as the Japan-based JCB Co. and China-based UnionPay International networks. No U.S. bank, retailer, consumer group, competitive network, core processor, fintech provider or any other stakeholder involved in payments is or can be on their board. FMI and the SPP see this as a glaring challenge and one ripe for reform.

The United States is the global leader in payment card fraud. According to *The Nilson Report*,<sup>4</sup> while the United States accounted for 21.54% of global card volume, we shouldered 33.99% of gross card fraud losses. In dollar figures, the U.S. economy was hit with \$9.47 billion in fraud losses. It is important to note, that figure does not include expenses U.S. merchants, issuers and acquirers bear in operations, chargeback management of fraudulent transactions and external recovery expenses. While all these sectors are shouldering these ever-rising costs, none of them are able to address or affect the underlying problem of our broken security standards-setting system and lack of competition in that space.

<sup>3</sup> Securepaymentspartnership.com

<sup>4</sup> The Nilson Report, November 2019, Issue 1164





FMI took heart from comments from both the majority and the minority during the hearing about a collective interest in inclusion, innovation and security in our electronic payments system. It is time for the United States to be a leader on payments, as it was when the magstripe was first introduced decades ago. Technology offers amazing opportunities never conceived before to help the unbanked and underbanked to participate in the digital economy and continue to shop in traditional brick and mortar stores. FMI members are finding ways to help unbanked and underbanked participate in the economy. Whether it is providing prepaid solutions, supporting cash preferring customers for digital purchases, low-cost cash checking services, or wire transfers, the grocery industry has helped meet the needs of millions of Americans who may lack traditional banking access.

More can and must be done to serve all our customers. True competition in payments would jumpstart innovation and drive secure transactions. FMI submitted comments in favor of the Federal Reserve setting up a real-time gross settlement system (FedNow) here in the United States. We firmly believe competition in this space will ensure access to all users, drive innovation, improve security and redundancy, and help keep costs down. FMI is also a member of the Faster Payments Council (FPC) and shares its goals of an inclusive system that serves all parties. In our most recent comments to the Federal Reserve on the FedNow implementation, FMI suggested that the FPC could be leveraged as a standards-setting body to ensure standards are developed and deployed equitably and in an open, collaborative way.

FMI believes the FPC is a great example of how collaboration can benefit all parties. Unfortunately, as highlighted above, the current security standards-setting body is being used by legacy systems to inhibit competition. The result is less innovation. As an example, FMI members today find themselves having to make the difficult choice of whether to accept technologies such as near field communication "NFC" transactions. NFC is only one technology solution for mobile payments. However, the legacy brands who prefer this solution over others, used EMVCo to push it into market in lieu of any others, such as QR codes. Under the global card brand rules, if a retailer turns on NFC it gives up choice in which mobile wallets they want to accept, potentially increasing their costs of acceptance and even having to share sensitive customer data with multiple





parties. Below is a chart from FMI's 2019 *Speaks* on the adoption of mobile payments by our members. FMI believes that greater competition and removal of barriers is essential as a growing number of retailers respond to consumer demand for mobile payment solutions.

TABLE 25 MOBILE PAYMENTS

Q19: DO YOU ACCEPT MOBILE PAYMENTS?

WEIGHTED	ALL (n=90)	Number of stores operated		
		1-10 (n=48)	11-100 (n=23)	>100 (n=19)
YES	46%	68%	87%	43%
NO, BUT WORKING ON IT	44%	10%	9%	47%
NO	9%	22%	4%	9%

Furthermore, the cost of accepting payments is an ongoing challenge for the food retail industry. FMI has been tracking member profit margins for over forty years. In that time, average profits have never reached 2%. In 2018, FMI members' average profit margin was 1.2 percent. This number is validated by the NYU Stern School of business, which tracks industry profit margins monthly. Its January report showed grocery with an average 1.4% profit margin.<sup>5</sup> While FMI members strive every day to find operational savings, their cost for accepting electronic payments continues to increase. The lack of competition on the payments space has had the opposite effect on the economies of scale model with costs going up rather than down with greater usage. According to *The Nilson Report*, American merchants paid \$107.78 billion in processing fees alone in 2018<sup>6</sup>, and as the chart below from FMI *Speaks* demonstrates smaller food industry operators are the most impacted by these fees.

<sup>5</sup> [http://pages.stern.nyu.edu/~adamodar/New\\_Home\\_Page/datafile/margin.html](http://pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/margin.html)

<sup>6</sup> The Nilson Report, June 2019, Issue 1155





TABLE 28 TOTAL CREDIT AND DEBIT FEES AS A PERCENTAGE OF TOTAL SALES

Q22: WHAT WERE YOUR TOTAL CREDIT AND DEBIT CARD FEES AS A PERCENTAGE OF SALES IN 2018?  
PLEASE INCLUDE PROCESSING COSTS AND OTHER FEES, SUCH AS DUES AND ASSESSMENTS.

AVERAGE   WEIGHTED	n	Total credit and debit fees as % of sales
ALL RESPONDENTS	77	.9%
COMPANY SIZE		
1-10 STORES	41	1.2%
11-100	21	1.2%
>100	15	.9%

As our members are accepting a greater number of “nontraditional” transactions, those outside the brick-and-mortar card-present space, those costs continue to increase. FMI members are responding to consumer demand and offering solutions like online order and delivery or curbside pick-up. With these services, FMI members are facing not only higher acceptance costs, but increased fraud liability. This problem will only be magnified as our members grow their online marketplace. According to FMI *Speaks*, most online sales in 2018 were handled with credit card payments (81%), with far fewer leveraging debit card payments (17%). In the United States, credit cards come with higher network and processing fees than debit cards, again driving up costs to retailers. According to *The Nilson Report*, U.S. merchants paid .66%, on average, for a Visa or Mastercard debit card transaction, whereas a Visa or Mastercard credit card transaction was three times more expensive at 2.26%<sup>7</sup>.

The lack of competition and broken security standards-setting scheme is leaving U.S. retailers and the entire economy at an economic disadvantage globally. In the ever-growing global economy, our foreign competitors are given a leg-up with faster, more secure, and different payment solutions than we have here. Congress can act to ensure that we have an open, transparent and deliberative payment security standards-setting body. By doing this, all stakeholders, new entrants, legacy platforms and emerging technologies can all compete on a level playing field. This would also ensure the American consumer has the safest, fastest and most reliable payment system in the world.

<sup>7</sup> The Nilson Report, June 2019, Issue 1155





Thank you again for your interest and attention to this important issue. FMI looks forward to working with the Task Force to ensure we have the safest, strongest and most inclusive payments system in the world.

Sincerely,

A handwritten signature in cursive script, appearing to read 'Hannah Walker', is positioned above the typed name.

Hannah vL Walker  
Vice President, Political Affairs  
FMI- The Food Industry Association

Cc: Members of the House Financial Services, Fintech Task Force.




**Innovative Payments Association**

777 6th Street, 11th Floor  
Washington, DC 20001  
202.548.7200

January 29, 2020

The Honorable Stephen Lynch  
Chairman  
Task Force on Financial Technology  
House Committee on Financial Services  
2109 Rayburn House Office Building  
Washington, DC 20515

The Honorable Tom Emmer  
Ranking Member  
Task Force on Financial Technology  
House Committee on Financial Services  
315 Cannon House Office Building  
Washington, DC 20515

Dear Chairman Lynch and Ranking Member Emmer:

This letter is being submitted by the Innovative Payments Association (“IPA”).<sup>[1]</sup> to the House Task Force on Financial Technology’s (the “Task Force”) in relation to its January 30, 2020, hearing entitled, *“Is Cash Still King? Reviewing the Rise of Mobile Payments.”* The IPA appreciates the opportunity to share its comments with the Task Force regarding the state of the prepaid payments industry in an effort to address concerns that may have been raised by the Task Force’s hearing memo.<sup>[2]</sup>

In our ever-changing and increasingly paperless world, consumers are looking for alternatives to traditional banking. Prepaid accounts are providing a broad array of American consumers with revolutionary ways to access, spend, and control their money. In many respects, prepaid accounts function like traditional bank accounts by providing the speed and accessibility to keep up with the pace and technology of our everyday lives in a way checks and cash do not. As a result, the prepaid card industry has experienced explosive growth in recent years as more and more consumers turn to prepaid accounts to manage their day-to-day financial needs.

Prepaid accounts are easy to use, provide quick access to funds, and offer convenient money management features. These attributes are why prepaid accounts are used by Americans from all walks of life, governments at all levels, and businesses of all sizes. I believe the Financial Health Network (formerly CFSI) said it best in their 2016 Prepaid Industry Scorecard, “[p]repaid cards

<sup>[1]</sup> This statement is submitted on behalf of the Innovative Payments Association (“IPA”). The IPA is a trade organization that serves as the leading voice of the electronic payments sector, including prepaid products, mobile wallets, and person-to-person (“P2P”) technology for consumers, businesses and governments at all levels. The IPA’s goal is to encourage efficient use of electronic payments, cultivate financial inclusion through educating and empowering consumers, represent the industry before legislative and regulatory bodies, and provide thought leadership.

<sup>[2]</sup> House Task Force on Financial Technology Committee Memoranda:  
<https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=406024>




**Innovative Payments Association**

777 6th Street, 11th Floor

Washington, DC 20001

202.548.7200

*are generally high-quality products that allow consumers to build financial health by helping them spend wisely, save, and plan for the future.”*

The IPA looks forward to continuing to work with the Task Force to create a thriving marketplace that properly balances protections for consumers with the benefits they receive from financial services providers offering diverse and innovative products to all Americans.

# **I. Prepaid Account Final Rule Extends Multiple Regulations to Prepaid Accounts**

On April 1, 2019, the Consumer Financial Protection Bureau’s (“CFPB”) Final Rule for Prepaid Accounts<sup>3</sup> under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z) (the “Final Rule”), went into effect. The Final Rule was the culmination of a seven-year rule making process that was initiated by then-CFPB Director Richard Cordray. The Final Rule was amended twice before Cordray stepped down in 2017. However, the Final Rule went into effect and is being enforced by the current leadership at the CFPB.

In brief, the Final Rule extends Regulation E coverage to several prepaid account products, which according to the CFPB’s definition, includes General Purpose Reloadable products, mobile wallets, and person-to-person payments (“P2P”). As a result, prepaid account products as defined by the Final Rule must comply with a number of regulatory obligations including the provision of account opening disclosures, offering limited liability and error resolution protection, and providing periodic statements or transaction histories to accountholders.

Accordingly, the Prepaid Rule requires an issuer to provide a consumer with three disclosures (the short form fee disclosure, the long form fee disclosure, and Terms and Conditions) prior to the acquisition of a prepaid account. Thus, a consumer obtaining a prepaid account receives agency mandated disclosures that describe in great detail the terms and conditions of use and the fees associated with using the product.

Next, the Final Rule contains strong limits regarding overdraft and credit features offered in connection with prepaid accounts. In brief, the Final Rule amends Regulation-E and Regulation-Z to regulate overdraft credit features offered in connection with prepaid accounts. As part of these amendments, the rule imposes, among other protections, a 30-day waiting period after a prepaid account is registered before a provider can solicit a consumer to add an additional credit feature. In addition, the Final Rule requires providers seeking to offer a covered separate credit feature to conduct an ability-to-repay analysis in evaluating an application for an additional credit feature, and comply with Regulation-Z requirements for account-opening disclosures, change in terms notices, error resolution, and periodic statements. The cumulative effect of these changes has resulted in the vast majority of providers covered by the Final Rule not offering overdraft

<sup>3</sup> CFPB Prepaid Accounts Final Rule (last amended Jan. 25, 2018), codified at 12 CFR §§ 1005.2 et seq.


**Innovative Payments Association**

777 6th Street, 11th Floor

Washington, DC 20001

202.548.7200

protection. Lastly, it is important to note that Prepaid Accounts are the only products in the marketplace with these restrictions even though Prepaid Accounts make up less than 1% of the consumer complaints the CFPB has received since it began collecting such data in 2011 (see *Consumer Response Annual Report, January 1 – December 31, 2018*).

The IPA (formerly the NBPCA) has engaged the CFPB in good faith throughout the agency's seven-year rule making process with the goal of urging the CFPB to finalize a regulation that protects consumers and simultaneously encourages innovation. Moreover, the association did not encourage efforts to utilize the Congressional Review Act to overturn the Final Rule. It is important to note, however, that the innovative prepaid payments community was providing consumer protections such as limited liability and account opening disclosures, as well as Federal Deposit Insurance Corporation (FDIC) insurance, years before the CFPB's rules were proposed, let alone finalized. For instance, payroll cards have been covered by Regulation-E since July 1, 2007.<sup>4</sup> Now that the CFPB's regulations have gone into effect, let's be clear - prepaid accounts are now full-fledged bank accounts with a full complement of consumer protections that mirror those of, and in some cases exceed, traditional checking accounts.

## **II. Who Benefits from Prepaid Accounts?**

The short answer is that practically everyone – individual Americans, tech innovators, businesses, and state, federal and local governments – save time and money through the use of prepaid cards.

### *Americans of All Kinds Make Use of Prepaid Accounts*

Americans who use prepaid cards are not defined by a single demographic or socioeconomic status. Nonetheless, in many ways the greatest benefits are for low- and moderate-income people who use prepaid cards when they cannot get a bank account, so prepaid accounts in its forms and variations are an efficient means to access the financial services system.

According to the most recent FDIC data on the topic, over twenty-five percent of U.S. households—totaling 32.6 million—were unbanked or underbanked as of 2017. With a quarter of American households requiring financial products and services outside the traditional banking system, prepaid accounts help service a significant portion of this demand.

According to the FDIC's 2017 report on Unbanked and Underbanked Households, about 9% of all U.S. households had a prepaid card in 2017 (the 2019 survey is not yet available). More specifically, the FDIC's report details that:

*"In this report and since the survey was first conducted in 2009, a household is categorized as unbanked if no one in the household has a checking or savings account. General purpose*

<sup>4</sup> <https://www.federalreserve.gov/newsevents/pressreleases/bcreg20060824a.htm>


**Innovative Payments Association**

777 6th Street, 11th Floor  
 Washington, DC 20001  
 202.548.7200

*reloadable prepaid cards that were obtained from banks may offer many of the same features as checking accounts as well as a relationship with a retail banking institution. As a result, unbanked households that use prepaid cards obtained from banks could be considered banked. If they were, the unbanked rate in 2017 would fall slightly from 6.5 percent to 6.4 percent."*

Prepaid accounts allow consumers to access the financial services system and avoid check-cashing fees and by paying bills online or over the phone instead of through money orders. They also save time by avoiding lines for check cashers or at bill-pay locations. Most importantly, however, the modern consumer requires access to ever-expanding digital economy. Prepaid accounts allow more consumers to shop online and access digital features such as real-time alerts and other budgeting tools.

The benefits of prepaid accounts are not, however, limited to unbanked and underbanked Americans. According to the same [FDIC data](#), individuals and families with traditional bank accounts take advantage of the benefits of prepaid accounts as well. These include help with budgeting, providing funds to family members, travel benefits, and gifting, to name a few.

Utilization of prepaid cards is especially strong with millennials, in particular. According to a 2015 study by the Federal Reserve Bank of Philadelphia entitled, "[Millennials with Money Revisited: Updates from the 2014, Consumer Payments Monitor](#)," 41% of millennials who earn less than \$50,000 annually; 49% of millennials who earn between \$50,000 and \$99,999; and 60% of millennials who earn more than \$100,000 annually reported owning a prepaid card. Additionally, 45% of millennials reported owning both a bank account and a prepaid card.

The same study also lays out that millennials have adopted prepaid cards and other non-bank providers for access to more services, access to cash, and convenience. When banked millennials who also owned a prepaid card and earned \$50,000 or more were asked why they utilized prepaid cards and other non-bank financial products and services; 34% cited banks not offering all the services they need, 30% cited banks not solving their immediate need for cash, and 29% cited a bank not being near their home.

In their May 23, 2018, "[Prepaid Card Buying Guide](#)," Consumer Reports notes a variety of reasons that Americans might want to use prepaid cards.

- If you don't want to open a checking account, perhaps because of minimum-balance requirements or fees, a prepaid card can be used as an alternative.
- It can also help you stay within budget. You could have one card, for example, just for buying gas, another to keep your coffee spending in check, and a third, perhaps, for holiday shopping.
- And there are other smart uses for prepaid cards, including teaching teens and younger children how to manage money, and protecting seniors from scams. It can also be a better way to give money, instead of a gift card, because of its wider acceptance and better loss-liability protections.


**Innovative Payments Association**

777 6th Street, 11th Floor

Washington, DC 20001

202.548.7200

In addition to all of these uses, recipients of government benefits like Social Security will opt to receive payments through prepaid cards. In a survey of Direct Express recipients conducted in 2012, 97% of recipients said that the Direct Express prepaid card was a safer way to receive their payments than paper checks. At the same time, 85% of recipients said that the card made it easier to manage money, and 91% said the prepaid card made it easier to pay bills.

Overall, 95% of Direct Express card users said they were satisfied and 93% said they would recommend the card to others.<sup>5</sup>

This data hints at the benefits of prepaid cards for government agencies, which we will cover in more detail in the next section.

***Government Agencies at all Levels Benefit from Using Prepaid Accounts***

Today, federal law mandates that all federal benefits shall be delivered electronically. As a form of electronic payment, government benefit cards have increased in popularity and use over the past several years as state and federal governments move consumers away from paper checks in order to reduce fraud, save money, and improve the overall customer experience in receiving benefits. The Federal Reserve regularly reports to Congress on the use of prepaid accounts for distributing government benefits. The first sentence in their September 2019 report ([Report to the Congress on Government-Administered, General-Use Prepaid Cards - September 2019](#)) explains why governments do this:

*Federal, state, and local government offices use prepaid cards to disburse funds at a lower cost than checks (or other paper-based payment instruments such as vouchers or coupons) and to provide an alternative to direct deposit for payment recipients, especially those recipients who do not have bank.*

In 2011, then U.S. Treasury Secretary Rosie Rios estimated the cost of issuing paper checks to be 92 cents higher than the cost of direct deposits. Further, the U.S. Treasury Department estimated federal beneficiaries to be 125 times more likely to have difficulties with paper checks versus electronic payments and an added taxpayer price tag of \$120 million for paper checks that would only increase as more baby boomers retire. The federal government disbursed \$137 billion in benefits, including Social Security, veterans' benefits, and child support, using prepaid cards in 2018.

They are not alone. Every state in the Union uses prepaid cards to distribute benefits such as Supplemental Nutrition Assistance Program (SNAP), Temporary Assistance to Needy Family

<sup>5</sup> "U.S. Treasury's Direct Express® Prepaid Debit Card Earns High Marks from Social Security Population," U.S. Department of Treasury, July 17, 2012.


**Innovative Payments Association**

777 6th Street, 11th Floor

Washington, DC 20001

202.548.7200

(TANF) benefits, and unemployment insurance to their citizens. In doing so, they save taxpayer dollars, administrative time, and bureaucratic troubles over paper check payments.

***Businesses of All Sizes Benefit from Using Prepaid Accounts***

In the same way that individuals and governments save time and money by using prepaid cards, so can businesses of all sizes. NACHA estimates substantial cost savings for businesses who use direct deposits “from as much as \$19,000 per year for a small business to over \$5.7 million for a business with 30,000 employees.”

When employees do not have bank accounts for the reasons noted above, prepaid accounts give businesses the option of using direct deposit regardless of the banking status of their employees.

In addition to distributing payroll, businesses can use prepaid accounts to manage money by providing funds to employees for business purposes. For example, a contractor who needs to give money to employees might use a prepaid card rather than just handing over a credit card or cash. Companies like home improvement chain Lowe’s have created their own in-house prepaid programs to meet this need, but a company might also choose an open-loop prepaid card so that employees could buy supplies and lunch for a work crew.

However, perhaps the most exciting way that businesses have used prepaid accounts is to serve as the foundation for entirely new classes of products and services, which we will explain in the next section.

**III. Prepaid Accounts Are the Foundation for Financial Innovation**

Practically every payment innovation of the last decade has borrowed from or been built on top of a prepaid platform. Take for example, fintech debit accounts that reside in mobile wallets. Fintech debit accounts such as the ones provided by Revolut, N26, Simple, Chime, or Varo are almost identical to a prepaid account. The only difference between the products lies in the account structure in that fintech debit accounts adopt a structure where their users have DDA accounts in an issuing bank and prepaid programs store funds in a pooled account. To the end user there is no difference. Each account pays the merchant on demand and both are FDIC insured.

The lines between prepaid accounts, traditional banking and fintech are so blurred that many industry experts are unable to identify where prepaid ends and traditional banking and fintech begins. According to Mercator Advisory Group’s 2018 report on the “*Blurred Lines Between Debit and Prepaid Cards*,” “*Debit cards issued by financial institutions and general purpose reloadable (GPR) prepaid cards have evolved over the last two decades to be nearly indistinguishable not only in appearance but also in features and functionality.*”


**Innovative Payments Association**

777 6th Street, 11th Floor

Washington, DC 20001

202.548.7200

In a 2018 brief entitled, the “CFPB Final Prepaid Rule,” Mercator states due to product evolution the CFPB clearly intended to regulate all transaction accounts (regardless of access device) uniformly. *“Upon reviewing the approximately 2,890 pages of amended prepaid regulations, which include detailed discussions from industry commenters, it becomes apparent the CFPB is trying to extend uniform consumer protections to the many payment card types now available. The goal seems to be coverage for unauthorized or disputed transactions for all financial access devices regardless of their ownership (financial institution or not), account type (credit, debit, or prepaid), or form (card, digital wallet, funds transfer app, wearable, etc.).”*

***The Heart of Today’s Payments Technology***

The true rise of prepaid platforms began in the late 1990s with the emergence of GPR cards and payroll cards used by unbanked and underbanked Americans. Shortly thereafter, open-loop prepaid gift cards emerged in the early 2000s and were quickly adopted by major card associations, such as Visa, Mastercard, American Express, and Discover. Underpinning most of today’s existing and emerging payments technology, prepaid account infrastructure allows companies to bring new products to market, including mobile wallets, payment-to-payment (P2P) services, and other consumer fund-holding products.

Over the past decade, prepaid became the “new normal” in the modern economy, changing the ways companies competed and driving new and existing firms to further disrupt the marketplace on the back of this traditional infrastructure. The result is that the reduction of fees associated with prepaid accounts has attracted millennials, smartphone users, and has driven the Silicon Valley technology revolution.

Mobile wallets (Apple Pay, Google Pay, Samsung Pay), popular P2P services (Venmo), and other fintech debit providers, began utilizing the prepaid platform to bring “new” products to market due to the efficiencies and cost to develop and maintain. Even companies that consumers might believe to be completely outside of the payments industry began outlining how to leverage their technology using the increasingly widespread prepaid infrastructure (i.e. Uber Money).

As such, we arrive at the modern day. Every company is a technology company, and therefore has the potential to be a payments company too. Consumers demand these capabilities from firms operating in a connected and convenient world. Without prepaid accounts, though, none of it would be possible. Traditional prepaid products might be on the decline, but traditional prepaid infrastructure is here to stay.

***The Modern American Wallet***

As technology has developed, so has the evolution of payments. Originally, consumers turned to traditional plastic prepaid cards, but now, Silicon Valley companies and others have taken this technology and created market disrupters such as mobile wallets, Google Pay and Apple Pay,


**Innovative Payments Association**

777 6th Street, 11th Floor

Washington, DC 20001

202.548.7200

which are now the new normal. The critical elements of privacy, safety and convenience, however, have remained steady over time.

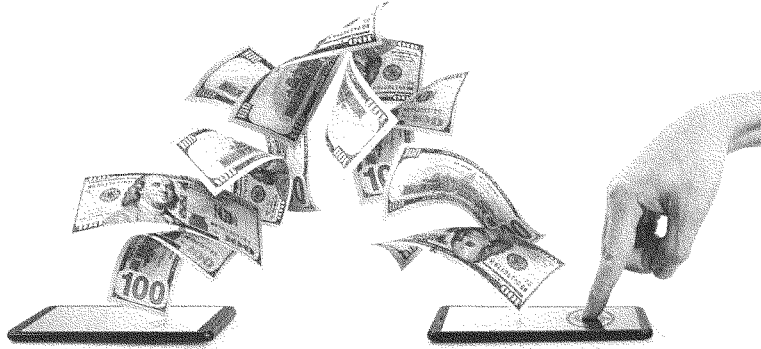
It is clear that the future of the American wallet will continue to rely on prepaid structures. In fact, almost every payments innovation over the past decade has borrowed from or been built on top of a prepaid platform. In today's world, finance and technology are nearly synonymous, and the emergence of "fintech" as its own industry is proof. Most emerging business models in the space are not new. Instead, the modern consumer is technologically savvy and values convenience above all else. As a result, fintechs offer products that meet these needs through mobile wallets and P2P services by leveraging existing prepaid technology.

So, what exactly is in your wallet? Does "wallet" even mean what it did just a decade ago? The modern consumer might not even have a wallet, in the traditional sense. It could be on their phone. This leads to many questions such as, how do you pay for products and services? You could Venmo someone or use Apple Pay at the grocery store. And why does all this matter? It matters because both consumers and regulators must understand why these services are available and what they depend on to operate: Prepaid Accounts.

In closing, the IPA supports a competitive marketplace where market participants play by easily understood and transparent regulations. The IPA's goals include supporting a more streamlined, collaborative, and efficient industry, where traditional payments companies and fintechs leverage each other's respective capabilities toward a common interest – helping consumers. If these goals are shared and this vision is accepted, the future is bright for the payments industry and all consumers.

Respectfully submitted,

Brian C. Tate  
 President & CEO  
 Innovative Payments Association  
[btate@ipa.org](mailto:btate@ipa.org)



---

This Report is being licensed by Franklin Square Group on behalf of  
Financial Innovation Now

## GROWING P2P ADOPTION

NOVEMBER 2019

Javelin Advisory Services  
*Retail Banking*  
javelinstrategy.com | 925.225.9100

**JAVELIN**



## TABLE OF CONTENTS

Executive Summary.....	4
Recommendations .....	5
P2P Payments Are Driven by Technology Companies.....	6
Most Consumers Use More Than One P2P App.....	8
Use Cases for P2P Are Expanding .....	9
Adding Features Will Increase Usage of Consumers Under 40 .....	11
65% of Consumers Over 45 Still Need to Be Convinced.....	12
Rewards Can Modify Behavior of Consumers Over 45 .....	14
Experiences That Wow Will Increase Adoption .....	15
Appendix A — Consumer Behavior Metric.....	17
Appendix B — Figures and Statistics .....	18
Methodology .....	20
Companies Mentioned.....	20

## TABLE OF FIGURES

Figure 1. P2P Services that Customers Used in past 12 months.....	6
Figure 2. Heat map: Reasons for Making P2P Payments, by Age .....	9
Figure 3. Factors That Would Motivate Non-Users to Adopt P2P .....	11
Figure 4. Annual Branch Banking Activity .....	13
Figure 5. Annual Rewards Programs Used by Consumers Over 45.....	14
Figure 6. Consumer responses to the question "Which of the Following Describes Your Actions When a New Technology Becomes Available".....	17
Figure 7. Methods of Funding P2P Transfers.....	18
Figure 8. Reasons for Making a P2P Payment .....	18
Figure 9. P2P Adoption by Age and Type, Past 12 Months .....	19
Figure 10. P2P Adoption by Type, Past 30 Days .....	19

<b>ABOUT JAVELIN:</b>	Javelin Strategy & Research, a Greenwich Associates LLC company, provides strategic insights into customer transactions, increasing sustainable profits for financial institutions, government, payments companies, merchants and technology providers.
<b>AUDIENCE:</b>	Issuers, card networks, merchants, POS providers, mobile wallet providers, card manufacturers
<b>AUTHOR:</b>	Krista Tedder, Director, Payments
<b>CONTRIBUTORS:</b>	Rachel Huber, Senior Analyst, Payments Ian Benton, Senior Analyst, Small Business Banking & Payments Kyle Marchini, Senior Analyst, Fraud Management Tyler Brown, Analyst, Digital Banking Crystal Mendoza, Production Manager
<b>EDITOR:</b>	Mark Stevenson
<b>PUBLICATION DATE:</b>	November 2019

## OVERVIEW

P2P growth in the U.S. market is on an upward trajectory with fintech providers leading the way. Apple, Google, PayPal, and others provide consumers a vital service as many financial institutions struggle to provide the needed financial services to their customers. Banking, specifically checking accounts, play a significant role in the success of P2P, and the convergence of banking and technology will come to a head in 2020 as Google launches a checking account in partnership with Citibank and Stanford Federal Credit Union.

Financial institutions are investing in P2P payments through Zelle; however, the technology being launched is currently not to consumer expectations. It is not too late for financial institutions to improve their own P2P experience, but without significant improvements, consumers may move their deposits to financial institutions that can meet the standards set by technology firms.

Delivering features that meet consumer expectations does not mean that all consumers will want to use P2P as it is defined today. A large group of consumers, primarily people over the age of 45, are not currently planning on using P2P activities based on their existing payment habits. However, there are multiple ways P2P applications can improve money management in addition to money movement, ways that will change the consumer mindset and increase use of the services.

## PRIMARY QUESTIONS

- What is the P2P market size for 2020, and what will impact future forecasts?
- Who uses P2P services and why? What use cases will grow?
- What do providers need to do to increase adoption by consumers who do not currently see the value of P2P?

## EXECUTIVE SUMMARY

**The financial services sector cannot conduct P2P on its own and must rely heavily on technology companies.** Technology companies were the first to recognize a need for person-to-person payments (Western Union, PayPal, etc.). However, banks and credit unions have not been able to unite under an interoperable scheme, leading to additional technology companies to enter the market. Although Zelle is now in market for financial institutions, this caused the market to be further fragmented.

**Google's partnership with Citibank and Stanford Federal Credit Union speaks to the need for partnership and the separate roles technology companies and financial services providers play in making P2P happen.** Google's entry as a technology provider for DDA accounts has implications for how P2P is leveraged in Google Pay. With a focus on consumer experience and analytics, Google can make attainable key features consumers want. Other financial institutions should look to partner with Google as its project known as Cache is rolled out. The API integrations with Google will enable seamless P2P integration while leveraging existing funds movement capability using debit payment rails.

**Facebook's re-entry into P2P expands from Facebook, Messenger, Instagram, and WhatsApp, which will enable additional commerce between marketplaces and platforms.** Consumers ages 25-34 are most likely to use P2P payments in online marketplaces (23%) while P2P activity at merchants is most popular (26%) with consumers 35-44.

**Bill pay has the highest usage factor for all age groups; however, it is an area where consumers would also like to have enhancements.** Paying an individual for a business, paying rent, and paying

individuals for bills are the key areas where advancements can be made in adoption. Making billers easier to find, available via direct biller site or app, and pulling in email notifications and e-invoices for easy payment are ways that bill payment can be simplified.

**The top use case for people over 45 years old is gift-giving — this indicates a need to build better value propositions for a large population of consumers.** Older consumers are more hesitant for access to the savings and/or checking account to be granted. Creating ways to leverage credit cards or stored value accounts would increase the likelihood of consumer adoption.

**Technology strategies need to be multichannel — app- and browser-based access — because consumers toggle between the two access points.** Consumers move between different device types and expect to have availability to the P2P payment method regardless of their interaction point.

**Usage of P2P applications by consumers under the age of 45 will improve with the addition of new security features and transparency.** Biometrics, data privacy standards, consumer alerts, and consumer controls each play a role in how consumers perceive the security of the product.

**Table stakes of P2P applications are currently not supported through banking P2P apps.** Ease of locating receiver and contacts, rewards and incentives, or multipurpose transaction-oriented applications (P2P, merchant payments, and bill payment) must be provided. Technology companies continue to add features as financial institutions remain in the implementation queue to deploy Zelle.

## RECOMMENDATIONS

**Build experiences that “wow.”** Different demographics have different ideas about the definition of an exceptional experience. For the market to reduce to several viable options, apps need to be able to pull in different consumers. Enabling end user configuration to meet individual needs will appeal to more people.

**Focus on money management in addition to money movement — consumers need to better understand their finances within the P2P application.** Enabling ways of saving and investing will provide greater flexibility and start to build on features readily found in neobanks. Enable cryptocurrency investment and management to provide consumers choice.

**Improve how consumers pay bills — consumers and merchants are seeking choices to streamline paying.** P2P applications should facilitate the monthly recurring payment capabilities that many are missing from direct biller capabilities. Financial institutions need to improve online and mobile bill payment options to prevent reduction in consumer engagement.

**Look beyond how funds move, and focus on how P2P activity is funded.** Provide funding mechanisms for consumers who prefer to use credit for daily purchases — either stored value or secondary checking which keeps funds separate from daily spend through the usage of real-time virtual card provisioning in the P2P app.

**Modify consumer payment habits leveraging techniques that work. Rewards and incentives have worked to ingrain credit card spending and merchant selection. Use rewards to drive P2P volumes.** Enable points to be used in P2P apps at any merchant, and provide automatic discounts based on where the consumer is located to provide real-time rewards.

**Provide P2P capability for instances when the consumer needs cash but does not know the receiver.** Integrating into hotel and restaurant applications to enable tipping via QR code would provide consumers the ability to express gratitude and enable workers to receive tips directly into a virtual account.

**Provide trust algorithms for consumers when using P2P applications for marketplace commerce.** With P2P focused on irrevocable funds, when scams occur, the consumer is harmed, and financial institutions cannot recoup the funds. Providing trust indicators and insights on the receiver prior to sending would reduce the likelihood that someone falls victim to fraud.

## P2P PAYMENTS ARE DRIVEN BY TECHNOLOGY COMPANIES

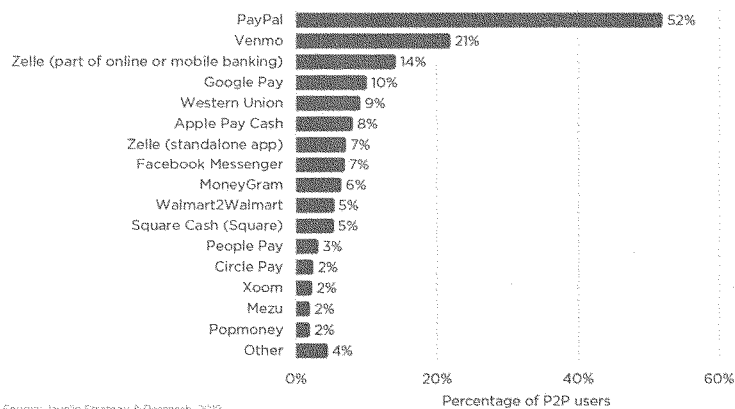
Banks are secondary to P2P payments and are considered laggards in the payment landscape. Person-to-person payments have been an established need since the late 1980s. First using a payment method launched by Western Union, then moving into the fintech world of PayPal in 1998, consumers are comfortable with using non-financial institutions to meet the needs that the financial institution industry was ignoring. Now, with Zelle becoming more widely accepted in the financial institution space, it can be easy to misinterpret the rise of Zelle as being the beginning of P2P. The truth, however, is that banks and credit unions have been laggards in meeting consumer needs.

In terms of market sizing, being a laggard means that Zelle and bank P2P payments have a lot of room for growth, but financial institutions have a long road before they can be seen as the dominant player in the field. Unless interoperability occurs, banks may be best served by supporting their customers in using multiple fintech solutions and becoming top of wallet. The fact that Zelle requires bank integration and a stand-alone app to have similar volume to Venmo demonstrates the growth challenges of adding new financial institutions.

The announcement Nov. 13, 2019, of Google's<sup>1</sup> first financial services partners in Cache, Citibank and Stanford Federal Credit Union, should also serve as

### Money Doesn't Move Without Technology Companies

Figure 1. P2P Services that Customers Used in past 12 months



Source: Javelin Strategy & Research, 2019

© 2019 GA Javelin LLC, a Greenwich Associates LLC company. All rights reserved. This report is licensed for use by Financial Innovation Now. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the permission of GA Javelin LLC. Licensors may display or print the content for their internal use only, and may not sell, publish, distribute, re-transmit or otherwise provide access to the content of this report without permission.

the canary in the coal mine for financial institutions. If they do not support digital payments, they lose deposit market share, and consumers will more likely leave or keep smaller deposits at their institution. The ability to integrate Google Pay and checking accounts can streamline P2P payments for consumers and businesses. Consumers use checking and debit to fund P2P activity 70% of the time — having a checking account available to consumers should increase the existing 10% usage of Google Pay to rival Venmo within the next several years (refer to Appendix B — Figures and Statistics).

The Google Pay integration has the potential to begin a rivalry with PayPal. Over a decade ago PayPal began integrating into financial institutions to increase the security of linking DDAs to the online payment platform — this provided a market advantage that other platforms have not benefited from. The leveraging of open banking API infrastructure will help in building P2P, bill payment, and merchant digital payments using existing payment rails. The usage of ACH and debit revenue and cost models could be more attractive to financial institutions instead of creating new lines of business. The integration will also enable consumers who only want to use their financial institution for payment initiation will have an option available to them through an online or mobile banking experience.

The challenge fintech platforms will continue to have is how to attract new users who are willing to open new accounts and download new apps if they do not offer integration to financial institutions.

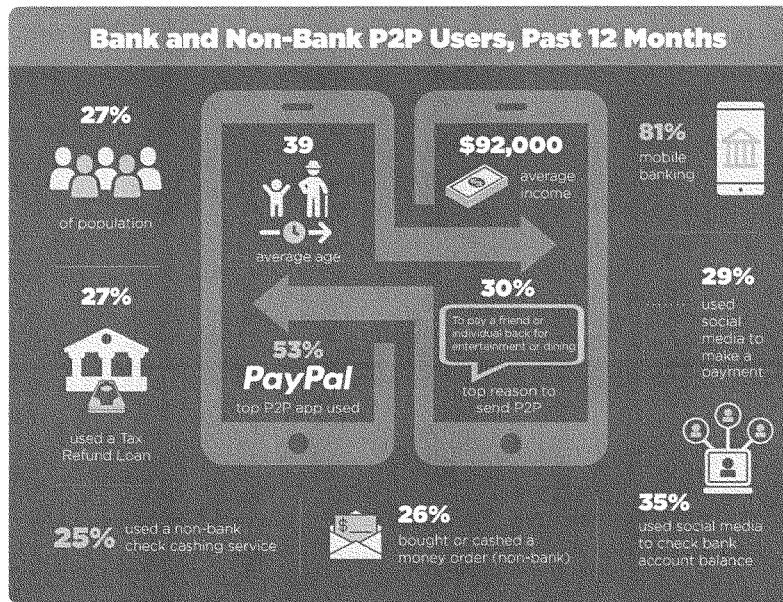
Some companies may collapse into each other with social media giants still looking for a viable way to perform cross-border P2P activity now that it appears Libra has been slowed or ultimately derailed by regulators. If cross-border P2P and social media can merge into a seamless experience, the market size of P2P should steadily increase. The launch of the new Facebook Pay, which will also be implemented into WhatsApp and Instagram, would make a formidable competitor in the global P2P market.<sup>2</sup> The market share for Facebook P2P should increase with the new interface and cross-platform integration.

The fragmented market means that consumers are using more than one app and completing transactions in apps and through browsers. For consumer loyalty to take hold to reduce the number of apps used, P2P platforms would need to be interoperable as outlined in the Javelin report *Prioritizing Real-Time Payments: Making Progress to Advance Modernization*. Today, senders and receivers need to be on the same platform to complete a transaction. It is still yet to be determined if the Federal Reserve's proposed FedNow Service would enable interoperability using a national gross settlement system. It is yet to be determined if The Clearing House will enable PayPal (through the sponsorship by Chase) to have interoperability with Zelle when Early Warning is fully integrated to real-time payments. Enabling users to send from one platform and receive on another would simplify the transaction process and enable consumers to use the payment experience that meets their needs.

## MOST CONSUMERS USE MORE THAN ONE P2P APP

Do most customers want to use two apps? Maybe, maybe not. What we do know is that 61% of P2P users are using a bank and a fintech P2P app. And within this population of heavy P2P users 40% are considered financially unstable – those who live paycheck to paycheck, have debt they cannot repay, or if they lost their job would not be able to

pay their bills. Similar to the 2018 Javelin report, Zelle vs Venmo: Financial Institutions and Third Party P2P Providers, consumers who use two P2P apps also use non-financial services products. Consumers might not prefer the fractured approach but will continue to use multiple applications due to the lack of interoperability and market coverage.



Source: Javelin Strategy & Research, 2019

© 2019 GA Javelin LLC, a Greenwich Associates LLC company. All rights reserved. This report is licensed for use by Financial Innovation Now. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the permission of GA Javelin LLC. Licensors may display or print the content for their internal use only, and may not sell, publish, distribute, re-transmit or otherwise provide access to the content of this report without permission.

## USE CASES FOR P2P ARE EXPANDING



Younger demographics have found more ways to use the P2P platforms in their daily lives, which increases confidence in the solution. The extended use cases, however, have created challenges of managing risks and reducing the vulnerability of consumers to scams. To further extend the use cases for P2P, a deeper look into consumer protections, including dispute rights and fraud liabilities, should be considered. Usage of P2P apps for merchant services does not offer the consumer

the same protections as using a debit or credit card, which inhibits consumers who are resistant to P2P platforms from using the P2P products. Consumers have demonstrated a propensity for paying monthly bills directly on the merchant or provider website. A Javelin report in 1Q 2020 will provide greater details into how consumers pay their bills. That being said, the recent integration of PayPal/Venmo by Paymentus, a direct biller provider, creates an interesting scenario that could

### Consumers Use P2P Differently Based on Age

Figure 2. Heat Map: Reasons for Making P2P Payments, by Age

	18-24	25-34	35-44	45-54	55-64	65+
Pay an individual back for entertainment/dining	47%	31%	30%	24%	21%	19%
Pay an individual for business	13%	22%	20%	13%	6%	9%
Gift	21%	23%	24%	31%	31%	30%
Pay an individual for rent	18%	19%	11%	16%	5%	4%
Pay an individual for bills	25%	24%	16%	24%	16%	10%
Pay a business	11%	16%	10%	8%	13%	9%
Purchase from a merchant	19%	22%	26%	20%	13%	17%
Purchase from an online marketplace (e.g. eBay, Craigslist)	17%	23%	19%	19%	15%	16%
Other	3%	2%	2%	6%	11%	10%

Source: Javelin Strategy & Research, 2019

© 2019 GA Javelin LLC, a Greenwich Associates LLC company. All rights reserved. This report is licensed for use by Financial Innovation Now. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the permission of GA Javelin LLC. Licensors may display or print the content for their internal use only, and may not sell, publish, distribute, re-transmit or otherwise provide access to the content of this report without permission.



increase the usage of the P2P platforms for bill payment services. The recent announcement that Amazon Pay will enable voice-based bill payment could create a new wave of P2P innovation by the different platforms to compete with voice-based commerce and payments. Being able to say to your mobile device “Send Jack from Facebook \$80 to pay for my share of Mom’s gift” might be closer to reality than financial institutions are prepared for.

Google’s foray into the checking account business extends what many bankers have been concerned about — that a technology company could potentially do banking better than they can. With millions of email accounts and the analytics to know what bills receive email notification, requests for splitting gifts, or receiving e-gift cards, Google will be able to prepopulate Google Pay to streamline funds movement. It is too early to tell how the checking account integration will look, however consumers seeking easier ways should see a value proposition for every age demographic.

## ADDING FEATURES WILL INCREASE USAGE OF CONSUMERS UNDER 40

In many cases consumers do not adopt technology that they do not understand or do not believe is safe. Explaining to a consumer that tokenized digital payment methods are more secure than swiping a card has not resonated with consumers. As an industry, we need to do better to increase the understanding and acceptance that tokenized payment platforms are secure. What is clear, however, is that consumers want transparency and visibility into P2P platforms before they adopt the payment method.

Security can mean different things to different people, and consumers can't explain what makes them secure, but they know it when they experience it. For some, it is the accessibility with biometrics — being able to log in seamlessly using the FIDO UAF protocol (PayPal and Bank of America currently leverage the protocol) or FIDO U2F protocol (Google, Facebook, Twitter, and

Dropbox currently leverage the protocol) to create frictionless dual authentication capabilities.<sup>3</sup> For other consumers, security may be requiring one-time passwords (please, no out-of-wallet questions), consumer alerts, and controls (refer to Javelin's January 2019 report *Payment Card Controls: Overcoming Impediments Through a Consumer Financial Enablement Strategy*), and improved transaction ledgers (refer to Javelin's August 2019 report *Why It's Time to Fix the Four Flaws of Transaction Ledgers*).

In addition to security, general usability features could help improve utilization and the financial welfare of the users. Creating gamification aspects of using the P2P payment method to earn rewards, seamlessly redeem merchant-funded discounts, and invest funds can each play a part in building adoption by 18-44-year-old consumers.

### New Features Increase Usage for People Under 40

Figure 3. Factors That Would Motivate Non-Users to Adopt P2P

	18 to 24 years	25 to 34 years	35 to 44 years
More security features (e.g., guarantee of refund in case of unauthorized payments)	40%	20%	16%
Confirmation the payment was received	31%	17%	13%
Receive rewards for making a P2P payment	31%	12%	12%
Ability to dispute a transaction	30%	8%	11%
More billers/locations that would accept the service (e.g., landlord)	29%	5%	8%
More of my friends/family/acquaintances accepting P2P payments	11%	5%	4%

Source: Javelin Strategy & Research, 2019

© 2019 GA Javelin LLC, a Greenwich Associates LLC company. All rights reserved. This report is licensed for use by Financial Innovation Now. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the permission of GA Javelin LLC. Licensors may display or print the content for their internal use only, and may not sell, publish, distribute, re-transmit or otherwise provide access to the content of this report without permission.

## 65% OF CONSUMERS OVER 45 STILL NEED TO BE CONVINCED

The number of Americans who do not currently see the value of P2P is too large to write off as a group who will never use the P2P product. The key to breaking the adoption barriers is to understand who this customer base is and what they value.

**It is not a lack of access to technology that causes resistance to using P2P payments.**

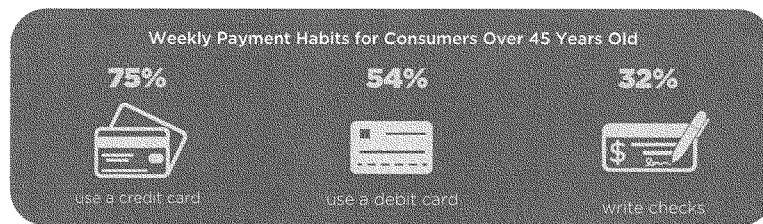
- Access to technology is not an impediment — 85% have a smartphone, 65% have access to a laptop or desktop computer, 60% have a tablet
- Online banking is important, with 68% of consumers logging in weekly; 55% have used mobile banking
- Online shopping (31%) is the preferred method of e-commerce over mobile browsers (10%) or in-app purchases (9%)

Today, P2P does not solve a problem; in fact, negative value propositions are created for older demographics. The payment habits of Americans over the age of 45 have been ingrained by how financial institutions have marketed and issued the card products over the past several decades. Even if the consumer is not thrilled with the experience, it is the process they know and trust.

**To change the behaviors of this consumer base, key payment behaviors need to be considered.**

- Credit (56%) is the most preferred payment method, compared with debit (24%) or cash (11%)
- Credit is preferred because it is easy (59%) and there are rewards (43%)
- Automated payments are not a preferred way of paying bills — 37% of the consumers do not use automated payments for any bill
- Financial institution relationships are based on where branches are located — approximately 60% indicate this is the reason they choose their financial institution

The critical component is the funding source of P2P activity — only 30% of funding is made with a credit card (refer to Appendix B). When a credit card is used, consumers are concerned about the cash advance fees and interest rates — even if the way the payment is processed means those concerns are not applicable. The majority of funding is debit cards, ACH, and stored value. By having liquid assets to source P2P activity, consumers have insight and control over how they spend their funds.



Source: Javelin Strategy & Research, 2019

© 2019 GA Javelin LLC, a Greenwich Associates LLC company. All rights reserved. This report is licensed for use by Financial Innovation Now. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the permission of GA Javelin LLC. Licensors may display or print the content for their internal use only, and may not sell, publish, distribute, re-transmit or otherwise provide access to the content of this report without permission.

Google's understanding of the consumer profiles of P2P and why people do not use P2P is critical to the decision to launch an integration around the checking account. Consumers will appreciate the ease of integration, and prepopulating receiver fields — regardless of if they are an individual or a business — will modify consumer behavior to increase adoption.

Almost 60% of consumers over the age of 45 select the financial institution based on the branch location. Leveraging the branch is essential in breaking through the resistance. The physical

community is part of how finances are managed. Over 65% of consumers deposited checks or cash, and 40% withdrew cash at a branch. Integration into Google APIs will enable the consumer to retain the local bank branch while receiving digital payment services.

The payment behaviors of consumers over 45 years old indicate that they are comfortable with checking accounts and banking activity, yet their preference is still to use a credit card. To move consumers to P2P, the reliance on credit cards needs to be moved to a reliance on debit.

#### Checking Accounts are Critical to Growing P2P Usage For Consumers Over 45

Figure 4. Annual Branch Banking Activity

	45 to 54 years	55 to 64 years	65+ years
Deposited checks or cash	57%	69%	73%
Withdrew cash at an ATM	35%	41%	43%
Cashed checks	30%	32%	39%
Transferred funds between your own accounts	15%	17%	20%
Withdrew cash (NOT at an ATM)	10%	14%	21%
I have not entered a bank branch	17%	11%	9%
Requested a cashier's check	3%	5%	6%
Sent a wire transfer or remittance payment	4%	3%	3%

Source: Javelin Strategy & Research, 2019








### REWARDS CAN MODIFY BEHAVIOR OF CONSUMERS OVER 45

Bank and credit union rewards on credit cards have driven behavior of consumers who prefer credit cards as their primary payment method. When asked why their preferred payment method is selected, 43% stated they selected their payment product for rewards, and 58% stated because it was easy. To drive different payment behavior for consumers over the age of 45, P2P platforms need to overcome the perception that the consumer should be paid to use the product and that it is easier than removing the card from the wallet.

More than 90% of consumers using card-based rewards programs redeemed rewards in the past 12 months. Rewards are further made enticing when the number of rewards programs is evaluated. Many consumers double-dip by using merchant rewards programs to layer rewards on top of rewards. If one reward is good, two or more is better.

#### Modifying Behavior Can Be As Simple As Streamlining Rewards

Figure 5. Annual Rewards Programs Used by Consumers Over 45

	 Airline	 Grocery Store	 Hotel	 Bank	 Restaurant	 Retail	 Gas/Fuel
45 to 54 years	41%	40%	35%	25%	28%	28%	22%
45 to 54 years	46%	38%	34%	27%	25%	25%	25%
45 to 54 years	53%	41%	47%	33%	27%	26%	23%

Source: Javelin Strategy & Research, 2019

© 2019 GA Javelin LLC, a Greenwich Associates LLC company. All rights reserved. This report is licensed for use by Financial Innovation Now. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the permission of GA Javelin LLC. Licensors may display or print the content for their internal use only, and may not sell, publish, distribute, re-transmit or otherwise provide access to the content of this report without permission.

## EXPERIENCES THAT WOW WILL INCREASE ADOPTION

Consumer-centric approaches are not new. Every organization likes to say it is customer-focused. Yet a failure to innovate and accepting the status quo because integration costs are high prevent increased revenue and engagement opportunities. Financial institutions face a growing demand to implement new strategies to remain relevant and be digital top-of-wallet in P2P applications. To increase consumer affinity, engagement, and ultimately volume, different experiences need to be explored to incorporate services that speak to larger groups of consumers.

Some features are now considered table stakes in P2P applications

- Easy ways to locate a receiver (QR code by Venmo or "Find Nearby" from Square Cash), through connecting friends/contacts or Google's use of Gmail to identify receivers
- Rewards for inviting friends, sign-up bonuses, wallet for merchant loyalty programs
- Multipurpose application — P2P, merchant payments, and bill payment (PayPal, Venmo, Google Pay, Apple Pay)

To wow consumers, P2P platforms need to look beyond how the money is being moved to how money can be managed.

### FUNDING SOURCE

- Create stored value accounts to be provisioned inside the P2P application to separate funding of P2P from the demand deposit account (checking and debit) and credit cards.

- Promote a secondary checking account to segregate funds, and do not link it to overdraft of the primary checking account.
- Automatic virtual card provisioning into digital wallets to provide immediate access to funds.
- Empower credit-based consumers to have specific card limits for P2P activity that do not have cash access fees or higher interest rates.
- Enable pay with rewards to send and receive rewards points as cash
- Provide balance and availability features in the P2P app to provide immediate insight to funds sent and received

### FUNDS MOVEMENT

- Connect P2P apps via QR code to merchant apps like hotels and restaurants to enable tipping of staff without needing to know contact information.
- Connect P2P applications to gaming and fantasy sports, enabling quick payouts, crowdsourcing funds for multiplayer activities, and making purchases in game.
- Enable P2P and paying with points without the need for financial institutions to integrate into merchant locations.
- Cross-border and domestic money transfers with transparent currency exchange rates and fees, empowering consumers who do not have a bank account to send and receive cash using a digital wallet.
- Create an investment program to enable fractional investing that can be used for gift-

giving, retirement management, or loyalty programs.

- Expand to digital currency P2P transactions to enable using cryptocurrency and manage it as an investment.
- Enable voice based P2P activity through home devices – creating a favorites list in app or online to direct payments

#### SECURITY ENHANCEMENTS

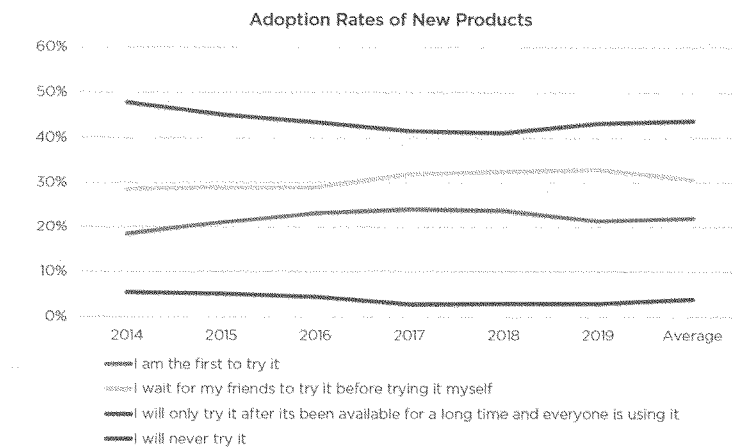
- Improve risk algorithms to look at the sender and receiver to reduce the negative impacts of KYC when the consumer is consistently transferring funds.
- Create trust indicators with AI empowering consumers to conduct marketplace commerce safely and reduce the likelihood of being scammed.
- Incorporate biometrics and reduce reliance on static and one-time use passwords
- Develop consumer controls which enable turning P2P on and off, building consumer notifications when sending and receiving funds

## APPENDIX A — CONSUMER BEHAVIOR METRIC

Consumer hesitancy in using new products can hinge on several factors. On average, 22% of consumers state that they will be the first to try a new product while a majority of consumers — almost 75% — state that they will use a product after a friend uses it or it has been widely available. Less than 5% of American consumers say they will never try a new product.

With the current P2P market penetration rate hovering at 30%, the industry has moved from early adopter phase to building mass appeal. To build appeal, new features and functionality need to be deployed to win over the next wave of customers.

**Consumer Adoption Of New Products Over the Past 6 Years Remains Consistent**  
Figure 6. Consumer responses to the question “Which of the Following Describes Your Actions When a New Technology Becomes Available”



Source: Javelin Strategy & Research, 2019

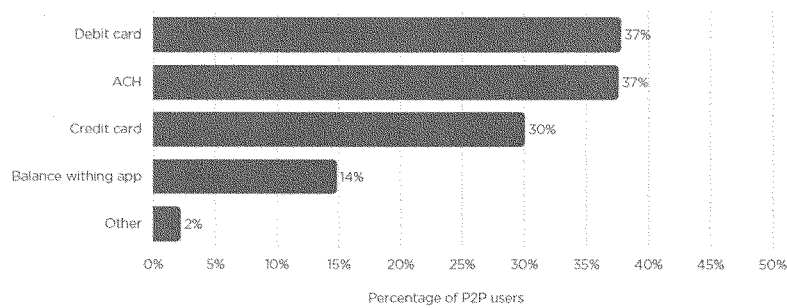
© 2019 GA Javelin LLC, a Greenwich Associates LLC company. All rights reserved. This report is licensed for use by Financial Innovation Now. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the permission of GA Javelin LLC. Licensors may display or print the content for their internal use only, and may not sell, publish, distribute, re-transmit or otherwise provide access to the content of this report without permission.



## APPENDIX B — FIGURES AND STATISTICS

**Demand Deposit Accounts are the Primary Funding Source**

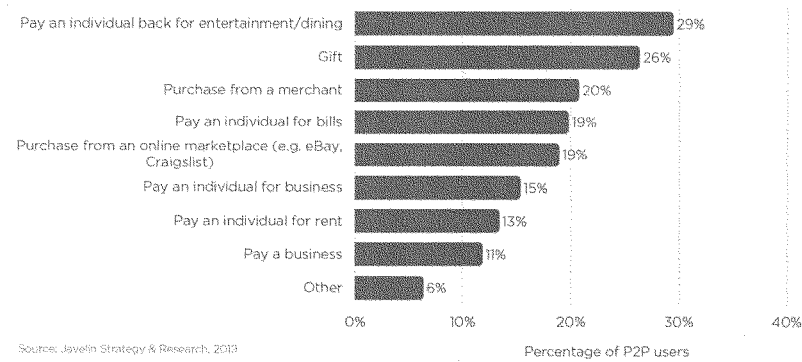
Figure 7. Methods of Funding P2P Transfers



Source: Javelin Strategy & Research, 2019

**Splitting the Bill and Gifts Lead, but Consumers Use P2P for a Wide Variety of Purposes**

Figure 8. Reasons for Making a P2P Payment

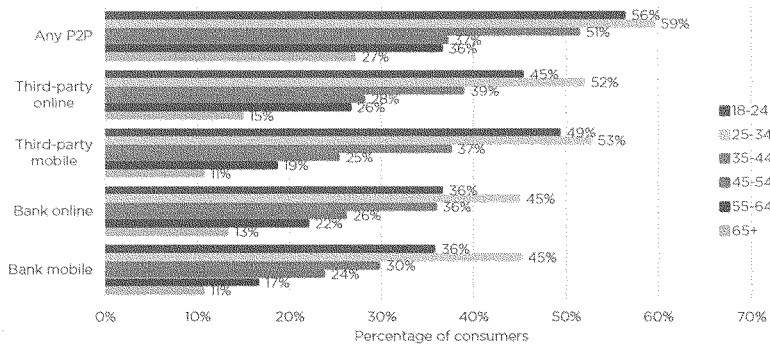


Source: Javelin Strategy & Research, 2019

© 2019 GA Javelin LLC, a Greenwich Associates LLC company. All rights reserved. This report is licensed for use by Financial Innovation Now. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the permission of GA Javelin LLC. Licensors may display or print the content for their internal use only, and may not sell, publish, distribute, re-transmit or otherwise provide access to the content of this report without permission.

### Consumers Need Mobile and Browser-Based P2P Methods

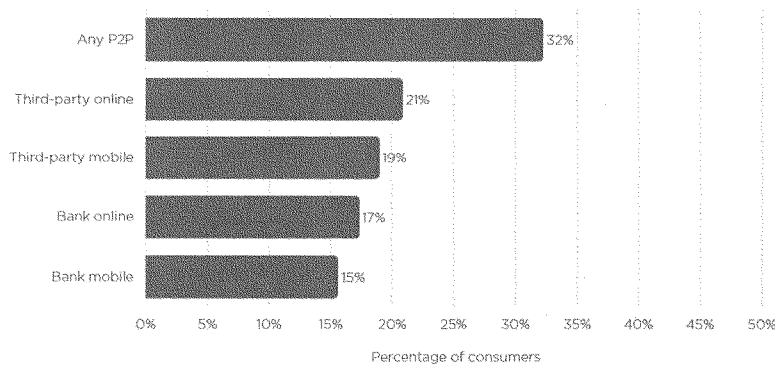
Figure 9. P2P Adoption by Age and Type, Past 12 Months



Source: Javelin Strategy & Research, 2019

### 3 in 10 Consumers Have Used P2P in the Past Month

Figure 10. P2P Adoption by Type, Past 30 Days



Source: Javelin Strategy & Research, 2019

© 2019 GA Javelin LLC, a Greenwich Associates LLC company. All rights reserved. This report is licensed for use by Financial Innovation Now. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the permission of GA Javelin LLC. Licensors may display or print the content for their internal use only, and may not sell, publish, distribute, re-transmit or otherwise provide access to the content of this report without permission.

## ENDNOTES

1. <https://www.cnbc.com/2019/11/13/google-reportedly-offering-checking-accounts-next-year.html>, accessed Nov. 13, 2019.
2. <https://www.theverge.com/2019/11/12/20961447/facebook-pay-whatsapp-instagram-messenger-feature>, accessed Nov. 12, 2019.
3. <https://fidoalliance.org/fido2/>, accessed Nov. 12, 2019.

## METHODOLOGY

The consumer data in this report was primarily collected from the following:

- A random-sample survey of 3,000 respondents conducted online in March 2019. Respondents are selected to be demographically representative of the U.S. population over the age of 18. The overall margin of error is +/-2% at the 95% confidence level for questions answered by all respondents.

The consumer adoption model in this report was collected from 2014 through 2019 using 19 different surveys from the consumer payments, online and digital banking, digital lending, and fraud management surveys.

Companies Mentioned	
Amazon	PayPal (including PayPal, Venmo, and Xoom)
Citibank	People Pay
Early Warning/Zelle	Popmoney
Facebook (including Facebook, Messenger, Instagram, WhatsApp)	Square
Federal Reserve FedNow	Stanford Federal Credit Union
Google	Walmart
Mezu	Western Union
MoneyGram	



The Merchant Advisory Group (MAG) appreciates the opportunity to comment on the House Financial Services Financial Technology Task Force Hearing examining “Is Cash Still King? Reviewing the Rise of Mobile Payments.”

The Merchant Advisory Group (MAG) was founded in 2008 by a small visionary group of merchants in the payments field dedicated to driving positive change in payments through multi-stakeholder collaboration. The MAG represents 160 of the largest U.S. merchants which account for over \$4.4 Trillion in annual sales at over 450,000 locations across the U.S. and online. Roughly \$3.9 Trillion of those sales and over 113 Billion card payments are electronic which represents approximately 59%<sup>1</sup> of total U.S. card volume. MAG members employ over 4 million associates.

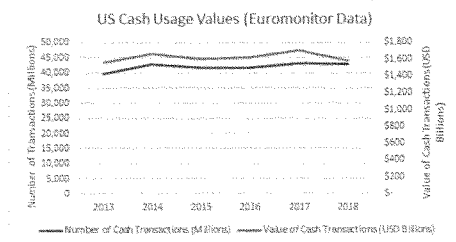
Merchants believe that competition, choice, transparency, innovation, safety, security, and balanced liability should be cornerstones of the U.S. payments system. Merchants prioritize the experience throughout the customer’s interaction regardless of channel. The payments transaction is one component of the customer experience, and merchants strive for their customers to have a seamless checkout. Friction during a transaction, whether in a physical location or in an online or mobile environment, leads to poor customer experience and cart abandonment. Retailers continue to accept many forms of payments, including new, innovative payment products and experiences being introduced globally.

Many payments industry experts project that mobile payments will continue to grow as a tender type. In the United States customers still use traditional payment tenders even as they are adopting other innovative ways to pay. According to Euromonitor, there are still more than 40 billion cash transactions annually accounting for more than \$1.5 trillion of annual expenditure in the United States.<sup>2</sup>

---

<sup>1</sup> *Source of Total U.S. card volumes: Federal Reserve Payments Study 2016*

<sup>2</sup> Euromonitor International. “Financial Cards and Payments in the US.” October 2019.



Even as customers continue to use cash for transactions, digital experiences across a customer's shopping journey are changing the payments landscape leading to growth in mobile and digital payments. Merchants prioritize a friction-free checkout experience as they think about the evolving way customers interact with them.

As the Task Force examines the use of mobile payments in today's various shopping environments, it is important to first look at what constitutes a mobile wallet. Credit cards, debit cards, prepaid cards, gift cards, cash and checking account numbers (ACH) can be stored within various mobile applications (apps), mobile wallets, or online retail accounts. Customer access to these products and services along with improved U.S. payment infrastructure, such as the development of FedNow real-time payments, is critical to enhancing digital financial inclusion. The aforementioned products are generally available in a digital format and function similarly to how they do in a plastic, physical environment.

There are various types of mobile wallets including, but not limited to, retail-specific mobile apps, such as Starbucks, other downloadable payments apps, such as Venmo and PayPal, and wallets associated with the phone hardware, such as Apple Pay and Android Pay. A mobile wallet may have multiple ways in which a customer can interact with a merchant and pay for products. Some mobile apps utilize closed looped gift cards which interact through Quick Response (QR) codes and bar code readers, which are two-dimensional machine-readable codes usually consisting of a matrix of black and white squares containing data that merchants scan to process the transaction. Wallets like Apple Pay and Android Pay mostly utilize Near Field Communication (NFC) technology, which allows the customer to tap to pay at the point-of-sale (POS) terminal, for in-store payments. These wallets and others such as PayPal also perform web-based or in-app purchases where a customer can shop on the Internet from their phone or tablet. These types of payments are also considered mobile payments.

Bluetooth Low Energy Technology (BLE) enables the contactless data transfer of stored card information to merchants' POS. In the mobile environment, BLE allows for a virtual card to be stored on a device and connects to the POS terminal and ultimately the payment network.

Magnetic Secure Transmission (MST) emits a signal emulating the information on a plastic card's magnetic stripe from the device to the POS terminal card reader when the device is in close proximity to the POS.

Merchants prefer to utilize emerging payments technologies that are competitive and transparent while offering security and safety for all parties to the transaction. Because of this, many merchants develop their own mobile wallet offering. In addition to supporting open-loop financial products, merchants' mobile wallets generally support their gift card products, which can be loaded with cash without any fees, providing a mobile entry point for customers who do not have access to credit cards or debit cards. This option gives cash preferring or unbanked customers greater accessibility because it lowers the barrier for them to utilize mobile payments and digital shopping options. Also, merchants who develop wallets tend to support QR and two-dimensional bar code scans, which can be enabled from a broader array of phones, compared to NFC which is more expensive technology usually found on higher cost phones.

A difference between a merchant wallet and an NFC wallet is that issuers are required to do specific programming ("provisioning") to make their cards functional in NFC technology. This results in fewer credit and debit cards being able to function in an NFC wallet and smaller banks and credit unions tend to be slower in their ability to add their products to NFC wallets, thereby limiting digital access for those institutions' cardholders. With an NFC wallet, the merchant risks losing control of how the product interacts with their customers and how much it costs to accept the payment. Merchants are interested in adopting new technology, but global card network rules and fees challenge merchant adoption because such rules and technology limitations may result in a costly, sub-optimal customer payment experience.<sup>3</sup> Rather than focusing on the network-owned NFC technology, which is really just a different way of doing the same thing customers have always done, merchants are looking to make the entire shopping experience easier for their customers. There are myriad examples of merchants implementing software-based experiences that are superior to the networks' costly, more fraud prone, hardware-heavy approach, including in the quick service restaurant industry. Customers can use mobile applications to order and pay ahead of their arrival. This allows customers to drive up and notify the restaurant they are in the parking lot, and the food is delivered to their cars.

The global card networks' honor-all-cards rule is one such rule that impedes merchants' acceptance of mobile wallets. The honor-all-cards rule is the global card networks' requirement that merchants who accept one of its payment products, such as a high-rewards Visa credit card issued by one bank, to accept all of its different credit card products from all issuers. Merchants have seen that the global card networks apply the honor-all-cards-rule to the digital environment, creating an honor-all-wallets policy. If a merchant decides to accept one NFC-based wallet,

---

<sup>3</sup> <https://www.bloomberg.com/news/articles/2020-02-04/visa-is-planning-the-biggest-changes-to-swipe-fees-in-a-decade>

therefore “turning on” NFC wallet acceptance in the store, that merchant has to accept all NFC-based wallets due to the global card networks’ rules and the lack of technology to differentiate between the various NFC-based wallets. This ‘Honor All Wallets’ rule causes multiple issues which will ultimately impact customer experience. This rule effectively forces merchants’ hand on many of the most important aspects of pricing, technology, security, data management, and customer payment experience when considering payments acceptance options for their businesses.

Merchants believe alternative payments products and services, especially as innovation occurs at a rapid pace, are critical for broader mobile payments adoption in the U.S. One area that merchants see potential for increased competition, security, and efficiency in mobile payments and wallets is through faster payments. Currently, MAG CEO John Drechny sits on the Board of the U.S. Faster Payments Council (FPC), alongside representatives from two MAG member organizations. Last summer, the Federal Reserve announced they will develop FedNow, a new 24x7x365 real-time payment and settlement service to support faster payments in the United States.<sup>4</sup> Merchants believe that the Federal Reserve’s involvement will lead to competition and broader customer access for U.S. real-time payment services and offer merchants an additional choice as they weigh their payments acceptance options, and MAG is strongly supportive of these efforts. There are opportunities for use cases beyond business-to-business transactions, and merchants are eager to explore innovative payment experiences that utilize faster payments infrastructure and services.

The U.S. payments system is evolving, and many industry stakeholders are innovating to meet customer expectations and demand. Merchants place great importance on giving their customers a good, seamless experience regardless of the tender either at POS in a physical location or in a digital environment. Thank you for the examination of cash and mobile payments in the United States and for the opportunity to submit comments to the task force. MAG merchants encourage you to review [KnowYourPayments.com](https://www.knowyourpayments.com), an online educational resource operated by MAG, that provides information which may be helpful in your review of mobile payments. MAG and our member merchants look forward to working with you as you consider payments issues and the implications new technology has for merchants, consumers, and all other system stakeholders.

---

<sup>4</sup> <https://www.federalreserve.gov/newsevents/pressreleases/other20190805a.htm>



February 10, 2020

Congressman Stephen F. Lynch  
Task Force on Financial Technology  
House Committee on Financial Services  
2129 Rayburn House Office Building  
Washington, DC 20515

Congressman Tom Emmer  
Task Force on Financial Technology  
House Committee on Financial Services  
2129 Rayburn House Office Building  
Washington, DC 20515

Congressman Lynch and Congressman Emmer,

We applaud the Task Force on Financial Technology (“Task Force”) for holding its recent hearing on “Is Cash Still King? Reviewing the Rise of Mobile Payments.”

The mobile payments ecosystem has grown exponentially over the past two decades, driven by promises of greater inclusion, efficiency, and functionality. Today, mobile payments technologies are at the vanguard of the emerging digital currency industry, due in part to the fact that more people around the world access the internet on their mobile phones more than any other kind of device. Nevertheless, a number of core regulatory issues remain unresolved, and policymakers lack a clear vision for the future of mobile payments, or its relationship to the future of the monetary system more broadly.

A comprehensive regulatory framework for mobile payments must consider a range of issues, from the legal classification of mobile money instruments, to data privacy and law enforcement, monetary and macroprudential policy.<sup>1</sup> At the same time, the growth of mobile payments raises novel questions about the enduring relevance of physical currency in the digital economy, and the advantages and disadvantages of a multi-layer approach to payments system design.

The Modern Money Network (“MMN”) is an educational non-profit organization that promotes public understanding of money and finance. Since its founding in 2012, MMN has advocated for the right of all to participate in economic life, and for monetary and macroeconomic reform consistent with principles of equity, justice, and public purpose. We commend the Committee for forming the Task Force, and for holding hearings such as this one to solicit input on pressing regulatory questions relating to the future of mobile payments. In this letter, we raise certain policy concerns relating to the ongoing relevance of physical cash, defending economic privacy, and guiding principles for designing the twenty first century payments system.

<sup>1</sup> See, e.g., Jonathan Dharmapalan & Rohan Grey, *The Case for Digital Legal Tender: The Macroeconomic Policy Implications of Digital Fiat Currency*, eCurrency Mint Ltd. (2017), <https://www.ecurrency.net/static/resources/201802/TheMacroeconomicImplicationsOfDigitalFiatCurrencyEVersion.pdf>.



### 1. The Ongoing Relevance of Physical Currency

Mobile payments technologies have the potential to improve the payments system for ordinary Americans in many ways that physical cash cannot. To that end, we should welcome – cautiously – the entrance of mobile payments into the broader payments ecosystem.

However, policymakers must be careful not to reinforce a false dichotomy or trade-off between investing in the future of mobile payments on one hand, and investing in the future of physical currency on the other. In reality, physical currency and mobile payments have distinct functions and risk profiles that render them more or less suitable in specific circumstances.<sup>2</sup> Furthermore, physical cash provides an important systemic hedge against certain catastrophic risks that can arise in a purely digital payments system.

**Consequently, mobile payments and physical currency should be understood as complementary rather than competing elements of a resilient, robust payments system.** To that end, instead of debating whether or not mobile payments have rendered cash obsolete, a more constructive approach would be to determine the contexts in which cash will continue to be necessary and/or useful, and to develop policies that support and promote the ongoing use of cash in those circumstances.

At the same time, policymakers must resist efforts by certain elements of the financial services and technology industries to eliminate physical currency as a competitor to their own digital payments services – the so-called “War on Cash.”<sup>3</sup> Instead, policymakers should affirm the enduring social value of physical currency, and emphasize the potential for mobile payments and physical cash to coexist in a mutually beneficial way.

### 2. Defending Economic Privacy

For centuries, societies have maintained a delicate but functional balance between privacy and transparency in the payments system. This balance should be preserved, not undermined, as we transition to a digitally-native economy.<sup>4</sup>

To that end, it is critical that the emerging mobile payments architecture include a decentralized, anonymous, peer-to-peer eCash layer, in addition to an intermediary-based account layer. **Failure to do so would represent an extreme departure from the status quo, and cannot be defended on the basis of technological necessity or inevitability.**

We recognize that the government has a legitimate interest in monitoring and restricting certain kinds of payment system activity, consistent with its mandate to enforce the law and defend national security. However, this interest is not in tension with the government’s responsibility to protect and defend the freedom to engage in legitimate forms of anonymous payments.

<sup>2</sup> See, e.g., David Clarke, *The Future of Cash*, Positive Money (2018), <http://positivemoney.org/wp-content/uploads/2018/03/Positive-Money-Future-of-Cash.pdf>.

<sup>3</sup> See Brett Scott, *The War on Cash*, The Long+Short (August 19, 2016), <https://thelongandshort.org/society/war-on-cash>; Daniela Gabor & Sally Brooks, *The Digital Revolution in Financial Inclusion: International Development in the Fintech Era*, 22 New Political Economy 423 (2017), <https://uwe-repository.worktribe.com/OutputFile/888361>.

<sup>4</sup> See Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight For a Human Future at the New Frontier of Power*, Public Affairs (2019).

To the contrary, **a fundamental goal of law enforcement and national security is to protect and defend individual rights, including the right to engage in legitimate economic activity without fear of surveillance or censorship.**<sup>5</sup> Anonymous, decentralized eCash is necessary, if not sufficient, element of a genuine privacy-respecting digital payments system.

More broadly, issues pertaining to law enforcement, national security, civil liberties, and privacy extend far beyond the statutory mandate and technocratic expertise of the Federal Reserve and other financial regulators in charge of the payments system. Thus, it is critical that policymakers considering the future of mobile payments solicit the input from a diverse range of stakeholders, including technology and privacy experts, community leaders, and ordinary Americans.

### **3. Guiding Principles for Payments System Design**

We are living through an pivotal moment in history, where decisions we make today regarding the material and legal architecture of our emerging digital economy will reverberate for decades, if not centuries. Consequently, it is critical that we take a long-term approach to system design, and **prioritize freedom and flexibility over approaches that seem easier in the short run, but increase the risk of technological lock-in and negative path dependency.**

For example, policymakers around the world are currently debating whether it is better for mobile payments systems to be designed around stored value “tokens,” or intermediated “accounts.”<sup>6</sup> While there are meritorious arguments on both sides, from a design perspective, there is an important asymmetry between the two approaches.

In particular, **it is possible to offer account-based services within a token-based payments system, but it is not possible to offer token-based services in an account-based system.** Thus, implementing a token-based architecture today would preserve the freedom of future generations to decide for themselves which option they prefer, while implementing an account-based architecture today would eliminate that choice permanently.

In addition, it is important to recognize that prevailing social attitudes and values can change, and wherever possible design technology that remains neutral on questions it does not need to answer. To that end, we should resist the temptation to frame core payments infrastructure debates in terms of short-term political considerations, such as minimizing tax-avoidance, if doing so obscures the larger social questions at play.

Finally, it is important that policymakers listen to the prevailing consensus among technological and security experts, and **demand that any system-critical hardware and software used in mobile payment systems be licensed under free and open source (F/OSS) licenses.** This encourages innovation, prevents vendor lock-in, and maximizes the resiliency and robustness of the system.<sup>7</sup>

<sup>5</sup> See Eben Moglen, *Privacy Under Attack: The NSA Files Revealed New Threats To Democracy*, The Guardian (May 27, 2014), <https://www.theguardian.com/technology/2014/may/27/-sp-privacy-under-attack-nsa-files-revealed-new-threats-democracy>.

<sup>6</sup> See Bank of International Settlements, *Central Bank Digital Currencies*, BIS (March 2018), <https://www.bis.org/cpmi/publ/d174.pdf>.

<sup>7</sup> See Eben Moglen, *When Software Is In Everything: Future Liability Nightmares Free Software Helps Avoid*, Software Freedom Law Center (June 30, 2010), [https://www.softwarefreedom.org/events/2010/sscl/moglen-software\\_in\\_everything-transcript.html](https://www.softwarefreedom.org/events/2010/sscl/moglen-software_in_everything-transcript.html).

**Conclusion**

We urge the Task Force to investigate the concerns outlined above as you consider policies to address the future of cash and mobile payments. Thank you again for your attention to these important issues.

Sincerely,

A handwritten signature in black ink, appearing to read 'Rohan Grey', with a stylized flourish at the end.

Rohan Grey  
President  
The Modern Money Network

CC: Chairwoman Maxine Waters and Ranking Member Patrick McHenry



Money Services Business Association  
[www.msbaassociation.org](http://www.msbaassociation.org)

Phone: 201-781-2590  
 Email: [kathy.tomasofsky@msbaassociation.org](mailto:kathy.tomasofsky@msbaassociation.org)

January 29, 2020

The Honorable Stephen F. Lynch  
 Chairman  
 Task Force on Financial Technology  
 House Committee on Financial Services  
 2129 Rayburn House Office Building  
 Washington, DC 20515

The Honorable Tom Emmer  
 Ranking Member  
 Task Force on Financial Technology  
 House Committee on Financial Services  
 2129 Rayburn House Office Building  
 Washington, DC, 20515

Dear Chairman Lynch and Ranking Member Emmer:

The Money Services Business Association, Inc. (MSBA) applauds the FinTech Task Force for holding a hearing examining the interplay between cash and mobile Payments and is grateful for the opportunity to provide comments to assist in its efforts.

The MSBA is a national trade association composed of direct and indirect participants in the non-bank money services industry. Launched in October 2015, the MSBA supports the non-bank financial services industry, encourages continued innovation and development in the payments industry and promotes education and communication with Federal and State regulators and legislators. Our members comprise traditional money transfer companies that operate through physical branches and agents; Financial Technology companies that offer virtual wallets or allow consumers to transfer value via a website or stored value devices including mobile phones and prepaid cards; and others who process money orders, in-person and online bill payment services, and currency exchange. I currently serve as the executive director of the MSBA.

Our members share a vision to bring essential financial services to consumers and businesses in an efficient, cost-effective, and transparent manner. The money services business (MSB) industry represents \$1.4 trillion as reported in October 2019 by the Conference of State Bank Supervisors' (CSBS) latest analysis.<sup>1</sup> CSBS obtains its data from the Nationwide Multi-State Licensing System (NMLS), of which 42 states, Puerto Rico and Washington DC are represented. According to the report, there is an increase in the FinTech solutions that are providing money transmission, which would include mobile payments. In 2018, approximately 55 percent (\$749 billion) of all MSB transactions were FinTech-based, per NMLS data.

The money transmission model represented by branch and agents is a robust community of mostly small businesses that serve consumers especially in areas where no bank branches exist, in places and at times that are more convenient. As of the end of 2018, with 40 states included, 204 companies reported 440,188 active authorized agent relationships, and 216 companies reported no agents used.

<sup>1</sup> Reengineering Nonbank Supervision, Chapter Four: Overview of Money Services Businesses. Available here: <https://www.csbs.org/csbs-white-paper-reengineering-nonbank-supervision>



Contrary to some popular misconceptions, MSBs are not risky because of under-regulation. In fact, MSBs are highly regulated and closely supervised. In the case of money transmitters, 49 states regulate their activities through licensing, bonding, scheduled reports and onsite visits. All licensed companies must have anti-money laundering (AML) compliance programs that meet Bank Secrecy Act (BSA) standards and that must be tailored to address and mitigate risks associated with the products and geographic footprint presented.

Moreover, MSBs are not a monolith; they vary in size and product offering. Consequently, the AML and regulatory risks they present likewise vary. The Financial Crimes Enforcement Network defines MSBs as entities doing business in one or more of the following capacities:<sup>2</sup>

- Issuer or seller of traveler's checks or money orders;
- Money transmitter;
- Dealer in foreign exchange;
- Provider of prepaid access;
- Seller of prepaid access;
- U.S. Postal Service; and
- Check casher.

MSB products and services shape the type of relationship that MSBs have with their consumers. Unlike banks, MSB products and services are not necessarily relationship- or account-based.

MSBs offer services that comply with all applicable legal requirements regardless of whether they are cash or digital in nature. Our membership includes both cash based and digital companies and provides their consumer with a choice as to which type of service best satisfies their financial needs.

The two most compelling reasons often cited as to why MSB customers don't use bank accounts are cost and mistrust associated with banking services. From a consumer perspective, cash transactions allow the consumer rational control over their funds in a low-cost manner. If consumers cash their paychecks for a small fee, they can then pay their bills with money-orders, send money home and retain money with explicitly disclosed fees.

If that same consumer were to place their check in a bank account, there are two scenarios that can occur. First, the consumer will have to wait for the check to clear before having access to the funds. Second, if the check is cleared immediately but is later returned for non-sufficient funds, the consumer is penalized with overdraft fees on the bank account, returned payment charges for any checks the consumer wrote on that account, and reputational injury and late fees from the parties to whom the consumer wrote those checks. If consumers have not built up

---

<sup>2</sup> See 31 CFR § 1010.100(ff).



sufficient savings to cover these scenarios, they have placed themselves in a difficult financial situation.

We understand that the foregoing hearing is intended to understand mobile payments and whether they will overtake cash as a primary method of payment. The MSBA believes that before an answer can be found to that question, the Task Force must recognize that neither cash nor cashless transactions can take place in absence of a bank. MSBs must be “sponsored” by a bank in order to function. As of the date of this letter, MSBs and agents that provide services to consumers are at risk of literal extinction because of the “de-risking” or more appropriately, “unjustified closing” of their business accounts by banks.

The limited access to bank accounts is not a new issue but one that has fluctuated over the last 20 years. In 2005, FinCEN and other regulators issued an Interagency Guidance, which, for a brief period, had a positive impact on MSBs’ access to banking services and caused those services to stabilize. However, the improved access was short-lived. In the aftermath of the 2008 financial crisis, MSB account terminations resumed and intensified with federal regulators placing pressure on banks to scrutinize their accountholders, which made banks hesitant about entering into correspondent banking relationships with MSBs.

Recently, in an official statement, the FDIC, affirmed that “Financial institutions that properly manage customer relationships and risks are neither prohibited nor discouraged from providing services to customers operating in compliance with applicable federal and state law.” The FDIC also affirmed that its internal policy is to *not* recommend or require account closings through informal suggestions. Rather, “[r]ecommendations or requirements for terminating deposit accounts must be approved in writing by the Regional Director before being provided to and discussed with institution management.” Furthermore, the letter to counsel notes that the FDIC is removing lists of examples of higher-risk merchant categories that were previously included in official FDIC guidance, as these lists “led to the misperception that the examples of merchant categories were prohibited or discouraged.” The industry viewed the statement as a positive message.

Unfortunately, the recent federal guidance regarding de-risking has not proven to be the magic elixir to getting and maintaining bank accounts for MSBs. Some recent bank mergers, for example, have brought systematic de-risking of MSB accounts, as the combined banks often adopt the more conservative institution’s approach and change focus to other product areas.

There is no one-size fits all solution to the denial of bank access. One of the key tenets in the MSBA’s outreach is to advance the understanding of the regulated nature of the products that MSBs offer. The Bank Secrecy Act (BSA) obligations provide protections against money laundering, and the CFPB and state regulation provide consumer protections.

It is important to recognize the significant role that state authorities play with respect to the licensure and supervision of MSBs. Leveraging of state agencies’ examination findings by federal supervisory agencies could ease some of the regulatory costs and burdens experienced by banks that provide banking services to MSBs. State agencies’ findings with respect to MSB



examinations could also be used by banks and regulators alike for purposes of differentiating among the relative risks posed by MSBs, and the commensurate level of controls necessary to manage those risks. Other actions that can be promoted for a positive impact on MSBs' access to banking services include strengthening examiner training, providing greater clarity with respect to examination procedures and ensuring that financial institutions are fully aware of the policy guidance that federal banking agencies have issued regarding supervisory expectations concerning MSB accounts.

**Conclusion:**

We ask the Task Force to consider the products that consumers and businesses are provided by Money Services Businesses. Include them in your determinations to broadening decisions in a cash versus mobile payment discussion.

Critically important in the continued growth in innovation and maintenance of the MSB products is the reliance on a bank account relationship. Currently, whether a new FinTech company or an existing MSB, access to a bank relationship is limited, expensive and subject to removal with short notice.

I welcome an opportunity to further discuss these topics at your convenience.

Sincerely,

A handwritten signature in dark ink, appearing to read "Kathy Tomaso".

Kathy Tomaso  
Executive Director  
Money Services Business Association, Inc.



2550 Wasser Terrace  
Suite 400  
Herndon, VA 20171  
703.561.1100  
www.nacha.org

January 29, 2020

*Via Electronic Submission*

The Honorable Stephen Lynch  
Chairman  
Task Force on Financial Technology  
2109 Rayburn House Office Building  
Washington, DC 20515

The Honorable Tom Emmer  
Ranking Member  
Task Force on Financial Technology  
1315 Cannon House Office Building  
Washington, DC 20515

Re: Task Force on Financial Technology Hearing, "Is Cash Still King? Reviewing the Rise of Mobile Payments"

Dear Chairman Lynch:

Nacha appreciates the Financial Technology Task Force's efforts to engage the payments industry in a dialogue on how Americans make and receive payments. Nacha welcomes the opportunity to submit a Statement for the Record to the Task Force in preparation for the Hearing on Is Cash Still King? Reviewing the Rise of Mobile Payments.

#### **The Modern ACH Network**

Nacha is the steward of the modern ACH Network, an electronic payment system that universally connects all U.S. bank accounts. The ACH Network serves as a secure, reliable and ubiquitous network for consumer, business and government electronic payments. In 2019, the ACH Network processed 24.7 billion transactions totaling \$55.8 trillion in value. The use of the ACH Network has grown by more than 1 billion payments each year for the past 5 years. The Federal Government is one of the largest user of the ACH Network, making use of its capabilities and efficiencies for 1) the Direct Deposit of salaries and retirement benefits; Social Security, veterans and other benefit payments; and tax refunds; 2) the collection of much of the Federal government's revenue through the remittance and collection of tax payments; and 3) the payment of government vendors and contractors.

In 2016, Nacha and the two ACH Network operators – the Federal Reserve and The Clearing House – introduced Same Day ACH for faster processing and funds availability for ACH payments. Since its inception, the ACH Network has moved more than 500 million Same Day ACH payments; and in 2019, Same Day ACH saw 250 million payments and \$247 billion in value.



**Nacha Comments on Direct Deposit**

**A. A Misconception about Paychecks and Direct Deposit**

There has been concern expressed that workers still getting paid by paper check don't have quick access to their funds, which can impact those living payday-to-payday. While paper paychecks are inefficient and should be replaced, most workers do not get paid with a paper paycheck anymore.

Direct Deposit via the ACH Network is the way in which nearly 93 percent of Americans get paid, according to a 2018 American Payroll Association survey. It's faster, safer and more reliable than a paper check, and can reach every bank account. Most importantly, by using Direct Deposit, workers get the money in their accounts at the opening of business on payday, without having to wait for a paycheck to clear. For example, an employee with a payday on Friday, January 31, 2020, using Direct Deposit will have their funds available for withdrawal or to cover payments at the start of that day, before the weekend.

For employees without set paydays, the ACH Network now enables faster processing of Direct Deposits with Same Day ACH. In the example above, the employee can still get access to money in his or her account by 5 p.m. via a Same Day ACH Direct Deposit, before the start of the weekend. Direct Deposits and other disbursements to consumers are the largest and fastest growing category of Same Day ACH payments. In 2019, the use of Same Day ACH for payroll and other Direct Deposits to consumers increased by 117% over 2018, demonstrating that there are real benefits to getting people money faster compared to a paper paycheck.

We have attached several fact sheets and a letter from banking trades that may help in hearing preparation and supporting the facts and benefits of Direct Deposit.

Nacha appreciates the opportunity to provide a Statement for the Record. If you have any questions regarding our comments, please do not hesitate to contact Nacha.

Sincerely,



Jane E. Larimer  
President & CEO

cc: The Honorable Maxine Waters. Chairwoman



Advancing Convenience & Fuel Retailing | [convenience.org](http://convenience.org)

January 30, 2020

The Honorable Stephen F. Lynch  
Chairman  
Task Force on Financial Tech. Subcommittee  
U.S. House Of Representatives  
Washington, DC 20515

The Honorable Tom Emmer  
Ranking Member  
Task Force on Financial Tech. Subcommittee  
U.S. House Of Representatives  
Washington, DC 20515

**RE: Hearing “Is Cash Still King? Reviewing the Rise of Mobile Payments”**

Dear Chairman Lynch and Ranking Member Emmer,

The National Association of Convenience Stores (NACS) represents the convenience store industry, which has 153,000 stores across the United States and employs over 2.375 million workers. In 2018, the convenience industry generated \$654.3 billion in total sales, and many retailers indicated that their sales went up in 2019. Convenience stores serve about 165 million people per day – around half of the U.S. population – and the industry processes nearly 75 billion payment transactions per year. Yet, the convenience industry is first and foremost an industry of small businesses – approximately 62 percent of convenience store owners operate a single store, and approximately 74 percent of NACS’ membership is composed of companies that operate ten stores or fewer.

Due to the sheer scale of payment transaction undertaken at convenience stores across the country, many of these electronic and mobile, NACS has an acute interest in the rapid rise and ubiquity of electronic and mobile payments and applauds the Task Force for holding this hearing.

NACS believes that the payments system is at a critical inflection point. Over the last decade, from 2010-2020, the electronic and mobile payments sector has exploded. In 2017, according to data from the Federal Reserve Bank of Atlanta, debit and credit card payments accounted for 54% of all consumer payments in the United States by number, and 55% of all payments by value. And the percentage of transactions made using debit and credit accounts experienced accelerated growth as the decade came to an end.<sup>1</sup> Now, we are seeing innovations in mobile payment platforms. This will accelerate the rise of electronic payments and creates the potential for consumer- and business-friendly innovations that could change the way Americans pay for goods and services for the better.

**Removing Barriers to Innovation**

Payments innovations are proliferating quickly. Not only are mobile payments growing, but cryptocurrencies and other technologies create the promise of faster, more secure, and more efficient payments on a large scale. All of these changes are desperately needed. The United States now lags much of the world in payments technology and security. Many other nations, for example, have moved to real-time payment systems – but the United States has not. In Asia and parts of Africa, mobile payments have become the standard rather than the exception. Again, the United States remains behind in adopting mobile payments. One reason the United States trails in these critical areas is the anti-competitive structure of the payments industry. It is not just that two large players (Visa and MasterCard) dominate the U.S. payment landscape,

<sup>1</sup> Claire Green and Joanna Stavins, “The 2017 Diary of Consumer Payments Choice,” *Diary of Consumer Payments Choice by the Federal Reserve Bank of Atlanta* no. 18-5 (2018), <https://www.frbatlanta.org/banking-and-payments/consumer-payments/research-data-reports/2018/the-2017-diary-of-consumer-payment-choice.aspx>

it is that they control the standards, rules and pricing of payments in such a comprehensive way that they have stifled the ability of other players to innovate for a generation.

Today, the technological potential is there for those large players to be disintermediated from their role in many payments. After all, in a society where individuals can be networked together to make payments, the value of large, exclusive networks to connect banks is questionable. But, the dominant incumbent players are using all of the tools they have to continue their domination of the market – and, in doing so, to block firms that might otherwise disrupt payments with new innovations from doing so.

Just one example of how Visa and MasterCard use their positions to dominate the market and block competitors is how they run standard-setting bodies that create basic rules of the road for payments technologies. For example, those companies control the activities of EMVCo. That body is run by Visa, Mastercard, American Express, Discover, China Union Pay, and JCB. That leaves U.S. technology companies, banks, consumers, and retailers, among others, outside of the decision-making on the standards that EMVCo sets for payments.

The results were well-documented last month in the report by the RPGC Group on “Payment Insecurity: How Visa and Mastercard Use Standard-Setting to Restrict Competition and Thwart Payment Innovation.” That report found, “EMVCo’s ownership by the credit card companies has put profits ahead of security, driven up costs for businesses and consumers alike, and has left the United States with a fraud-prone payments card system even as fraud has been reduced in the rest of the world.”

At every turn, EMVCo has developed standards that protect the market share of the incumbent card networks while undermining new innovators in the marketplace that might improve payment security and efficiency.<sup>2</sup> The efforts of these incumbent players to block new innovation that could threaten their market position needs to be curbed to ensure that American consumers and businesses enjoy the benefits of new payment innovations in the future.

#### Moving Forward

As this Task Force moves forward in considering the rise and future of mobile and electronic payment systems, NACS would recommend that it carefully study the role of Visa and MasterCard in controlling payment standard-setting. The focus of standards should be to help facilitate payment security, efficiency, and innovation. That is not the system we have today, but it is a future that new technology innovators have the potential to deliver. We welcome the opportunity to work with the Task Force to advance those goals.

Sincerely,



Anna Ready Blom  
Director, Government Relations  
National Association of Convenience Stores

<sup>2</sup> For more on these issues, we recommend “Payment Insecurity: How Visa and Mastercard Use Standard-Setting to Restrict Competition and Thwart Payment Innovation,” RPGC Group, December 2019 (at [https://www.securepaymentspartnership.com/wp-content/uploads/2019/12/Payment\\_Insecurity\\_Final.pdf](https://www.securepaymentspartnership.com/wp-content/uploads/2019/12/Payment_Insecurity_Final.pdf)).



## National Grocers Association

January 31, 2020

The Honorable Stephen Lynch  
Chairman  
Task Force on Financial Technology  
U.S. House of Representatives  
Washington, DC 20515

The Honorable Tom Emmer  
Ranking Member  
Task Force on Financial Technology  
U.S. House of Representatives  
Washington, DC 20515

**RE: National Grocers Association Statement for the Record on January 30, 2020 Hearing  
Entitled "Is Cash Still King? Reviewing the Rise of Mobile Payments"**

Chairman Lynch and Ranking Member Emmer,

Thank you for holding a hearing focused on mobile payments and the trend in consumer payment methods towards cashless options. While cashless payments continue to increase – as adoption of payment technology by both younger and older generations grows – grocery continues to be a retail industry where cash, and even check, is still used broadly.

The National Grocers Association (NGA) is the national trade association representing the retail and wholesale grocers that comprise the independent sector of the food distribution industry. Roughly sixty-five percent of our membership is comprised of single-store owners and operators, many of whom serve communities where larger, big box grocery retailers have left the market. Many of these communities – both urban and rural – also have a significant number of customers who would be categorized as “unbanked” or “underbanked”, making access to cashless payment options difficult. Furthermore, low-income customers are disproportionately affected if their cashless payment methods are compromised by fraud, theft or burdensome delays in account or funds settlements.

To combat the concerns raised by the trend towards cashless payments, NGA has advocated – and will continue to advocate – for several innovations in the electronic payments marketplace. First, NGA supports the Federal Reserve’s work towards standing up the FedNow Service, making real-time gross settlement and instantaneous payments a reality across the United States. We have also provided comments to the Federal Reserve outlining our hope that both person-to-person and person-to-business functionality are available from day one of the FedNow Service coming online.



---

## National Grocers Association

---

Secondly, NGA is a founding member of the Secure Payments Partnership, a coalition of retailers, payment processors, debit networks, and community banks that is working to advocate on behalf of greater security, innovation, competition and transparency within the card payment industry. According to the Nilson Report, in 2018 alone the United States made up roughly twenty-two percent of global card transaction volume but accounted for nearly thirty-four percent of global card fraud. For years, our country has held the dubious distinction as the “leader” in global card fraud. It is long past due that something needs to be fixed.

As referenced previously, payments fraud disproportionately affects lower-income populations, and while almost every stakeholder in the card payment industry must contend with the problems that fraud presents, unfortunately the largest players – the global card networks – are immune. With their sheer market presence and having coopted the de facto standard setting bodies within the card payment industry – namely EMVCo – the card networks have routinely stifled innovation, technological advancements, and commonsense security improvements that could disrupt their business streams and transaction volumes. The Secure Payments Partnership is working on a number of necessary reforms to the card payment industry which could be presented in another capacity or as a follow-up to the January 30, 2020 hearing.

Lastly, NGA supports the work of many members of Congress who have advocated for a framework to allow for Open Banking in the United States. In many countries, this concept is already in place, providing customers and small- and medium-size businesses the ability for greater financial transparency and a litany of new applications and services being brought to market by financial technology companies.

NGA is committed to working with the Task Force on Financial Technology to advance solutions to mobile and cashless payments and other issues for the benefit of all communities and businesses across the country.

Sincerely,

Robert Yeakel  
Director, Government Relations  
National Grocers Association  
[ryeakel@nationalgrocers.org](mailto:ryeakel@nationalgrocers.org)

**Statement for the Record**

**Troy Leach**

Senior Vice President, Engagement Officer  
Payment Card Industry Security Standards Council  
House Financial Services Committee  
Task Force on Financial Technology  
United States House of Representatives

**Is Cash Still King? Reviewing the Rise of Mobile Payments**

January 31, 2020

**Introduction**

Chairman Lynch, Ranking Member Emmer, and Members of the Task Force; thank you for the opportunity to offer testimony for the record on this important topic. My name is Troy Leach and I am the Senior Vice President, Engagement Officer of the Payment Card Industry (PCI) Security Standards Council (SSC), a global industry initiative and membership organization focused on securing payment data. Working with a broad global community of industry experts, our organization has created data security standards—notably the PCI Data Security Standard (PCI DSS)—certification programs, training courses and best practice guidelines to help improve payment security. What makes us unique is that we don't just collaborate to develop standards but also provide the necessary certification, education and training programs to help implement them. Our work is broad because there is no silver bullet to securing payment data. No single technology is a panacea; security technology is constantly evolving and requires a multi-layered approach across the payment chain.

Together with our global community of hundreds of the world's leading businesses, we're tackling data security challenges to protect the existing payment infrastructure and develop security to address the next generation of solutions wherever digital commerce may occur. As the global adoption for mobile payments continues to rise, PCI SSC has published new data security standards for solutions that enable merchants to use mobile devices to accept payments using a smartphone or other commercial off-the-shelf (COTS) mobile device with near-field communication (NFC) such as contactless transactions. We are also leading the industry in looking at new ways to address software security that mobile payments rely upon with the release of two new standards as part of our Software Security Framework to address emerging risks to commerce such as online skimming attacks.

Among the ways that the payment industry is minimizing the risk for mobile payments is the introduction of payment tokens as an alternative to the traditional credit or debit card number. This limits the exposure of the cardholder information to prevent future fraud. PCI SSC does not develop any specification for tokenization or guidelines on how those specifications should be implemented but does provide security requirements for Token Service Providers to enhance the integrity and protection of those card data environments. This process helps remove the value of stealing payment data and minimizes the incentive for attempting to compromise a company for that purpose.

Work by the PCI Security Standards Council demonstrates effective voluntary industry collaboration to develop private sector standards. A great example of this is our recent Request for Comments (RFC) period for input into our PCI DSS v 4.0 standard development which garnered 3,254 comments from 154 companies.

Simply put, the PCI Standards are the best line of defense globally against the criminals who seek to steal and utilize payment data. Our standards are updated to address new payment technology and emerging threats to the payment industry and through a collaborative cross-industry approach, we continue to build upon the way we protect payment data.

#### **About the PCI Security Standards Council**

##### **The PCI SSC's Mission**

The PCI SSC was formed in 2006 by the global payment brands and our mission is straightforward: to enhance global payment account data security by developing standards and supporting services that drive education, awareness, and effective implementation by stakeholders.

Very simply, this means that the PCI SSC's goal is to foster standards to protect not just consumers, but also industry players such as merchants (retailers, transportation companies, hotels, airlines, etc.), banks, government, academia and all other organizations that store, process and transmit payment data. It's this wide range of stakeholders that make up the PCI SSC's global base of more than 750 leading national, regional and global participating organizations. We are the leading expert on security standards for payment environments.

##### **The Council's Work**

The growth and improvement in payment security over the past few years is directly to the global industry involvement in the work of the PCI SSC.

It's through the voluntary and active participation of this global community that the PCI SSC sets and develops technical standards and other resources that comprise the essential tools needed to protect payment data against breaches and reduce payment fraud. Protecting payment data is a shared responsibility across the payment's ecosystem. Together with our industry participants, we drive education and awareness of payment security globally.

### Our Approach

The PCI SSC achieves our mission with a strategic framework to guide our decision-making process and ensure that every initiative is aligned with our mission and supports the needs of the global payment industry. The four pillars of our strategic framework are:

- Increase Industry Participation and Knowledge
- Evolve Security Standards and Validation
- Secure Emerging Payment Channels
- Increase Standards Alignment and Consistency

### Industry Working Together

Collaboration is central to the PCI SSC's mission. Payment security is everyone's responsibility. It can't fall to one entity – bank, card brand or retailer – to secure the whole system. Every entity that stores, processes or transmits cardholder data must play a role. The PCI SSC provides an open forum for the industry to come together to develop security standards and programs that help secure payment data globally.

To ensure that the PCI SSC has a broad range of input and perspectives, we provide a multitude of ways for organizations from across the payment world to voluntarily participate and impact payment data security in a positive way. Some of the ways the PCI SSC collaborates with a wide range of global payment stakeholders includes:

- The PCI SSC is composed of more than 750 Participating Organizations (POs) that represent companies from across industries and around the world, including retailers, hotels, banks, technology companies, payment processors and industry associations. These organizations play a key role in both influencing the ongoing development of PCI Security Standards and programs, and in helping ensure that PCI Security Standards are implemented globally to help secure payment data.
- The PCI SSC Board of Advisors (BoA) is a 29-member Executive Committee liaison board elected by the PCI Participating Organizations around the globe to ensure industry involvement in the development of PCI Security Standards. As strategic partners, they voluntarily bring market, geographical and technical insight into PCI SSC plans and projects. BoA members include Amazon, Walmart, Target, Starbucks, AccorHotels, Microsoft, PayPal, and Walt Disney.
- The PCI SSC Technical Advisory Board (TAB) is a technical liaison board that brings subject matter technical expertise from a broad range of stakeholders to the security standards process. The TAB provides guidance and recommendations to the PCI SSC on technical matters related to payment security.



- The PCI SSC Regional Engagement Boards provide region specific leadership. The first Regional Engagement Board started in Latin America. The Regional Engagement Board – Brazil represents the perspectives of PCI SSC Participating Organizations and constituents in Brazil, providing feedback and guidance to the PCI SSC on payment security standards, program development and adoption in the region. The PCI SSC plans to create more Regional Engagement Boards in other parts of the world in the future.
- PCI SSC Affiliate Members, who represent regional and national payments organizations, help define standards and influence their adoption. Currently eight organizations serve as Affiliate Members representing a global footprint of payment systems. Affiliate Members actively participate on the various PCI SSC Working Groups playing an important part in the standards development process.
- PCI SSC Strategic Regional Members represent national payment systems at a regional level (such as LAC, Europe, MEA, and APAC). Strategic Regional Members actively participate on the various PCI Working Groups as well as advise on regional specific payment security initiatives.
- The PCI SSC Global Executive Assessor Roundtable is an advisory board composed of senior executives from PCI assessor companies. The PCI SSC trains and validates thousands of assessors that help ensure the correct adoption and implementation of PCI Security Standards. Assessors provide input on the development of PCI Security Standards and programs and PCI SSC holds regular sessions to engage with the assessment community.
- PCI SSC Task Forces provide high level advice and even help draft our standards. These task forces are composed of members who volunteer from our over 750 Participating Organizations (POs) worldwide. A great example of their work is the Small Merchant Task Force which drove the creation of PCI SSC's small merchant dedicated webpage and small merchant materials that address the problem areas of passwords, patching and remote access.

#### **How PCI SSC Turns Feedback into Action:**

The PCI SSC has many examples of taking industry feedback and turning it into actions that benefit payment stakeholders. Just a few examples include:

- Merchants suggested the PCI SSC develop training to help in-house security personnel assess their security risks and PCI DSS compliance – they got it! The Internal Security Assessor (ISA) program was born.
- The industry – particularly small merchants - wanted guidance on how best to understand and address their greatest security challenges – they got it! The PCI SSC put together easy to understand information and tools aimed at helping the small merchant which can be seen on the "Getting Started with PCI Merchant Webpage".

- The marketplace asked for changes to the Qualified Integrators and Resellers (QIR) to improve training and increase the number of QIRs available to merchants – they got it! The PCI SSC made the new changes and the program is underway.

Our Board of Advisors asked the PCI SSC to take an active role in educating the marketplace about the growing threat of online skimming and the “Magecart” attacks. The PCI SSC partnered with the Retail and Hospitality ISAC and issued a bulletin alerting the payment world to this dangerous threat and offering guidance on how to defend against it.

#### **Public – Private Collaboration**

The PCI SSC welcomes this hearing and the government’s attention on the critical issues facing payment security. The data breaches we hear about in the news underscore the importance of constant vigilance in the face of threats to payment data. We are hopeful that this hearing will help raise awareness about the future of payments.

There are very clear ways in which the government can help improve the payment data security environment. For example, government can champion stronger law enforcement efforts worldwide, particularly due to the global nature of these threats. It can encourage stiff penalties for cybercrimes to act as a deterrent. Also, there is much public discussion about simplifying data breach notification laws and promoting information sharing between public and private sectors. These are all opportunities for the government to help tackle this challenge.

The PCI SSC is an active participant in government research in this area: we have provided resources, expertise and ideas to FS-ISAC, NIST, DHS, and the Secret Service, as well as global agencies such as Interpol and Europol. Just last year, we mapped our DSS standard to the NIST cybersecurity framework in an effort to foster greater understanding on how our standards compliment the great work NIST is doing. We remain ready and willing to do more.

Twenty-five years ago, through its passage of the Technology Transfer and Advancement Act of 1995, Congress recognized that government should rely on the private sector to develop standards rather than to develop them itself. The substantial benefits of the unique, U.S. “bottom up” standards development process have been well recognized. They include the more rapid development and adoption of standards that are more responsive to market needs, representing an enormous savings in time to government and in cost to taxpayers.

Given the complexity and speed at which new threats emerge (and therefore must be responded to), the PCI SSC believes that the development of standards to protect payment card data is something the private sector, and PCI specifically, is uniquely qualified to do. It is unlikely any government agency could duplicate the expansive global reach, expertise, and decisiveness of the PCI SSC. High profile events such as the recent breaches are a legitimate area of inquiry for the Congress, and we welcome the opportunity to comment and testify on the role of government and how public and private sector entities can best respond. And while PCI does not take formal positions on proposed legislation or regulation, we strongly believe that PCI’s constantly evolving standards are a significantly effective way to address current threats and remain nimble in protecting consumers. Any government standard in this area would likely be significantly less

effective in addressing current threats, and less nimble in protecting consumers from future threats, than the constantly evolving PCI Standards.

### **The Future of Payments**

While this hearing tackles the question of “is cash still king?”, one thing we know for sure is that the future of payments is ever changing and becoming more and more complex as new technology and new forms of payment acceptance continue to evolve and grow. At the PCI SSC we are dedicated to securing existing and emerging payment channels.

Today the entire shopping experience, from creating a grocery list to paying for the items on that list, can be realized using mobile technology. Last year, the Electronic Payments Association (ETA) in their “The State of Mobile Payments” report found that U.S. consumers spent \$64 billion through mobile wallet apps or dedicated apps from retailers in 2018. That represented a 42 percent growth from the previous year. <https://www.rollcall.com/news/policy/mobile-payments-up-but-pace-of-growth-slows> While the U.S. has been slower than other international markets to transition to mobile payments, we are quickly catching up. Being a global standards body, the PCI SSC has had to address the challenges of mobile payment security around the globe and is confident that our approach to securing mobile payments is a sound one that relies on industry feedback and input.

In late, 2019, the PCI SSC released two new standards for solutions that enable merchants to accept contactless payments using a smartphone or other commercial off-the-shelf (COTS) mobile device with near-field communication (NFC). The new PCI Contactless Payments on COTS (CPoC™) Standard and its supporting validation program will lead to more options for merchants to accept contactless payments in a secure manner.

Many of the newer technologies rely more heavily on software development by third parties, which is why the PCI SSC has focused our efforts to evolve software standards for the next generation of payments. We recently published two new software security standards as part of the PCI Software Security Framework. The framework provides developers of payment applications with better support for modern software development techniques, while ensuring greater transparency into the security capabilities of payment software and payment software vendors. In turn, this should provide the overall payment industry with more consistency in how software can be assessed for security and result in a broader range of secure payment solutions.

Innovation in payments moves at an incredible pace. Every few years, it seems, there is a more popular software platform to design from, or entrepreneurs discover new ways to accept payments. For example, 12 years ago, we were just becoming familiar with the term ‘smartphone’, let alone the idea that billions of dollars might someday be processed through this type of device.

Each significant breakthrough requires that generation of software developers to have guiding principles for how to test their software and protect users from being a victim of a data

compromise. I've heard from several developers that our standards and best practices are the best starting point for understanding their role in protecting payments, even if the technology is not yet mainstream.

The PCI Software Security Standards provide increased flexibility and transparency for software vendors to achieve common sense software security objectives, while also supporting a more agile approach to software development techniques and release cycles.

**Conclusion**

I want to thank Chairman Lynch, Ranking Member Emmer, and Members of the Task Force and the members of the House Financial Services Committee for providing the PCI SSC the opportunity to submit comments and share our perspective on this important issue. As the payments system changes and new technologies evolve, we will continue to work with our global stakeholders to develop the industry standards and provide the resources necessary for the protection of payment data across all payments channels and for the reduction of fraud for consumers and businesses globally.

# # #



2005 Market Street, Suite 2800 215.575.9050 Phone  
Philadelphia, PA 19103-7077

901 E Street NW 202.552.2000 Phone  
Washington, DC 20004  
[www.pewtrusts.org](http://www.pewtrusts.org)

January 30, 2020

The Honorable Stephen Lynch  
Chairman, Task Force on Financial Technology  
House Committee on Financial Services  
2129 Rayburn House Office Building  
Washington, DC 20515

The Honorable Tom Emmer  
Ranking Member, Task Force on Financial Technology  
House Committee on Financial Services  
4340 O'Neill House Office Building  
Washington, DC 20024

**Re: Is Cash Still King? Reviewing the Rise of Mobile Payments**

As the Task Force on Financial Technology for the House Committee on Financial Services undertakes an analysis of the use of cash and the rise of mobile payments, The Pew Charitable Trusts is pleased to offer comments on the implications of our research on consumers' use and adoption of various payment types. Pew is a non-profit, research-based organization, and our interests include providing data and analysis to help ensure a safe and transparent marketplace for consumer financial services. Pew's [consumer finance project](#) conducts research that identifies the needs, perceptions, and motivations of consumers, as well as the impacts of market practices and potential regulations.

Pew's research in this area focuses on consumers' use of not only mobile payments but also cash, bank accounts, debit, credit, and prepaid cards – including a focus on how consumers without checking or savings accounts adopt and use payments differently from banked individuals. Our findings demonstrate that mobile payment adoption has lagged compared with the robust smartphone adoption in the U.S. and consumers often avoid these transactions due to concerns about the risks of loss of funds, privacy, and/or security. An analysis of the hurdles underserved populations face should be useful for policymakers as they think about ways to help foster innovation while ensuring strong consumer protections are in place to support growth of a safe and healthy market. We thank the Task Force on

Financial Technology for the House Committee on Financial Services for its request and exploration of cash use and mobile payments.

### Introduction

Cash use has declined over time as consumers have adopted mobile payments (a transaction made using a cellphone), debit, credit, and prepaid cards. However, cash is used monthly by more Americans than any other payment type and remains the primary way that one in seven adult consumers pay. This is especially true for consumers who are without a bank account (unbanked), have a household income of under \$50,000, or are minorities. At the same, though uptake has been slower than projected, mobile payments have gained in popularity and are now used by more than half of adult Americans. Consumers tend to be more worried about payment issues (i.e., theft, merchant disputes) or their protections against loss of funds when using mobile payments compared with their other payment choices – including cash. Compared with debit and credit cards those with mobile payment disputes find the process more difficult. Adoption is especially slow for certain segments of the population such as the Baby Boomers generation or older, the unbanked, and those with lower household income. Though mobile payments have helped give consumers without a bank account in developing countries an electronic option for storing and spending money, they have yet to reach most unbanked households in the U.S. and are unlikely to do so unless the products serve their specific needs and challenges – which differ somewhat from those in Africa or other regions.

Faster payments (that move funds in seconds or minutes rather than the days the U.S. system currently takes) holds promise for making electronic transactions as instantaneous as handing a person cash. The system, if widely adopted, could help give customers certainty about when funds will be available to use and reduce costs borne by families who incur overdraft and other fees due to current delays. However, outside of receiving wages, consumers are likely to access faster payments using apps and it is not clear that those who hesitate to use mobile payments now will overcome their concerns to access this system.

Yet faster payments could widen an existing gap in consumer financial protections and expose users to increased liability due to scams. The Consumer Financial Protection Bureau's new Prepaid Rule has done much to ensure that prepaid accounts – including most mobile payments – are protected against fraud and theft. However, unless the minimum protections found in the Prepaid Rule are maintained across all electronic payments and enhanced to combat victim initiated faster payments (aka push payment) fraud, it is likely that faster payments and other innovations will also expand risks.

Research suggests at least three actions that could improve inclusion and consumer adoption of innovative payment options.

1. Create ways for cash to be easily, inexpensively, and safely moved into an electronic format compatible with mobile, faster, and other innovative payments
2. Improve funds availability (via changes to regulations and/or access to faster payments) to give consumers certainty about their ability to use their money without risk of overdraft or other fees
3. Maintain consistent consumer protections across electronic payments especially with regard to dispute resolution and push payment fraud

### Consumer Cash Use, Reliance, and Views of Protections

According to a Pew survey conducted in 2018, one in seven Americans say that they primarily pay with cash and it remains the most widely used payment type with 78 percent of consumers using it in the last month. However, some groups are more likely than others to use cash, including minorities, households with incomes under \$50,000, and unbanked consumers. Minorities are nearly twice as likely to say they primarily pay this way (20 percent compared with 11 percent of whites). In addition, 23 percent of households with incomes under \$50,000 say they primarily pay with cash compared with just 10 percent of households earning \$50,000 or more per year.<sup>1</sup>

Some restaurants, stores, and stadiums around the country have stopped accepting cash as payment and instead are requiring patrons to pay with cards or digital devices, although some have already abandoned the practice in response to a public backlash and many businesses say that they want to continue taking cash payments.<sup>2</sup> Policymakers around the country have reacted swiftly to the changing payments market. In Massachusetts, where lawmakers banned cashless businesses in 1978, legislators have been considering a repeal of the prohibition. Meanwhile, New Jersey, Philadelphia, San Francisco, and New York City acted to prohibit cashless storefronts in the last two years.<sup>3</sup>

Though cash can be cumbersome and carries no recourse against loss or theft (the way debit, credit, prepaid cards, and most mobile payments do), it is protective in certain respects as it also carries no personal or financial data that can be hacked or stolen. Consumers are split on their views of cash: A quarter of consumers in the U.S. view it as carrying no protection against payment issues (like theft, fraud, or merchant disputes) but a third say that it is “perfectly protected” against such problems.<sup>4</sup>

### Why Unbanked and Low-to-Moderate Income Households Are More Likely to Use Cash

To help underserved Americans it is important to understand why they are choosing to use cash or options outside of the traditional banking system. Unbanked households – who also tend to be lower income – do not use checking accounts for a variety of reasons. More than half say they don’t have enough money to keep in an account and about a third list that as the main reason. But trust in banks, privacy, and high or unpredictable account fees are all cited.<sup>5</sup>

The use of cash cannot lead to overdrafts, whereas low bank account balances can leave a consumer vulnerable to fees either due to minimum balance requirements or overdrafts. Overdraft fees are most onerous for a small number of bank customers. Research from the Consumer Financial Protection

<sup>1</sup> The Pew Charitable Trusts, “Rise of Cashless Retailers Problematic for Some Consumers: Cash Remains Important Payment Option for Many” (2019), 4-6, [https://www.pewtrusts.org/en/research-and-analysis/articles/2019/11/08/rise-of-cashless-retailers-problematic-for-some-consumers?utm\\_campaign=finance\\_economy&utm\\_source=twitter&utm\\_medium=social](https://www.pewtrusts.org/en/research-and-analysis/articles/2019/11/08/rise-of-cashless-retailers-problematic-for-some-consumers?utm_campaign=finance_economy&utm_source=twitter&utm_medium=social).

<sup>2</sup> Square, “Is the ‘Cashless Society’ All Hype?” (2019), <https://squareup.com/us/en/making-change>.

<sup>3</sup> C. Jones, “New York Says Don’t Ditch Your Cash: City Is Latest to Ban Cashless Restaurants, Stores,” *USA Today*, 01.23.2020, <https://www.usatoday.com/story/money/2020/01/23/new-york-city-bans-cashless-businesses/4551974002/>.

<sup>4</sup> The Pew Charitable Trusts, “Are Americans Embracing Mobile Payments?; Survey of Consumer Experiences Finds Greater Trust in Credit, Debit Cards” (2019), <https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2019/10/are-americans-embracing-mobile-payments>.

<sup>5</sup> G. Apaam et al., “Fdic National Survey of Unbanked and Underbanked Households” (Federal Deposit Insurance Corp., 2018), 24, <https://www.fdic.gov/householdsurvey/2017/2017report.pdf>.

Bureau shows that less than a fifth of account holders pay more than 90 percent of all overdraft fees – generating tens of billions of dollars per year for banks.<sup>6</sup>

#### Mobile Payments and Financial Inclusion

Mobile payments have provided a way to increase financial inclusion in developing regions such as Sub-Saharan Africa. As a result, some believe that mobile payments should improve financial access in the U.S. However, there are distinct differences between these populations that should be considered. In Sub-Saharan Africa just, 43 percent of adults have an account at a bank or mobile money service. This has improved quite a bit in the last few years largely due to uptake of mobile money on cellphones, but the majority of the population continue to rely completely on cash as their only payment option.<sup>7</sup> In the United States 93.5 percent of American households have a bank account. The unbanked in both the U.S. and in Sub-Saharan Africa cite not having enough money and high costs as the largest reasons for lack of an account.<sup>8</sup> However, about a quarter of unbanked individuals in Sub-Saharan Africa said that financial institutions (FIs) are too far away<sup>9</sup> compared with just nine percent of Americans without accounts.<sup>10</sup> In addition, consumers in the U.S. have many payment types to choose from and, though they don't serve the needs of all Americans, they provide reasonably well protected options for most whereas Africans largely have no other option but cash or mobile money. Cash currently makes up just 26 percent of transactions in the U.S. and individuals often decide which payment method to use based on the transaction and circumstances.<sup>11</sup> But 90 percent of transactions in Sub-Saharan Africa in 2017 were made in cash – and mobile payments are nearly the only alternative – leaving customers and businesses far more susceptible to theft and in need of better alternatives.<sup>12</sup>

#### Americans Have Many Payment Options

In a given month, most Americans use a range of methods to make payments: cash (78 percent), credit cards (70 percent), debit cards (61 percent), checks and money orders (37 percent), and prepaid cards (12 percent). Fifty-six percent (roughly 143 million adults)<sup>13</sup> have made at least one mobile payment in

<sup>6</sup> J. Chang, "Americans Paid \$34 Billion in Overdraft Fees Last Year. Here's How to Stop the Charges," *Forbes*, April 5, 2018, <https://www.forbes.com/sites/learnvest/2018/04/05/americans-paid-34-billion-in-overdraft-fees-last-year-heres-how-to-stop-the-charges/#4fb5546b3ce9>.

<sup>7</sup> L. Klapper et al., "Sub-Saharan Africa Series: Mobile Money and Digital Financial Inclusion" (World Bank, 2019), 3, [https://globalfindex.worldbank.org/sites/globalfindex/files/referpdf/FindexNote1\\_062419.pdf](https://globalfindex.worldbank.org/sites/globalfindex/files/referpdf/FindexNote1_062419.pdf).

<sup>8</sup> Ibid., 4. Apaam et al., "Fdic National Survey of Unbanked and Underbanked Households," 4.

<sup>9</sup> Klapper et al., "Sub-Saharan Africa Series: Mobile Money and Digital Financial Inclusion," 4.

<sup>10</sup> Apaam et al., "Fdic National Survey of Unbanked and Underbanked Households," 4.

<sup>11</sup> R. Kumar and S. O'Brien, "2019 Findings from the Diary of Consumer Payment Choice" (Federal Reserve Bank of San Francisco, 2019), 3, <https://www.frbsf.org/cash/publications/fed-notes/2019/june/2019-findings-from-the-diary-of-consumer-payment-choice>.

The Pew Charitable Trusts, "Are Americans Embracing Mobile Payments?; Survey of Consumer Experiences Finds Greater Trust in Credit, Debit Cards."

<sup>12</sup> K. Ighobor, "Africa's Quest for a Cashless Economy Gains Momentum," *Economic Development* (blog), United Nations, 07.2017, <https://www.un.org/africarenewal/magazine/may-july-2017/africa%E2%80%99s-quest-cashless-economy-gains-momentum>.

<sup>13</sup> The Census Bureau estimated the U.S. population at 327,167,434 as of July 1, 2018, with 77.6 percent being adults 18 or older. U.S. Census Bureau, Quickfacts, 2010-2018, last modified June 20, 2019, <https://www.census.gov/quickfacts/fact/table/US/PST045218>. Pew's survey found that 56.29 percent of adults



the past year – though 32 percent of U.S. adult consumers chose not to use a mobile payment even though they own a phone capable of a transaction.<sup>14</sup>

#### Overarching Concerns with Mobile Payments

A quarter of U.S. adult users and more than half of non-users ranked mobile payments as poorly protected against issues like theft or double billing. Twenty-nine percent of consumers said they sometimes or always avoid mobile payments for fear of loss of funds – usually because of distrust or concerns about either their phone or the merchant. Unsurprisingly, avoidance of mobile payments correlates with respondents' views of security: Those who rated mobile payments as poorly protected tended to avoid them more often than those who viewed their safeguards favorably (43 percent vs. 15 percent). Debit cards are eschewed at similar rates to mobile payments (53 percent and 19 percent, respectively), and respondents often said that they opted not to use debit cards in unfamiliar or unsecured situations because direct access to a bank account could expose their personal funds. These findings do not mean that consumers with concerns about the security of a payment type never use it, but they do indicate that people are consciously choosing other methods in certain circumstances. Even though nearly 30 percent of mobile payment users sometimes avoid them, few discontinue using them altogether: 84 percent of those who used a mobile payment in the past year also used one in the past month.<sup>15</sup>

#### Demographics of Mobile Payment Customers

Mobile payment users are more likely than nonusers to be millennials or Generation Xers, live in metropolitan areas, have bank accounts, and have college or postgraduate degrees. Of these demographic categories, age is the most predictive of mobile payments use, particularly as it relates to smartphone ownership. These findings suggest that if innovations are dependent on adoption of a mobile payment solution older Americans are the most likely to be left behind.<sup>16</sup>

#### Challenges for Unbanked Consumer Adoption of Mobile Payments

Those without a bank account face additional hurdles to adopting mobile payments in the U.S. These consumers generally lack access to electronic forms of payment such as debit and credit cards. Prepaid cards can bridge this gap and 22 percent of unbanked consumers report using them to receive income or pay bills.<sup>17</sup> Unbanked individuals also tend to have a lower household income (the majority are paid under \$25,000 per year), and three-quarters of them said that they have not adopted mobile payments

(142,910,138 people) have used mobile payments in the past year. Some respondents who made payments in the past year did not complete the survey accurately, so this finding probably underreports payment activity.

<sup>14</sup> The Pew Charitable Trusts, "Are Americans Embracing Mobile Payments?; Survey of Consumer Experiences Finds Greater Trust in Credit, Debit Cards," 4.

<sup>15</sup> Ibid., 9, 12.

<sup>16</sup> In a relative importance analysis, age explained more variance between mobile payments users and nonusers than banked status, residential status (metropolitan versus nonmetropolitan), education, or income. The Pew Charitable Trusts, "Who Uses Mobile Payments?" (2016), 3, <https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2016/05/who-uses-mobile-payments>.

<sup>17</sup> Apaam et al., "Fdic National Survey of Unbanked and Underbanked Households," 9-12.

because they mostly use cash.<sup>18</sup> Though a growing majority own a phone capable of a mobile payment, unbanked consumers are more likely to face disruptions in access because they are nearly twice as likely as banked consumers to suspend or cancel their cellphone plans due to the cost of maintaining coverage. Forty-two percent of these consumers are paid by check or money order and another 14 percent are paid in cash. Thirty-seven percent of the unbanked did report receiving direct deposit to either a bank account owned by someone else or prepaid card. Comparatively, 84 percent of banked consumers receive income via direct deposit to a bank account – which reduces barriers to using these funds electronically. Cash and checks are both cumbersome to upload onto a mobile payment app as they must be deposited into a bank account or prepaid card. Those without these options generally lack a way of uploading money into an app.<sup>19</sup>

#### **Faster Payments Will Solve Some Consumer Pain Points, But Not All of Them**

In October, the Federal Reserve announced its intention to expand a faster payments system that will allow transactions at its member banks to process funds between accounts instantaneously and irrevocably, unlike today's system that usually takes several days. This will affect not only how quickly individuals are paid but also how quickly they can pay other people or businesses.<sup>20</sup> For faster payments to effect meaningful change in the way Americans pay and get paid, a new system will need to achieve high rates of adoption. In 2016 the Federal Reserve's Faster Payments Task Force collected proposals from 16 different financial firms detailing how they would send and deliver funds instantaneously. Most proposals required the use of a smartphone to access the technology. However, the task force's report indicates that mobile technology is not an essential component of an effective faster payments system, and a few companies have proposed models that would allow customers to make payments at kiosks in brick-and-mortar stores, or with a basic cellphone or other internet-connected device.<sup>21</sup>

The speed and irrevocability of faster payments will undoubtedly have consumer benefits such as helping to give families certainty that their funds are available to use and protecting them from overdrafts due to timing issues. They will also help families who struggle to make ends meet due to current delays to access funds and pay bills on the same day as a deposit is made. However, faster payments will not solve the problem of expensive overdrafts, payday loans, or other credit for customers who do not have enough money to cover expenses.<sup>22</sup>

<sup>18</sup> The Pew Charitable Trusts, "What do Consumers Without Bank Accounts Think About Mobile Payments?" (Jun. 22, 2016), <https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2016/06/what-do-consumers-without-bank-accounts-think-about-mobile-payments>.

<sup>19</sup> The Pew Charitable Trusts, "What Do Consumers without Bank Accounts Think About Mobile Payments?" (2016), 6, <https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2016/06/what-do-consumers-without-bank-accounts-think-about-mobile-payments>.

<sup>20</sup> L. Brainard, "Delivering Fast Payments for All," news release, August 5, 2019, <https://www.federalreserve.gov/newsevents/speech/brainard20190805a.htm>.

<sup>21</sup> Faster Payments Task Force, "Final Report Part Two: A Call to Action" (2017), 14–16, <https://fedpaymentsimprovement.org/wp-content/uploads/faster-payments-task-force-final-report-part-two.pdf>.

<sup>22</sup> Consumers overdraft their bank accounts for several reasons. Timing issues can cause overdrafts when, for example, a deposit takes several days to post to an account and a consumer does not know when the money actually becomes available. However, not all overdrafts are mistakes: 31 percent of overdrafters view them as a way to borrow when short on cash. The Pew Charitable Trusts, *Overdraft Does Not Meet the Needs of Most Consumers: Bank Programs Often Function as Costly, Inefficient Credit*, 2017, accessed Dec. 20, 2017,

### Consumer Risk with Expansion of Faster Payments

The Consumer Financial Protection Bureau's new Prepaid Rule has done much to ensure that prepaid accounts – including most mobile payments – are protected against fraud and theft. But gaps remain that could widen with increased payments innovation. In particular, faster payments could increase customer risk of scams that will be quicker and easier for criminals to carry out. Currently the most common and costly cause of losses in the U.S. payment system are victim assisted frauds (when the person being defrauded initiates and/or authorizes the payment to a scammer, also known as “push payment” fraud). These thefts most often rely on wire transfers with a growing number of gift card frauds and together they make up more than 50 percent of total losses and reported frauds that involve a payment method.<sup>23</sup> Wire transfers and gift cards are payment types that are relatively cumbersome for the victim to initiate – giving the payment sender the benefit of time to realize the scam and choose not to transmit funds.<sup>24</sup>

Increasing access to nearly instantaneous faster payments will intensify the risks of loss. In the United Kingdom (which has had faster payments for more than a decade) personal losses due to authorized push payment fraud<sup>25</sup> accounted for 30 percent of fraud losses in 2018 totaling £354.3 million<sup>26</sup> (approximately \$472.4 million U.S. dollars<sup>27</sup>). Sixty-four percent of these were personal losses and 36 percent were business losses. In the absence of regulatory control and increased consumer access to faster payments there will be more exposure to risk of loss of funds. Disclosure of risk to is not sufficient to protect customers from these thefts largely because individuals believe that they are completing a legitimate transaction at the time they execute it. In order to create a system that is well trusted and adopted it is essential that such liability is minimized.

### Ways to Improve Inclusion and Adoption of Innovative Payment Options

<https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2017/12/overdraft-does-not-meet-the-needs-of-most-consumers>.

<sup>23</sup> The current magnitude of losses due to victim assisted fraud aren't generally gathered by U.S. financial institutions, however, in 2018 the Federal Trade Commission's Consumer Sentinel Network received nearly 350,000 complaints of fraud that also resulted in a financial loss. These totaled \$1.48 billion, an increase of 38 percent compared to the year before. Of these, nearly \$488 million were lost to imposter scams (the top reported category) with a median victim loss of \$375. Federal Trade Commission, “Consumer Sentinel Network Data Book 2018” (2019), 4, 11, [https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2018/consumer\\_sentinel\\_network\\_data\\_book\\_2018\\_0.pdf](https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2018/consumer_sentinel_network_data_book_2018_0.pdf).

<sup>24</sup> N.C.I. Center, “Fintech and Consumer Protection” (2019), 19, <https://www.ncic.org/images/pdf/cons-protection/rpt-fintech-and-consumer-protection-a-snapshot-march2019.pdf>.

<sup>25</sup> S. Rutherford, “What Is Authorized Push Payment Fraud,” FICO, 12.05.2017, <https://www.fico.com/blogs/what-authorized-push-payment-fraud>.

<sup>26</sup> UK Finance, “Fraud and the Facts 2019; the Definitive Overview of Payment Industry Fraud” (2019), 7-8, 41, <https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf>; Federal Reserve Bank of Atlanta, “What Can We Learn About Fraud from the United Kingdom?,” accessed Jan. 1, 2019, <https://www.frbatlanta.org/blogs/take-on-payments.aspx?keywordsIDs=0b770cab-ac2e-4330-917a-c002b39ef241>.

<sup>27</sup> In 2018 the exchange rate was \$1 in United States currency to buy £.75 United Kingdom currency. Internal Revenue Service, “Yearly Average Currency Exchange Rates,” accessed 1.21.2020, <https://www.irs.gov/individuals/international-taxpayers/yearly-average-currency-exchange-rates>.

Available research suggests that there are at least three ways that adoption of innovative payment options could be encouraged and fostered in the United States safely and while improving inclusion of un- and underserved populations:

1. Create ways for cash to be easily, inexpensively, and safely moved into an electronic format compatible with mobile, faster, and other innovative payments
2. Improve funds availability (via changes to regulations and/or access to faster payments) to give consumers certainty about their ability to use their money without risk of overdraft or other fees
3. Maintain consistent consumer protections across electronic payments especially with regard to dispute resolution and push payment fraud.

In sum, Pew's research demonstrates that cash use is still an important way that Americans pay, though mobile payment adoption is growing. If greater financial inclusion is to be achieved through innovations and mobile payments it will be necessary to take thoughtful steps to ensure that underserved populations are not left behind and consumers are exposed to unreasonable liability by gaps in protections. We encourage the Task Force on Financial Technology for the House Committee on Financial Services to utilize our research as it considers the role of cash, mobile payments, and innovation in the United States.

Sincerely,



Nick Bourke

Project Director

[www.pewtrusts.org/money](http://www.pewtrusts.org/money)



## Payment Insecurity

### How Visa and Mastercard Use Standard-Setting to Restrict Competition and Thwart Payment Innovation

René M. Pelegero  
President and Managing Director  
December 2019

#### An Investigative White Paper

##### ABSTRACT:

*How standards are produced is a critical consideration in modern economies. If decisions about standards creation are made in furtherance of private companies' preferences alone, the public benefit of the standards will be reduced, or even eliminated.*

*EMVCo is an organization owned by the world's six largest payment card companies that has positioned itself as the representative of the global payments industry. The organization asserts that it produces technical "specifications" needed to ensure interoperability, but those specifications become de facto standards with implications far beyond technical compatibility. In fact, EMVCo has a collusive relationship with its owners. This paper shows a systemic pattern by the card companies to use EMVCo to develop anticompetitive standards that protect the interests of its owners and preempt competition in the market that could lower costs and improve security for businesses and consumers alike.*

*This paper is the result of an in-depth examination of each of the major areas for which EMVCo is responsible for defining standards, including chip-based credit and debit cards, tokenization of payment data, near-field communication for cards and mobile-device payments, and both the Three-Domain Secure and Secure Remote Commerce standards for online card payments.*

*RPGC concludes that EMVCo is not the appropriate organization to develop and implement payment specifications that become de-facto standards and strongly recommend that these standards be set by an independent and established open standards-setting body.*

---

## NOTICE OF CONFIDENTIALITY

No portion of this document can be copied or reproduced in any way without the express consent and written permission from Retail Payments Global Consulting Group LLC.

## TABLE OF CONTENTS

<b>PART I—INTRODUCTION</b>	<b>5</b>
1. ABOUT THIS WHITE PAPER	5
1.1 Background	5
1.2 Methodology	6
1.3 Organization	6
2. EXECUTIVE SUMMARY	8
3. HISTORICAL PRIMER	10
3.1 U.S. Payments Framework	10
3.2 The Need for Standards	10
3.3 Networks Compete for Transaction Volume	11
3.4 EMVCo's Role in Supporting Card Companies' Recapture of Volume	13
4. WHAT IS A STANDARD?	14
4.1 Open Standards-Setting Organizations	14
4.2 EMVCo: from Consortium Specifications to De Facto Standards	15
4.3 Comparing EMVCo with Open Standards-Setting Bodies	15
5. THE EVOLUTION OF EMVCO FROM 2007 TO 2019	17
5.1 EMVCo Organization and Decision Making	17
5.2 EMVCo Staffing	18
5.3 Conclusions	19
<b>PART II—STANDARDS REVIEW</b>	<b>21</b>
6. EMV CHIP AND PIN (OR SIGNATURE)	21
6.1 Background on Chip Cards and Risk Management	21
6.2 Introduction of Chip Cards in the United States Delayed by Lack of Business Case	22
6.3 Visa and Mastercard Compete with Debit Networks	22
6.4 Visa Launches Its EMV Migration Plan	23
6.5 EMV Preventing Merchant Choices in Debit Card Routing	24
6.6 EMVCo Failures with EMV Chip Cards	25
8. NEAR-FIELD COMMUNICATION	26
8.1 Background	26
8.2 EMVCo Entering Mobile Payments	26
8.3 EMVCo Selects NFC for Mobile Payments	27
8.4 EMVCo NFC Specification Complicates Merchant Choices in Debit Card Routing	27
8.5 NFC: A Tool to Prevent Competition	28
8.6 EMVCo's NFC Standard Drawbacks	29
8.7 EMVCo's QR Code Standards	30
8.8 EMVCo's NFC Specification and Apple Pay	30
8.9 EMVCo Failures with NFC	31
9. TOKENIZATION	32
9.1 Background	32
9.2 Standards-Setting Organizations Developing Open Tokenization Standards	32
9.3 Industry Calls for Open Standards	33
9.4 Apple Pay's Role in Tokenization	33
9.5 EMVCo Takes Ownership of Card Companies' Tokenization	34
9.6 EMVCo Tokenization Framework 1.0 Deficiencies	36
9.7 EMVCo Tokenization Framework 2.0 Updates and Remaining Deficiencies	37
9.8 Network Tokens Introduce Challenges to Merchant Debit Card Routing Choices	37
9.9 EMVCo Failures with Tokenization	38

<b>PART III—CONCERNS WITH NEW STANDARDS</b>	<b>39</b>
10. 3-D SECURE VERSION 2.0	39
10.1 Background	39
10.2 Evolution from 3DS 1.0 to 2.0	39
10.3 3DS 2.0 Pre-empting Competition	40
10.4 3DS 2.0 Positioned as a Strong Customer Authentication Standard	40
10.5 EMVCo Ignores Authentication Standards from Other Standards-Setting Bodies	41
10.6 Industry Concerns with 3DS 2.0	42
10.7 Conclusion	43
12. SECURE REMOTE COMMERCE	44
12.1 Background	44
12.2 Game of Buttons	44
12.3 SRC User Experience	47
12.4 EMVCo SRC Standard Components	48
12.5 Issues with the Development of SRC Standard	48
12.6 Industry Concerns with SRC Standard	49
12.7 Conclusion	51
<b>PART IV—CONCLUSIONS</b>	<b>52</b>
13. CONCLUSIONS	52
13.1 Is EMVCo Protecting Visa's and Mastercard's Market Share?	52
13.2 Is EMVCo Capable of Developing Standards in Areas Beyond its Original Charter?	52
13.3 Is the U.S. Payments Industry's Competitive Landscape Being Hurt by Allowing EMVCo to Set Standards?	53



## PART I—INTRODUCTION

### 1. ABOUT THIS WHITE PAPER

Retail Payments Global Consulting Group was engaged by the Secure Payments Partnership to study and determine whether the U.S. payments industry is best-served by EMVCo as the standards-setting organization for consumer payments.

SPP<sup>\*</sup> represents and advocates on behalf of industries that span the payments system, ranging from retailers to the financial services industry. In keeping with its mission, SPP commissioned RPGC to research whether the standards set by EMVCo unfairly advance card companies' dominance in the United States.<sup>†</sup> This research also examined whether EMVCo standards deliver the most secure and efficient payment experiences for U.S. consumers and merchants.

The objective of this white paper is to educate readers on the critical role EMVCo plays in how payments are conducted in the United States and how EMVCo impacts the economic, security and competitive aspects of the U.S. payments landscape. The audience for this paper includes merchants, payment service providers, consumer protection and advocacy organizations, policymakers and all other payments industry participants concerned with the welfare and competitiveness of the U.S. payments system.

This research intends to answer the following four questions:

- Is EMVCo furthering the entire U.S. payments industry or simply protecting Visa and Mastercard's market share?

- Is EMVCo capable to develop standards in areas beyond its original charter and are these standards delivering more efficient and secure payments?
- Is the U.S. payments industry's competitive landscape being hurt by allowing EMVCo to establish broad payment standards and should this work be performed by true open standards-setting bodies?

#### 1.1 Background

EMVCo was established in 1999 by Europay (now part of Mastercard), Visa and Mastercard as a global technical body charged with setting interoperability standards for chip cards and chip terminals.<sup>‡</sup> Since then, EMVCo's ownership has grown to include four additional card companies – American Express, Discover, Japan's JCB and China's Union Pay – but Visa and Mastercard remain the most influential owners.

EMVCo expanded its scope in 2007 with the publication of a white paper in which it announced its intention to define standards for the mobile contactless payments' infrastructure. EMVCo further expanded its charter in 2013 to "facilitate worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV specifications and related testing processes."<sup>1</sup> In doing so, EMVCo – an organization accountable only to its owners – appointed itself the arbiter of U.S. and global payment standards.

Card payments have experienced explosive growth in the United States over the last ten years. As of

<sup>\*</sup> SPP founding members include the Food Marketing Institute, National Retail Federation, National Association of Convenience Stores, National Grocers Association, First Data's STAR Network, and SHAZAM. SPP advances policies that drive state-of-the-art technologies, competition, and collaboration to continually improve the nation's payment infrastructure, meet the evolving needs of commerce, and provide businesses and consumers with convenience, flexibility, and security in payment options.

<sup>†</sup> Henceforth, the term card companies will be used to identify the six EMVCo owners: Visa Inc., Mastercard Incorporated, The American Express Company, Discover Financial Services, Inc., JCB Co. Ltd, and Union Pay International.

<sup>‡</sup> In 2002, Europay International merged with Mastercard International to form Mastercard, Inc. Today the combined company is known as Mastercard Incorporated.

2017, debit and credit card payments accounted for 54% of all U.S. consumer purchase payments by count and 55% by value, dwarfing even cash (at 35% and 15% respectively), according to a report from the Federal Reserve Bank of Atlanta.<sup>2</sup> The same report states that card payments are seeing robust growth, increasing 10.1% by number and 8.4% by value from 2016 to 2017. Those increases represent an acceleration in overall card payment growth when compared with the previously reported 2015-2016 and 2012-2015 periods.<sup>3</sup>

Therefore, a study of the organization setting the standards for the payment industry is timely and appropriate. It is timely because of the dominant position of the card companies over this sector of the economy. It is appropriate because standards contribute to public welfare by improving economic efficiency – ensuring compatibility and interoperability. Any standards that give advantage to certain companies over their competitors are a valid concern as this impacts the welfare and competitiveness of the U.S. payments system.

### 1.2 Methodology

This paper synthesizes a year of research and analysis on the evolution and operations of EMVCo. Its conclusions are derived from an in-depth review of three areas for which EMVCo is now responsible: EMV chip cards, Near Field Communications (NFC) and Tokenization. This paper further looks at upcoming standards such as 3-D Secure 2.0 and Secure Remote Commerce (SRC) which, although not yet fully deployed, have the potential to significantly alter the U.S. payments landscape and have raised many questions and concerns among the U.S. merchant community.<sup>4</sup>

A very important editorial note: EMVCo calls their outputs specifications. Although we acknowledge EMVCo's desire to call their products specifications, we will use the term standards to refer to them because the manner these specifications are implemented, using rules established by the card

companies, makes them de facto standards. Because the entire U.S. industry must invest and comply with these specifications, EMVCo specifications, developed jointly with the card brands in an orchestrated strategy, are effectively standards.

The approach used for this research was twofold: First, using publicly available sources and insights from industry experts, we reviewed each standard, noting where and how EMVCo could have produced more open and inclusive standards that would have benefited the overall U.S. payments system. Next, our network of industry experts identified events and other developments that may have brought competition to the card companies and mapped their timing to decisions made by the card companies and EMVCo.

### 1.3 Organization

Part I includes this introduction, an executive summary, a review of standards and standards-setting organizations, and finally a high-level overview of EMVCo's organization and its specification development processes.

Part II includes an in-depth review of each of the standards for which EMVCo is currently responsible: EMV cards, NFC and tokenization. This in-depth review covers the standard's development process (to the extent that it is documented), discusses the market context in which the standard was developed, explores alternative approaches that would have better served the larger U.S. payments industry, and summarizes how each of these standards benefited the card companies at the expense of competitors, merchants, and consumers.

Part III reviews recently introduced, but not fully implemented, standards such as 3-D Secure 2.0 and Secure Remote Commerce that can significantly disrupt e-commerce and mobile commerce. We will outline the concerns that the U.S. payments community has with regards to these standards and how they can negatively impact the competitiveness

<sup>2</sup> For the 2012-2015 period card payments grew 7.7% by number and 6.5% by volume and, for the 2015-2016 period, they grew 7.8% by number and 6.3% by value

<sup>4</sup> As of the time of this writing, 3-D Secure 2.0 is slowly being adopted, primarily by U.S. merchants selling into Europe and Secure Remote Commerce has been installed at a small number of merchants under the commercial name of "Click to Pay"

Payment Insecurity  
How Visa and Mastercard Use Standard Setting to Restrict Competition and Thwart Payments Innovation

of payment solutions in the fastest growing segments of the U.S. economy

Part IV documents our conclusions that EMVCo is not an appropriate organization to develop standards that have such a massive impact on the U.S.

payments industry. Our research spotlights the nature of EMVCo as a mechanism for the card companies to collude on the delivery of standards that further their already entrenched market dominance.

## 2. EXECUTIVE SUMMARY

Understanding the U.S. payments structure and how it has evolved reveals how the card companies compete with other payment networks and how standards have become competitive weapons. The creation of standards is not just a technical matter — politics and market conditions are highly influential in the process, and EMVCo's ownership embeds its own business preferences into the standards-setting process. Because the United States has relatively few regulations with regards to payments (compared to other countries), and there is no governmental or quasi-governmental body that sets baselines for how payments should operate, EMVCo operates as the de facto body that establishes such standards.

Our research reveals an insidious pattern in which the card companies use EMVCo as a tool to maximize their share of transaction volumes: when the card companies feel threatened by competitive pressures or economic challenges, they — or EMVCo supporting their strategies — assume responsibility for the definition of a standard, which results in technical specifications that only benefit the card companies, not the U.S. payments industry at large. EMVCo is an armory for the card companies' arsenal of standards that have been repeatedly brandished against competing payment methods and against merchants' ability to route transactions through unaffiliated debit networks.<sup>\*</sup> This paper will show:

- How EMVCo supported Visa's 20-year-plus battle against unaffiliated debit networks, resulting in the implementation of less-secure chip-and-signature EMV cards in the United States rather than the more secure chip-and-PIN cards used elsewhere, limiting the competition that Visa and Mastercard could face from those networks. (Section 6)

- How EMVCo (with support of the card companies) adopted expensive, complex and difficult-to-implement technology such as NFC because it preserved the status quo for the card companies and protected their market share. (Section 7)
- That EMVCo decided to establish tokenization standards that excluded non-card payments, ignoring the work of other standards-setting organizations such as the American National Standards Institute or The Clearing House. EMVCo pushed aside calls for open standards and instead issued a tokenization standard that discriminates against unaffiliated debit networks (Section 8)
- How EMVCo ignored the work of other standards-setting organizations such as the Fast Identity Online (FIDO) Alliance and World Wide Web Consortium (popularly known as W3C) that were developing open authentication standards for both card and non-card systems. Instead, EMVCo is regressing to 3-D Secure, an old standard inherited from the card companies which EMVCo is trying to position as a global authentication standard. 3-D Secure 2.0, as this new standard is being called, is likely to introduce much friction during the checkout process and create obstacles for routing of debit transaction through unaffiliated debit networks. (Section 9)<sup>†</sup>
- That EMVCo has introduced the Secure Remote Commerce standard, which purports to become a new integrated checkout platform for online payment. Neither EMVCo nor the card companies have fully explained and justified the reason for

<sup>\*</sup> Unaffiliated debit networks, also known as EFT networks, ATM networks or PIN-based networks, includes networks that were established in the 1970s-1980s to manage automated teller machines and which later expanded into processing transactions at the point of sale using personal identification numbers or PINs. These include networks such as STAR, NYCE, Pulse, and others.

<sup>†</sup> The FIDO ("Fast Identity Online") Alliance is an open industry association with a focused mission: authentication standards to help reduce the world's over-reliance on passwords. The World Wide Web Consortium (W3C) is an international community where member organizations, a full-time staff, and the public work together to develop Web standards, and which includes the Web Payments Working Group whose charter is to make payments easier and more secure on the Web.

this standard. Secure Remote Commerce has the potential to be leveraged as competitive pre-emption tool that may limit participation from non-card company payment methods and to hinder merchants' ability to route transactions through unaffiliated debit networks, creating higher dependencies on the card companies and increasing merchants' payment processing costs, as well as potentially violating federal law for debit transactions. (Section 10)

The card companies claim to support open standards. In 2013, Visa's then-CEO Charlie Scharf responded to industry calls for more open standards by saying, "This is an area where everyone needs to work closely together and it's paramount that we ensure transparency, security and integrity so that the integrity of the payment system remains. ...It's got to be standards-based, technology-agnostic. It needs to address the needs of everyone globally, not just in the United States".<sup>4</sup>

Given what we have come to know, Scharf's words have proven to be disingenuous. EMVCo portrays itself as a technical specification development organization with no enforcement power over the card companies. Yet, the card companies *are* EMVCo. As will be shown in this paper, both EMVCo's executive committee and its management board are composed of long-term card company employees.

Accordingly, it is of little surprise that all its specifications and ensuing de facto standards are designed to meet the needs of the card companies rather than the U.S. payments system as a whole.

EMVCo standards help the card companies maintain their dominance in payment processing volume. They preempt the market by assuming responsibility for other standards, even seizing the work of more qualified standards-setters as their own. EMVCo provides credibility to the card companies' public calls for global payment security standards, all the while directing EMVCo toward standards that provide them with unfair advantages.

EMVCo uses the language of "compatibility," "interoperability" and "secure transactions" but these concepts are belied by EMVCo's own practices. This rhetoric is invoked even though EMVCo or the card companies routinely preempt competing standards and innovations in its quest to maintain EMVCo owners' dominance over the industry.

The next section, Section 3, is a historical primer for non-technical readers who might be unfamiliar with the granularity of payments industry maneuverings, both economic and political. People who are already familiar with the evolution of the U.S. payments industry since the 1980s may choose to rejoin this paper at Section 4.

### 3. HISTORICAL PRIMER

#### 3.1 U.S. Payments Framework

A payment is an exchange of value. For most people in the United States today, this is represented by money stored in checking or savings accounts at banks or through bank-issued credit lines in the form of credit cards.<sup>\*</sup> Banks give their customers payment instruments in the form of checks, credit or debit cards, or user IDs and passwords in order to access

Visa, Mastercard, American Express and other credit card networks. Debit cards and prepaid cards access checking or savings accounts either through Visa and Mastercard networks or through the many competing unaffiliated debit networks that operate in the United States such as STAR, NYCE and Pulse. Checks and routing numbers/bank account numbers access bank accounts through check clearing networks or the Automated Clearing House network.

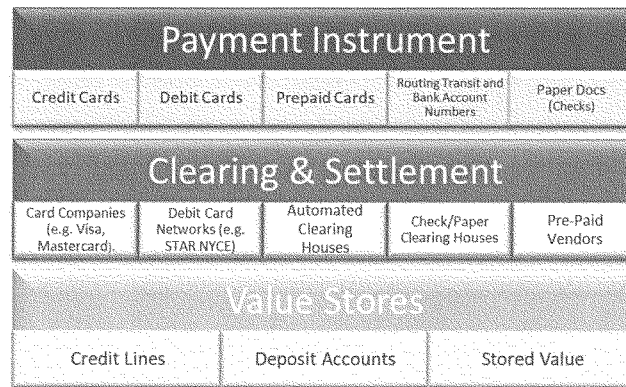


Figure 1 – RPGC's Payments Framework® explains how these components interact with each other

their money and credit lines. These instruments have numbers or other identifiers which are the payment credentials exchanged between payers and payees to initiate a payment.<sup>†</sup> To function properly, payment instruments need a clearing and settlement mechanism – a payment network – to deliver the required information to the appropriate parties and transfer funds between payment senders and receivers.

Depending on the instrument, payments are processed by accessing different networks. For example, credit cards access credit lines through

The network used to process the payment defines the standards for accessing it, its cost and the regulations that govern the behavior of the transaction. Thus, network choice is very important for merchants and financial institutions.

#### 3.2 The Need for Standards

Standards are needed for interoperability of bank-issued payment instruments among the networks. For example, checks need a standard representation of check information in a manner that can be read by

<sup>\*</sup> To be clear, consumers and businesses also have other stores of value such as retailer credit lines, stored value accounts, etc. This chapter is concerned only with bank accounts and bank credit lines.

<sup>†</sup> For clarification purposes, this paper uses the term *Payment Instrument* to refer to the device or form factor that carries the information allowing the initiation of a payment (e.g. a credit or debit card, a check, mobile phone)

other banks using automated machines.<sup>8</sup> Similarly, debit and credit cards need standards to be accepted by any automated teller machine or point-of-sale device so their information can be transmitted across multiple networks.<sup>9</sup> Thus, standards are critical in deciding who can participate in a payment network. This paper's operating principle is that standards that exclude certain payment instruments or prevent participants from routing payment transactions in a low-cost and efficient manner are not beneficial to the U.S. payments industry and in the case of debit transactions, may violate federal law. To the extent that standards result from a closed or collusive decision-making structure and exclude some participants or payment methods, then antitrust law and policy may be implicated.

### 3.3 Networks Compete for Transaction Volume

Payment networks – including those run by the card companies and others – compete for transaction volume. The more transactions that flow through a network, the more money and profits the network

makes. Because transactions that flow through competing networks do not typically generate revenue for the card companies, maximizing transaction volume is a matter of high priority for them.

The choice of the network processing these transactions also has significant financial implications to merchants and card issuers. The fee paid by merchants for accepting a payment card, sometimes referred as the “swipe fee” by the media, is split into three components: the merchants’ processor fees, the card companies’ processing fee and interchange which is usually the largest of the three fees that goes to the issuer of the card.<sup>10</sup> The interchange that issuers get when a debit card is routed through Visa and Mastercard is generally greater than the interchange fee they receive from the unaffiliated debit networks. As a result, the fees paid by merchants are greater when a debit card transaction is routed through Visa and Mastercard than when the same transaction is routed through the unaffiliated debit networks.<sup>11</sup>

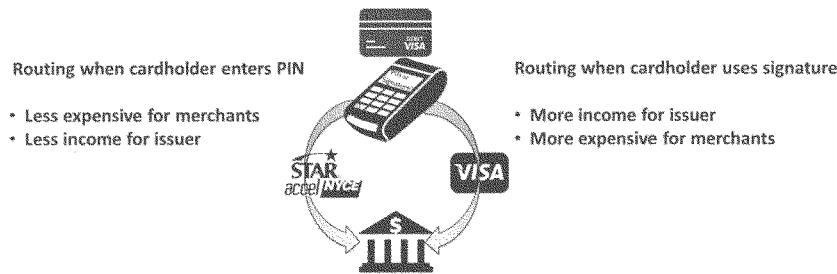


Figure 2 – Debit Card Routing Options

<sup>8</sup> U.S. banks began using the E-13B font developed by American Bankers Association for Magnetic Ink Character Recognition or MICR in 1958. This was adopted by the American National Standards Institute (ANSI) in 1963. MICR enabled checks must meet ANSI standard X9.27-1995 and ANSI X9.7-1990.

<sup>9</sup> Among others, payment cards must comply with ISO/IEC 7813 (properties of financial transaction cards, such as debit or credit cards) and ISO 8583 (a standard for financial transaction messaging for systems that exchange electronic transactions initiated by cardholders using payment cards)

<sup>10</sup> How interchange and is set is beyond of the scope of this paper. For a more detailed explanation of interchange and how network pricing works we recommend Darryl E. Getter paper “Regulation of Debit Interchange Fees”, Congressional Research Service, May 16, 2017, <https://fas.org/sgp/crs/misc/R41913.pdf>

<sup>11</sup> It should be noted that Visa and Mastercard also accept PIN debit transactions through their Interlink and Maestro networks. However, these networks are considered affiliated to Visa and Mastercard and they do not provide as much pricing differential to merchants as the networks considered to be non-affiliated.

To maintain market share and transaction volume, the networks run by the card companies historically have relied on massive marketing efforts that have made Visa, Mastercard, American Express and Discover household names in the United States and most of the rest of the world. Services such as PayPal also lean heavily on brand recognition to compete for transaction volume.

But the traditional competitors of the card companies – the unaffiliated debit networks as well as non-card payment networks such as the Automated Clearing House and paper-based systems – typically compete without major marketing campaigns. Furthermore, even though U.S. debit cards carry the brand of the debit networks, like STAR or NYCE, over which they can function, Visa and Mastercard require that their brands be featured more prominently on the cards. These practices leave the names of unaffiliated debit networks virtually unknown to most consumers, giving Visa and Mastercard a mindshare monopoly.

Since the 1990s the card companies, primarily Visa, have been engaged in an ongoing battle with the unaffiliated debit networks for transaction volume.<sup>5</sup> The card companies and the banks that issue their cards prefer routing through Visa and Mastercard because it generates more revenue for them. Merchants have preferred routing through the unaffiliated debit networks because of their lower processing fees. In addition, the unaffiliated debit networks offer the additional security option of requiring personal identification numbers, or PINs, to approve a transaction, while the Visa/Mastercard networks historically offered only the less-secure signature option.

Many experts and industry observers have argued that a secret PIN is a more secure authentication

method than an easily forged and often-illegible signature, and studies have shown that PIN can

substantially reduce fraud compared with signature.<sup>5</sup> While the chip makes it more difficult to create counterfeit payment cards, the National Retail Federation has noted that it does nothing to prevent the fraudulent use of lost or stolen cards. Enabling merchants' option to require the use of a PIN is necessary in order to realize the full advantages of chip cards as has been done in most other countries.

To increase their share of the growing debit market, Visa and Mastercard along with many of their card-issuing banks discouraged cardholders from using PINs. This had the desired effect of increasing transaction volume to Visa's and Mastercard's signature-only processing networks.<sup>6</sup> Further, many issuers had special routing arrangements with Visa and Mastercard that forced merchants to route debit transactions through Visa and Mastercard rather than through the less expensive and more secure PIN-based unaffiliated debit networks.

In 2010, the U.S. Congress passed the Wall Street Reform and Consumer Protection Act, which included a provision, known as the Durbin Amendment, to address rising debit card interchange fees. At the time, debit card interchange was a percentage of the transaction amount and nearly the same as credit card interchange, with an average of about 1.5 percent of the value of the transaction. The Durbin Amendment directed the Federal Reserve Bank to establish limits for debit interchange. These limits, embodied in Regulation II, cap debit interchange at 21 cents plus 1 cent for fraud protection plus 0.05 percent of the transaction amount. The cap, which took effect in 2011, meant that merchants – who were previously charged as much as \$1.50 to process a \$100 transaction – would typically pay about 25 cents regardless of the

amount of a transaction.

campaigns sacrificed payments security for higher revenue.

<sup>5</sup> Visa has the largest debit volume of all the card companies. Mastercard has smaller market share and all the other networks are predominantly credit card networks and do not compete for debit volume

<sup>6</sup> During the 1990s-2000s, many Visa and Mastercard issuers ran advertising campaigns calling for cardholders to "Skip the PIN, and Win!" in order to generate more interchange income, these



Payment Insecurity  
How Visa and Mastercard Use Standard Setting to Restrict Competition and Thwart Payments Innovation

This cap only applies to debit cards issued by banks with greater than \$10 billion in assets. These cards make up approximately 65 percent of all debit cards in the United States. Smaller banks and credit unions still get interchange based on a percentage of the transaction value, estimated at 1.16 percent for 2018.

In addition to limiting the ability of Visa and Mastercard to fix debit interchange fees, the Amendment also required that each debit card must be able to be processed over an unaffiliated debit networks – such as NYCE or STAR – in addition to the Visa/Mastercard networks. Under Durbin, the interchange received by the issuer is the same regardless of the debit network on which the transaction was processed. However, the unaffiliated debit networks offer lower rates for other processing-related fees as well as the option of more secure PIN authentication resulting in less fraud.<sup>\*</sup> Network choice is both basic and vital to merchants.

The Durbin Amendment was a massive blow for Visa because it moved significant transaction volume away from its network. Visa was under tremendous pressure from issuers and shareholders to regain that volume.

#### **3.4 EMVCo's Role in Supporting Card Companies' Recapture of Volume**

A few months before the Durbin Amendment went into effect, Visa announced its plan to roll out chip cards in the United States. This plan, the U.S. EMV Migration Plan, stated that signature would be the preferred cardholder verification method (referred in the industry as "CVM"). The plan was adopted by the other card companies shortly thereafter and was endorsed by EMVCo even though it delivered a less secure payment authentication method than PIN. EMVCo — despite its claimed commitment to deliver interoperability and acceptance of secure payment transactions — supported Visa's decision for signature authentication of purchases even as merchants and other industry stakeholders demanded PIN.

The Durbin Amendment took effect as the card companies were beginning the rollout of EMV "chip" cards, which culminated in October 2015, when merchants were required to have chip readers in

operation or face increased fraud responsibility. The chip card technical specifications established by EMVCo had embedded routing rules that, in combination with Visa's and Mastercard's operating rules, made it very difficult for merchants to route debit cards through unaffiliated debit networks, thus undermining the Durbin Amendment. Through this default setting, Visa and Mastercard could retain transaction volume that might otherwise have shifted to the unaffiliated debit networks.

Not surprisingly, EMVCo did little to address this problem. Instead, the EMV Migration Forum, a cross-industry group, came up with a solution that allowed merchants to recognize and route debit cards through unaffiliated networks. Visa's response to this solution was to require merchants to display to consumers a choice between "Visa Debit" and "U.S. Debit" at checkout. Merchants opposed the Visa requirement because it gave consumers a choice between an unknown name and a familiar name with greater consumer mindshare, likely prompting most consumers to choose the Visa network (this topic is discussed more thoroughly in Section 6.5).

Later, mirroring its attempt to direct payment traffic through the chip-and-signature implementation, EMVCo introduced standards for tokenization that also created obstacles for routing debit card transactions through unaffiliated debit networks (Sections 8). The EMVCo tokenization standard is not based on open standards. The standard does not allow tokenization interoperability among different types of networks and makes it difficult for merchants to choose where tokenized transactions are routed. Worse, no provision was made for the tokenization of bank accounts or any other competing payment method. While these examples are particular to tokenization, they merely represent a small part of EMVCo's pattern of boosting card companies' volumes while hindering that of their competitors at the expense of the security of the entire payments system.

<sup>\*</sup> Visa and Mastercard support PIN transactions through their Interlink and Maestro networks but these are more expensive to the merchants than the unaffiliated network. Even today, the preferred choice for the Visa and Mastercard is to route debit transactions via their signature debit networks

#### 4. WHAT IS A STANDARD?

According to the World Trade Organization, a standard is “a document established by consensus that provides rules, guidelines or characteristics for activities or their results.”<sup>6</sup> The now-defunct U.S. Office of Technology Assessments issued a study called “Global Standards: Building Blocks for the Future,” which said “how standards are set is a matter of some concern because the economic and social stakes in standards are so large. The standards development process must be fair to prevent any single interest from dictating the outcome.”<sup>7</sup> Economists see standards as contributing to public welfare by improving economic efficiency.<sup>8</sup> Most standards-setting organizations agree that to achieve these goals, all stakeholders should participate in the development of the standard, the process should be transparent and that information should be openly shared.

Economist Edwin Mansfield calls standards “impure public goods” and emphasizes why it is important that they be developed with a broad stakeholder input:

*Other goods, like education and standards, are impure public goods. These combine aspects of both public and private goods. Although they serve a private function, there are also public benefits associated with them. Impure public goods may be produced and distributed in the market or collectively through government. How they are produced is a societal choice of significant consequence [emphasis added].... If decisions about impure public goods are made in the market, on the basis of [corporate] preferences alone, then the public benefits associated with them may not be efficiently produced or equitably distributed.<sup>9</sup>*

As Mansfield shows, privately set standards impact public wellbeing. While there is nothing inherently wrong with private consortia standards, they cause societal harm when they become unfair or biased. For this reason, it is paramount to the U.S. payments

industry that a recognized standard-setting body replace the EMVCo which sets standards for the benefit of the card companies.

##### 4.1 Open Standards-Setting Organizations

There are many better-suited organizations to which EMVCo's work could be migrated. In fact, it is likely that the U.S. payments industry and consumers would be better served if different open standards bodies specialized to do the type of work in question.

For instance, the private, non-profit American National Standards Institute or ANSI provides all interested U.S. parties with a neutral venue to work toward common agreements developing U.S. standards. ANSI has an Accredited Standards Committee responsible for developing voluntary open consensus standards for the financial services industry, known as ASCX9. This group has developed a standard called “Protection of Sensitive Payment Card Data - Part 2: Tokenization.” This standard, also known as X9.119-2, defines minimum security requirements for implementing tokenization with post-authorization systems to protect sensitive payment card data. As such, ANSI's ASC X9 would be a clear candidate to create and maintain open tokenization standards.

New organizations have been established in last decade that address e-commerce and mobile commerce authentication standards. The FIDO Alliance and W3C are industry consortia currently developing open interoperable authentication standards. Although EMVCo claims to work with these organizations, there have been few, if any, deliverables resulting from these cooperation efforts.

These organizations — ANSI, ISO, IEC, W3C and the FIDO Alliance — have consistent approaches to developing standards: open, inclusive, balanced, not dominated by a single-interest category, and consensus-driven. To reaffirm their commitment to open standards, W3C, the Internet Engineering Task Force and the Institute of Electrical and Electronics Engineers Standards Association signed an

agreement to adhere to a set of principles in support of a “modern paradigm for standards.” The principles include cooperation, due process, broad consensus, transparency, balance, openness, collective empowerment, availability and voluntary adoption. EMVCo does not follow any of these principles.

#### 4.2 EMVCo: from Consortium Specifications to De Facto Standards

Financed by its member owners, EMVCo is not subject to public oversight, nor is it required to keep records of proceedings during the creation of its standards. It is therefore difficult to obtain systematic information about these processes. Since EMVCo does not offer decision-making roles to other industries, its perspective is biased toward the card companies.

EMVCo asserts that it uses “its own approval and decision-making processes, [and thus] operates separately from the international payment systems which own EMVCo.”<sup>10</sup> This is misleading – EMVCo is heavily influenced by its member-owners. There is a long history of card companies developing technologies and turning them over to EMVCo for legitimization as standards. EMVCo says that it is the card companies that “assume the role of defining and issuing products and enforcing EMV compliance for products that carry their respective brands.”<sup>11</sup> But trying to differentiate specifications from implementation is a distinction without a difference.

Card companies build products in lockstep to implement the specifications that they themselves designed, usually led by Visa. The member-owners implement these specifications consistently and synchronously, making them de facto standards for the United States and other markets in which the card companies’ global payment networks dominate.

#### 4.3 Comparing EMVCo with Open Standards-Setting Bodies

Global private regulation has become vastly important in recent decades and is now a phenomenon of considerable social and economic consequence.<sup>12</sup> Outcomes notwithstanding, standards set by consortiums using open processes will always be preferable to closed ones. Though EMVCo’s private standards may appear to be irrelevant to broader economic health, payment cards dominate the U.S. payments marketplace to such an extent that these standards negatively impact competition and payments security. Figure 3 shows a comparison between EMVCo and other standards-setting bodies such as W3C and ANSI in terms of membership, mission and decision-making authority.

EMVCo’s standards-development process is a closed system operating without any accountability to stakeholders in the U.S. payments system. In contrast with other standards-setting organizations, which advocate openness and inclusivity, EMVCo decisions are effectively made by its six owners, and

	W3C	ANSI	EMVCO
Is active membership (i.e. not just in an advisory capacity) open to all?	Y	Y	N
Is mission and work defined and agreed to by all participating members?	Y	Y	N
Are decision making roles available to all participating members?	Y	Y	N
Are meetings and proceeds documented and open to public review?	Y	Y	N
Are members specialized in the specific technical areas where they contribute to standard development?	Y	Y	Primarily Chip Cards
Appeals process open to all members to resolve differences in standard?	Y	Y	N

Figure 3 – Organizational and Decision-Making Comparison between W3C and ANSI and EMVCo

Payment Insecurity  
How Visa and Mastercard Use Standard Setting to Restrict Competition and Thwart Payments Innovation

generally dominated by Visa and Mastercard. Despite claiming to work with other standards-setting bodies, EMVCo sets standards that can only be met by products that were developed by the card companies. Worse, EMVCo has used the guise of global interoperability to co-opt or preempt work being performed by other standards-setting bodies.

The impact of the lack of multi-stakeholder representation in EMVCo is real and measurable. In the United States, the payments industry spends millions of dollars every year complying with

standards set by EMVCo and implemented by the card companies as de facto standards. This high level of investment prevents the use of capital to innovate or develop other alternative payment methods. The fact that a standard is enforced by default does not imply it is serviceable, let alone the best.

## 5. THE EVOLUTION OF EMVCO FROM 2007 TO 2019

In October 2007, EMVCo published a white paper titled “The Role and Scope of EMVCo in Standardizing the Mobile Payments Infrastructure,” which stated:

*There is an increasing need for EMVCo to address and resolve a number of technical infrastructure issues associated with enabling contactless proximity payments via mobile phone handsets. This “technical development” responsibility is in line with EMVCo’s traditional role within the payments industry as a technology standards body [emphasis added].*

EMVCo’s “traditional” background and expertise at that point were in chip card deployment, not mobile payments. However, in this paper EMVCo claimed that it should be “the common voice of the payments industry ... [assuming] the central role in defining the requirements” for technologies beyond chip cards and presaged greater ambitions. In 2013, EMVCo appointed itself as facilitator of “worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV specifications and related testing processes.”<sup>13</sup>

With this expanded scope, EMVCo sought to establish itself as the master and arbiter of all payments technology.

### 5.1 EMVCo Organization and Decision Making

EMVCo started without any permanent staff. All working groups were led by representatives from the participating card companies, an arrangement that has changed little over time.

Since its inception, EMVCo has been run and operated by its Board of Managers with equal representation from each of the card companies. As it deems appropriate, the board delegates work items, functions and responsibilities to working

groups. The Executive Committee provides strategic focus to the board but makes the ultimate decisions.

There is also a Board of Advisors made up of organizations that have an interest in the specifications; most of them processors or technology companies. These are organized as business associates, technical associates, and subscribers. As of July 1 2019, only five out of the 59 EMVCo business associate members were non-payment companies and only one was a traditional merchant. Similarly, only three out of 69 EMVCo technical associate members were not payment companies.<sup>14</sup> Notably, associate members do not have any decision-making power. Figure 4 visualizes EMVCo’s entity organization and decision-making process.

<sup>13</sup> To see the current list of both business and technical associates, visit <https://www.emvco.com/get-involved/business-associates/> and <https://www.emvco.com/get-involved/technical-associates/>

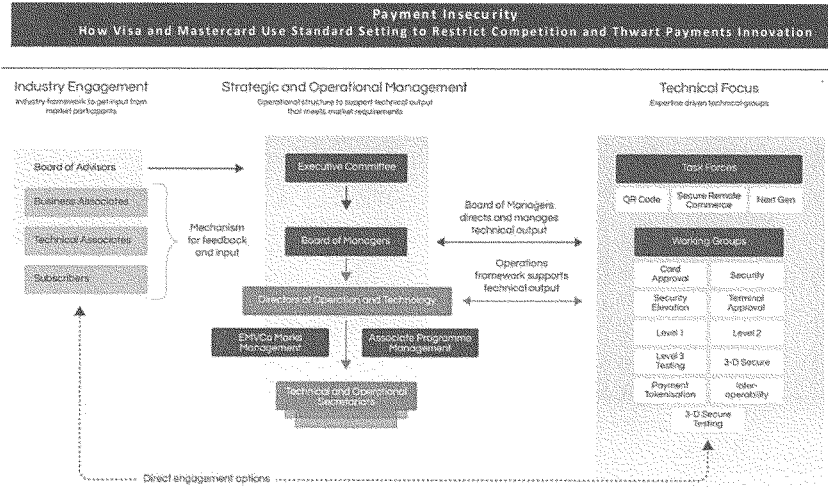


Figure 4 – EMVCo Organizational Structure - 2019

### 5.2 EMVCo Staffing

Executive Committee members and all Board of Managers members are long-term employees of the card companies. Using publicly available information, we identified several recent chairs of the EMVCo Executive Committee and their respective areas of expertise (Figure 5)<sup>7</sup>. The chart

identifies lifelong card company employees with narrow technical expertise who speak under the

pretext of being the “common voice” of the payments industry.

A similar story was found when looking into the background of the current EMVCo Board of Managers (Figure 6), where, again, all members are

long-term employees of the card companies. Given interviews.

Name	Period	Employment Company and Length	Experience in
Kartek Patel	2019	17 years with Visa	Processing and Product
Stephanie Ericksen	2018	24 years with Visa	Technology, Chip cards, Risk, Operational Resilience
Jack Pan	2017	3 years with Union Pay and 6 years with Visa	Chip cards
Dave Meadon	2013	17 years with Mastercard	Technology, chip cards
Jim Lee	2011	11 years with Visa and 8 years with JCB	Smartcards and contactless technologies
Tad Fordyce	2009	16 years with Visa	B2B, corporate cards, loyalty, risk and business intelligence products

Figure 5 – Selected EMVCo Executive Committee Chairs 2009 through 2018\*

<sup>7</sup> EMVCo does not publish an official list of its Executive Committee Chairs nor the length of their tenure. The list presented was compiled from public sources such as press release and media

Payment Insecurity  
How Visa and Mastercard Use Standard Setting to Restrict Competition and Thwart Payments Innovation

this organizational structure, it is fair to ask where

<sup>†</sup> EMVCo's website reports that the Board of Managers consists of two representatives from each owner company



Payment Insecurity How Visa and Mastercard Use Standard Setting to Restrict Competition and Thwart Payments Innovation			
Name	Company	Employment length	Experience in
Christian Aabye	Visa	17 years	Systems Architecture
Robert Burns	Amex	27 years	Technical Architecture
Dhaval Chauhan	Discover	5 years (+ 6 years with Visa)	Mobile payments
Sean Conroy	Amex	32 years	Product Development Chip
Cheryl Mish	Discover	18 years	Payment Security
Jonathan Main	Mastercard	17 years	NFC & mobile devices
Jianhua Ni	Union Pay	1 year (10 years with UL)	Smart cards
Masao Noda	JCB	> 10 years	Chip cards
Jack Pan	Union Pay	3 years (6 years with Visa)	Chip cards
Mark Rigby	Visa	14 years	Chip cards
Patrik Smets	Mastercard	NA	Telecom h/w and s/w design
Junya Tanaka	JCB	17 years	Chip cards

Figure 6 – EMVCo's Board of Managers Members – Early 2019

the allegiances of these individuals lie with regards to their own organizations as compared with the broader charter required of a true industry standards-setting body. By design, EMVCo's Board of Managers is not set up to be impartial third-party experts, instead they are there to represent their company's respective interests.

Perhaps the biggest concern regarding EMVCo as a broader standards-setting body is its failure to include any other stakeholders in its governance structure. Figures 5 and 6 show that there are no other payments industry representatives with extended exposure to any other payment method on either the board or the Executive Committee.

Standardization leader Carl F. Cargill writes that the creation of standards assumes that participants follow rational economic models in their decision making. Yet, he also recognizes that all standard-setting participants are human beings that bring with them their individual backgrounds and biases – professional pride, organizational goals and interests, personal friendships – and this makes standard creation a non-rational human being activity.<sup>14</sup>

With that in mind, our intent in naming the above individuals is not to suggest that they are acting unprofessionally or to attack them personally. Our

intent is to demonstrate that EMVCo lacks the neutrality required to develop industry standards through an open, inclusive structure.

Further, EMVCo has refused to work with open standard-setting bodies despite claims that it engages with “other relevant industry bodies.”<sup>15</sup> EMVCo has been asked, for example, to include bank account numbers and other forms of payments in the tokenization standard but still limits the standard to work only with products from the card companies.

### 5.3 Conclusions

Since its 2007 overreach into mobile payments, EMVCo has continued to demonstrate that it is not designed to develop, nor capable of developing, open standards. Its “closed” standards have repeatedly failed to properly address ongoing challenges to payment security and inclusivity at a time when collaborative and competitive standards will be needed to innovate, and most immediately, keep up with upcoming industry developments such

Payment Insecurity  
How Visa and Mastercard Use Standard Setting to Restrict Competition and Thwart Payments Innovation

as open banking or “push” payments.<sup>7</sup> Given its organization, staffing, areas of expertise, internal policies and inclinations, it is unlikely that EMVCo can

ever truly be a neutral technology standards body let alone “the common voice of the payments industry.”

<sup>7</sup> Open Banking is a concept being implemented in Europe under the second Payments Services Directive (PSD2) that requires all banks to open APIs to allow accredited Payment Initiators (e.g. merchants, Payment Service providers, etc.) access bank accounts bypassing the card companies; “push” payments are customer-initiated payments where the consumer send payment for goods and services to merchants, sometimes in real-time, using a non-card payment

Payment Insecurity  
How Visa and Mastercard Use Standard Setting to Restrict Competition and Thwart Payments Innovation  
network such as ACH or a Real Time Payment service.

## PART II—STANDARDS REVIEW

This part contains an in-depth review of each of the standards for which EMVCo is currently responsible: EMV cards, near field communications and tokenization. This review covers each of these standards' development process (to the extent that it is documented), the market context in which the standard was developed, explore alternative approaches that would have better served the larger U.S. payments industry and how each of these standards benefited the card companies at the expense of competitive networks or methods of payment.

### 6. EMV CHIP AND PIN (OR SIGNATURE)

#### 6.1 Background on Chip Cards and Risk Management

Prior to the late 1980s, merchants who accepted credit cards were required to telephone a call center to obtain voice authorization if a transaction was above a certain amount, called the "floor limit."<sup>2</sup> Merchants also had to check a bulletin that listed all reported lost and stolen credit card numbers and could accept a transaction only if the card presented was not in the bulletin. Because bulletins were only updated monthly, thieves had plenty of time to use stolen cards before merchants could be notified. Further, merchants were not equipped to detect forged credit cards despite security features introduced to protect them such as holograms or micro-printing.

To address escalating fraud in the United States, Visa and Mastercard moved to electronically authorize every transaction and eliminate the floor limit practice of exempting those below a certain dollar amount. This process is still in use today. Cards are swiped or inserted in a reader and the information

contained in the magnetic stripe or chip is transmitted via telephone lines or over the internet through the Visa or Mastercard networks, to the card issuer for authorization.

The information transmitted contains certain data elements that allow the authorization center to

determine, with a reasonable degree of certainty, whether the card presented was forged or reported as lost or stolen. It is critical that a robust and inexpensive telecommunications infrastructure be in place for this approach to work, and the United States had such infrastructure in place at that time.

In Europe, however, a similar approach was not practical due to higher telecommunications costs and lower reliability. Instead, local card companies developed cards enabled with an integrated circuit or chip that could verify the authenticity of a card without the need for a telephone or internet connection. The results were impressive and offered a better alternative to Visa and Mastercard's magnetic-stripe cards. The Carte Bancaire chip card program deployed in France caused fraud to drop from 0.27 percent in 1987 to 0.03 percent in 1995. Similarly, the U.K.'s Association for Payment Clearing Services created the Plastic Fraud Prevention Forum and ran several successful chip-and-PIN trials demonstrating that local card companies were perfectly capable of developing standards for chip

cards as a fraud management tool.

In order to protect market share from local card networks, Visa, Mastercard and Europay (which later merged into Mastercard) developed initial technical specifications for smart, secure computer chips that could run verification routines when used in conjunction with PINs. Field trials began in 1996 and,

<sup>2</sup> The term "credit card" is specifically being used in this section, as in those days, debit cards operated in completely different networks and were protected by PINs. The level of fraud on those cards was a fraction of what banks were experiencing in credit cards. For this reason, credit cards implemented strategies like "floor limits" and

Payment Insecurity  
 How Visa and Mastercard Use Standard Setting to Restrict Competition and Thwart Payments Innovation  
 "voice authorizations" while debit cards did not.

after successful testing, the first production specification for chip cards was published in 1998. EMVCo was established shortly thereafter.

EMVCo developed standards for chip cards that could work with credit, debit and stored-value cards such as gift cards. In countries that had a national PIN debit network, chip-and-PIN was EMVCo's preferred approach for verifying transactions. But to accommodate countries that did not yet have a robust PIN-debit network such as Russia, China and India, EMVCo compromised and offered the signature option in order to discourage growth of local chip-based card systems and to ensure growth in its members' transaction volumes.<sup>16</sup> So when the card companies took over the role of standards-setting for chip, their motives were clearly rooted in market power, not security.

By 2010, U.K. counterfeit card fraud rates had

declined 63 percent following the implementation of chip-and-PIN in 2004.<sup>17</sup> In France, also using chip- and-PIN, the fraud rate from domestic in-person transactions fell by over 50 percent from 2004 to 2009 to 0.01 percent. However, these markets also saw a migration of fraud to online commerce and remote purchases channels as well as to cross border transactions where cards issued in these countries were forged and used in countries without EMV deployment. Clearly, chip-and-PIN had helped reduce fraud rates, but all innovations from local card companies were edged out by EMVCo.

#### **6.2 Introduction of Chip Cards in the United States Delayed by Lack of Business Case**

Even as chip cards were being rolled out around the world and fraud numbers were being brought under control, the United States remained embroiled in a debate about whether to implement them. Carl Pascarella, then president and CEO of Visa U.S.A. Inc., testified at a 2001 trial in an anti-trust case brought by the Department of Justice against Visa and Mastercard that Visa U.S.A. had "not been able to find a cogent business case or business model" in

favor of the chip card.<sup>18</sup> The massive costs involved in converting the U.S. market to chip cards was many times the cost of fraud at the time. This reasoning kept chip cards out of the United States until industry stakeholders voiced concerns in the mid-2000s that the United States was "falling behind."

Still, even as late as 2008, mainstream bankers were skeptical of rolling out chip cards in the United States. Don Rhodes, director of risk management policy at the American Bankers Association, stated that because of the "cost associated with replacing all the checkout terminals ... and ... because the cost of fraud in the United States is manageable, there is little incentive to change." He continued, "I don't think, based on my discussions with big banks that issue most credit and debit cards, or with card associations, that they envision rolling out so-called

chip-and-PIN in the U.S. today." Thus, even though

the United States led the world in card fraud at the time, the card companies and their issuers did not feel it was in their best business interests to introduce chip cards at that time.

#### **6.3 Visa and Mastercard Compete with Debit Networks**

2010 marked nearly 20 years of battle for debit transaction volume between the card companies, primarily Visa and Mastercard, and the unaffiliated debit networks such as STAR, NYCE and Pulse. Before chip cards, Visa and Mastercard had other strategies for directing debit card transactions to their networks. They introduced their own debit card products, and in 1991 Visa acquired the Interlink debit network. Under its new ownership, Interlink raised interchange fees, driving up costs for merchants but making the network more attractive to banks, which could receive higher revenue from transactions processed over Interlink than they would from transactions on other debit networks. The other debit networks also had to raise their own rates to remain competitive, making banks happy

<sup>16</sup> In 2005 Sberbank in Russia launched its proprietary chip-based scheme called Sberkart which it scuttled in 2010 and replaced it instead with EMV compatible Universal Electronic Cards (PRO100).

Payment Insecurity  
How Visa and Mastercard Use Standard Setting to Restrict Competition and Thwart Payments Innovation  
which itself was scrapped in 2015 for the new Russian payment system Mir.

but driving up costs for merchants and, ultimately, consumers.

During the 2000s, and strictly for revenue motivations, banks issuing Visa and Mastercard cards discouraged cardholders from using a PIN for debit card purchases and encouraged them to sign instead. These campaigns were generically called “skip the PIN and win.” In addition, Visa and Mastercard began signing exclusive routing agreements with card issuers requiring merchants to route all their debit card transactions through Visa and Mastercard, further locking in their respective debit market shares.

In 2011, the Durbin Amendment went into effect and banned exclusive routing agreements between card issuers and networks. It required issuers to allow their debit cards to be routed through at least two unaffiliated networks. While the affiliations were technology-based—signature debit versus PIN debit—the distinction signaled was also a branded one: Visa and Mastercard versus the unaffiliated debit networks.

This battle over debit transactions was vital to both groups, as debit card use had overtaken credit card use by 2008. Further, the financial crisis of 2008-2010 significantly reduced credit card use because of consumers’ concerns over increasing their debt.<sup>20</sup> Pulse’s 2010 Debit Issuer Study found that between 2008 and 2009, the use of PIN debit, largely handled

by the unaffiliated debit networks, grew by 13% with an average ticket size of \$41 while signature debit

transactions, at that time exclusively handled by Visa and Mastercard, increased by 9% with an average ticket of \$35.<sup>21</sup>

The provision of the Durbin Amendment that required all debit cards to have at least two unaffiliated networks, along with the new rights given to merchants to decide how to route a transaction (also called “merchant routing rules”) had an immediate effect. Interlink volume dropped 54 percent and large debit card issuers saw their

average debit card interchange drop from about 44 cents for a typical transaction to 24 cents.

PIN posed an existential threat to Visa and Mastercard’s relationships with their largest issuers. Under Durbin, regulated banks (those with over \$10 billion in assets) would get the same interchange from a debit card transaction regardless of the network used. Issuers’ cost and assessments, however, are generally higher for Visa and Mastercard than for debit networks. Thus, a rational issuer – given the same income from a transaction – would prefer networks that deliver the transaction at a lower cost. PIN was Visa’s and Mastercard’s enemy because it allowed other networks to compete successfully with Visa and Mastercard for debit transaction volume.

It was within this context that Visa announced its EMV migration program in August 2011.

#### 6.4 Visa Launches Its EMV Migration Plan

Just a few months prior to the Durbin Amendment going into effect, Visa launched its EMV Migration Plan for the United States. That was followed shortly by similar announcements from the other card brands. Surprisingly, given the precedent of requiring PIN in other countries, Visa indicated that its U.S. EMV chip cards would cardholder verification methods, including signature, PIN, and no-signature for low value, low risk transactions rather than chip-<sup>22, 23</sup>

and-PIN as deployed in many other countries. All other card brands followed this guidance.

This decision was beneficial to Visa and Mastercard. Under the EMVCo standard, the point-of-sale device uses an “application identifier”<sup>\*</sup> to route transactions according to information encoded in the chip. The AID is used by the POS to select the application that contains the rules governing the

<sup>\*</sup> Application Identifier, or AID, refers to information contained in the Chip. This information includes ways for the POS to identify what



Payment Insecurity  
How Visa and Mastercard Use Standard Setting to Restrict Competition and Thwart Payments Innovation  
kind of card is being used, as well as procedure for routing it.

transaction.<sup>\*</sup> AIDs are registered with EMVCo and this information is distributed to all POS device manufacturers to code into their terminals as well as to issuers and card manufacturers. At the time of the announcement, there was no AID for unaffiliated debit networks, meaning that all debit card transactions had to be routed through Visa and Mastercard.

#### 6.5 EMV Preventing Merchant Choices in Debit Card Routing

The proposed EMV migration plan immediately brought to light a major conflict with Durbin's debit card routing regulations. The United States has over a dozen unaffiliated debit networks and some issuers belong to multiple networks to cover different geographic areas; often they change debit network affiliations. Encoding an AID for every network into every card was not practical. Cards would have to be re-issued each time an issuer changed its network affiliation, and the testing and certification process for POS manufacturers would have been lengthy and expensive. The inability to do so under the EMV chip system minimized the number of debit transactions that could be steered to the debit networks, benefitting Visa and Mastercard. Visa's initiative to launch chip cards in the United States threatened to circumvent the Durbin Amendment's requirement for unaffiliated network routing.<sup>†</sup>

Most countries have only one domestic debit network so, encoding an AID for a single debit

network is easily done but this was complicated by the number of debit networks in the United States. EMVCo was unable and unwilling to resolve the lack of a debit AID because EMV was never designed for the U.S. market. The EMV Migration Forum — a multi-stakeholder industry association formed to

support the U.S. migration to chip technology — appointed itself to resolve the chip debit card problem, resulting on an inelegant solution: the "Common Debit" also called the "U.S. Debit" AID.

The U.S. Debit AID is encoded into every U.S.-issued debit card, which aggregates all the debit networks not affiliated with Visa and Mastercard into one single application.<sup>‡</sup> Importantly, because Visa and Mastercard are on both the Global AID and on the U.S. Debit AID, effectively double-dipping, they can also handle the debit card transaction. For merchants to retain their routing choices they must program their POS devices to select the unaffiliated debit-routing option, but this is far from an ideal solution.

Visa fought back, requiring issuers to prioritize the Visa proprietary AID over the common AID and then demanding that consumer make a choice at the POS between "Visa Debit" and "U.S. Debit." Selecting "Visa Debit" would override merchant routing choice and send the transaction to Visa, while selecting "U.S. Debit" would allow the merchant to route to any network enabled on the card, including Visa. Obviously, consumers had no knowledge about the ramifications of this selection, nor should they need to. Given that the choice between a widely recognized global brand backed by extensive marketing and a name not known or trusted by consumers, these demands highlighted what was important to Visa: steer debit card traffic back to

Visa.

Visa's activities asking card issuers and point of sale providers to prioritize its proprietary AID as well as lobbying regulators to mandate consumer choice at the point of sale has given Visa a head start recovering some of its lost debit volume. Ultimately,

<sup>\*</sup> For example, Maestro has an AID of A0000000043060 whereas a Mastercard credit or debit has an AID of A0000000041010 and Canada's Inerac has an AID of A0000002771010. This allows the POS device to identify which application it is to work with. The application defines the characteristics of a transaction indicating, for example, what type of Cardholder Verification Method is required from the Cardholder.

<sup>†</sup> Visa's initial intention was to require exclusivity on the chip, relegating the debit networks to the less secure magnetic stripe but this was deemed non-compliant by the Board of Governors of the Federal Reserve System — <https://www.federalreserve.gov/paymentsystems/regii-faqs.htm> — Q1 under Sec. 235.7

<sup>‡</sup> As noted earlier, Visa operates the Interlink network and Mastercard operates the Maestro network, both PIN-based networks, but these are considered "affiliated" for the purposes of Durbin compliance.

<sup>§</sup> US Debit was chosen because the individual debit networks had to

Payment Insecurity  
 How Visa and Mastercard Use Standard Setting to Restrict Competition and Thwart Payments Innovation  
 share the U.S. Common Debit AID.

the Federal Trade Commission opened an investigation into the matter, and the Federal Reserve again issued an FAQ clarifying that Visa's activities violated the law, so the battle continues even today as merchants fight to enforce this right.<sup>6</sup>

#### 6.6 EMVCo Failures with EMV Chip Cards

In implementing chip cards in the United States, EMVCo unequivocally failed at its mission to "facilitate worldwide interoperability and acceptance of **secure payment transactions** (emphasis added) by managing and evolving the EMV specifications and related testing processes." It betrayed its own principles by acquiescing to a less-secure verification method by accepting signature as the cardholder verification method. In addition, all payment credentials remained in-the-clear rather than encrypted during the card-to-POS exchange. That meant that the EMV chip cards were not compliant with requirements set by the Payment Card Industry Security Standards Council, another organization dominated by the credit card companies that sets credit and debit card security

standards.<sup>7</sup>

Furthermore, EMVCo failed to protect the interests of all stakeholders in the U.S. payments industry by agreeing to an aggressive timeline established by Visa which was quickly adopted by the other card companies<sup>24</sup>. Its accelerated timing was surprising considering that it required large monetary investments by merchants and issuing banks at a time when the United States was just recovering from one of the worst financial recessions in its

history. Visa gave the U.S. payments industry — one of the most complex, if not the most complex payments system in the world — just over four years to accomplish the massive switch from traditional magnetic-stripe credit cards to chip-based EMV cards. Without any other stakeholders at the table to provide other perspectives, EMVCo went along with the plan.

EMVCo's mismanagement of the certification process also led to delays in EMV terminal certification and deployment, with some merchants saying they waited six months or more for certification of EMV chip card readers they had installed. Without the installations certified, merchants were open to — and suffered — increased fraud liability the same as if they had not installed the equipment at all. And some unscrupulous card-issuing banks allegedly took advantage of the absence of certified chip readers to issue "chargebacks" of transactions against merchants even if the cardholder had not complained of a fraudulent purchase, costing merchants millions of

dollars.

Visa's and Mastercard's choice of signature debit over PIN debit meant that generating transaction volume was more important than payment security, prioritizing their business interests over the security of the U.S. payments ecosystem. Clearly, EMVCo was a tool used by the card companies to help promote their own strategic objectives to capture market share and increase income.

<sup>6</sup> In 2016 Kroger Co. sued Visa alleging that Visa threatened Kroger with fines and possibly the loss of the ability to accept Visa debit cards due to its plans for its point-of-sale configuration that would have diverted transactions from Visa's payment network. Visa denied those accusations and the lawsuit was settled out of court in August, 2019, <https://www.bizjournals.com/cincinnati/news/2019/08/05/kroger-visa-settle-lawsuit.html>

<sup>7</sup> Payments Card Industry/Data Security Standards (PCI/DSS) is an information security standard for organizations that handle branded credit cards from the major card companies. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council

<sup>24</sup> At a 2016 EMV Migration Forum meeting, a Texas based bank reported they had made \$18 Million in chargebacks since liability shift as "Visa had predicted" in a presentation made a few years earlier when banks were looking to Visa for financial remuneration

Payment Insecurity  
 How Visa and Mastercard Use Standard Setting to Restrict Competition and Thwart Payments Innovation  
 after losing nearly half their debit interchange.



## 8. NEAR-FIELD COMMUNICATION

### 8.1 Background

Near-field communication is a technology used in manufacturing, retail and transportation to convey information between two electronic devices in a wireless manner over a short distance, typically just a few inches. Many organizations were involved in setting the underlying standards and data exchange protocols including the International Standards Organization, the International Electrotechnical Commission, the GSM Association and the NFC Forum. The NFC communications protocols were developed by open standards setting bodies and are articulated in ISO/IEC 18092.

NFC began to be used in payments in the late 1990s and early 2000s. Devices and services including Vivo, Bling Nation, the London subway system's Oyster card, Mobil Oil's Speedpass keychain for paying for gasoline at the pump, and contactless PayPass cards from Mastercard and payWave from Visa, used NFC chips to be tapped, touched or waved at NFC-equipped readers. Around 2005-2007, several companies began to incorporate payment functionality into mobile phones by attaching NFC tags to them or by inserting Subscriber Identification Module (SIM) cards with the NFC information. Visa and Mastercard became involved in early pilots to experiment with these new innovations.<sup>\*</sup> Nonetheless, one of the outcomes from these pilots was that the card companies soon saw the risk of lost

revenue as these new products were based on stored value accounts or set up to directly access bank accounts bypassing the card companies' networks.

<sup>\*</sup> In 2007 Royal Bank of Scotland launched a "Tap-and-Go" program in partnership with Mastercard in the UK whereas in Atlanta's Philips Arena, NFC developer Philips, Chase, ViVOtech, Cingular and Nokia ran a test in partnership with Visa USA.

<sup>†</sup> These documents include EMVCo Mobile Contactless Payment – Technical Issues and Position Paper (2007), EMVCo Mobile Proximity Contactless Payment FAQ#1 (2008), EMVCo Contactless Mobile Payment Application Activation User Interface (2010), and EMVCo Contactless Mobile Payment Architecture Overview (2010).

### 8.2 EMVCo Entering Mobile Payments

In October 2007, EMVCo published a white paper titled "The Role and Scope of EMVCo in Standardizing the Mobile Payments Infrastructure," in which EMVCo designated itself as the "representative of the global payments community" and the "common voice of the payments industry on mobile contactless proximity payments standardization." In this paper, EMVCo gave itself the role of definer of standards for mobile contactless payments infrastructure and to consolidate industry standardization efforts.

This was the first time EMVCo looked at enabling payment devices beyond cards and represented the organization's first foray into NFC. During 2007-2010, EMVCo published NFC-related documents that provide insight into EMVCo's continued evolution from a self-appointed standards-setting organization to an instrument to pre-empt the market on behalf of its owners.<sup>†</sup>

The 2007 paper said EMVCo members had agreed "to allow and support the presence of multiple brands, multiple issuers and multiple payment instruments on the same mobile device" to conduct mobile contactless payments regardless of whether the mobile device used a single "secure element" or multiple secure elements to store sensitive information such as bank or payment card account

numbers. This indicated that, at least initially, EMVCo considered including competing brands and methods of payment into its standard.

The story changed in June 2010 with EMVCo's release of the "Contactless Mobile Payment Architecture Overview," where it required that

<sup>\*</sup> EMVCo describes the Secure Element (SE) as the place where one or more payment applications are hosted, providing a secure area for the protection of the payment assets (e.g. payment data, keys, the payment application code). Secure Element can be deployed as an embedded Hardware Secure Element in mobile phones, on a Universal Integrated Circuit Card (UICC) (i.e. in the physical card), in a removable Hardware Secure Element (e.g. smart card or secure core on multimedia card) not associated with a mobile carrier subscription, or in a Mobile Device Baseband Processor.

“payment credentials” – basically a card’s primary account number (colloquially known as the PAN) and expiration date – be held in the secure element and that transmission of that data between the mobile device and point of sale systems must use the NFC communications protocol.<sup>26</sup> By specifying 15-19 digit card numbers and expiration dates as the only acceptable payment instruments the standard blocked potentially innovative and efficient new payment methods that could have been developed if other types of payment instruments had been allowed such as bank routing code and account number, for example.

### 8.3 EMVCo Selects NFC for Mobile Payments

NFC is just a communication technology. It replaces the “swipe” of a magnetic stripe card with a “tap” of an NFC-enabled mobile phone onto an NFC-enabled point-of-sale device. Whereas the swipe read the primary account number, expiration date and other security data from the card’s magnetic stripe, NFC achieves the same objective by transmitting that same information using the NFC communications protocol.

This meant that card companies could move into

mobile payments with very little infrastructure investment but, to implement NFC, merchants had to add NFC capabilities to their card swipe POS devices, placing the economic burden on merchants. The rest of the payments’ infrastructure remained unchanged because merchants’ banks (also known as acquirers) and card-issuing banks had to make minimal if any changes to their systems since, once the cards’ information was transmitted from the phone to the POS, transactions behaved just like those initiated by cards.

EMVCo’s original architecture had several drawbacks: It was difficult to load the payment credentials onto the secure element (an action called “provisioning”). Only NFC-enabled devices could participate, forcing consumers to acquire NFC- equipped smart phones and obtain NFC-enabled payment cards from participating banks. Under the EMVCo proposed approach, the number of payment instruments that could be provisioned into the secure element was limited to the cards accepted by the mobile phone carrier or manufacturer.

### 8.4 EMVCo NFC Specification Complicates Merchant Choices in Debit Card Routing

In violation of the Durbin Amendment’s requirement that merchants be given the choice of routing debit card transactions over at least two unaffiliated debit networks, the NFC standard omits debit networks that compete with the card companies. The 2011 version of the standard states that the NFC POS or “entry point” software<sup>27</sup> “queries” the card and, based on its response, identifies the list of products supported by the card, the operating system “kernel”<sup>28</sup> they will run with, and their priority relative

to one another. Since the “kernels” only support

a mobile phone, or another form factor.

<sup>26</sup> Entry Point is software in the POS System that is responsible for pre-processing, discovery and selection of a contactless application that is supported by both the card and the reader, activation of the appropriate kernel, handling of outcomes returned by the kernel, including passing selected outcomes to the reader.

<sup>27</sup> The Kernel is the central module of an operating system. In the NFC standard it is the part of the system that provides all the essential services required by the application. EMVCo’s standard defines the “card” as any consumer token supporting contactless payment transactions, whether in the form of a payment Chip card, a key fob,

Payment Insecurity  
How Visa and Mastercard Use Standard Setting to Restrict Competition and Thwart Payments Innovation

the EMVCo member networks, the standard accommodates only cards from Visa, Mastercard, American Express, Discover, JCB and Union Pay.

In the early NFC implementations such as Isis and Google Wallet, issuers determined the type of cards that were provisioned to the mobile phones.<sup>5</sup> Very few, if any, loaded debit cards to these wallets.<sup>6</sup> Google addressed this provisioning issue with the introduction of host card emulation that allowed consumers to load whatever card they wanted into Google cloud servers. With this architecture, phones were provisioned with Google-issued pre-paid cards

<sup>5</sup> Isis was a joint venture between AT&T, T-Mobile and Verizon who ran unsuccessful mobile payment pilots in Salt Lake City and Austin in 2012. The company renamed itself Softcard in 2014 but in 2015 the venture was wound up with intellectual property and some assets acquired by Google for integration into its own Google Wallet.

<sup>6</sup> The number of participating issuers was limited to very large credit card issuers such as J.P. Morgan Chase, Bank of America, Capital One, and American Express that were willing to pay Isis a \$3 to \$5 per year fee per card fee



that were used to initiate the transaction, but the final charge was made to the consumer's card stored by Google. Still, there was little consumer uptake because of the lack of NFC-equipped phones and point of sale devices.

Since the introduction of Apple Pay, consumers have been able to provision their own cards into the Apple Pay wallet, including debit cards. However, another routing complication arose; because these cards are tokenized before being stored in the iPhone, merchants face challenges when attempting to route these cards through the unaffiliated debit networks. These issues are discussed in greater detail in our analysis of the tokenization standard in Section 8.

In the particularly anticompetitive way that EMVCo drove the industry to NFC technology, EMVCo ignored other communication technologies such as QR codes and also excluded other forms of payment such as direct bank transfer to and from bank accounts, which would have created a competitive threat to the card companies for mobile payments volume. To better grasp the narrowness of the proposed approach, it is useful to review, as we do in the next section, what possible alternatives could have been considered for mobile payments in the United States, and why EMVCo chose to protect its owners rather than act in the interest of innovation, speed and security.

#### 8.5 NFC: A Tool to Prevent Competition

There are alternative communication technologies that allow the exchange of payment credentials between consumers and merchants at the point of sale, which is NFC's sole objective. These include magnetic secure transmission technology originally developed by LoopPay and acquired by Samsung; sound wave technology, which leverages mobile phones' ability to generate and understand sounds;

and quick response codes, known in the industry as QR codes.

Beyond the data exchange technology, there are also other available technological solutions for storing payment credentials. Payment credentials such as primary account numbers or other similar numbers required to access an account can be stored in the cloud or in secure servers and can be encrypted or tokenized, which would be an alternative to storage in the phone's secure element. Benefits attained by implementing mobile payments using these alternative technologies would include:

- Compatibility with feature phones and other non-smartphone devices
- Less investment at the point of sale to support mobile payments
- Ease of provisioning payment credentials
- Inability of secure element owners to control or charge rent to payment instrument providers
- Unrestricted debit transaction routing
- Ability to support other payment networks besides those supported by EMVCO's owners
- Flexibility to implement "push" or "pull" payments<sup>\*</sup>
- Access to more than one funding source, including bank accounts rather than just cards

Of these benefits, the last two are the most threatening to the card companies: the ability to introduce other funding sources and the ability to bypass the card companies' networks. Doing so would add competition and allow merchants to avoid the card networks' high fees. EMVCo's choice of NFC for mobile payments preserved Visa's and Mastercard's market positions, and did not enable the best technology.

<sup>\*</sup> A "pull" payment is when the payer (i.e. the buyer) shares payment credentials with the payee and the payee (i.e. the merchant) initiates the transaction. An example of that is a debit card transaction. A "push" payment is when the payee (i.e. the merchant) shares its payment credentials with the payer (i.e. the buyer) and the payer initiates the payment transaction. An example of this would be a bill payment transaction.

**Payment Insecurity**  
**How Visa and Mastercard Use Standard Setting to Restrict Competition and Thwart Payments Innovation**

The Federal Reserve Bank of Kansas City compared the merits of EMVCo's NFC-based approach to mobile payments with systems such as QR codes and cloud-based approaches such as PayPal. The study showed that NFC compared unfavorably with other technologies in terms of cost, labor and flexibility (Figure 7).<sup>28</sup>

inefficient collaboration between business participants, and was weak from a security standpoint because payment credentials were exchanged unencrypted at the point of sale.

NFC was difficult to adopt because NFC-equipped phones were not widely available until 2014 and

	Technology	NFC	Code-Based	Cloud-Based
1	Examples	Google Wallet, Isis	Starbucks, LevelUp, MCX	PayPal, Square Wallet
2	Required Investment: Consumer	Moderate: NFC-enabled smartphone	Minimal: Smartphone	Minimal: Smartphone
3	Required Investment: Merchant	Significant: NFC-capable POS terminals; Software installation and integration with accounting system	Moderate: QR code scanners; Software installation and integration with accounting system	Moderate: Software installation and integration with accounting system
4	Business Models: Participants	Mobile wallet providers; Hardware providers; Tech providers; App vendors; Mobile network operators; Card issuers/Networks; Handset providers	Mobile payment provider; Hardware providers; Tech providers; App vendors	Mobile payment provider; Tech providers; App vendors
5	Business Models: Coordination and Collaboration besides Merchants	Critical	Less important	Less important
6	Funding Sources	Debit, credit, and prepaid cards	Pre-funded accounts or bank accounts	Bank account and/or debit, credit, and prepaid cards

*Figure 7 – Mobile Payments' Required Investment, Business Models, and Funding Sources by Technology from "Mobile payments: Merchants' Perspectives," by Fumiko Hayashi and Terri Bradford.*

#### 8.6 EMVCo's NFC Standard Drawbacks

Despite all of NFC's shortcomings, the card companies and EMVCo promoted this sub-optimal approach which, at that time, was difficult for consumers to adopt, required expensive and

most consumers had yet to acquire one. In addition, NFC required merchants to make expensive equipment upgrades. Few contactless cards were initially available and even fewer cards were loaded to NFC wallets such as Isis and Google Wallet. Prior

to the deployment of EMV in 2015, merchants had to buy and deploy expensive NFC-equipped devices at a time when the industry was already gearing up for a massive replacement of POS devices in support of chip card introduction. Rather than facilitating collaboration from all parties, EMVCo created an unfavorable environment for competing mobile payment methods for the sake of enhancing card companies' market share.<sup>8</sup>

More importantly, EMVCo's NFC standard had major security issues. As noted earlier, the data-exchange of payment credentials between mobile phones and POS devices was unencrypted. Card numbers stored in the secure element were vulnerable to many hacking techniques including malware and "man in the middle" attacks.<sup>9</sup>

Meanwhile, QR codes ascended to primacy in mobile payments: Starbucks and many other loyalty-based applications made huge inroads using them. The Clearing House ran a pilot using QR codes and tokens as alternatives to secure elements in mobile phones. In late 2015, the largest U.S. card issuer introduced Chase Pay using this technology; Walmart introduced its wallet, Walmart Pay, which also uses QR codes.

#### 8.7 EMVCo's QR Code Standards

QR-code payments were a clear alternative to NFC. Many consumers and merchants found QR codes – the two-dimensional "matrix" bar codes that smartphones can scan to obtain additional information about a product – appealing because all they needed were phones capable of reading the codes. EMVCo kept pushing NFC, however, until issuers in Asia pressured card companies to support QR codes. EMVCo eventually released two QR code

standards in July 2017, one for a "consumer-presented" mode and the other for a "merchant-presented" mode.

In the QR Code consumer-presented mode, the funding account can only be attached to "credentials associated with their EMV card previously provisioned to their device."<sup>29</sup> In other words, the QR code can only be generated from EMVCo payment cards. There is no support for any other type of payment instrument such as bank routing and account numbers or private label cards. The specification also assumes that all transactions are processed through the card companies' networks, just as if they were NFC-initiated at the point of sale. By doing so, the QR code consumer-presented standard blocked potential new competitors and technologies from entering the market.

The QR Code merchant-presented mode erects hurdles against competition as well. That mode provides several fields to enter merchants' accounts, which can be in different formats based on the card company or the merchant's "acquiring" bank that processes payments.<sup>30</sup> This standard falls in line with EMVCo's pattern of driving all transactions to be processed through the card companies' networks and obstructing the possibility of these transactions to be processed through alternative payment networks such as clearing houses or unaffiliated debit networks.

#### 8.8 EMVCo's NFC Specification and Apple Pay

In 2011-2012, Apple, working together with Visa, Mastercard and American Express developed a tokenization system that protected the payment credentials during the information exchange between the mobile phone and the POS device. This

<sup>8</sup> At the time of the NFC specification release and the introduction of products such as Isis or Google Wallet (2010) there was no EMV requirement for the United States. Thus, all POS were card swipe based. Even when new EMV devices were introduced, not all of them came equipped with both EMV and NFC as this was an additional feature that increased the device's cost

<sup>9</sup> Malware is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. Malware is used by cybercriminals to target point of sale and payment terminals with the intent to obtain credit card and debit card information. Man-in-the-middle is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other

<sup>30</sup> Merchants accounts with their acquirers are called "Merchant IDs" or "MIDs". Each acquirer has a different format for their MIDs and the templates provide for this variety but these templates are not intended to be used for the entry of bank routing and bank account numbers

system was extended to protect the payment credentials all the way to the networks, launching the concept of “network tokens.” After their work with Apple, the card companies passed their proprietary designs to EMVCo to build a specification around them, making NFC a part of EMVCo’s design for an integrated payments platform.\*

#### 8.9 EMVCo Failures with NFC

Designating itself as “common voice of the payments industry” was a self-serving move on the part of EMVCo. Rather than addressing common concerns like security and interoperability, EMVCo has repeatedly ignored the best interests of the mobile payments system. EMVCo’s choices around NFC preempted the market of competitors instead of improving “interoperability and... secure payment transactions”. The result was deficient in many areas:

- EMVCo’s approach for NFC was cumbersome, unwieldy and ignored the burdens placed on consumers and merchants. It required extensive collaboration between business participants in which they participated reluctantly and, in the end, only nominally.
- EMVCo betrayed its own charter to provide safe payments by introducing a specification that was weak from a security perspective (until the work with Apple Pay offered a tokenization solution).

- EMVCo’s selection of secure elements as the account number storage location preserved the existing infrastructure and card company dominance.
- EMVCo did not incorporate alternatives such as cloud-stored payment credentials, which could support alternative payment instruments and systems in competition with EMVCo owners.
- EMVCo’s QR code specifications support EMV the card companies’ cards as the only payment instruments and do not support any payment method that could possibly compete with EMVCo owners.

The EMVCo NFC standard is another example of EMVCo pre-empting competition, creating barriers to entry and increasing complexity for both merchants and consumers, all for the sake of increased market share for its owners and at the expense of secure payments. EMVCo continues to demonstrate – despite its claims of being the “representative of the global payments community” – that it will not create specifications that benefit the entire payments industry.

Allowing EMVCo to “assume the central role in defining the requirements for an EMV mobile contactless payments infrastructure” does not serve the U.S. payments industry or the global payments industry.

\* In August 2011 Visa laid out a vision that merges contact (Chip cards) and contactless (NFC-enabled devices) into a single platform with Secure Remote Commerce (SRC) all integrated into one single infrastructure with Tokenization and 3-D Secure technologies

## 9. TOKENIZATION

### 9.1 Background

In the payments industry, tokenization is the process of replacing sensitive account credentials (e.g. a card's primary account number) with a random string of numbers. These strings, called "tokens," unlike encrypted numbers, are generated in a manner that cannot be mathematically reversed to obtain the primary account number. Tokens are therefore safer than encryption because they cannot be reverse engineered making them useless to fraudsters.

EMVCo did not pursue tokenization until 2014. As early as 1998, however, e-commerce merchants were using tokens to hide primary account numbers from being used in-the-clear by their own internal systems. In 2010, acquirers and payment processors began to offer security token services and token "vaults." Through these services, merchants can mitigate PCI Data Security Standards compliance burdens as the card's primary account numbers are stored outside of the merchants' servers.

The card companies, on the other hand, were slow and late to the get into tokenization. The first mention of a token from the card companies was in October 2009, when Visa released its "Best Practices for Data Field Encryption Version 1.0." In this document, Visa said that if a primary account number is needed after authorization, "a single-use or multi-use transaction ID or token should be used instead."<sup>31</sup> Visa advocated for tokenization of the primary account number in its release of "Visa Best Practices for Tokenization Version 1.0" on July 14, 2010.<sup>32</sup> The PCI Security Standards Council released its own tokenization guidelines a year later in August 2011. It is a telling example of Visa's influence over standards and standards-setting organizations that sections of the PCI document are copied verbatim from Visa's best practices document. This should not be surprising, however, as the PCI Security Standards Council is led by an Executive Committee composed of representative from five of the six EMVCo owners (Union Pay is not listed as participating).

### 9.2 Standards-Setting Organizations Developing Open Tokenization Standards

At the time, other organizations were developing open standards for tokenization, including ANSI's ASC X9.119 and The Clearing House's Secure Token Exchange program. These organizations were proposing tokenization standards that could be used for cards and bank account numbers, supported by multiple data-exchange technologies such as QR codes, NFC and dynamic tokens.

TCH's Secure Token Exchange launched in 2012 and started its pilot in 2013. Recognizing that card companies' participation was ultimately needed to achieve market scale, TCH reached out to them. David Fortney, TCH's senior vice president of product development and management, testified before Congress in March 2014:

*The only way to gain broad adoption of tokenization and ensure a consistent customer experience is to develop an open tokenization standard. Open standards promote innovation and allow customers and merchants to choose the point-of-sale technology that works best for them. But it will require banks, merchants, networks and processors to work together to accomplish these goals.<sup>33</sup>*

TCH called for an open tokenization standard even while EMVCo was beginning its work. In Fortney's view, a truly open standard would involve choice for merchants and consumers, including choice of payment method. TCH recognized the dominance of the card companies in the U.S. payments industry, and that no compelling standard could be developed without their participation.

Shortly after Fortney's testimony, Charlie Scharf, Visa's CEO from 2012 to 2016, responded to industry groups that were calling for open tokenization with the following statement:

*This is an area where everyone needs to work closely together and*

*it's paramount that we ensure transparency, security, and integrity so that the integrity of the payment system remains. ...It's got to be standards-based, technology-agnostic. It needs to address the needs of everyone globally, not just in the United States.<sup>34</sup>*

Although Scharf appeared to support Fortney's position, EMVCo and the card companies did not work with TCH or ANSI. Instead, they developed their own tokenization standard that was closed to other forms of payment such as bank accounts, private label credit cards and any other alternative method of payment. Any card company rhetoric around openness, collaboration and inclusion was simply that: empty rhetoric, devoid of intent.

### 9.3 Industry Calls for Open Standards

With so many initiatives for tokenization standardization under way, the Secure Remote Payments Council, which represents unaffiliated debit networks, released a statement the week of July 24, 2014 asking payment industry stakeholders for a collaborative approach in the creation of open tokenization standards.\*

The National Retail Federation, Food Marketing Institute, Merchant Advisory Group, National Association of Convenience Stores, National Grocers Association, National Restaurant Association and Retail Industry Leaders Association released a similar announcement on July 28, 2014.<sup>35</sup> These parties called for open standards and requested that work be migrated away from EMVCo to a true standards organization such as ISO or ANSI. Doing so would enable all industry stakeholders to compete equally and support tokenization for all uses, networks and brands in a manner agreed upon by all.

Unsurprisingly, the card companies and EMVCo did not migrate this work to a more inclusive and transparent organization, presumably because their focus was to promote their cards as the dominant payment mechanisms, not to promote competition or more secure payments.

### 9.4 Apple Pay's Role in Tokenization

In 2012-2013 Visa, Mastercard and American Express worked with Apple to expand the concept of tokenization to provide end-to-end protection of payment credentials, resulting in the beginning of "network tokens." Apple combined tokenization with biometric security – first fingerprint readers on its phones and then facial recognition – which

\* The Secure Remote Payments Council (SRPC) is a cross-industry trade association dedicated to the growth, development and market adoption of debit-based internet e-Commerce and mobile channel payment methods that meet or exceed the security standards for PIN-based card-present payments. SRPC's definition of debit means any device that accesses a checking or deposit account (or prepaid debit account) including: Card (Signature or PIN), ACH Debit, E-Check, Push-Credit, Chip Device, USB Device and alternative

Payment Insecurity  
How Visa and Mastercard Use Standard Setting to Restrict Competition and Thwart Payments Innovation  
paymentinstruments

augmented the security of EMVCo's original specification.<sup>36</sup>

As the work with Apple was wrapping up in October 2013, Visa, Mastercard and American Express jointly announced a new framework, with the shared goal "to enhance the security of digital payments and simplify the purchasing experience when shopping on a mobile phone, tablet, personal computer or other smart device."<sup>36</sup> That announcement was made just three months after TCH released its own comprehensive open tokenization specifications. The key goals of this newer card company tokenization framework were to:

- Ensure broad-based acceptance of a token as replacement for the traditional primary card account number
- Enable all participants in the existing system to route and pass through the payment token
- Improve cardholder security with tokens that are limited for use in specific environments<sup>37</sup>

In contradiction of these principles, the resulting tokenization specifications were proprietary and only applicable to the card companies' credit and debit cards. Although the card companies claim input of "many stakeholders, particularly card issuers and merchants," no merchant can be identified in the documentation and consumer groups were notably missing.

In lockstep with the launch of Apple Pay in October 2014, Visa and Mastercard launched their own token services: Visa Tokenization Services and the Mastercard Digital Enablement Service. Visa and Mastercard began to use tokenization to give their digital wallets a competitive advantage rather than

number and passes that information to the issuer for authorization.

<sup>36</sup> Different from Google Wallet, cardholders provisioned the card number themselves by entering the card number and other information directly into the iPhone (or loading it from their iTunes accounts). Cards had to be from participating issuers that had agreed to pay Apple a percentage of the interchange generated by these cards. In the enrollment process, Apple Pay sends the card number along with other device and consumer related information (e.g. device name, iTunes purchasing history) to the card company for tokenization. The card company, acting as the Token Service Provider or TSP, sends the information to the card issuer for approval and further cardholder authentication. Upon authentication, the TSP issues a Network Token and a unique shared key that is returned to Apple Pay for storing in the iPhone's Secure Element. This token is linked with the device to create a strong association between the device and the token, meaning that payments initiated by that token could only originate from that specific iPhone (and, of course, the Apple Pay application could only be launched by the owner of the iPhone via fingerprint authentication or a PIN). During the purchase process, the Apple Pay application authenticates the phone user via fingerprint or PIN. Apple Pay then generates an authorization cryptogram that that can only be created by that particular iPhone and which Apple Pay transmits to the POS device. The merchant's POS sends the cryptogram to the acquirer, who forwards it to the card company's TSP. The TSP decrypts the cryptogram, validates its authenticity, and detokenizes the provided token back to the original primary account



as a universal security standard.

#### **9.5 EMVCo Takes Ownership of Card Companies' Tokenization**

Up until 2014, the card companies' tokenization services were proprietary and directly performed by the card companies. Around that time, the card companies granted EMVCo their intellectual property with the explicit purpose of formalizing it as an EMVCo standard. Almost overnight, EMVCo

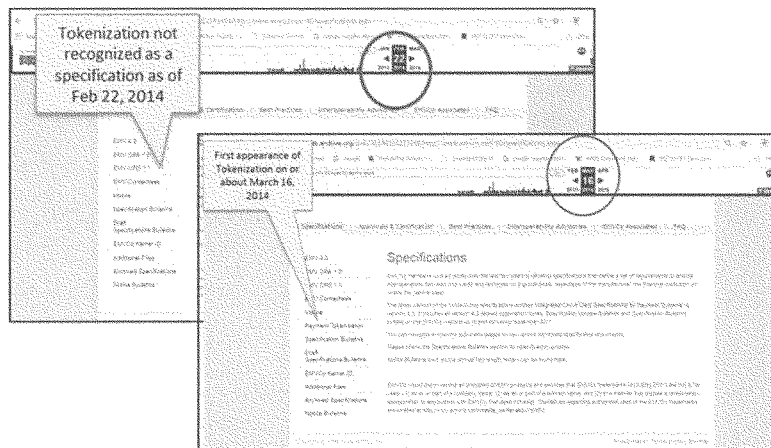
<sup>4</sup> Under a token interchange arrangement, Visa can get tokens from Mastercard for Mastercard cards stored in its Visa Checkout wallet and Mastercard can get tokens from Visa for Visa cards stored in its Masterpass wallet. Both schemes also opened their Token Service Providers or TSP services to third party wallets (e.g. Android, Samsung), as long as the tokens passed through Mastercard's Digital Enablement Service and Visa's Token Service. This is a key point because these tokens (now called "Network Tokens" to differentiate them from tokens generated by PSPs and gateways, called "PCI Tokens") can only be detokenized by the card companies' TSP.

published a fully developed “Technical Framework” in 2014 with no bulletins, lead time or third-party involvement of any kind.<sup>38</sup>

The framework document essentially echoed the work done for Apple Pay and positioned it as a “standard” even though EMVCo conceded that many important issues remained unresolved, such as whether tokens could be reused because of the limited number of bank identification numbers available for tokenization.<sup>39</sup> Figures 8 and 9 show the sudden appearance of a fully formed tokenization specification (Version 1.0), using web archives to

revisit EMVCo’s site in 2014, when these standards were released.<sup>40</sup>

Although EMVCo does not generally release information about its internal proceedings and decision making, its web site contains some information on its work. Examples of these documents are draft standards which are normally shared and posted during the development process. EMVCo also posts notices and bulletins that are issued prior to the release of a final specification. None of that information was available during the process of developing the tokenization standard.



**Figure 8 – EMVCo Web Site from February 22 and March 16, 2014 Shows the Sudden Appearance of Tokenization Specification.**

<sup>38</sup> A Bank Identification Number or BIN is the primary account number's (or PAN's) first 6 digits that identifies the issuer of the card and the type of product the card is (e.g. regular consumer credit, Signature Elite, etc.). To protect the card companies' infrastructure, Network Tokens need to look like regular PANs (e.g. 16 digits, start with a "5" or a "4", etc.) so they can be passed around as regular PANs without modifying their systems. Visa and Mastercard allocated special BINs to issue Network Tokens so they can be distinguished from regular PANs but there are a limited number of these BINs, meaning the number of Network Tokens that can be issued is limited. The TSP assigning these tokens are called BIN Controllers

<sup>39</sup> Fully formed standards have whole numbers (e.g. 1.0, 2.0, etc.) Draft specifications have fractional numbers (e.g. 0.8, 0.9, etc.).

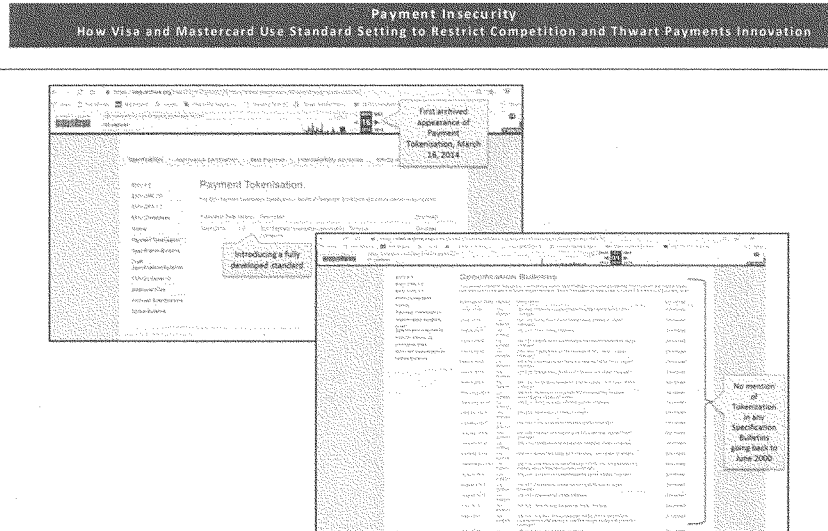


Figure 9 – EMVCo's website shows a lack of bulletins or other development documentation prior to the release of its tokenization standard on March 16, 2014.

#### 9.6 EMVCo Tokenization Framework 1.0 Deficiencies

Industry observers quickly identified major deficiencies in Version 1.0. "Network tokens" introduced friction in customer service and chargeback management environments and created significant challenges for merchants trying to route debit cards through nonaffiliated debit networks.

For example, the use of alternative bank identification numbers or BINs hid useful information from merchants, which is very important to locate orders to address customer service calls as well as to identify chargebacks that could be disputed. More importantly, merchants use BINs to identify the card type as credit versus debit versus pre-paid or business versus consumer, for example, which may determine card acceptance flows. Crucially, BINs are critical to route the transaction through unaffiliated debit networks.

Version 1.0 was based on ISO's older ISO8583 standard for transmitting card data rather than the newer and more flexible ISO20022 standard for

older systems. This meant that less information about a card and the cardholder could be passed to the issuer. For example, tokens were required to look like cards' 11- to 19-digit account numbers, were assigned from specially designated bank identification numbers used for tokenization and prevent the use of other payment instruments such as bank accounts or private label cards.

Under Version 1.0, there could be multiple tokens for the same primary account number at one merchant. This happened when a cardholder used the same card in multiple smartphones. Version 1.0 did not provide a way for merchants to link these tokens, making it appear as though two different customers were making purchases. Merchants needed to see all these tokens as a single customer so they could provide good customer service, provide loyalty points and manage customer risk.

Finally, it was reported by industry observers that dynamic tokens (a more secure type of tokens that change for each transaction) were excluded from the specification because some large issuers could not

support that capability.

financial data in order to maintain compatibility with

### **9.7 EMVCo Tokenization Framework 2.0 Updates and Remaining Deficiencies**

Although promised for late 2014, EMVCo did not complete Version 2.0 until September 2017. Version 2.0 remedied the customer-friction shortcomings of Version 1.0 with the introduction of a “payment account reference” number. Nonetheless, suggestions for mandated sharing of key fields such as type of card, support for ISO20022, inclusion of dynamic tokens and support of other payment methods were all rejected. Crucially, EMVCo also did not address the issue of routing debit cards outside of the card companies’ networks, leaving those details to each card company’s implementation.

The new payment account reference numbers, also known as PARs, link multiple tokens together for the same customer. A PAR is a 28-digit string that cannot be used to initiate financial transactions, so their sole purpose is to create a single view of a customer’s payment channels and methods. Unsatisfactorily, Version 2.0 did not require the card companies to pass the PAR back to merchants. As a result, merchants are more dependent on the networks, potentially having to pay a fee to get PAR numbers.

### **9.8 Network Tokens Introduce Challenges to Merchant Debit Card Routing Choices**

Version 2.0 continued EMVCo’s practice of creating obstacles for merchants to exercise their rights to route debit cards through unaffiliated debit networks.

To route debit card transactions from pay wallets such as Apple Pay for in-person transactions through unaffiliated debit networks, the following needs to happen: (1) the bank identification number used to tokenize the debit cards must be registered with the debit networks, (2) the point of sale terminal must be programmed to select the U.S. Common AID (see Section 6) and (3) unaffiliated debit networks must follow rules established by Visa and Mastercard to be able to detokenize a token back to the primary account number or PAN.

These requirements are challenging for merchants for the following reasons: if Visa or MasterCard were to issue a token for a debit card that participates in an unaffiliated debit network but the corresponding

token BIN was not enrolled, a merchant would either not route the transaction to the unaffiliated debit network or, if it did, the transaction would be rejected. It is very difficult, if not impossible, to continuously monitor if Visa and MasterCard are issuing tokens that use BINs that may be solely enabled on their networks or hold the card companies accountable for the timeliness of such enrollment with the unaffiliated debit networks.

Further, unaffiliated debit networks can only detokenize transactions that originate using the U.S. common AIDs. Since many terminals have been configured to prioritize Visa and MasterCard global AIDs, a merchant terminal will only select the common AID if it’s been configured to ignore the EMV priority. Any merchant that wants to accept mobile wallet-based transactions (e.g. Apple Pay / Google Pay / Samsung Pay) and benefit from the frictionless experience afforded by biometric-only authenticated transactions must choose the global AID rather than the common AID, effectively giving up routing choice.

Once a merchant identifies a debit card token that can be routed through the unaffiliated debit network, the unaffiliated debit network can request that the token be detokenized back to the primary account number. Because the merchant configured the terminal to default to the common AID, however, the transaction is processed as a “no cardholder verification method” transaction. In this scenario, even if the customer uses biometric authentication, the unaffiliated debit network is prohibited from sending that information along to the issuing bank. It is important to point out, there are no technical or security challenges with the unaffiliated networks sending this data, it is just an arbitrary card rule. As a result, an issuing bank would consider an unverified transaction as inferior and is more likely to decline it.

Similar obstacles are also found in the card not present environment which includes Internet, mobile commerce and other transactions in which a merchant does not observe a physical card. Visa and Mastercard are actively promoting network tokens to e-commerce and subscription merchants on the basis that their Account Updater service is not

needed.<sup>8</sup> But while merchants enjoy full routing choice when the primary account number is used, the same is not true of tokenized card-on-file credentials. Mastercard prohibits the routing of such tokenized card-on-file transactions to any other unaffiliated debit networks enabled on the actual card and requires all tokenized transactions run exclusively through their network.

Visa doesn't prohibit the routing of tokenized card-on-file transactions to unaffiliated debit networks, but Visa will only de-tokenize such transactions if the issuer instructs them to do so and will subsequently degrade the service. If a merchant routes the same transaction to an unaffiliated debit network, Visa will detokenize the transaction but will not perform any token domain restriction or cryptogram validation, thereby eliminating the core security capabilities available on such transactions. Because of the perceived lesser security, issuers are more likely to decline these transactions, seriously impacting approval rates and discouraging merchants from routing through unaffiliated debit networks.

Finally, it has been reported by industry observers and representatives of the unaffiliated debit networks that both in the future Visa and MasterCard might require any transaction where the cardholder was authenticated through 3-D Secure on their respective network that the corresponding authorization be processed on their networks. With the push to make adoption of 3DS 2.0 as broad as possible, this will further reduce the number of transactions that can be routed through unaffiliated debit networks.

#### 9.9 EMVCo Failures with Tokenization

With "EMV Payment Tokenization Specification, Tokenization Framework Version 2.0," EMVCo failed to be a "representative of the payments community" in favor of delivering tokenization standards that:

- Are narrowly focused on card companies' products
- Preserve the current infrastructure by using the older ISO8583 communication protocol rather than the more flexible ISO 20022
- Create complexity for merchants and make them even more dependent on services from card companies, with potential new fees
- Are not transparent to merchants, negatively affecting approval and decline rates as well as creating friction for customer service and chargeback departments
- Hide key information such as card type, impacting routing and interchange calculations
- Create obstacles for merchant routing debit of cards through unaffiliated debit networks, in effect providing the card companies with a mechanism to avoid complying with the Durbin Amendment
- Demonstrate, given the difficulty they had evolving the initial tokenization framework to version 2.0, that EMVCo is not the right body to develop these specifications and standards.

Tokenization is one more example of the card companies — specifically Visa, Mastercard and American Express — appropriating an open standard and preempting collaborative industry efforts. EMVCo did not develop the initial tokenization standard at all; the card companies leveraged EMVCo's imprimatur to create the perception that the tokenization framework was an industry standard. In so doing, EMVCo demonstrated, once again, that it creates standards that benefit the card companies at the expense of merchant choice for affordable routing.

<sup>8</sup> Account Updater is a service offered by Visa, Mastercard and American Express that automatically updates the primary account number and the expiry date of cards-on-file when this information changes. Examples are replacement cards when the card is reissued based on its expiration date. This is an important service for subscription merchants and for merchants that offer cardholders the option to store their cards with merchants for future purchases.

## PART III—CONCERNS WITH NEW STANDARDS

This part reviews recently introduced, but not fully implemented standards such as 3-D Secure 2.0 and Secure Remote Commerce that have the potential to significantly disrupt e-commerce and mobile commerce. We will outline concerns with these standards and how they negatively impact the competitiveness of payment solutions in the fastest growing segment of U.S. retail shopping.

### 10. 3-D SECURE VERSION 2.0

#### 10.1 Background

Three-Domain Secure, also known as 3-D Secure or 3DS, is a security protocol originally developed by Visa. It has been adopted by all the card companies to help prevent fraud when using credit and debit cards to make e-commerce purchases online. It is also the generic name for authentication technology presented to online buyers under the names Verified by Visa, Mastercard Secure Code, SafeKey (American Express), ProtectBuy (Discover), and J/Secure (JCB). 3DS originated with the 2001 Visa Payer

Authentication System, which encouraged cardholders to use only Visa cards for online shopping by promoting its exclusive authentication features. That initiative had more to do with brand marketing (with Visa claiming to be secure and others appearing unsafe by comparison) than it did with payment security. Within months, however, the other card companies offered similar solutions. Maintaining multiple authentication standards created logistical problems for merchants, and the card companies acquiesced to a common approach that became 3DS.

The original 3DS scheme, called 3DS Version 1.0, requires that cardholders register with their card issuing banks and that, prior to any e-commerce transaction, they be authenticated by the card issuer. This authentication is performed by redirecting cardholders to issuers where they enter their user-identification and password information.

When cardholders are authenticated, the liability for any fraud shifts from the merchant to the issuer.

The initial release of 3DS was not well thought-out and it showed the card companies' inexperience when it came to online shopping. Issuers had little incentive to enroll cardholders because of the liability shift. Aside from the lack of issuer support, online shopping cart abandonment under 3DS 1.0 was high. Many merchants who implemented 3DS 1.0 reported lost sales as customers who were redirected never returned to complete their purchases, either because they had forgotten their passwords or because the redirection process took too long creating a timeout condition on the

merchants' checkout processes.

Despite efforts from Visa and Mastercard to convince online merchants to participate, efforts that included meaningful financial incentives, adoption remained low due to increased friction and lost sales.<sup>4</sup> More importantly, 3DS 1.0 lacked support for card-on-file and recurring payments, important payment modes for online shopping and subscription merchants. Thus, what is now called 3DS 1.0 was poorly designed, mismanaged in its implementation and was minimally adopted by U.S. merchants.

#### 10.2 Evolution from 3DS 1.0 to 2.0

Like tokenization, 3DS was not developed by EMVCo. Its implementation as a standard is another case of the card companies using EMVCo to bolster technologies that structurally support their objectives. 3DS was "re-invented" by the card

<sup>4</sup> A "timeout" is the cancellation of an order that automatically occurs when a predefined interval of time has passed without a certain event occurring such as getting a response from a provider

<sup>5</sup> Visa offered merchants large cash or marketing rebates, sometimes in the multi-million-dollar range. Mastercard introduced interchange reduction on 3DS transactions in addition to the liability shift.

companies during 2013-2014 because of separate compounding circumstances:

- Increases in online fraud rates led issuers to tighten their risk scores and to decline authorization requests at higher rates. For this reason, merchants and issuers, dissatisfied with the card companies' solutions to the problem, decided to explore ways for merchants to share richer information with issuers, potentially using third party solutions that would pass this information outside the card companies' control
- The emergence of competing authentication standards from the FIDO Alliance and W3C
- The impending arrival of European Commission's Payment Services Directive 2, which required "strong customer authentication" on all online transactions.\*

These events led the card companies to rethink how online transactions are authorized and how they could avoid being disintermediated by creating an authentication standard.

### 10.3 3DS 2.0 Pre-empting Competition

To increase approval rates, large merchants such as Microsoft, Google and Netflix reached out to selected issuers around 2013 to explore "out of band" solutions. Both merchants and issuers concluded that approval rates could be improved if better data were available during the issuer's decision-making process. Additional data discussed included information such as email address, IP address, device fingerprint and length of relationship between the cardholder and merchant.

Unfortunately, the card companies and many issuers were, and still are, running their authorization platforms on the ISO8583 message format standard, which, although very robust, is not very flexible. ISO8583 does not have the capability to carry the

additional information issuers wanted. Issuers realized that they were missing out on interchange income due to unnecessarily declined transactions and began cooperating with merchants in exploring solutions that bypassed the card companies. Some innovative financial technology companies offered "out of band" messages running parallel to the authorization flow, which conveys the data to the issuer. Companies such as Ethoca and Cardinal Commerce, for example, were well-positioned to provide such services.

Faced with these issues, Mastercard announced in November 2014 that it would join Visa in creating a new version of 3DS that would carry richer data, a move that preempted the work of other companies.<sup>†</sup> In January 2015, EMVCo owners agreed that the draft framework and corresponding intellectual property developed by Visa and Mastercard would be handed off to EMVCo for further development. Although promised for late 2015, it was not until October 2016 that EMVCo published its standard for 3-D Secure 2.0, which could deliver much of the data sought by issuers to increase approval rates.

### 10.4 3DS 2.0 Positioned as a Strong Customer Authentication Standard

On November 16, 2015, the European Commission enacted Payments Security Directive 2, which extended changes originally implemented in 2009.<sup>‡</sup> Under PSD2, financial institutions were mandated to open access to bank accounts to any qualified payment initiation service providers. In order to protect consumers, PSD2 also required —with some exceptions — that account access must be done with strong customer authentication, which is generally referred as SCA, a methodology to authenticate the

\* The EU Committee released its PSD2 proposal in 2013 and was finally adopted in 2015.

† This risk of disintermediation is no longer the case after Visa's acquisition of Cardinal Commerce in 2016 and Mastercard's acquisition of Ethoca in 2019.

‡ The original PSD regulation opened the payment markets to payment service providers who were not financial institutions. Payment Service Directive 2 is officially known as Directive (EU) 2015/2366 amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

account owner based on multi-factor authentication.<sup>7</sup>

The requirement applies to all remote payment transactions initiated by a payer within the European Economic Area, including card transactions, but applies only on a “best-effort” basis when one of the parties is located outside of Europe. Exemptions are also allowed for low-value and recurring transactions.<sup>8</sup> However, it is believed that U.S. merchants selling in Europe that do not perform strong customer authentication could see significant loss of sales as European card issuers expect this authentication to be performed regardless of the “best-effort” exclusion.

Visa and Mastercard immediately positioned EMVCo’s new standard, 3DS 2.0, as the best tool to perform strong customer authentication for card transactions both in Europe and the United States.<sup>9</sup> The decision is another example of EMVCo standards being developed and leveraged in a way that benefits the card companies’ existing practices while increasing merchants’ payment processing costs and inhibiting true security innovation.<sup>6</sup>

#### **10.5 EMVCo Ignores Authentication Standards from Other Standards-Setting Bodies**

EMVCo’s traditional area of expertise has been chip cards and terminals, not biometric technologies nor consumer authentication. By contrast, the FIDO Alliance has been developing alternative authentication approaches for several years. Similarly, the Web Payments Working Group of the

World Wide Web Consortium (W3C) initiated work

on its Payment Request application programming interface with participation from a cross-section of industry stakeholders intended to create the concept of “payment apps.”

In collaboration with the FIDO Alliance, W3C advanced the Web Authentication API, named WebAuthn and in March 2019, WebAuthn became an official web standard. WebAuthn, is supported in Windows 10 and Android and it is being implemented in Chrome, Firefox, Edge and Safari. WebAuthn addresses some of the risk analysis goals of 3DS 2.0 through new browser capabilities that enhance user privacy.

Payment apps like WebAuthn are intended to standardize the buying experience and run on desktops, laptops, tablets and phones. They provide services such as strong user authentication, loyalty program integration, and back-channel communications with the merchant for fraud analytics. More importantly, WebAuthn is designed to “support the broadest possible array of payment methods.” Yet none of these approaches to customer authentication have found their way into the card companies’ initiatives for safer payments in the United States.

Instead of collaborating with open standards-setting organizations, EMVCo pursued expanding the 3-DS-based framework developed by Visa and Mastercard. In so doing, the card companies retained control of the authentication process and prevented other payment methods from participating in it.

<sup>7</sup> PSD2 regulations define strong customer authentication, or SCA, as an authentication based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent and that protect[s] the confidentiality of the authentication data. The regulation was originally scheduled to be effective on September, 2019 but due to the lack of industry readiness, the effective date for the application of this regulation has been moved to the last day of December, 2020

<sup>8</sup> The Regulatory Technical Standards or RTS provides detailed specifications to achieve the strict security requirements for payment service providers in the EU.

<sup>9</sup> Even though neither PSD2 nor RTS mention 3DS, many merchants believe that PSD2 have mandated 3DS, failing to recognize that 3DS is just one alternative to comply with the SCA requirement.

<sup>6</sup> Mastercard charges a \$0.03 for each Secure Code verification attempt and acquirers planning to offer SCA are quoting charges from \$0.02 to \$0.07 per 3DS 2.0 verification on top of that.

<sup>10</sup> EMVCo collaborates with open standards-setting organizations but only when it benefits their owners. In one example, EMVCo provided payment use cases to the FIDO Alliance for incorporation into its Authentication Suite. Doing so allows FIDO certified authenticators such as fingerprints and facial recognition to authenticate card transactions. By working with W3C and the FIDO Alliance, EMVCo can claim that they collaborated in payment technology. In the end, providing these use cases had the desired optics: In its related press release, the FIDO Alliance unfortunately mislabels EMVCo “the global payment standards body,” continuing to foster the image that EMVCo speaks for the entire payments industry.



#### 10.6 Industry Concerns with 3DS 2.0

3DS 2.0 is a new standard that has not been widely deployed by vendors or adopted by merchants. Much of the recent impetus for its implementation was driven by the European strong customer authentication requirements.<sup>\*</sup> Because it is still early days, there are few 3DS 2.0 practical experiences to study its impact on the U.S. payments industry. However, observers have identified issues and expressed concerns regarding this standard that echoes problems noted with other EMVCo standards.

- The architecture of 3DS 2.0 is essentially similar to 1.0 – a 3DS server connecting to a directory server which, in turn, connects to an issuer's access control service. Given that the amount of data being passed is greater, there are significant concerns about performance and the possibility of cart abandonment because of timeout conditions. This was a big problem under 3DS 1.0 and reports from a recent EMVCo meeting indicate that the 3DS 2.0 authentication roundtrip suffers the same performance issues.
- 3DS 1.0 had little adoption amongst U.S. merchants because of the friction it introduced in the shopping process but, at least, merchants had the option to use 3DS 1.0 or not. There are concerns within the merchant community that the card companies will mandate 3DS 2.0. Under EMVCo's secure remote commerce, also known as SRC but branded as "Click to Pay", merchants lose control over whether 3DS 2.0 is executed as the authentication process is now being performed by the wallet operating under SRC.<sup>†</sup>
- Another major concern about EMVCo's 3DS 2.0 standard is that it lets the card companies define rules that prevent routing of debit cards through unaffiliated debit

networks. Unconfirmed reports from merchants and other industry sources indicate that Mastercard will require all 3DS 2.0 authenticated transactions to also be authorized and settled through their network instead of the unaffiliated debit networks, violating the spirit and the letter of the Durbin Amendment.

- The card companies continue to position the EMVCo 3DS 2.0 standard as the tool to address the European requirement for strong customer authentication, pushing merchants to implement it even though there are also concerns, voiced by the European Banking Authority that, under certain conditions, 3DS 2.0 does not meet their authentication requirements.<sup>‡</sup> Thus, merchants are concerned about implementing 3DS 2.0 but still not being compliant. A companion concern from industry observers is that, by putting all the attention on EMVCo's 3DS 2.0 standard, other authentication approaches from competing companies or open standards bodies are being pre-empted.
- Conveniently, EMVCo's definition of the 3DS 2.0 standard allows the card companies to define fees and other governance rules. The card companies have historically taken advantage of these opportunities to introduce additional merchant fees. For example, when tokenization was introduced in 2013, Mastercard began assessing a 0.01 percent Digital Enablement Fee which applies to all online transactions – e-commerce and mobile commerce – even if the merchant does not use Mastercard's tokenization services. Similarly, since approximately 2013 Mastercard has also been charging a Secure Code transaction fee of \$0.03 for every 3DS 1.0 verification attempts. Given this precedent, it is reasonable to be concerned about the

<sup>\*</sup> Strong Customer Authentication was scheduled to go live in September 2019 but has been delayed until the last day of 2020

<sup>†</sup> This will be discussed at length in the next section on secure remote commerce

<sup>‡</sup> 3DS 2.0 without biometric authentication cannot be used to satisfy the inherence factor requirement under strong customer authentication, just knowledge and possession.

possibility of the card companies introducing or raising 3DS 2.0 fees.

#### **10.7 Conclusion**

While EMVCo did not develop the original 3DS standard, its assumption of the standard was critical to its credibility. 3DS 2.0 follows the pattern of the card companies preempting industry efforts and creating barriers to market entry for better payment

methods as well as creating standards that introduce fee-generating services. 3DS 2.0 shows, once again, that EMVCo acts as a pass-through company to create standards that benefit the card companies, not the overall payments industry.

## 12. SECURE REMOTE COMMERCE

### 12.1 Background

Secure Remote Commerce is a recently introduced EMVCo standard intended to provide a unified checkout for remote commerce where purchases are done via web browsers or mobile phones and where the physical payment card is not present. To users, SRC will appear as a single button with a variety of payment methods from the card companies that are enrolled in the SRC system the merchant has implemented.

The document that defines the SRC standard is a technical framework draft released in March 2017 that broadly described its concepts, including the roles and responsibilities to be held by the different participants in the SRC system. Early merchant implementations of SRC began to appear in October 2019 under the name “Click to Pay” but the card companies do not expect major adoption until after the 2019 holiday season.<sup>40</sup>

The SRC standard creates a new checkout experience while enabling integration with other EMVCo standards such as 3D Secure and tokenization with the objective of delivering to merchants an experience similar to the point of sale: receipt of a payment token that the merchant can use to initiate a secure remote payment.

EMVCo has stated that the objectives of the EMV SRC standards are to:

- Design uniform interfaces that allow for secure exchanges of payment data among participants in the digital commerce environment
- Accommodate options for using dynamic data — such as cryptograms or other transaction-unique data — to enhance the security of payment transactions on a merchant’s SRC-enabled website, mobile app or other e-commerce platform
- Enable compatibility with other EMVCo technologies such as payment tokenization and 3-D Secure

- Facilitate consumer recognition of a common user experience by display of the SRC icon

EMVCo states that today’s e-commerce environment “...has many different integration models and practices. The variety of implementations and the lack of common specifications for this environment results in fragmentation, complexity and inconsistency.”<sup>41</sup> EMVCo purports to address the need for consolidation, simplicity and interoperability by providing a “universal buy button” that contains cardholder payment information which can be used at all SRC-enabled merchants.

The card companies claim that their motivation for introducing this standard is to simplify the checkout process and eliminate the confusion created by the large number of checkout buttons. Ironically, the proliferation of checkout buttons was caused by the card companies themselves trying to compete with other user-friendly and secure solutions such as PayPal. Since the card companies have failed to gain much market adoption, SRC seems to be an attempt to rewrite the checkout button display rules. EMVCo’s SRC is a solution in search of a problem—unless one concedes that the problem is branding and increased market share for EMVCo’s owners.

### 12.2 Game of Buttons

The card companies care about both their brands and about transaction volume; one is critical to maintaining the other. That is why, for example, Visa and Mastercard lament that consumers often say they are “paying with PayPal” when the actual funding instruments are their credit or debit cards linked to consumers’ PayPal accounts. It was not surprising that when PayPal grew out of its eBay origins around 2006, the card companies became concerned that it would be considered a competing “acceptance brand”.

Prior to 2006, the card companies had very strict rules regarding the display of their logos on websites. All logos had to be displayed equally and there could

**Payment Insecurity**  
**How Visa and Mastercard Use Standard Setting to Restrict Competition and Thwart Payments Innovation**

not be a preference between logos. The card companies were so concerned that they required that the PayPal logo on merchant sites comply with their regulations with regards to size, color and other considerations as a “comparable” logo. A pre-2006 merchant checkout logo display looked like that shown in Figure 10.

introduced PayPass Wallet Services in 2012 which evolved into Masterpass and Amex Express Checkout was introduced in 2015. Each of these buttons appeared with varying degrees of marketing fanfare but they all had low customer and merchant adoption. Their functionality was still rudimentary and comparable with what PayPal had offered in



Figure 10 — Checkout logos prior to 2007



Figure 11—Logos from 2007-2009 featuring “Check out with PayPal”

Around 2007-2008, however, PayPal found a way to achieve prominence by convincing merchants to implement a larger button that initiated a new “process” running in parallel to the process of card-based checkouts. “Check out with PayPal” gave PayPal greater visibility, as shown in Figure 11.

Despite the negative reaction and threats from the card companies, PayPal was able to prevail because it argued that this approach did not violate the rules, as “Check out with PayPal” was not a comparable product but a different “process.” PayPal created multiple versions of its “buy buttons.” Some merchants even presented the “Check out with PayPal” button alongside plain text saying “check out with credit cards” that did not show any of the card companies’ logos.

Around 2011-2013, the card companies tried to compete with PayPal at its own game by developing their own checkout buttons. Visa introduced V.me in 2011 which evolved into Visa Checkout; Mastercard

2002. Still, the card companies persisted, leading to the proliferation of buttons — as shown below — that EMVCo now claims is causing consumer confusion and creating a reason to introduce SRC (see Figure 12).

The card companies’ concerns are not just about brand prominence. E-commerce provides a real opportunity for new, competing payment methods to be introduced. Consumers are more likely to adopt new online payment forms while the infrastructure cost for merchants to implement them is a fraction of the cost associated with adopting new forms of payment in-store. EMVCo consolidates the resources of the card companies against services like PayPal and interferes with efforts of other standard bodies before they can gain momentum.

Shortly after EMVCo’s announcement of the Secure Remote Commerce initiative in late 2017, the card schemes—led by Visa, Mastercard, and American Express—launched public relations efforts to

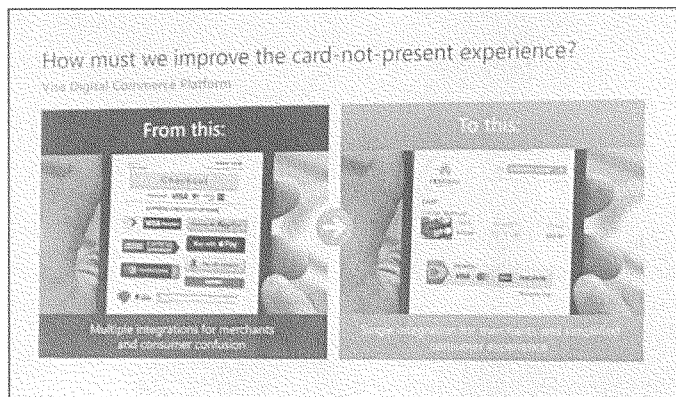


Figure 12—Logos in checkout page circa 2015 cluttering the checkout page with a button for each major brand

**Payment Insecurity**  
**How Visa and Mastercard Use Standard Setting to Restrict Competition and Thwart Payments Innovation**

buttress EMVCo and SRC which left no doubt as to who their target was (see Figure 13 below): wallets not associated with the card companies' checkout buttons.\*

Similarly, the World Wide Web Consortium, known as W3C, launched its Web Payments Initiative in 2014. Its stated objective was to enable consumers to choose their preferred payment options across all



*Figure 13—Slide from a Visa presentation showing replacement of all competing checkout logos with a single SRC logo\**

One of SRC's functions is to authenticate cardholders before adding their payment cards to the SRC wallets. In the early implementations, this authentication is being performed via one-time codes sent to the e-mail address or mobile phone registered with the card. This approach ignores the ongoing authentication work of the FIDO Alliance and W3C. For example, the FIDO Alliance's open standards-making process, started in 2013, encouraged

and invited participation from all companies and organizations that wanted simpler and stronger online payment authentication. Participation in FIDO, in contrast with EMVCo, is open to any paying member and includes voting in board meetings. FIDO Alliance's objective is to define an open system that benefits *all* users of the internet.

their devices, for merchants to transparently support a growing number of payment options, for new payment providers to enter the market more easily with innovative solutions and payment systems, and to support new payment models such as micropayments and payment wallets. W3C's standards development process is fully inclusive and transparent. From its launch, W3C's initiative was open to participation from all the members of the payment community. The initiative speaks directly

about preventing vendor monopolies and includes all forms of payment, including ACH and non-traditional payment methods.

Rather than pursuing similarly open systems, EMVCo states that "EMV SRC is focused on providing consistency and security for card-based payments [emphasis added] within remote payment environments" and that "EMVCo aims to work

\* Picture from a presentation by Alfred Kelly, Visa CEO at JP Morgan Global Technology and Communications Conference, Boston, May 2018

\* To see the inclusiveness of W3C participating members, see <https://www.w3.org/Payments/WG/charter-201803.html>

closely with industry participants such as W3C to capitalise on opportunities for alignment where appropriate."<sup>42</sup>

In a June 2018 EMVCo ad-hoc meeting in San Diego to discuss SRC, EMVCo stated that its inability to work with W3C was due to intellectual property issues because W3C and EMVCo work under different confidentiality models. W3C's working groups operate in public, so if a group reviewed an EMVCo standard it would have to release those findings publicly, which EMVCo would not allow as it operates behind closed doors. EMVCo's opposition to transparency in the standard setting process is, in fact, the problem itself. At the same meeting, attendees criticized EMVCo's inability to define specific roles and processes for participation by any competitors to the card companies in the SRC programs.

It was not until April 2019 that EMVCo joined the FIDO Alliance and W3C in creating a new interest group to collaborate on a vision for web payment security and interoperability. In its press release, EMVCo said it looked forward to "productive discussions and ultimately increased interoperability for payments."<sup>43</sup> It remains to be seen what develops from this interest group, given EMVCo's history of superseding other standards-setting bodies' work and operating in a closed-door environment.

### 12.3 SRC User Experience

The initial SRC implementation at merchants' checkout pages shows a process very similar to what

consumers do when they create PayPal accounts (the numbers detail the windows in Figure 14 below):

1. In merchants' pay page consumers click on the Click to Pay button. This brings up a widget or java script window where consumers enter their e-mail address to register or login. The widget or java script is hosted by the company or SRC program with whom merchants entered into an agreement with, either Visa or Mastercard. In the example below, the widget presented is by Visa.
2. The window asks for payment card information from new consumers. Note that the window only allows entry of 15 to 16-digit payment card numbers (rather than bank or other account number) and that once the card number is determined to be a Mastercard, the host of the window changes to Mastercard.
3. Consumers must provide additional information such as billing address which is also used as the default shipping address. This process is similar to enrollment in any other e-wallet enrollment.
4. The SRC program sends a one-time use code to the email address of record for that payment card. It is not known at this time whether this process uses the 3-D Secure or another proprietary protocol. The e-mail

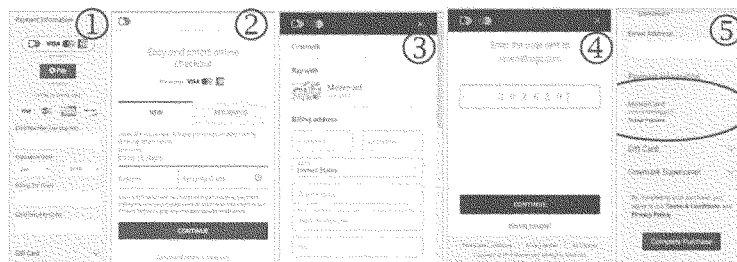


Figure 14—SRC user experience

- comes from Visa or Mastercard, depending on the card type, not from the issuer.
5. Once the number is entered and verified, a token is passed back to the merchants who can either use it to initiate the payment or store it for future use. The actual primary account number may or may not be passed to the merchant depending on SRC program's implementation rules. The primary account number is optionally tokenized and bound to the device that initiated the transaction by means of an algorithm that indicates the token associated with the primary account number can only originate from that device.

In subsequent SRC experiences – either with the same merchant or any other merchant, consumers do not have to re-enter their primary account number or credentials as the card number is already registered and bound to the device in question. Consumers enter their e-mail addresses and the one-time code on the widget or java script window which will cause the SRC programs to pass the payment data to the merchant. Optionally, consumers can set their phones or computers as trusted devices and this will prevent the need to enter the one-time code when they do subsequent purchases.

#### 12.4 EMVCo SRC Standard Components

The unprecedented collaboration between the card companies and EMVCo has delivered a complex standard with many participants and roles:

- SRC program: Responsible for the policies and processes associated with the oversight of SRC participants within an SRC system. This role is expected to be performed by the card companies.
- SRC system: Orchestrates all activities between participants and manages technical aspects of the SRC program. This role is also

fulfilled by the card companies.

- Digital shopping application: A payment application (on the merchant side) driving the consumer experience for SRC. This function can be provided by the merchant or a payment service provider.
- SRC initiator: Supports checkout and/or the secure retrieval of payment data from the SRC system on behalf of a digital shopping application. This is provided by merchants or their payment service providers.
- SRC participating issuer: Issuers who decide whether to enroll their payment cards with a given SRC system.
- Digital card facilitator: Holds payment card data and makes it available to support the checkout process. The role is rather open and, while card companies' payment wallets — such as the replacements for Masterpass and Visa Checkout — could fulfil this role, the question is whether the role is open to any other participants and, if so, under what conditions.

Understanding these roles is important because rules and regulations for these programs flow from the top. Both Visa and Mastercard have introduced SRC programs but few details have been published publicly about their implementation, especially about rules and fees.

#### 12.5 Issues with the Development of SRC Standard

The history of SRC reveals a pattern of the card companies trying to create a card-biased future for remote payments. The EMVCo SRC standard was developed in a closed collaboration between the card companies that own EMVCo, primarily Visa, Mastercard and American Express. Early versions of the SRC standard were developed with little influence outside of the card companies but, given the continued volume growth in the web and mobile commerce channels, industry stakeholders clamored

for the opportunity to provide input.

\* In 2017, consumers spent \$453.46 billion on the web for retail purchases, a 16.0% increase over 2016. Overall, e-commerce accounted for 49% of the growth seen in retail in 2017.

Payment Insecurity  
How Visa and Mastercard Use Standard Setting to Restrict Competition and Thwart Payments Innovation  
<https://www.paymentscardsandmobile.com/major-card-schemes-set-for-simpler-e-commerce-via-emvco-secure-remote-commerce/>



After considerable pressure, and in an unprecedented move, EMVCo released a draft standard – “Version 0.9” – for public comment in the fourth quarter of 2018. However, the public was given only forty-five days to review 329 pages of technical content with no context beyond the published 30-page high level framework. Despite request for clarification and for opening of the standard from the broader market, little changed from the draft standard when the final Version 1.0 was published in June 2019. In a prime example of its flawed structure, EMVCo purports to allow others the opportunity to be heard, and “have a voice” but, in the end, no one outside the core owners can really influence outcomes. Shortly thereafter the card companies announced their plans to launch Secure Remote Commerce programs during the latter part of 2019. Based on the timing of these announcements and the publication date of the final Version 1.0, the card company product plans were likely developed based on a draft specification prior to public input.

Despite EMVCo’s claims of incorporating extensive industry feedback during this review process, sources interviewed for this paper (who wished to remain anonymous because of the nonpublic nature of their discussions) reported having been left with many unanswered questions about the participation of U.S. unaffiliated debit networks and the ability of merchants to route transactions to the networks of their choice. Participants also reported questions about key roles and responsibilities that were delegated to the card companies.

#### **12.6 Industry Concerns with SRC Standard**

EMVCo leaves many SRC operational implementation choices to the sole discretion of the card companies. Although the use of 3-D Secure and tokenization are optional, there are major concerns that choice and routing limitations experienced with other EMVCo standards will be replicated within SRC. EMVCo states that use of non-EMV tokens and routing decisions are outside the scope of the SRC standard and leaves those decisions to the card companies, potentially limiting the choice of products or solutions that support enhanced security and competitive choice for merchant routing.

The rules and regulations for SRC programs are proprietary to the card companies. EMVCo has chosen to defer to its member owners in strategic areas where the companies can leverage their market strength to create entry barriers for competitors. SRC threatens PayPal, Alipay, Google Pay and Amazon Pay by potentially limiting their participation in SRC programs. Such reduction in competition would also affect merchants’ and consumers’ choices.

Merchants are also concerned that they might not be able to incorporate or prioritize their own proprietary payment products within SRC digital card facilitators. Despite feedback provided during the draft specification public comment period, the initial Version 1.0 specification does not allow a merchant or consumer to prioritize the payment cards within the candidate list presented to the consumer within SRC checkout on a merchant’s own website. Mastercard has subsequently pushed EMVCo to modify the standard to enable prioritization within the candidate list of its co-branded cards. However, the optimal solution calls for merchant and consumer choice of that prioritization for all cards within and outside of SRC.

Based on SRC program hierarchy, a high-level review of both the SRC framework and draft standard as well as review of the early SRC implementations, we identify potential outcomes that could negatively impact other payment industry stakeholders:

- In theory, merchants can create their own proprietary SRC programs. However, both networks have communicated that existing wallets, such as the reincarnated Visa Checkout and Masterpass, will be the first ones to transition consumers to SRC. Both Visa and Mastercard have been able to launch their SRC programs in October of 2019 due their “inside” view into the development of the standard through EMVCo. Neither EMVCo, Visa or Mastercard have published their implementation guides for merchants at large to consider the effort, investment, or opportunity of taking this step.

- Early merchant implementations show the digital card facilitator or wallets to be a re-incarnation of Visa Checkout and Masterpass. There can be multiple digital card facilitators connected to one SRC program, but it is the SRC program that determines the facilitator selection criteria.<sup>44</sup> These criteria are not defined in the standard and are left to the discretion of the SRC program owners. Will the card companies, in their roles as SRC program owners, limit or deprioritize facilitators other than their own, limiting competition?
- All the account information stored in digital card facilitators is card-based and does not provide for any other type of account. Payment card data as defined in the standard is an 11- to 19-digit account number generated within ranges associated with a bank identification number by a card issuer.<sup>45</sup> This automatically limits payment instruments to cards, preventing any competing payment methods from participating.
- The EMVCo standard leaves to the discretion of the SRC programs whether to share payment data beyond the token, expiry date, and other relevant information required to process a payment. Merchants are concerned that the card companies may choose not to share other important information such as the primary account number, bank identification number or card product type, all important elements for merchants to decide their routing and processing options.
- The EMVCo standard offers choices with regards to the level of security enabled, which suggests security is dependent on the SRC implementation. For example, device binding may not be implemented in the

initial market deployment by one SRC system while another SRC system may choose to enable device binding upon the initial market deployment. An open payment standards body should be setting standards that meet minimum security requirements based on collective aggregate input from all stakeholders versus leaving those decisions to the card companies, which are the early implementors.

- The implementation by each SRC program imposes costs, rules and requirements that are set by the card companies. This creates a large concern for merchants as to what SRC will do to their total cost of payments: Will there be a fee for associating third-party digital card facilitators to an individual SRC program? Will there be a digital card facilitator fee to resolve a request for payment data to the merchant or to provide additional payment data? Will Visa and Mastercard also assess additional fees for their tokenization services, as was originally suggested when the Visa Token Service and Mastercard Digital Enablement Service were introduced? Will Visa and Mastercard, the two initial SRC program owners, charge an additional fee for processing transactions through their SRC systems?

Finally, although merchants' acceptance of SRC has been communicated initially as a choice, it is concerning that card companies could, in the future, mandate merchants' participation under their proprietary rules. Smaller merchants may not have a choice of SRC participation as they are heavily dependent on their payment service providers. In addition, the card companies may use financial penalties or incentives to force merchant adoption of SRC and restrict competition on merchants' checkout pages.<sup>46</sup>

<sup>44</sup> The SRC Program establishes proprietary criteria that defines the selection of a specific Digital Card Facilitator

<sup>45</sup> Although the standard specifies 11 to 19 digits, the early implementations of SRC by Visa and Mastercard under the banner "Click to Pay", limits the types of forms of payments even further by only allowing account numbers of 15-16 digits in length

<sup>46</sup> There is a precedent for this behavior. In the early 1990's Visa established the electronic interchange reimbursement fee, also known as EIRF, to incentivize merchants to adopt electronic authorization rather than continue using floor limits. It is, therefore, reasonable to be concerned that the card companies could price non-SRC transactions at a higher interchange.

### 12.7 Conclusion

In theory, some of the ideas behind SRC are good: lowering fraud while enhancing consumers' experiences are hard to argue against. Complaints

are not with the concept behind SRC, but with the

development of this standard without meaningful public input. EMVCo claims standardization and interoperability justify SRC's existence, but EMVCo is a closed environment providing prioritized benefit to its owners. At this time there is no indication that SRC will be interoperable with unaffiliated debit networks or any other competing system, other than general oral representations at public forums that "nothing will change" with regards to processes behind the button. If history is an indicator, SRC will be restricted to the card companies' brands and products, just as all other EMVCo's standards have restricted competitive products and services.

EMVCo claims that it "has the strategic breadth, industry knowledge and technical ability, coupled

with a proven record of specification delivery, to facilitate the development of secure and interoperable remote payment solutions ... that maintain compatibility with the existing payment

infrastructure." What is clearly missing from this list is an open and inclusive environment for all stakeholders to participate and affect outcomes.

With SRC, the card companies are leveraging EMVCo standards in a bid to limit competition in online commerce. Cards are losing market share to alternative payment methods, and their own Visa Checkout and Masterpass were dismal failures. The card companies' concern for e-commerce customer experience is a veil for revitalizing card-brand dominance in online commerce. Merchant and consumer groups are justified in their growing skepticism about SRC even as the card brands continue to increase their drumbeats for premature adoption that preempts both present and future competition.

## PART IV—CONCLUSIONS

### 13. CONCLUSIONS

The questions asked in the beginning of this paper were:

- Is EMVCo furthering the entire U.S. payments industry or simply protecting Visa and Mastercard's market share?
- Is EMVCo capable of developing standards in areas beyond its original charter and are these standards delivering more efficient and secure payments?
- Is the U.S. payments industry's competitive landscape being hurt by allowing EMVCo to establish broad payment standards and should this work be performed by true open standards-setting bodies?

#### **13.1 Is EMVCo Protecting Visa's and Mastercard's Market Share?**

Yes. EMVCo is a vehicle for collusion among the card companies on payment standards. Visa and Mastercard use this process to jointly work on technology and processes that benefit them, preserving or increasing their market dominance, while stifling the emergence of any competition. The card companies hand their work to EMVCo, which turns it into standards, giving the patina of credibility to technology that is biased in favor of the card companies. Despite claiming to only create "specifications," EMVCo produces standards implemented in a near-identical manner by the card companies and, when EMVCo releases standards, the card companies are immediately ready to implement them because the card companies *are* EMVCo and they design the standards to meet their needs.

Visa's and Mastercard's obfuscation efforts to create the impression that EMVCo is an independent organization are unconvincing. EMVCo's Board of Managers is made up exclusively of long-term card company employees, none having less than 10 years' tenure. These individuals' function without any checks from other sectors of the U.S. payments

industry such as bankers, merchants or consumers to counterbalance their perspective.

EMVCo operates in opacity and with no accountability to anyone but its owners. The input provided by its technical and business associate members is limited almost entirely to card payment processing companies that need to understand the impact of the new standards to their own platforms. Because all decision-making powers are limited to only EMVCo's owners, merchants recognize that joining EMVCo is not effective and are underrepresented.

EMVCo claims to be the representative of the global payments industry. This paper concludes that EMVCo is not an appropriate standards body and does not represent the industry. True standards are developed in a collaborative manner in open forums with diverse and inclusive representation of all stakeholders. That is not the case with EMVCo which is structured to deliver standards that benefit only the card companies and protect their market share.

#### **13.2 Is EMVCo Capable of Developing Standards in Areas Beyond its Original Charter?**

No. Throughout its history, EMVCo has sacrificed payment security for the convenience of the card companies and for retaining or increasing those companies' transaction volume. Its standards constantly limit merchant choice for transaction routing, in violation of U.S. federal law. This paper concludes that:

- EMVCo betrayed its own charter to provide secure chip card payments by acquiescing to, and ultimately supporting, Visa's 20-year-plus battle against U.S. PIN-based networks and Visa's insistence on chip and signature instead of PIN.
- EMVCo introduced a complex, expensive and unwieldy system for mobile payments using near-field communication technology

because it protects the status quo of its owners while preempting the work of other standard-setting organizations and preventing competitors entering mobile payments;

- EMVCo co-opted tokenization standards work from other organizations and developed an anticompetitive tokenization standard that discriminates against debit networks and non-card forms of payment.
- EMVCo ignored the work of the FIDO Alliance and W3C regarding open standards for authentication that would have also been available to non-card payment systems, instead adapting the card companies' 3DS system to preempt the market from competitive solutions.
- EMVCo is now preempting the market and coopting standards for e-commerce by asserting itself as the "representatives of the payments community" to develop a Secure Remote Commerce standard that will make it difficult to route transactions through unaffiliated debit networks, create higher dependence on the card companies and increase merchants' payment processing costs.

**13.3 Is the U.S. Payments Industry's Competitive Landscape Being Hurt by Allowing EMVCo to Set Standards?**

Yes, the United States lags many countries when it comes to payments. QR code-based mobile payments are the norm in many Asian countries, for example, while tap-and-go contactless payments have been widely adopted in the United Kingdom, Canada and Australia, and both UK and European consumers have access to real-time bank transfers. Consumers in these countries have more options to pay that are convenient to them whereas merchants

also benefit as competition keeps lower payment costs lower than what U.S. merchants pay.

Meanwhile, the card companies — primarily Visa and Mastercard — use EMVCo as their surrogate as they seek to foster an archaic, card-based environment that is one of the most expensive and fraud-prone systems in the world. EMVCo missed the mark in selecting NFC instead of opening mobile payments to other technologies such as QR codes and stifled new possible payment systems by implementing a narrow tokenization standard that does not accommodate other payment methods.

While EMVCo claims to promote "compatibility" and "interoperability" in order to provide "secure" transactions, those are code words for control and preservation of the status quo for card companies. EMVCo standards exclude other forms of payment and create barriers to merchant choice in a way that is continuous and stifling. EMVCo's de facto standards cause all payment industry participants — including merchants, card-issuing banks and merchants' "acquiring" banks — to spend millions of dollars on implementation. Doing so all but eliminates the possibility of investing in alternative payment methods.

It is our conclusion that the U.S. payments industry is being harmed by the card companies and EMVCo. The setting of payment standards for topics such as authentication and tokenization should be migrated away from EMVCo to independent and neutral national or international standards-setting bodies. EMVCo's collusion with the credit card companies has put profits ahead of security, driven up costs for businesses and consumers alike, and has left the United States with a fraud-prone payment card system even as fraud has been reduced in the rest of the world.

## PART V—ENDNOTES

- <sup>1</sup> “A Guide to EMV Chip Technology Version 3.0,” EMVCo, December 18, 2017, <https://www.emvco.com/terms-of-use/?u=wp-content/uploads/documents/A-Guide-to-EMV-Chip-Technology-v3.0-1.pdf>.
- <sup>2</sup> Claire Greene and Joanna Stavins, “The 2017 Diary of Consumer Payments Choice,” *Diary of Consumer Payments Choice by the Federal Reserve Bank of Atlanta* no. 18-5 (2018), <https://www.frbatlanta.org/banking-and-payments/consumer-payments/research-data-reports/2018/the-2017-diary-of-consumer-payment-choice.aspx>.
- <sup>3</sup> “The Federal Reserve Payments Study: 2018 Annual Supplement,” the Federal Reserve System, December 2018, <https://www.federalreserve.gov/newsevents/pressreleases/files/2018-payment-systems-study-annual-supplement-20181220.pdf>.
- <sup>4</sup> Jim Daly, “Interlink Starts Growing Again And Visa Prospers Despite Legal and Regulatory Uncertainties,” *Digital Transactions*, July 24, 2013, <http://www.digitaltransactions.net/interlink-starts-growing-again-and-visa-prospers-despite-legal-and-regulatory-uncertainties/>.
- <sup>5</sup> Douglas King, “Chip-and-PIN: Success and Challenges in Reducing Fraud,” Retail Payments Risk Forum Working Group of the Federal Reserve Bank of Atlanta, January 2012, [https://www.frbatlanta.org/-/media/documents/rprf/rprf\\_pubs/120111wp.pdf](https://www.frbatlanta.org/-/media/documents/rprf/rprf_pubs/120111wp.pdf).
- <sup>6</sup> “The WTO Agreements Series Technical Barriers to Trade,” World Trade Organization, 2014, [https://www.wto.org/english/res\\_e/publications\\_e/tbttrade\\_e.pdf](https://www.wto.org/english/res_e/publications_e/tbttrade_e.pdf).
- <sup>7</sup> “Global Standards: Building Blocks for the Future,” U.S. Congress Office of Technology Assessment, <https://www.princeton.edu/~ota/disk1/1992/9220/9220.PDF>, 101.
- <sup>8</sup> Masami Tanaka, “Tools for leaders – Demonstrating and exploiting the benefits of standards,” *ISO Focus+*, June 2010, vol. 1 (6):1, [https://www.iso.org/files/live/sites/isoorg/files/news/magazine/ISO%20Focus%2B%20\(2010-2013\)/en/2010/ISO%20Focus%2B%2C%20June%202010.pdf](https://www.iso.org/files/live/sites/isoorg/files/news/magazine/ISO%20Focus%2B%20(2010-2013)/en/2010/ISO%20Focus%2B%2C%20June%202010.pdf).
- <sup>9</sup> Edwin Mansfield, *Microeconomics Theory and Application* (New York NY:W.W. Norton 1970)
- <sup>10</sup> “A Guide to EMV Chip Technology Version 3.0,” EMVCo, December 18, 2017, <https://www.emvco.com/terms-of-use/?u=wp-content/uploads/documents/A-Guide-to-EMV-Chip-Technology-v3.0-1.pdf>.
- <sup>11</sup> *ibid.*
- <sup>12</sup> Tim Büthe and Walter Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy*, (Princeton: Princeton University Press, 2011).
- <sup>13</sup> “A Guide to EMV Chip Technology Version 3.0,” EMVCo, December 18, 2017, <https://www.emvco.com/terms-of-use/?u=wp-content/uploads/documents/A-Guide-to-EMV-Chip-Technology-v3.0-1.pdf>.
- <sup>14</sup> Carl F. Cargill, “Why Standardization Efforts Fail,” *Standards* 14, no. 1 (2011), doi: <http://dx.doi.org/10.3998/3336451.0014.103>.
- <sup>15</sup> “EMVCo Operating Principles,” EMVCo, 2017, [https://www.emvco.com/wp-content/uploads/2017/03/EMVCo-Website-Content-8.0-Operating-Principles-PDF\\_v1.1-1.pdf](https://www.emvco.com/wp-content/uploads/2017/03/EMVCo-Website-Content-8.0-Operating-Principles-PDF_v1.1-1.pdf).

- <sup>16</sup> Douglas King, "Chip-and-PIN: Success and Challenges in Reducing Fraud," Retail Payments Risk Forum Working Group of the Federal Reserve Bank of Atlanta, January 2012, [https://www.frbatlanta.org/-/media/documents/rprf/rprf\\_pubs/120111wp.pdf](https://www.frbatlanta.org/-/media/documents/rprf/rprf_pubs/120111wp.pdf).
- <sup>17</sup> *ibid.*
- <sup>18</sup> *United States of America v. Visa U.S.A. Inc., Visa International Corp., and Mastercard International Incorporated*, (98 Civ. 7076 BSJ) U.S. District Court Filed 10-9-2001 Southern District of New York
- <sup>19</sup> Allie Johnson "U.S. credit cards becoming outdated, less usable abroad", CreditCards.com, October 1, 2008, <https://www.creditcards.com/credit-card-news/outdated-smart-card-chip-pin-1273.php>.
- <sup>20</sup> Robin Sidel, "Debit-Card Use Overtakes Credit," The Wall Street Journal, May 1, 2009, <https://www.wsj.com/articles/SB124104752340070801>.
- <sup>21</sup> "Debit Card Use Remains Robust in Midst of Economic Downturn," Pulse, June 14, 2010, last accessed July 11, 2019, <https://www.pulsenetwork.com/news/archive/2010/debit-use.html>.
- <sup>22</sup> "Visa Recommended Practices for EMV Chip Implementation in the U.S.," Visa, July 11, 2012, <https://technologypartner.visa.com/Download.aspx?id=153>.
- <sup>23</sup> "Visa Announces Plan to Accelerate Chip Migration and Adoption of Mobile Payments," Visa, August 8, 2011, <https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.8916.html>
- <sup>24</sup> *ibid.*
- <sup>25</sup> "Mobile Proximity Contactless Payment FAQ#1," EMVCo, July 2008, [https://2426-9805.el-alt.com/best\\_practices.aspx?id=162](https://2426-9805.el-alt.com/best_practices.aspx?id=162).
- <sup>26</sup> "Contactless Mobile Payment Architecture Overview," EMVCo, June 2010, [https://www.emvco.com/wp-content/uploads/documents/Contactless\\_Mobile\\_Payment\\_Architecture\\_Overview\\_2010062808363068.pdf](https://www.emvco.com/wp-content/uploads/documents/Contactless_Mobile_Payment_Architecture_Overview_2010062808363068.pdf).
- <sup>27</sup> "EMV Contactless Specifications for Payment Systems, Book A, Architecture and General Requirements Version 2.1," EMVCo, March 2011, [https://www.emvco.com/wp-content/uploads/2017/05/Book\\_A\\_Architecture\\_and\\_General\\_Rqmts\\_v2\\_6\\_Final\\_20160422011856105.pdf](https://www.emvco.com/wp-content/uploads/2017/05/Book_A_Architecture_and_General_Rqmts_v2_6_Final_20160422011856105.pdf).
- <sup>28</sup> Fumiko Hayashi and Terri Bradford, "Mobile payments: Merchants' Perspectives," *Economic Review, Federal Reserve Bank of Kansas City*, Second Quarter (2014): 33-58, <https://www.kansascityfed.org/~media/files/publicat/econrev/econrevarchive/2014/2q14hayashi-bradford.pdf>.
- <sup>29</sup> "QR Code Specification for Payment Systems (EMV QRCPs) Consumer-Presented Mode, Version 1.0," EMVCo, July 2017, <https://www.emvco.com/wp-content/uploads/documents/EMVCo-Consumer-Presented-QR-Specification-v1-1.pdf>.
- <sup>30</sup> "QR Code Specification for Payment Systems (EMV QRCPs), Merchant-Presented Mode Version 1.0," EMVCo, July 2017, <https://www.emvco.com/wp-content/uploads/documents/EMVCo-Merchant-Presented-QR-Specification-v1-1.pdf>.
- <sup>31</sup> "Visa Best Practices for Data Field Encryption Version 1.0," Visa, October 5, 2009, <https://bd.visa.com/dam/VCOM/global/support-legal/documents/bulletin-encryption-best-practices.pdf>.
- <sup>32</sup> "Visa Best Practices for Tokenization Version 1.0," Visa, July 14, 2010, <https://usa.visa.com/dam/VCOM/global/support-legal/documents/bulletin-tokenization-best-practices.pdf>.

- <sup>33</sup> “Testimony of David Fortney The Clearing House Payments Company House Committee on Financial Services Subcommittee on Financial Institutions and Consumer Credit,” Subcommittee on Financial Institutions and Consumer Credit, March 5, 2014, <https://www.theclearinghouse.org/-/media/files/association-related-documents/20140305-david-fortney-testifies-on-tokenization.pdf>.
- <sup>34</sup> Jim Daly, “Interlink Starts Growing Again And Visa Prospers Despite Legal and Regulatory Uncertainties,” Digital Transactions, July 24, 2013, <http://www.digitaltransactions.net/interlink-starts-growing-again-and-visa-prospers-despite-legal-and-regulatory-uncertainties/>.
- <sup>35</sup> “Merchant community coalesces behind open process for security standards to better protect U.S. businesses and consumers from cybercriminal activity,” PR Newswire, July 28, 2014, <https://www.prnewswire.com/news-releases/merchant-community-coalesces-behind-open-process-for-security-standards-to-better-protect-us-consumers-and-businesses-from-cybercriminal-activity-268879481.html>.
- <sup>36</sup> “Mastercard, Visa and American Express Propose New Global Standard to Make Online and Mobile Shopping Simpler and Safer,” Mastercard, October 1, 2013, <https://newsroom.Mastercard.com/press-releases/Mastercard-visa-and-american-express-propose-new-global-standard-to-make-online-and-mobile-shopping-simpler-and-safer/>.
- <sup>37</sup> *ibid.*
- <sup>38</sup> “EMV Payment Tokenisation Specification - Technical Framework v1.0,” EMVCo, March 10, 2014, [https://www.emvco.com/wp-content/uploads/documents/EMVCo\\_Payment\\_Tokenisation\\_Specification\\_Technical\\_Framework\\_v1.0.pdf](https://www.emvco.com/wp-content/uploads/documents/EMVCo_Payment_Tokenisation_Specification_Technical_Framework_v1.0.pdf).
- <sup>39</sup> “The Fed Wants To Clean Up Token Confusion,” Pymnts.com, September 29, 2014, <https://www.pymnts.com/in-depth/2014/the-fed-wants-to-clean-up-token-confusion/>.
- <sup>40</sup> “Visa CEO Predicts a ‘Relatively Easy’ Conversion to the New Secure Remote Commerce System,” Digital Transactions, October 24, 2019, <http://www.digitaltransactions.net/visa-ceo-predicts-a-relatively-easy-conversion-to-the-new-secure-remote-commerce-system/>.
- <sup>41</sup> “EMV Secure Remote Commerce Technical Framework - Version 1.0,” EMVCo, November 1, 2017, <https://www.emvco.com/wp-content/plugins/pmpro-customizations/ov-getfile.php?u=/wp-content/uploads/documents/Secure-Remote-Commerce-Framework-FINAL-v1.0.pdf>.
- <sup>42</sup> *ibid.*
- <sup>43</sup> “EMVCo, FIDO Alliance, and W3C Form Interest Group to Enhance Security and Interoperability of Web Payments,” W3C, April 17, 2019, <https://www.w3.org/2019/04/pressrelease-wps.html.en>.
- <sup>44</sup> “EMVCO Secure Remote Commerce Specification, Version 0.9 DRAFT,” EMVCo, October 19, 2018, <https://www.emvco.com/wp-content/uploads/documents/EMVCo-Secure-Remote-Commerce-Specification-v0.9-2.zip>.
- <sup>45</sup> *ibid.*

<sup>i</sup> Claire Greene and Joanna Stavins, “The 2018 Diary of Consumer Payments Choice,” *Diary of Consumer Payments Choice by the Federal Reserve Bank of Atlanta* no. 19-03 (2019), <https://www.frbatlanta.org/-/media/documents/banking/consumer-payments/diary-of-consumer-payment-choice/2018/2018-diary-of-consumer-payment-choice.pdf>.

<sup>ii</sup> The Nilson Report, “Card Fraud Losses Reach \$27.85 Billion,” November 2019 Issue 1164.

<sup>iii</sup> Open Banking is a concept being implemented in Europe under the second Payments Services Directive (PSD2) that requires all banks to open APIs to allow accredited Payment Initiators (e.g. merchants, Payment Service providers, etc.) access bank accounts bypassing the card companies; “push” payments are customer-initiated payments where the consumer send payment for goods and services to merchants, sometimes in real-time, using a non-card payment network such as ACH or a Real Time Payment service.



February 3, 2020

The Honorable Stephen F. Lynch Chairman  
Task Force on Financial Tech. Subcommittee  
U.S. House Of Representatives Washington, DC  
20515

The Honorable Tom Emmer Ranking Member  
Task Force on Financial Tech. Subcommittee  
U.S. House Of Representatives Washington, DC  
20515

RE: "Is Cash Still King? Reviewing the Rise of Mobile Payments"

Dear Chairman Lynch and Ranking Member Emmer:

The Secure Payments Partnership represents industries that span the payments system and we are committed to making the U.S. payments infrastructure the strongest, most innovative, and most secure in the world. We advance sound policies that drive state-of-the-art technologies, competition and collaboration to continually improve the nation's payment infrastructure, meet the evolving needs of commerce, and provide businesses and consumers convenience, flexibility and security in payment options. We thank Chairman Lynch, Ranking Member Emmer, and the Task Force for holding this important hearing, and we appreciate the opportunity to provide comments and to share a white paper that examines this timely topic.

Card and electronic payments have experienced explosive growth over the last ten years. As of 2019, card payments accounted for more than 58% of all U.S. consumer purchase payments by count according to a report from the Federal Reserve Bank of Atlanta<sup>1</sup>. The same report states that while card payments are seeing robust growth, consumer use of cash decreased to 26 percent of all transactions in 2018, down from 30 percent in 2017.

The change in the way Americans engage in commerce represents a critical juncture for payments in this country. Innovation is happening rapidly across the globe, but in many ways the U.S. lags behind. For example, real time payments are a reality in numerous countries. And mobile payments are the norm in countries across Asia and Africa.

In terms of security, the U.S. has the dubious distinction of leading the world in fraud. The U.S. alone accounts for more than a third of the card fraud in the world, while only accounting for about twenty-one percent of all transactions<sup>2</sup>.

The failure of the U.S. to adopt payment innovations that have become ubiquitous in other parts of the globe as well as our high rates of fraud can be attributed in part to our closed standard setting practices that are dominated by a handful of global networks.

How standards are produced and who produces them is a critical consideration in modern economies. Any standards that give advantage to certain companies over their competitors are a valid concern as this impacts innovation as well as the welfare and competitiveness of the U.S. payments system. Such advantages are also detrimental to security and innovation, as the dominant industry's interests are naturally prioritized often at the detriment of security and the preclusion of competitive innovators.

Exemplary of this is the standards setting body, EMVCo. In contrast with other standards-setting organizations, which advocate openness and inclusivity, EMVCo's decisions are effectively made by their owners – Visa, Mastercard, Discover, American Express, JCB, and China UnionPay. There is no consumer group, merchant, unaffiliated network, or US financial institution that has a final voting voice in EMVCo's standard setting process.

The impact of the lack of multi-stakeholder representation in EMVCo is real and measurable. In the United States, the payments industry spends millions of dollars every year complying with standards set by EMVCo and implemented by the card companies. This high level of investment prevents the use of capital to innovate or develop other alternative payment methods. The attached white paper examines how EMVCo standards negatively impacted security and/or prioritized the competitive interests of its executive committee members over that of security and innovation.

EMVCo's current structure is not designed to develop, nor capable of developing, open standards. Its "closed" standards have repeatedly failed to properly address ongoing challenges to payment security and inclusivity at a time when collaborative and competitive standards will be needed to innovate, and most immediately, keep up with upcoming industry developments such as open banking or "push" payments.<sup>iii</sup>

If the United States is going to lead the world in payments innovation, security, and inclusivity we cannot continue to allow two players, Visa and Mastercard, to dominate standards setting. A truly open standards setting process that is transparent and gives a meaningful voice to all players within that system will lay the foundation for a U.S. payments system that is secure, competitive, innovative, and inclusive.

As the Task Force continues to examine mobile payments and other emerging payments technologies, SPP would request the examination the practices and roles of Visa and Mastercard and the standard setting bodies that they govern. We believe that standards setting bodies should promote standards that increase security, enhance competition, and foster innovation. We would appreciate the opportunity to work with the Task Force as you continue to work on these important topics.

Sincerely,

Secure Payments Partnership



<sup>1</sup> Claire Greene and Joanna Stavins, "The 2018 Diary of Consumer Payments Choice," *Diary of Consumer Payments Choice by the Federal Reserve Bank of Atlanta* no. 19-03 (2019), <https://www.frbatlanta.org/-/media/documents/banking/consumer-payments/diary-of-consumer-payment-choice/2018/2018-diary-of-consumer-payment-choice.pdf>.

<sup>2</sup> The Nilson Report, "Card Fraud Losses Reach \$27.85 Billion," November 2019 Issue 1164.

<sup>3</sup> Open Banking is a concept being implemented in Europe under the second Payments Services Directive (PSD2) that requires all banks to open APIs to allow accredited Payment Initiators (e.g., merchants, Payment Service providers, etc.) access bank accounts bypassing the card companies; "push" payments are customer-initiated payments where the consumer send payment for goods and services to merchants, sometimes in real-time, using a non-card payment network such as ACH or a Real Time Payment service.