

EXAMINING SCAMS AND FRAUD IN THE BANKING SYSTEM AND THEIR IMPACT ON CONSUMERS

HEARING

BEFORE THE

COMMITTEE ON

BANKING, HOUSING, AND URBAN AFFAIRS

UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

ON

EXAMINING SCAMS AND FRAUD IN THE BANKING SYSTEM AND THEIR
IMPACT ON CONSUMERS

FEBRUARY 1, 2024

Printed for the use of the Committee on Banking, Housing, and Urban Affairs



Available at: <https://www.govinfo.gov/>

U.S. GOVERNMENT PUBLISHING OFFICE

59–592 PDF

WASHINGTON : 2026

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

SHERROD BROWN, Ohio, *Chair*

JACK REED, Rhode Island	TIM SCOTT, South Carolina
ROBERT MENENDEZ, New Jersey	MIKE CRAPO, Idaho
JON TESTER, Montana	MIKE ROUNDS, South Dakota
MARK R. WARNER, Virginia	THOM TILLIS, North Carolina
ELIZABETH WARREN, Massachusetts	JOHN KENNEDY, Louisiana
CHRIS VAN HOLLEN, Maryland	BILL HAGERTY, Tennessee
CATHERINE CORTEZ MASTO, Nevada	CYNTHIA M. LUMMIS, Wyoming
TINA SMITH, Minnesota	J.D. VANCE, Ohio
RAPHAEL G. WARNOCK, Georgia	KATIE BOYD BRITT, Alabama
JOHN FETTERMAN, Pennsylvania	KEVIN CRAMER, North Dakota
LAPHONZA R. BUTLER, California	STEVE DAINES, Montana

LAURA SWANSON, *Staff Director*

LILA NIEVES-LEE, *Republican Staff Director*

ELISHA TUKU, *Chief Counsel*

AMBER BECK, *Republican Chief Counsel*

CAMERON RICKER, *Chief Clerk*

SHELVIN SIMMONS, *IT Director*

PAT LALLY, *Assistant Clerk*

C O N T E N T S

THURSDAY, FEBRUARY 1, 2024

	Page
Opening statement of Chair Brown	1
Prepared statement	38
Opening statements, comments, or prepared statements of:	
Senator Scott	3
Prepared statement	39

WITNESSES

Carla Sanchez-Adams, Senior Attorney, National Consumer Law Center	6
Prepared statement	42
Response to written question of:	
Senator Butler	89
Paul Benda, Executive Vice President, Risk, Fraud and Cybersecurity, American Bankers Association	8
Prepared statement	76
Response to written question of:	
Senator Britt	91
John Breyault, Vice President of Public Policy, Telecommunications, and Fraud, National Consumers League	10
Prepared statement	85
Response to written question of:	
Senator Butler	93

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

Statement submitted by BPI	94
Letter submitted by AFSA	99
Letter submitted by CBA	101
Statement submitted by ICBA	103

EXAMINING SCAMS AND FRAUD IN THE BANKING SYSTEM AND THEIR IMPACT ON CONSUMERS

THURSDAY, FEBRUARY 1, 2024

U.S. SENATE,
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
Washington, DC.

The Committee met at 10:06 a.m., in room 538, Dirksen Senate Office Building, Hon. Sherrod Brown, Chair of the Committee, presiding.

OPENING STATEMENT OF CHAIR SHERROD BROWN

Chair BROWN. The Banking, Housing, and Urban Affairs Committee will come to order.

When consumers send money through an app or send a check in the mail, they are supposed to be able to trust that financial companies are protecting their money and will help them if something goes wrong. Yet that is not what we see.

Scammers and fraudsters have ramped up their efforts to take people's money. Banks and payment apps have stood on the sidelines while the problem has only gotten worse. Pretty much everyone has either been scammed, or knows someone who has been scammed, when trying to use a financial service.

Today one of the most popular ways people send money is through so-called peer-to-peer apps like PayPal, Venmo, Cash App, and Zelle. These apps are now part of most Americans' day-to-day lives. Seventy-five percent of adults have used at least one of them. Forty percent of Americans report using them at least once a month.

Where consumers see convenience and accessibility, scammers see an opportunity.

In 2022, one major payment app had more than \$100 million in "unauthorized transactions." Another had almost \$60 million.

Of course, it is not just new technology or payment methods, of course, that scammers target. Check fraud is as old as our banking system. They will steal a check from the mail, use chemicals to wash off the key details, then fill it in with the details they want and deposit it.

You might think that more people using apps would make checks less of a target, but it seems to be the opposite—check fraud is getting worse too. Last year, the Financial Crimes Enforcement Network noticed a rise in check fraud so drastic that they issued a public alert.

My colleagues and I wrote to the American Bankers Association expressing concerns on the issue, and they created an information directory providing contact information for banks to resolve check fraud claims. By the end of 2022, depository institutions had reported more than 500,000 incidents of check fraud, more than double the year before. Scammers broke their record again in 2023. So the evidence clearly shows it is getting worse.

The same goes for wire transfers. Scammers target wire transfers because they can steal a larger portion of consumers' savings through wire transfers. Americans will often use wire transfers when they want to send large amounts of money, like when buying a house.

Imagine a family in the process of buying a home, juggling all the details of the process, along with the excitement that they have of reaching a major life milestone. On top of everything else they have to worry about, they have to defend against scammers posing as a real estate agent or title company targeting the family's down-payment. In 2023, consumers lost at least \$270 million to wire fraud.

And now we are faced with the possibility that artificial intelligence will make these problems worse. As just one example, scammers can now use AI to clone a person's voice to bypass voice authentication procedures. Banks, payment apps, and other financial institutions are not doing nearly enough to prepare for the threat AI poses in increasing the scale and the impact of scams.

All of these problems with scams are rampant.

In Dublin, Ohio, a suburb of Columbus, a retired FBI agent, wrote a check for less than \$200. Someone stole that check from a mailbox right in front of a post office, changed the number to \$8,590 and cashed it.

In another case, a 17-year-old student in Ohio received an acceptance letter from her dream college. Someone posing as another admitted student reached out and scammed her out of almost \$3,000 of her own money through Zelle. That \$3,000 was three-quarters of her college money she saved up by working at a discount drugstore. None of this mattered to the bank. As far as the bank was concerned, this young woman was responsible for the money and additional fees for depositing bad checks. In the end, she got her money back, but only after the efforts of a very tenacious mother, who tracked down the local executive of the bank.

No one should have to go to those lengths because banks, payment apps, and other financial institutions cannot get their act together to protect their customers. When these incidents happen, people lose their hard-earned money. And they are often made to feel ashamed and embarrassed.

No one ever tells a victim of a hold-up or a break-in at their home that they were stupid or should have known better than to be robbed, but that is exactly what consumers who are scammed too often hear.

Let's be clear, being scammed has nothing to do with savviness or intelligence or education.

Just last year, a retired White House scientist was scammed out of \$655,000 of her retirement savings. Those scammers were organized. They sent her a pop-up message on her computer, rerouted

a phone call she meant for her bank, and kept her on the phone for days on end. She still wonders about what she could have done differently. But no one should have to think about that question.

And to be clear, the answer to these types of stories is not to warn people to be better prepared or put millions of consumers through a so-called “financial education” course. Of course we all need better financial education, but that is not the backstop for all of this. Americans do not have time for that. They have jobs and kids and bills to worry about. It is not on them. It is on the companies that allow the scam. People should be able to have an expectation their money is safe when they have a reputable bank.

People lose their money because payment apps and banks do not put enough measures in place to protect their customers.

For example, among the peer-to-peer companies, Cash App refunded just 16 percent of unauthorized transactions in calendar year 2022, just \$1 out of \$6. Zelle claims they reimburse consumers who have been victims of imposter scams, but their website states that since the consumer “authorized the payment, you may not be able to get your money back.” It is unclear whether Zelle will actually reimburse victims of imposter scams. They need to clarify instead their reimbursement policy.

These companies need to step up, and they apparently need rules to make them do it, not more financial education. These banks, payment apps, and other financial services companies have shown us they need, shall we say, some encouragement.

The Consumer Financial Protection Bureau has a proposed rule that is one strong first step. It would help ensure that companies like Venmo, Cash App, and Zelle follow Federal consumer protection laws. This is what the CFPB does—protect consumers and their hard-earned money. When the CFPB is empowered, it ensures that the financial system works for consumers, not just big companies.

With millions of users, it only makes sense that these companies do more to protect consumers’ money. Because as we have seen in previous hearings in the last 3 years, frauds and scams are not unique in consumer finance. They are also common within cryptocurrency. We will keep pushing to make our financial system safer, whether its stopping rampant frauds and scams in cryptocurrency or in apps and check fraud.

I hope we can discuss more today about how banks, payment apps, and other financial service companies can step up for their consumers and actually earn their trust back.

Senator Scott.

OPENING STATEMENT OF SENATOR TIM SCOTT

Senator SCOTT. Thank you, Mr. Chairman.

I will start off by saying, I guess Steven Spielberg was onto something when he named the movie “Catch Me If You Can”.

Recently, I saw a movie called “The Beekeeper”, which starts off about financial scams that led to the grandmother’s suicide. Now, financial scams may not today lead to suicide, but without any question, they certainly kill your hopes, your dreams, and your sense of financial security.

The impact of financial scams, especially on our senior citizens, is undeniable. Having been the Ranking Member on the Aging Committee, we have had many, many hearings about the devastation of retirement savings lost. Lives changed. Grandmothers looking for a place to call home, moving back in with their kids or their grandkids. The devastation is so real, and so often, goes unreported in some instances. And certainly, the investigations leave many wanting.

Even in a largely digital age, more traditional forms of fraud continue to flourish. We think about the fact that whether it is check fraud, wire fraud, or mail fraud, we have seen a resurgence of criminal activity in these spaces, in addition to of course the new types of fraud that comes along with the technological advancements that we have seen around our country, and certainly the innovations around the world.

Not only do I think of my own mother—who celebrates a birthday this weekend as a senior citizen—I think of every single South Carolinian who trusts that their money is safe when they write a check and place it in the mail, or transfer money to their grandkids.

Mr. Benda, I thank you for bringing your expertise and talking about the different kinds of fraud that can impact American consumers. Protecting consumers and preventing fraud are critical pillars of our financial system and, frankly, what our society deserves.

For many families, becoming a victim to these scams is equivalent to wiping out a lifetime of savings, and not just the dollars in the account, but the thought that you are no longer safe to transact business anywhere, in any form.

For many, it is the worry that their identity is compromised, that their credit score is impacted, and they struggle to realize just how will they survive and afford, whether it is their rent, or mortgage, or even simply groceries, which in today's inflationary economy is even harder than it was before.

Speaking of dollars, let's just count the costs. Nine billion dollars in 2022 is the cost of financial fraud. A staggering number.

Unfortunately, these criminal acts of fraud and theft are not new, and criminals like these continue to prey on the vulnerable.

This is precisely why our financial institutions and financial industry participants should—and do—spend billions of dollars developing and implementing innovative technologies to strengthen security that will protect families and businesses from fraud.

But on the other side of the coin, we have not seen the same commitment from our Federal regulators. Recently, our regulators seem to be more focused on political grandstanding than promoting innovative solutions, protecting consumers, and increasing efforts that support financial education. And instead of focusing on real crimes and holding criminals responsible, this Administration seems intent on tying up financial institutions with ever-increasing amounts of Washington red tape.

Recently, the CFPB has continued its deceptively named “junk fee” campaign, targeting legitimate, contractually agreed upon payment incentives. In its latest proposals, the CFPB uses legal gymnastics to turn penalty fees into loans while slapping the label “abusive” on any practice it just does not like. The CFPB is sending

a clear message: it is willing to stretch the law beyond its limits to suit Director Chopra's political agenda.

And every dollar spent navigating Washington red tape is a dollar less on initiatives that actually help families and protect businesses. It is a dollar less for bolstering a firm's cyber defenses in the investment world that may prevent or even catch fraud before it happens. Unfounded bureaucratic regulations take resources away from financial innovation and education, both of which can help lift up the underserved and minority communities.

What concerns me even more than all of this is recent allegations that suggest that Federal law enforcement and financial regulators may be expending their resources to target Americans for their political and religious beliefs. Instead of targeting Americans for purchasing Bibles or shopping at the Bass Pro Shops, our Government should focus on doing its job, protecting our families and prosecuting actual criminals, including those behind financial scams. Unfortunately, these examples are part of a larger trend we have seen from this Administration of putting politics first.

For example, banking regulators were so focused on climate change that they failed to identify the key risk factors leading to the second-, third-, and fourth-largest bank failures in our Nation's history last spring. And again, if the CFPB was not so focused on building a public pressure campaign against so-called "junk fees," maybe it could do its job and actually protect consumers from the real harm that comes from being a victim of financial crime.

One of the best tools any of us have to fight back against financial crimes is to become better educated, both about the financial products and protections that are available to us and about the scams and methods criminals are using against us. In fact, I have long championed the idea that financial education and financial literacy is one of the most important and most critical tools for climbing the ladder of success in America.

It is why I have worked so hard to incorporate financial literacy in my work here on this Committee, and financial literacy is a core pillar of two of my initiatives, the ROAD to Housing and Capital Markets framework. And I was so proud to work across the aisle with Senator Reed last spring to pass a resolution declaring April Financial Literacy Month.

As we discuss the very real issues of financial fraud and crime, we must take a holistic approach. Our financial institutions must do their part to protect, to serve, and educate customers. And our regulators must do their job and implement the law Congress enacted, not their political wish list.

We must all work together to gain a better understanding of the options before us so that we are able to best serve our communities, our constituents, and our Nation.

I look forward to hearing from each of the three witnesses.

Chair BROWN. Thank you, Senator Scott.

I will introduce the witnesses. Ms. Carla Sanchez-Adams, Senior Attorney, National Consumer Law Center. She focuses on banking and payment systems, fintech, and high-cost lending. Welcome, Ms. Sanchez-Adams.

Mr. Paul Benda is Executive Vice President of Risk, Fraud, and Cybersecurity with the American Bankers Association. Mr. Benda, welcome.

Mr. John Breyault is the Vice President for Public Policy, Telecommunications, and Fraud for the National Consumers League. Welcome, Mr. Breyault.

Ms. Sanchez-Adams, please begin.

**STATEMENT OF CARLA SANCHEZ-ADAMS, SENIOR ATTORNEY,
NATIONAL CONSUMER LAW CENTER**

Ms. SANCHEZ-ADAMS. Chairman Brown, Ranking Member Scott, and Members of the Committee, thank you for this opportunity to testify on behalf of the National Consumer Law Center's low-income clients.

Payment fraud is everywhere and impacts all Americans, even Members of Congress. In fact, if you do a Google search on how to address payment fraud you will get 491 million responses.

However, the impacts of payment fraud are most keenly felt by certain low-income communities, older Americans, and communities of color. These communities, who are already struggling and often pushed out of the traditional banking system, can least afford to lose money due to payment fraud and errors.

Fraud is also occurring over all types of payment methods, as you heard earlier. Bank-to-bank wire transfers, checks, can now be done online and through mobile and digital applications. And fraudsters exploit the ease of these newer technologies as well. As you heard, they spoof phone numbers from real financial institutions, they utilize deep fakes, psychological manipulation, and even use force and threats of violence to get consumers to initiate transactions.

Payment fraud can be sorted into two buckets: unauthorized and fraudulently induced. The unauthorized bucket is the one where fraudsters initiate a transaction without the consumer's authority. The fraudulently induced bucket is the one where the consumer initiates a transaction but only does so as a result of a fraudulent scheme involving deception and manipulation by the fraudster.

Now consumers are impacted by both, but the responses they receive will depend on the type.

Currently, if you are a victim of payment fraud, your only hope of getting your money back is if it happened through an unauthorized electronic funds transfer, and that is because of the strong protections of the Electronic Funds Transfer Act, or the EFTA. However, even if you are in this unauthorized bucket, if it happens through a bank-to-bank wire transfer, through check fraud, forgery, or alteration, or through an Electronic Benefits Transfer card, then you are going to face an uphill battle in trying to get your money back, and that is because these are excluded from the EFTA.

And if you find yourself over here, your story fits into the fraudulently induced bucket, you are going to hear, "Too bad, so sad," because there are no clear protections currently under Federal or State law.

But there are steps that we can collaboratively take to keep impacts of fraud to a minimum, on both financial institutions and

consumers, and to incentivize more effective use of innovation to prevent payment fraud.

First, we absolutely cannot push the entire burden of payment fraud onto consumers, hoping that financial education will solve it. It is important, but it is not key.

Second, we need to update antiquated laws that offer little to no protection to consumers who have been impacted by payment fraud. In this day and age where the vast majority of transactions happen online or through mobile and digital technologies, it makes no sense that only some of these transactions are covered by the EFTA while others are not. Wire transfers and EBT cards and maybe even checks should have the protection of the EFTA. As well as fraudulently induced transactions that should have protections under the EFTA.

Third, receiving institutions should bear more responsibility. Currently in the United States there is no mandate that institutions who allow fraudsters and money mules to open an account and to receive fraudulently induced payments reimburse the consumer or the consumer's institution. They have Bank Secrecy Act obligations to make sure that their customers are not engaging in unlawful activity, including payment fraud, but they do not have any monetary incentive to make sure that they can effectively prevent their own customers from committing fraud.

Conversely, in the United Kingdom, they have mandated reimbursement for fraudulently induced transactions where the consumer's institution and the receiving institution split the cost 50/50. Now if we did that here, and the receiving institutions were obligated to pay 50 percent, you could believe that they would be doing more to prevent their own customers from committing fraud. And they should bear the cost because they are allowing this to happen.

Fourth, any attempts to combat fraud must also be coupled with policies and procedures that protect innocent consumers who have not engaged in payment fraud but who may have had their accounts frozen or their accounts closed due to overly aggressive fraud monitoring. They must have the ability to dispute the freeze or the closure, to expect money that they need to eat or pay rent to be returned in a timely manner, no longer than the 10 days provided under the EFTA.

Fifth, the financial institutions that design and run these payment systems need to take more responsibility for making these systems safe. It is in their financial interest to do so. Confidence and use of these systems will increase as they contemplate consumer protections when deciding things like safety features, speed bumps, how much fraud screening to employ, and whether to sacrifice safety for convenience.

Finally, we need to share more information about fraud, how it is happening, through what payment systems, and who is doing it. We need interagency cooperation on the Federal and local level, combined with input from financial institutions, trade associations, consumer advocacy groups, and other stakeholders.

Thank you, and I am happy to take any questions.

Chair BROWN. Thank you very much. Mr. Benda, welcome.

**STATEMENT OF PAUL BENDA, EXECUTIVE VICE PRESIDENT,
RISK, FRAUD AND CYBERSECURITY, AMERICAN BANKERS
ASSOCIATION**

Mr. BENDA. Thank you, Chairman Brown, Ranking Member Scott, and Members of the Committee. I appreciate the opportunity to testify today before you.

My name is Paul Benda. I serve as the Executive Vice President for Risk, Fraud, and Cybersecurity for the American Bankers Association. Before joining the ABA I had the honor of serving in the Air Force and worked at both the Pentagon and Department of Homeland Security in leading roles to enhance both physical and cybersecurity. I am an engineer by training and try to apply those skills to help our members navigate a range of operational challenges, including fraud. Our members know that fraud takes a financial and emotional toll on their customers, and banks of all sizes are taking extraordinary efforts to protect and safeguard customer accounts as fraud has become more sophisticated.

Today's fraudsters are using artificial intelligence and modern tools to scam customers and small businesses out of their money. Banks have a long history of innovating to protect their customers, and ABA is doing what we can to support our members in this fight.

In the last year, for example, we launched a new industry platform to make it easier for banks to resolve check fraud claims. We also developed a new information-sharing tool that we believe will make it easier to spot financial fraud. Unfortunately, however, the fight against these criminals is one that the banking industry cannot win on its own. We believe that a unified, cooperative effort between banks, law enforcement, regulators, and other stakeholders offers us the best chance to fight back against fraud and protect consumers.

There is no doubt that bank customer scams and fraud have been increasing. According to a recent FBI report, there is a 50 percent increase in reported fraud losses from 2021 to 2022. The top three categories of fraud were investment scams, business email compromises, and technical support scams. Impersonation is a common factor in nearly all of these scams, with the criminals often impersonating a bank and asking the customer for critical financial information.

Also worrisome is the rise of check fraud, which has become one of the fastest-growing categories of consumer fraud across the country, even as the use of checks continues to decline.

In response to the growing fraud threat, banks are deploying new tools and capabilities to identify suspected fraud and stop it from happening in the first place. Still, there are limits to what banks can do when checks get stolen or when sophisticated criminals scam customers into giving them their money.

Here are some of the ways other stakeholders can help us in this fight. As detailed in my written testimony, our members believe that there are four pillars that will enhance our antifraud efforts. First, increase consumer education. The best way to reduce fraud is to prevent it from happening in the first place, and the best way to do that is empower consumers to protect themselves.

One of ABA's most important consumer protection initiatives is our award-winning "Banks Never Ask That" campaign. Through social media, TV ads, and even stadium scoreboards we have educated millions of bank customers on how to spot common scams from criminals posing as their bank. The point is to drive home the message that a bank will never ask for your password, PIN, or Social Security number but a scammer will. To date, more than 2,300 banks have participated in the campaign, using creative content provided by ABA, entirely free.

Separately, our Safe Banking for Seniors program also provides banks and consumers with free tools and tips on how to spot and avoid elder financial abuse. We think there are opportunities to expand this kind of consumer education.

Second, close regulatory loopholes to stop impersonation scams. Telephone number spoofing is a major problem. Criminals have been able to misrepresent themselves either through a spoofed caller ID that shows a legitimate business name or phone number or through stolen social media accounts that are indistinguishable from real account. ABA supported the FCC's efforts to protect consumers from illegally spoofed robocalls and the need to have effective authentication requirements for calls and texts. We have also weighed in strongly on the need to hold any telecommunication provider accountable that knowingly allows criminals to impersonal legitimate numbers and company names.

Third, improved information-sharing. The banking sector works closely with law enforcement and the regulatory agencies and are always looking to develop new ways to share and act on critical threat information. At the same time, the regulators should exercise care in developing new regulations that could inhibit or impede banks' anti-fraud efforts.

Fourth, enhance collaboration with law enforcement and regulators. ABA has a long and proud history of partnering with law enforcement and the public sector on outreach activities. We work closely with the FBI, the Secret Service, and Treasury, and in recent months we launched a nuclear energy initiative with the U.S. Postal Inspection Service to combat check fraud. We still believe there are additional opportunities for public-private partnerships in support of fraud prevention.

In conclusion, banks are working every day to protect their customers from fraud by investing in new technologies, deploying public education campaigns, and partnering with law enforcement and other Federal agencies. We all recognize that more must be done, however, if we are really going to crack down on the criminals. It will take a partnership with banks and telecom firms, technology companies, and the public sector all working together. ABA and our member banks stand ready to work with all stakeholders to win the fight against fraud and protect consumers.

Thank you again for the chance to testify, and I look forward to answering your questions.

Chair BROWN. Thank you. Mr. Breyault, welcome.

STATEMENT OF JOHN BREYAULT, VICE PRESIDENT OF PUBLIC POLICY, TELECOMMUNICATIONS, AND FRAUD, NATIONAL CONSUMERS LEAGUE

Mr. BREYAULT. Good morning Chairman Brown, Ranking Member Scott, and Members of the Committee. My name is John Breyault and I am the Vice President of Public Policy, Telecommunications, and Fraud at the National Consumers League. For more than 25 years, NCL has worked via our Fraud.org campaign to educate consumers about the warning signs of fraud and promote public policies that protect the American public from scams of all kinds.

There is an epidemic of fraud and identity theft in the United States. Since hitting a record of 5.96 million in 2021, during the height of the COVID-19 pandemic, consumer complaints to the Federal Trade Commission have remained exceptionally high. Fraud losses have continued to mount, increasing from \$3.3 billion in 2020 to a staggering \$8.8 billion in 2022. Median fraud losses more than doubled during that period, from \$311 to \$650. And as you mentioned, Mr. Chairman, these losses can often be life savings, a lifetime of work that consumers have built up, that is lost to scams.

When NCL last testified before this Committee in 2021, we warned that peer-to-peer or P2P, payment platforms such as Zelle, Venmo, Cash App, and others had become a payment method of choice for scammers. Unfortunately, the problem has only worsened since then. In 2020, the FTC received 62,000 complaints where payment apps were the method of payment, with total reported losses of \$87 million. By 2022, reported losses from fraud involving these apps had grown to \$163 million. We anticipate that when the FTC reports its 2023 data this regrettable trend will only continue.

The situation is similarly dismal when it comes to fraud involving one of scammers' other favorite payment methods: gift cards. In 2020, the FTC received more than 43,000 complaints where a gift card was the method of payment, with reported losses of \$124 million. In 2022, complaints rose to 48,800, with losses nearly doubling to \$228 million. Just this week, NCL itself was targeted by scammers who tried to get our staff to purchase gift cards by impersonating our CEO.

As bad as those numbers are, the harm from scammers using cryptocurrency as the payment method is even worse. Since the FTC first began reporting it as a payment method in 2020, losses involving cryptocurrency payments have ballooned from \$129 million to \$1.59 billion in 2022, a tenfold increase in just 2 years. Complaints received at NCL's *fraud.org* website last year were littered with references to fraudulent cryptocurrency investment schemes, and such scams were by far the costliest type of fraud for their victims.

We are not winning the fight against fraud, and we need Congress to act.

While P2P platforms, banks, and cryptocurrency trading platforms profit from ever-increasing transaction volumes, they bear little of the cost of fraud that occurs on their systems. Instead, the liability for fraud falls on those who can least afford to absorb the losses, individual consumers. No amount of voluntary consumer

education, better disclosure, or friction put into payment flows will solve this problem. We believe the payment platforms where fraud occurs must have a bigger financial incentive to stop scams before they happen. By spreading risk across all the participants in the system, the costs can be better absorbed, resulting in a safer and more secure payments marketplace for everyone.

Congress can and should play a leading role in creating these incentives and preventing fraud on P2P platforms and gift cards. We urge Congress to give special priority to passing legislation such as the Protecting Consumers From Payment Scams Act, which would expand EFTA's definition of "unauthorized electronic fund transfer" to cover fraudulently induced payments. As my colleague, Ms. Sanchez-Adams mentioned, the United Kingdom recently enacted a new law that shifts liability for fraudulently induced payments from consumer victims onto the issuing and receiving banks. We believe the United Kingdom is a model for U.S. regulation in this area.

Cryptocurrency will soon become, and by some estimates already is, the payment method of choice for criminal scammers. The proliferation of cryptocurrency kiosks in relatively insecure retail locations has made them a favorite tool of scammers. By one estimate there are more than 34,000 of these kiosks across the country.

Kiosk operators, one of whom was reportedly making a 20 percent commission on every transaction, lack sufficient incentives to crack down on these scams. Senator Warren's Digital Asset Anti-Money Laundering Act of 2023 includes many needed protections and would do much to begin cracking down on the use of cryptocurrency as a payment method. Her bill has NCL's full support, and we urge the Committee to approve it.

In conclusion, I would like to thank you, Chairman Brown and Ranking Member Scott, for your continuing work to protect consumers and for holding this hearing. On behalf of the National Consumers League, thank you for including the consumer perspective as you consider these important issues.

Chair BROWN. Thank you. The questions will begin with Senator Tester from Montana.

Senator TESTER. Thank you, Mr. Chairman, and I want to thank you and the Ranking Member for holding this hearing, and I want to thank the panelists for their testimony. I appreciate it very, very much.

I do not think anybody is immune from consumer fraud. I certainly have experienced it personally at a time when I was very young and could least afford it. Montanans reach out to me literally daily about these problems. Constituents have paid for services online that they never receive or bad actors overseas claiming that something that really does not exist, and luckily we were able to connect them with the FBI or other resources.

But these are tough times for people to go through. There is no doubt about it. When they have to call my office it shows what kind of, quite frankly, difficult times those really are and the desperation that they have. We need to be proactive, and we all need to be on the same page. I think all the stakeholders need to bear some responsibility for what goes on here.

Mr. Benda, you mentioned bipartisan efforts we have taken in the Senate Appropriations Committee to facilitate public-private partnership to prevent fraud and supporting law enforcement to combat these people that are probably the lowest forms of life on Earth. So Mr. Benda, are there additional tools that law enforcement could use right now that we should be looking at?

Mr. BENDA. Thank you for the question, Senator. I think information-sharing is going to be the key to help defeat this. I think when you look at the lack of coordination that we have got on fighting fraud, whether it is the FBI or whether it is reporting to FTC, whether it is reporting to regulators, whether it is reporting to the U.S. Secret Service, it is fragmented, and so it is difficult to spot trends. It is difficult to spot where these people are targeting. It is difficult for banks to get ahead of it.

And so I strongly recommend—and I appreciate the language that was in that appropriations report. We think coordination amongst both law enforcement and private entities is going to be key there.

Senator TESTER. One of the things that has always, quite frankly, amazed me is when a credit card number is used somewhere else and the bank makes me aware of it very quickly. I give an example, and I have given it before. Two hoverboards were bought in Cleveland, Ohio, on my credit card—and it takes two hoverboards for me, so it made sense.

[Laughter.]

Senator TESTER. And the bank called me up immediately and said, “Have you been in Cleveland, Ohio?”, and they took care of it. And I appreciate that and I want to pass that along because sometimes we go somewhere, make a charge, and they will call us up and say, “Are you in Spokane, Washington? Is this really legal?” So I appreciate that.

Senator Hagerty and I have a piece of legislation, with other folks on this Committee, the Financial Exploitation Prevention Act, which would help folks who lose their retirement money to scam. Look, as I see this, from this perch, I think the people—and I would like to get a comment on this, actually—the people most vulnerable are young people and old people. Does that tend to be true? Ms. Sanchez-Adams.

Ms. SANCHEZ-ADAMS. Yes, sir. You know, you generally think it is older Americans. They lose the most amount of money, the older Americans do, but the ones that are victimized the most are younger Americans.

Senator TESTER. OK. That is good to know.

Well, with this bill that we have with Senator Hagerty, it looks to prevent fraudulent activity because it has increased over the years. And it allows the company to delay payments if they think fraud is going on.

Mr. Benda, I think it is a really good bill, not just because I am carrying it and Hagerty is carrying it but I think it could help. It would not absolutely solve all of the problems, but I think it could help. Would there be other actions you would like to see be done by this Committee or other committees to help you do your job?

Mr. BENDA. You know, I am sorry to sound like a broken record, Senator, but it really is the information-sharing piece. And the

example I like to give is the sharing of the scam-reported data that the telecoms receive. Banks would like to analyze that data, look at that data, and then reach out and shut down those links and those phone numbers—open source—they do not work, so consumers cannot reach them. Right now we do not necessarily get access to that data.

Senator TESTER. So one of the things—and I am just going to close out with this—one of the things that has me worried is AI. You talked about customers and small businesses being scammed, and quite honestly, AI is going to start playing in this, and hopefully we can use AI to our advantage on the other side to prevent it.

But regular people, myself included, do not understand AI, period, and it is going to take a lot of working together to make sure that we do not end up in a worse situation than we are right now. Because you can damn well bet the bad guys are going to use every method they can to try to rip people off of money because they do not even know how to get their hands dirty to make money in the first place. So thank you.

Chair BROWN. Thank you, Senator Tester. Your experience notwithstanding, Cleveland is a great place to live.

Senator TESTER. I hear it is the heart of rock and roll.

Chair BROWN. Yes, and other things.

Senator SCOTT. I will direct my first question to Senator Tester and the hoverboard. Having been on it for 7 seconds, sir, are you sure you did not order either one of those hoverboards?

Senator TESTER. I would not know how to ride one of those dog-gone things if I had one, much less two at a time.

Senator SCOTT. That is why you remain healthy. Those things are crazy. Anyways, thank for the comic relief there, Senator Tester. We needed that.

Senator TESTER. Any time.

Senator SCOTT. Yes sir. As I emphasized in my opening statement, financial fraud and bad actors are not new. Check fraud, for instance, has been around, from my perspective, forever, since we have had checks, it seems like. And yet surprisingly, despite many of the technological advancements that we have seen in the financial industry, check fraud incidents nearly doubled from 2021 to 2022, and it is on pace to increase even more in 2023.

Mr. Benda, can you please explain how the majority of check fraud is being conducted today and who check fraud impacts the most?

Mr. BENDA. Thank you for the question, Ranking Member Scott. So check fraud is a big challenge for us today, and really it impacts Americans of all types. The challenge we have got is—and it started with the fact that the mail system is not really as secure as we thought. So we are seeing a huge increase in the theft of mail. We are seeing mail carriers being assaulted so that they could steal the mail as well as steal the arrow keys that are there. And what this allows the criminals to do is actually gain access to these checks.

And unfortunately, the marketplace today allows them access to tools we did not even dream of 20 years ago. They can access chemicals to wash these checks. They can access cardstock from overseas suppliers so they can print checks that look exactly alike.

Frankly, it is a very challenging fight for us, to try and stop these trends unless we can start securing the mail.

Senator SCOTT. So to that point, if someone can literally just steal the check from the mailbox what should we be doing to educate consumers about check fraud, that we are not doing right now?

Mr. BENDA. I think there are a lot of efforts underway to educate consumers. That is why ABA entered a partnership with the U.S. Postal Inspection Service. But I think people need to recognize that if you give someone your name, your address, your bank account number, and the bank routing number you are giving them access to your bank account, potentially. And so looking at other more secure forms of payment. Senator Tester talked about credit cards. That may not be viable all the time. But ACH and other forms of payments can be useful ways to transfer money.

Senator SCOTT. Thank you. I frequently hear from bankers across the country about their frustration with the Government's handling of suspicious activity reports, or SARs, and the effectiveness of our anti-money laundering regime. Bankers spend significant resources filing SARs with FinCEN, which are intended to help catch criminals and prevent abuse within the financial system.

But more often than not, millions of SARs are essentially sent into a black box where banks receive no feedback and most of which are never acted upon by agency personnel or law enforcement.

Again Mr. Benda, you have spent most of your professional life working in fraud and cybersecurity. Having worked with both law enforcement and financial institutions do you believe that the current system is working efficiently?

Mr. BENDA. I think there are definitely improvements that could be made to the current system. I know there is frustration on the bank side, and I know there is frustration on the law enforcement side. I think better coordination between law enforcement and private sector, a feedback mechanism, so that banks understand what law enforcement is looking for, so it can provide them the information they need, but then again, law enforcement providing tips and tactics and trends so that banks can better protect their customers from fraud.

Senator SCOTT. Great. As I stressed in my opening statement, consumer education is critically important when it comes to preventing or trying to reduce that sort of fraud. It breaks my heart, as someone will place a check in their mailbox, assuming they are paying a bill or sending money to a loved one, only to find out that a stranger has taken it.

It seems that ABA is working around the clock to figure out ways to protect consumers and help institutions ensure this sort of fraud will not happen again. In fact, ABA has worked to develop a Check Fraud Claim Directory, that provides contact information for banks to file a check warranty breach claim with another financial institution.

Can you walk us through the ins and outs of how this directory works, Mr. Benda, and the importance of it?

Mr. BENDA. So we know this does not solve the check fraud problem, but we are trying to do what we can. One of the challenges banks have is finding out who is the right point of contact to send that claim to so they can get reimbursed for it, so they can provide those funds back to the consumer.

But we have taken it further than that. We had recognized check fraud is happening to all Americans, and we are trying to figure out ways that we can make filing the claims, from the customer perspective, easier. We are trying to get rid of things such as requiring notarizations or pay affidavits, trying to make sure that when a decision is made the customer is reimbursed more quickly.

It is a challenge. It is a very complex thing to do, but we are working to try and make this process better for banks and customers alike.

Senator SCOTT. Thank you.

Chair BROWN. Thank you, Senator Scott.

Senator Menendez, of New Jersey, is recognized.

Senator MENENDEZ. Thank you, Mr. Chairman.

Mobile peer-to-peer payment applications are growing more popular and are expected to facilitate transactions worth over \$1 trillion this year. Unfortunately, these platforms, which include apps such as Venmo, Zelle, PayPal, and Cash App, are also rife with scammers and fraudsters seeking to steal from hard-working consumers. Members of this Committee, including the Chairman, Senator Reed, Senator Warren, and myself, have led letters to banks, regulators, and the apps themselves, urging them to adopt better user protections. And I was pleased to finally see some action when the CFPB, in November, proposed a rule establishing supervisory authority over large nonbanks with person-to-person payment apps, and I know Zelle has made some changes to its own policies.

Ms. Sanchez-Adams, can you comment on these actions taken so far and tell the Committee what next steps we should consider to take to better protect consumers from scams and fraud on P2P apps.

Ms. SANCHEZ-ADAMS. Yes. Thank you, Senator, for the question. The CFPB's proposed rule would allow them to supervise these institutions—the Cash App, the PayPal, the Venmo—particularly to see whether they are reimbursing consumers for unauthorized fraud and their policies for reimbursing consumers when there are fraudulently induced payments. So basically to check their policies and procedures and make sure they are complying with the law. And that is extremely important, and we support that rule.

More actions we can take is to make sure that the law actually protects victims of fraudulently induced payments. So that would be amending the EFTA or allowing the CFPB, through rulemaking, to do so, and that is one huge step that we can take.

Senator MENENDEZ. OK. Now according to the 2017 American Community Survey, nearly 26 million people, which is roughly 9 percent of the U.S. population, have limited English proficiency. And we know consumers who lack access to information are prime targets for predatory behavior.

Can you talk about the unique vulnerabilities consumers with limited English proficiency face when combating scams?

Ms. SANCHEZ-ADAMS. I mean, absolutely, you named them. The fact that we talked about consumer education, consumer disclosure, knowing products, knowing protections. Well, one, if you do not speak the language or read the language, how are you going to know that? And two, if it is buried in fine print or in some contract that you never see, you will not know those either.

So absolutely it impacts them, and then I would say that there are certain payment systems that target low-income consumers and minorities because they are pushed out of the banking system. So they are targeting these folks and they are more rife with fraud, and so they really need to be doing more to protect these consumers.

Senator MENENDEZ. In addition to being disproportionately targeted by a wider variety of scams, Limited English Proficiency (LEP) consumers can also face difficulties in accessing anti-scam and fraud resources. For instance, there is no CFPB online complaint system in Spanish, or for that fact, in any other language. And IC3, the FBI's website that provides education resources to protect individuals from cybercrimes and allows victims to report internet crimes is only available in English.

Would making more anti-fraud and scam resources available in other languages help protect LEP consumers?

Ms. SANCHEZ-ADAMS. Yes, absolutely.

Senator MENENDEZ. Yes. Talking about different groups of consumers, Mr. Breyault, another group often targeted by scammers are seniors. Crimes targeting older Americans were up 84 percent in 2022 over the previous year, and furthermore, older adults report higher median losses than younger adults.

According to the Federal Trade Commission, the median loss from fraud was \$1,750 for those 80-years old or older, compared to \$548 for those in the 20 to 29 age group. These losses can have significant impact on the financial security of older Americans as they rely on these critical funds for their retirement.

What sort of procedures or training should financial institutions be implementing to improve the institutions' abilities to detect and prevent fraud committed against seniors?

Mr. BREYAULT. Thank you for the question, Senator. So seniors are uniquely vulnerable to fraud. They are inviting targets for scammers because they often have access to more assets that the scammers can steal because they have been working for their entire lifetime. Unfortunately, they also have less ability to recover. They do not have as much time to go back to work and recover these lost funds. So they do present uniquely vulnerable type of victim.

In terms of what institutions can do, number one, I would say is make sure that you are training all of your employees to understand that fraud victims are not the ones who are at fault. Too often we have a stigma against older Americans who report this. We wonder, how can you be so stupid? You know, you fell for this. You know, didn't you know better? As was mentioned earlier, those are not terms we use for victims of violent crime, and I do not think we should use it for older Americans, or frankly, any scam victim.

So I think training of frontline employees to show some grace when they get these kinds of questions is important. I think also we need to be able to provide anti-fraud services to people in ways that do not involve technology. Unfortunately, many older Americans often have difficulty using advanced technology. They actually want a real person to speak with. They want somebody in a bank branch they can go and talk to about that. And those avenues are often more difficult or more costly for all consumers but particularly older Americans to access.

So certainly if there are policies that could make that avenue of getting fraud redressed easier for older Americans is another step I would encourage you to take.

Senator MENENDEZ. Thank you. Thank you, Mr. Chairman.

Chair BROWN. Thank you, Senator Menendez.

Senator Tillis, of North Carolina, is recognized.

Senator TILLIS. Thank you, Mr. Chair. Thank you all for being here.

Mr. Benda, you mentioned the need for a partnership. Give me just a quick back-of-the-napkin list of people who should be at the table, particularly the ones who should be that are not right now.

Mr. BENDA. Thank you, Senator. I think right now there really is no table, and so it is hard to say who is there or who is not. There is not that coordination that we would like. I think the appropriations language that is in there, having Treasury look at who could convene the right people, makes a lot of sense.

Senator TILLIS. Yes, if I were just kind of spitballing, obviously banks, credit companies, payment platforms, like Senator Menendez put together, consumer advocacy groups, law enforcement, but really the whole of Government, too.

Mr. BENDA. Yes, absolutely.

Senator TILLIS. And one partner that I am kind of wondering whether or not they are already taking steps in the wrong direction would be the CFPB. Last year, in August, I think it was August of last year, Director Chopra mentioned that it may be more difficult to get credit header data. We are going to go from maybe minutes for law enforcement getting it to a subpoena process. Is that like a partnership that is actually going to put us further away from a viable solution?

Mr. BENDA. That is not the direction we would like to see them go, Senator.

Senator TILLIS. You are very diplomatic. It would just seem to me when you are taking that law enforcement tool off the table, at the end of the day law enforcement has to be at the table. We have to enable them. In fact, we need to take a look at increased penalties.

I, for one, think that is taking a step in the wrong direction, so I understand the motivations on some part. I disagree with most of Mr. Chopra's motivations, to be honest with you, in this case. I think it is cross purposes to the problem we are trying to address today.

Ms. Sanchez-Adams, I really struggle with this, because you hear Senator Tester had two hoverboards charged to his account. I had my bank call me up and ask me if I had charged \$100 at a hardware store in Chicago. I have not been to Chicago in almost 10

years, certainly not a hardware store, so we said no and it was covered. That was clear fraud. The banks covered it. I want to come back on a question related to this to you, Mr. Benda.

But how do we kind of strike the balance? We had a hearing yesterday about social media platforms, and we had some horrible stories told about the children that had lost their lives, suicides, a number of other things. But at the end of the day, there is a parental responsibility there. These devices that we are giving children, these tablets, phones, that we have to be very careful with how they are used.

Similarly, I do not believe that you can just hold the payment platforms or the banks or the intermediaries responsible for all fraud, and I know you said it will not work just with financial literacy or education. I agree with that. But at some point, I mean, do you agree that at some point, if we are striking the right balance, that the consumer has to own some level of responsibility? And I say that with some trepidation because I have heard these stories of people being scammed into keeping on the line, and going to a Walgreens and getting a \$500 payment to somebody that they think is an IRS agent. I get all that. But at some point we cannot possibly build into the system someone other than that individual who is making that horrible decision.

So how do you strike the balance in a partnership to address a problem that I think we all need to address?

Ms. SANCHEZ-ADAMS. Yes. As I mentioned, the U.K. example. Initially they had an industry-led response. It was called the Contingent Reimbursement Model, and there they would, again, apportion the responsibility between three parties—the consumer who was victimized, the receiving institution, and the consumer’s institution. And so the consumer would be on the hook for like the first 10 pounds or so, and they would be reimbursed up to a certain amount.

So there are different ways we can do that. If we change the law to allow, again, the receiving institution to bear some responsibility, not just the consumer’s institution, then you can build other types of protections like only allow a certain amount of dollar transactions per day because you are going to be bearing that responsibility, or verifying that your new customer, who is receiving all of these new transactions, is not committing fraud. So there are different things that I think we can do.

Senator TILLIS. Well, the reason I worry about, you know, we cannot let people off the hook, even if it is devastating consequences. The reason I worry about that is that the industry that will serve customers will then have to start thinking about who they serve, based on a potential risk.

Ms. SANCHEZ-ADAMS. Absolutely.

Senator TILLIS. We have already said that the vast majority of the money comes from senior citizens. The vast majority of the fraud are individual interactions coming from young people. Then I could see a financial institution saying their sweet spot is not them.

Ms. SANCHEZ-ADAMS. Right.

Senator TILLIS. But when I am talking about a partnership, that is what I am saying. Let’s not throw a baby out with the bathwater

and unbank. There are a number of times, we are proposing legislation up here that on the surface looks good, but it ultimately underbanks or unbanks people. So we have just got to strike the right balance.

Ms. SANCHEZ-ADAMS. Absolutely. I mean, with credit cards, consumers are already responsible for like up to \$50 of unauthorized transactions, and you are right that people who can get credit is limited because of that credit risk. So all of those balances can be struck, but if people are more protected then they are more apt to feel safe and to actually choose to bank.

Senator TILLIS. Well, I have gone over my time, but Mr. Chair, just food for thought because of what Mr. Benda said, and I am sorry I was not able to get to the third witness. But the fact that we need a partnership but we do not really have a convener now, I do not think we have done it in this Committee, Mr. Chair, but it may be helpful outside of a formal Committee hearing to have a workgroup and get all the players, and let's see who is absent, who we think are a necessary part of the team. But maybe to host a workgroup at some point in the future so that we can get out there, in a less formal setting, and say how do we initiate this, and ultimately get a response from law enforcement and all the other stakeholders. That is something I would love to participate in.

Chair BROWN. Thank you for that thought, Senator Tillis.

Senator Smith, from Minnesota, is recognized from her office, I believe.

Senator SMITH. Thank you, Mr. Chair, and everybody, thanks to our panelists, and I am sorry I cannot be with you in person today.

I really appreciate this hearing, Mr. Chair, and I think what I am gleaning from what everyone is saying is just how ubiquitous these scams are across the country, and I know it is true in Minnesota.

But I want to ask about particularly this question of spoofing, and Mr. Breyault, I will address this question to you. You know, scammers have been spoofing phone numbers of banks and other financial institutions for years, but it feels like they are refining their contacts. I am sure it has something to do with how AI can be deployed. And it can leave even the savviest consumer susceptible to being victimized by this. My own dad, who is nearly 94 but totally on top of it in so many ways, had this happen to him and was well down the path of providing lots of information about his bank because he thought he was talking to the bank. And luckily he was able to stop it in time, but it created quite a ruckus.

So, Mr. Breyault, I am wondering about whether telecom companies should have some responsibility for preventing spoofing, and also how banks and telecoms can work together to ensure that scammers are not so easily able to impersonate a legitimate call or a legitimate institution.

Mr. BREYAULT. Thank you for the question, Senator. Certainly we need a multifaceted solution to this problem, and how scammers contact their victims is certainly one of the channels that needs to be addressed. Spoofing, as you mentioned, has for a long time been a tactic that scammers have used to impersonate not just banks but Government agencies, like the IRS. We know that they use spoofing to impersonate agencies like Immigration, when

they reach out to particularly vulnerable, limited English proficiency communities.

And so more definitely needs to be done. The telecoms certainly have a role to play in this. Mr. Benda mentioned better information-sharing between the telecoms and the banks on this. I think that is a great idea. And to the extent that that is not happening I think it is a role for this Committee to play in making sure that that cooperation does happen.

Beyond simply spoofing, I think we need to look at the epidemic of texting and how text messages are being misused to impersonate not just banks but like Government agencies. We hear a lot about scammers impersonating retail, like Amazon or UPS telling you about package delivery.

So definitely going after the channels that scammers use to reach their victims and making those safer is an appropriate thing to do, and I think would have an impact.

Senator SMITH. Thank you. Thanks very much.

I would like to just quickly talk about an issue that is quite related, I think, to this topic today, which is how businesses and other institutions are targeting shady practices at home buyers and homeowners. Ms. Sanchez-Adams, I would like you to answer this question.

One of the things that has been happening in Minnesota, and I think around the country, is we are seeing a proliferation of these very predatory contract or deed contracts where a home purchaser enters into a contract with a home seller to pay for the home in installments, thinking that they are in the process of buying their own home. This has been targeted specifically to Somali Minnesotans who, in their faith traditions, are discouraged from either paying or profiting from interest. So this is often marketed falsely as an interest-free way to buy a home.

And then what happens, of course, is folks get into this contract and they realize that if they miss just one payment they end up forfeiting all of the money that they put into the home and losing the home. They find out, for example, that they have balloon payments at the end, none of the protections that exist with a traditional mortgage.

So, Ms. Sanchez, could you just talk about this a bit, from your perspective as a consumer advocate, and what we should be doing a better job of here. Senator Lummis and I introduced a piece of legislation yesterday just to help protect homeowners—help protect people from these predatory practices.

Ms. SANCHEZ-ADAMS. Yes, thank you for the question, and absolutely. I was a legal services attorney for 13 years, and would hear of these stories all of the time. And my colleague, Sarah Bolling Mancini, actually testified on this very issue, so I would recommend you look at her testimony—she is absolutely the expert on this—for recommendations on what you can do.

Senator SMITH. Thank you. Thanks, Mr. Chair.

Chair BROWN. Thank you, Senator Smith.

Senator Britt, from Alabama, is recognized.

Senator BRITT. Thank you, Mr. Chairman. We are fortunate to have a growing number of innovation and just different ideas coming into the financial sector, as we look to find new ways to make

sure that we are serving existing clients, that they are doing that, and then also how do we reach individuals and families and communities that have not always had traditional access to different things in the financial markets. So I have been glad to see that innovation begin to occur.

However, we know that bad actors are exploiting our financial industry only to continue to adapt to the new innovation that we are having and finding ways to undermine consumers, and ultimately fraudsters are targeting these individuals. They are targeting vulnerable Americans with phone, internet scams to the tune of almost \$9 billion a year. And in Alabama, in 2022, we were actually defrauded, Alabamians, by nearly \$55 million. And so that number is not only alarming but even worse, it continues to rise.

So we must do more to protect consumers, and while thinking carefully about regulatory changes that would impact the benefits provided by banks, or P2P apps that provide fast and nonfee payments between friends, we have got to look at what is happening and figure out how we—we being Congress, industry, Government agencies like the CFPB—can actually get to the root of the problem.

And the CFPB, they are supposed to be the agency that focuses on protecting consumers, but time and time again it seems that they are utilizing their resources, their time, and their energy to pursue regulations that actually only perpetuate the problem. For instance, I am concerned that the Bureau's expected changes to the Fair Credit Reporting Act could directly stifle banks' fraud prevention efforts.

Mr. Benda, you mentioned this specifically in your written testimony, that the CFPB's proposal could create new legal, practical, and procedural difficulties for banks to detect and prevent fraud and crime. Can you elaborate a little bit more on that for me?

Mr. BENDA. Thank you for the question, Senator. The concern here is that banks routinely access this information, and they use that information for fraud purposes. I think the CFPB is targeting others that might use it for commercial purposes, but when you put the Fair Credit Reporting Act around that information, access to that type of information, it creates a whole series of barriers that require notifications to the potential criminals that banks are taking certain actions on their accounts.

So for normal Americans it does not make any sense. You know, I would not mind being notified. But when banks have these requirements placed on them by FCRA for this type of anti-fraud information it creates notifications to criminals and reduces the ability, frankly, for them to share that type of information or use that type of information.

Senator BRITT. So what would be a better path forward on this, do you think?

Mr. BENDA. I think it is a complex issue. We would be happy to get back to you with any details on that, but we would love to work with you on that.

Senator BRITT. Absolutely. Well, it just seems that financial regulators tend to be less focused on actually stopping the fraud and more determined just to see the institution itself pay for it, and this approach, I believe, is not only misguided but I think it fuels

criminal activity. The solution to preventing financial fraud is not to create additional hurdles for banks and law enforcement or to halt innovation completely through excessive and burdensome red tape. Rather, we have to continue to adapt ourselves.

I think that this includes increasing consumer education efforts across the board. This is one of the most important undertakings, I think, that we could do to help get fraudsters out of the way and allow Americans to preserve their savings and small business accounts, among so many other things. So greater security and anti-fraud mechanisms do not help, though, if consumers can be convinced to willingly hand over their money and their login credentials to a fraudster.

So just in followup on that, what are banks currently doing to educate, Mr. Benda, their customers about fraud and help them to prevent this, keep them from falling victim to what we are seeing occur across the country?

Mr. BENDA. The biggest effort we have is our Banks Never Ask That campaign. I was interested in Senator Menendez's comments about non-English speakers. We recently launched that campaign in Spanish. So we recognize we need to reach all types of consumers to educate them. You know, banks will never ask for your password, PIN, ask you to send money to yourself.

We also have an ABA foundation that looks at elder-scam awareness. We create training courses for our bankers so they can help their customers. And we are interested in partnering with the Government and other public sectors to try and amplify these messages. We worked with other associations like the AARP, but we have not seen as much engagement as we would like to see from maybe some of the regulators.

Senator BRITT. Well, I hope that those people will step up to the plate so that we can help prevent the fraud and protect our consumers across the country. Thank you.

Chair BROWN. Thank you, Senator Britt.

Senator Warner, from Virginia, is recognized.

Senator WARNER. Thank you, Mr. Chairman. Thank you for holding this hearing. And I want to jump right into it on some of the tech issues.

I know some of my colleagues were mentioning the Judiciary Committee hearing yesterday. As someone who thinks, has felt for a long time that while the original intent of Section 230 back in 1996 might have made some sense then, this has turned into a "Get Out of Jail Free" card for all the social media companies, and I was glad to hear Senator Graham talk about it yesterday, and others members.

I have had what I thought was a fairly simply reform of Section 230 for a while out there called the Safe Tech Act, which would basically say if it is illegal in the real world, it ought to be illegal in the online world, and there ought to not be this kind of—and again, I cannot think of any other term other than a "Get Out of Jail Free" card.

That obviously hits us in the consumer fraud area. I think the FTC just did a study that said that, the way I read it was that when you use typical contact methods—phone, email, whatever—fraudsters have about a 6 to 17 percent hit rate. But when it

appears on a social media platform or an online ad, that fraud rate goes up to 61 to 63 percent. So whether it was the kind of gripping testimony we heard yesterday of parents who have lost their kids or the ability to have Americans ripped off.

I know this may be a little out of your lanes, but have any of you got any thoughts on whether we ought to have a thorough re-examination of Section 230, even in terms of consumer protection? Why don't we start with you, Ms. Sanchez-Adams.

Ms. SANCHEZ-ADAMS. Yes, thank you for the question. You know, I agree. As we have all talked about, there are so many different avenues that we need to take to address the issue of payment fraud. You know, as we heard earlier, holding those telecom companies that are allowing robocalls and robotexts to happen, yes. Holding social media platforms that are allowing these fraudsters to do the work that they are doing on that—

Senator WARNER. But if you are going to hold them accountable, does that not require a change in Section 230?

Ms. SANCHEZ-ADAMS. Well, I will agree with you that, yes, we need to find a way to hold all players accountable, and that is why we also think institutions that are banking the fraudsters should also be held accountable. So it is a multipronged approach.

Senator WARNER. Mr. Benda? Mr. Breyault?

Mr. BENDA. Thank you, Senator. I am not familiar with the Act but I truly believe focusing on impersonation scams that allow people to basically con people out of money is a great area, and we would love to work with you on that.

Senator WARNER. Sir?

Mr. BREYAULT. Senator Warner, thank you for the question. You know, I think as you have heard from all the witnesses today, we need the actors where these frauds are being facilitated to have more skin in the game. They need more incentives to invest and to protect their users, because ultimately it is the users who are the ones who are making them their money.

Senator WARNER. But again, the fact is—I am an old telecom guy so this is where I am a little just crazy to me. Section 230 basically, the 1996 Telcom Act, said if you are one of these platforms, you have no responsibility at all for any of the content that appears. So the distribution model for this fraudster activity goes through the platforms, and if we do not hold them accountable, I do not think we are ever going to get there.

I also know some of you touched on—I am going to get one more question in—on how we can do more real-time reporting. I am Chairman of the Intelligence Committee. We have managed to move forward on real-time reporting as we see threats in the intelligence system. We have still got a ways to go. I do think, in terms of internet-based fraud, real-time reporting has to be a component.

But I want to move my last question to AI. One of the things that scares the dickens out of me on AI, some good things coming out of this, but the scale and speed with which these tools can be used, and they do not have to have a lot of sophistication. Senator Kennedy and I have a bipartisan bill that looks at could we bring FSOC to the table to look at where there are gaps, could we end up saying if you use these tools you might even have things like trouble damages, which already exists in the SEC world. We have

been thinking about this on market manipulation. But we have also been thinking about it in terms of consumer fraud.

And one of the things that really concerns me is a lot of these AI tools, you may say just go make the most money possible, and that may then result in screwing around with consumers. But it goes to the question of intent.

My time is clicking down. Do any of you have any thoughts on how we get at this intent issue around AI tools?

Mr. BREYAUULT. So Senator Warner—

Senator WARNER. Maybe you could take it for the record.

Mr. BREYAUULT. Yes.

Chair BROWN. Be brief, each of you, if you would.

Mr. BREYAUULT. Sure. I definitely like the idea of increasing penalties for bad actors who use AI.

Senator WARNER. Good. Well, if you could think about the intent question I would love to get some thoughts on that.

Thank you, Mr. Chairman.

Chair BROWN. Thank you, Senator Warner.

Senator Butler, from California, is recognized.

Senator BUTLER. Thank you, Mr. Chairman. If it is OK I would love to sort of go back to the point of conversation that Senator Tester, actually, introduced, and this question of “who”. There are a lot of perceptions that these kinds of scams and fraudulent activities happen mostly directed toward older people, and we have had a lot of conversation here about that. And I think it is important as we have started to uncover in this hearing that we paint a full picture of who actually are victims and how they are being impacted.

There has been some research put forward focused on Gen Z and their impact here. The 2022 Annual Cybersecurity Attitudes and Behaviors Report shows that Gen Z and Millennials were actually more likely to fall victim to certain types of scams like phishing than other generations. The data also showed that Gen Z Americans were three times more likely to get caught up in online scams than Boomers, and the cost of falling victim to online scams has risen. In 2017, young victims under 20 are estimated to have lost \$8.2 million in online scams, and that rose dramatically from 2017 to 2022, where that loss has now exceeded \$210 million.

Ms. Sanchez-Adams, I would love to just start with you on this question. Given that the younger generations are already struggling financially compared to their parents and grandparents, are there specific examples that you are aware of that are happening in the financial services sector that are working with schools and youth organizations to raise greater awareness about online scams? We have talked a great deal about partnership here, and what I am trying to get at are there actually targeted efforts focused on this younger population.

Ms. SANCHEZ-ADAMS. None that I am aware of.

Senator BUTLER. Mr. Benda, do you have any specific examples that you are aware of?

Mr. BENDA. ABA does run a Teach Children to Save effort, where we partner with bankers and we go out to different communities. It is financial education but also has a scam component.

Senator BUTLER. Mr. Breyault.

Mr. BREYAUULT. Senator Butler, at NCL we have a program called LifeSmarts, which is targeted at high school students, and one of the parts of the curriculum at LifeSmarts is to teach younger consumers, particularly, those in high school, how to spot and avoid scams, including the ones that you just described.

I would also just like to point out that while the numbers—you have talked about \$210 million for losses. We have also talked about \$9 billion in losses overall. I think it is important to stress that those numbers, by almost every cybersecurity expert and fraud expert that we talk to, those numbers are a significant undercount.

Senator BUTLER. Sure.

Mr. BREYAUULT. We know that consumers do not report these scams as much as they happen. So the numbers you see here are bad, but the real situation is likely much worse.

Senator BUTLER. I appreciate you making that point because that is a little bit of what I am trying to get at. Young people are falling victim to these crimes, and the shame and stigma associated with, you know, falling for them, being so stupid as to, as the term was used earlier, to fall for them does not really help us get at prevention.

And so I just wanted to follow up. Mr. Benda, Mr. Breyault, you mentioned some specific programs. Is there any information that you could share relative to scale of those programs? How many high schools are you working with? You know, I have six million children who are residents of California. One-in-four American kids are residents of my State. And so I am trying to figure out what is the scale at which we are actually moving and if there are recommendations that you would have to get to a greater scale faster.

Mr. BENDA. Senator, that program is run by our ABA Foundation, and they would love to share that detail with you. I will make sure that we get that to you.

Mr. BREYAUULT. And while our program reaches tens of thousands of students across the country, and the content reaches hundreds of thousands more, with additional resources we can always reach more. But yes, certainly programs like LifeSmarts, programs like the one Mr. Benda discussed do play a role in helping consumers build a resistance against these scams. But that is not the only thing that is going to stop this. We need legislation that actually goes at the incentives that companies have to actually protect their customers from these scams in the first place.

Senator BUTLER. Thank you. Mr. Chair, I would love to submit a followup question for the record with the staff. But thank you for the time.

Chair BROWN. Of course. Thank you, Senator Butler.

Senator Reed, of Rhode Island, is recognized.

Senator REED. Thank you very much, Mr. Chairman, and I thank the panel for their testimony.

Ms. Sanchez-Adams and Mr. Breyault, the Electronic Fund Transfer Act and its implementing rules cover transfers done through the ACH system, where it is not clear if a transfers done through wire transfer systems are covered. And I am very concerned that this gap or ambiguity leaves consumers unprotected

against fraud for very large electronic payments they are doing for things like a downpayment on a home.

Ms. Sanchez, first, how widespread is the issue of wire fraud for consumers, and can you walk us through some common scams?

Ms. SANCHEZ-ADAMS. Yes. So it is unfortunately exploding. I get two or three emails a week about it from consumer lawyers, and sometimes even from consumers themselves, and there are always news reports on this. Some of the common scams, you have one that is horrible. It is a tech support scam, and they gain access to somebody's laptop or computer and then gain access to their financial information without the consumer knowing, and then they get onto their bank account and do a wire transfer to a crypto account, and then the consumer is out of luck. Even though State law says that consumers should not be held liable for unauthorized wire transfers, there are all of these caveats. If there was a security procedure in place, if the consumer agreed to it in the account agreement then generally the banks will say either, sorry, it was sent out and there was a security procedure that was used so we cannot help you, or if you, by chance gave your account information to someone it would be protected under the EFTA but not under the UCC.

Senator REED. And Mr. Breyault, your comments.

Mr. BREYAUULT. Certainly in addition to the type of scams that Ms. Sanchez-Adams discussed we see this where scammers get in between consumers during a real estate transaction. For example, when you are sending money to a title agent, a scammer may impersonate the recipient of those funds in order to disrupt that transaction.

And I think certainly one of the things that all of these transactions have in common, whether we are talking about ACH or peer-to-peer, or gift card to some extent, is that the money is transferred very quickly, nearly instantaneously. In fact, that is why it is so attractive to the scammers.

So I think as part of the solutions that you consider in this is do we need to slow down some of those transactions? Is the benefit we are getting from instantaneous payments, that are oftentimes irreversible, even after fraud is discovered, are those benefits outweighed by the cost to consumers of the fraud that is occurring on these systems?

Senator REED. Now can the Consumer Financial Protection Bureau deal with these issues under current law, or do we have to pass additional legislation to try to address these scams?

Mr. BREYAUULT. The CFPB does a tremendous amount of authority to start to address some of these scams, and they are exercising it. But I would say there is more that could be done. We discussed, particularly in my testimony, the Protecting Consumers from Payment Scams Act, which would redefine what is an unauthorized transaction to include these kinds of induced fraud, or also known as authorized push payments, as covered under EFTA. So certainly that is one area where the CFPB could help us, and this Committee could help the CFPB do its job even better.

Senator REED. Ms. Sanchez-Adams, your solutions?

Ms. SANCHEZ-ADAMS. The CFPB has authority under Regulation E, or the EFTA, to do rulemaking. So through rulemaking they

could clarify, you know, there was the exemption to wire transfer that the Federal Reserve Board said included Fed wire, CHIPS, and so they could change that after doing a rulemaking, open comment, and all of that. They can clarify things, like what fits under errors, because they can create additional errors under the EFTA, so they can do that through rulemaking.

Senator REED. Well, thank you very much. Thank you all for your testimony today. Mr. Chairman, I will yield.

Chair BROWN. Thank you, Senator Reed.

Senator Vance, from Ohio, is recognized.

Senator VANCE. Thank you, Mr. Chair, and thanks to our three witnesses for being here.

You know, I wanted to ask a series of questions to Mr. Benda, because this is a very important topic, fraud, how it affects consumers. But in particular I hear a lot about how it affects elderly consumers in the State of Ohio. You know, we spend a lot of time in Congress, I think rightfully, lauding innovation and advancements in technology, and they do bring a lot of benefits, but of course they bring a lot of risks.

One of the things that I hear a lot about from constituents back home is that there are a lot of spoofing scams sort of deploying and employing modern technology to basically trick a lot of our elderly folks into giving money, very often preying on sort of the best sentiments, you know, a grandchild calling needs bail money, something like that. And, of course, it is not. It is very often a person who is just trying to scam them.

And so I really worry about what this looks like and whether the modern technology infrastructure that we have in this country, while obviously it has a ton of benefits, has also enabled this massive amount of scam on our elderly Americans. It is not just anecdotal. Americans lost, in 2019, over \$3 billion due to financial exploitation, and seniors are particularly targeted by a lot of this.

So I want to ask this question, Mr. Benda. I know this is an issue that affects your member banks, and obviously it is customers. I know that you guys deal all the time with these scams, and you have to pick up the pieces and hopefully help the customer address some of the problems.

Could you build on sort of what you guys are seeing, what is out there, what are the spoofing scams that are particularly concerning to you and what we can do from a financial and banking perspective to mitigate some of this stuff?

Mr. BENDA. Thank you for the question, Senator. So I think you are hitting the nail on the head. The FCC even put out an alert just last summer that talked about bank impersonation scams being the number one scam. Everyone probably on this dais has gotten that text message that says, "Did you have this fraud alert? Did you make this transaction?" and you reply to that because it looks exactly like something coming from your bank. And then they lure you in. They socially engineer you.

And I want to be clear. These people are very good at what they do. They are very bad people. They are criminals. They are very convincing. It is not stupid people that fall for these.

So what we would like to see happen is trying to attack these impersonation scams. Can we figure out a way—and you are right,

our technology infrastructure is not where it needs to be to ensure that that caller ID message is accurate. If, at any point in that process, that authentication drops—there is a process the FCC has, but it can be worked around—if that authentication drops it should be an unknown caller. We should not allow people to fraudulently display wrong names. My dad is 86. If it says his bank on that caller ID, he thinks it is his bank.

So we need to stop that because they are the ones that are enabling those scams to occur.

Senator VANCE. And is that something that the telecommunications companies—maybe this is outside the jurisdiction of this particular Committee, though. I know a guy on the Commerce Committee. Is this something that our technology and communications infrastructure should be better at? I mean, recognizing it is not necessarily your area of expertise, what can we be doing to better police this stuff and preventing it from happening?

Mr. BENDA. So the FCC has active rulemaking on the implementation STIR/SHAKEN. We would like to see that move more quickly. We would like to see it more default to versus right now they let messages through if they meet certain things, basically default to you do not get to display any message unless you are at the gold standard level. I think that is one thing, a change we could make right now that would really help.

Senator VANCE. OK. Great. I will yield the remainder of my time, but appreciate the guests being here and appreciate the Chairman for hosting the Committee.

Chair BROWN. Thank you, Senator Vance.

Senator Van Hollen, of Maryland, is recognized.

Senator VAN HOLLEN. Thank you, Mr. Chairman, and thank all of you for being here and for your testimony.

Earlier this month the FTC released its annual report on consumer activities, and they reported that my State of Maryland is among the top five States with the highest per capita rates of reported fraud. And this has been an ongoing issue in Maryland, as around the country, and it takes all forms, as the conversation today has indicated. I want to focus, for a moment, on one area of this kind of fraud, and right now the failures of our system to catch it and compensate people for it.

We have an open case in Maryland where the victim of check fraud reported the fraud right away, but their local bank, their home community bank, is still awaiting payment from the much bigger bank in which the fraudulent check was deposited. And I am hearing a lot from Maryland community banks about this, and I think their view is well expressed by a letter that I have here from the Community Bankers Association of Illinois, written about a year ago. And I am just going to quote a part of it:

Our members have been particularly frustrated because these fraudulent returns have been deposited into accounts at the Nation's largest banks, and the process to determine the liability for the fraud losses and reimbursement is protracted. When this issue has been raised to Federal regulators the responses have been that it is not their responsibility to intervene in bank-versus-bank disputes. Our members respectfully urge the OCC, Federal Reserve, and the FDIC to reconsider your position regarding fraudulent returns in light of the information included in this letter.

This is a letter that was addressed to them. They make the point that they are not asking Federal regulators to pick winners and

losers. They just want to expedite this process so that those who have been defrauded can be made whole, and those who were negligent in cashing the fraudulent check will end up making the payment.

If I could start with you, Ms. Sanchez-Adams, can you speak to this issue and whether or not, in your view, the larger banks are taking advantage of the weaknesses in the system to prevent quick payment to the local banks so that they can, in turn, reimburse a defrauded customer?

Ms. SANCHEZ-ADAMS. Yes. So one story that we were contacted about was a man who sent a check to the IRS, and it was deposited into, I believe it was a Wells Fargo account, and it was to the U.S. Treasury. And so clearly they are not the U.S. Treasury. But they delayed for 2 years to refund the consumer's bank. Though the law says that consumers should be reimbursed by their own bank, that bank was dragging their heels because they were waiting to get payment. And the consumer bank was also a large bank, so it is not like they did not have the funds to refund the consumer.

And I also just want to point out another problem with check fraud and check alteration is that it is not just them stealing it in the mail, but I have heard a lot of stories about, in particular, one that I mentioned in my written testimony, where they did not even have checks associated with their account, and fraudsters create checks out of thin air. And because banks do not often provide written statements anymore and they do not provide copies of checks back to consumers, it is hard for them to know that this is happening, or especially when it is altered to know that it was altered if you do not see the check to see that it was altered.

Senator VAN HOLLEN. I appreciate that, and we saw a big rise in this sort of check fraud during COVID, but it has continued. And obviously it impacts those who do not do online transactions, mostly the elderly.

Mr. Benda, if you could talk to this issue. I mean, obviously you have got members of different sizes, member banks. But this is clearly an issue that is hurting community banks. Do you agree that the Federal regulators should be more engaged in resolving these issues?

Mr. BENDA. So, Senator, I appreciate the question. I do not think anyone thinks that the check fraud processing system is working as well as it could. Banks of all sizes agree the timelines to process these are taking too long, and that is why the industry is taking its own steps to try and figure out ways that we can accelerate this process, such as developing a universal claim form. We see sometimes banks will file a claim with one bank and they will have to go iterate to make sure they provide the required information, trying to reduce the information the customer is trying to provide. So trying to make this process easier.

In terms of the regulator involvement in this, I agree with them that they do not pick winners and losers. Because each case is so different, it really needs to be that determination between the banks.

Senator VAN HOLLEN. Well, I understand. You know, FinCEN and other regulators, they do pay attention, obviously, to the SARs reports and sort of major fraud, but a lot of this fraud that is

impacting, you know, regular people, is falling between the cracks, and those regular people are left holding the bag. So I appreciate that you, as well as—I think you, Ms. Sanchez-Adams, also spoke to some language that we put in the FSGG appropriations reporting language. I chair that subcommittee. It is aimed at creating more of a public-private partnership to really try to plug the holes and gaps in the system, and I understand you both agree that that would be a smart move. Is that right?

Mr. BENDA. Yes, Senator.

Ms. SANCHEZ-ADAMS. Agreed.

Senator VAN HOLLEN. Thank you. Thank you, Mr. Chairman.

Chair BROWN. Thank you, Senator Van Hollen.

Senator Warnock, from Georgia, is recognized.

Senator WARNOCK. Thank you very much, Mr. Chair. Fraud is a serious problem in the United States, and this sector is growing. A Gallup study found that 8 percent of respondents said that they had personally been a victim of fraud in the past year—8 percent. In the first quarter of 2023, reports of financial fraud per capita occurred more often in Georgia than in any other State, according to data published by the Federal Trade Commission. Forbes Advisor ranked Georgia the fifth-most financially scammed State during that time period.

With these incidents of fraud becoming more sophisticated and more realistic, unsuspecting folks, seniors, and others are being targeted directly and personally, meaning that consumer education plays a key role in stopping scams and fraud before they start.

Ms. Sanchez-Adams, what have been some effective ways to educate consumers regarding the risks of financial fraud and scams?

Ms. SANCHEZ-ADAMS. Well, sir, I think that financial education is extremely important but it does not solve the problem, especially because the scams change overnight. So you tell them about one thing and then it changes to the next day.

So, you know, there are things that could be done, like in-app warnings, and I know that Mr. Benda has spoken about some of the things that the banks do. You can make some things in-app. But I think more than that you need to hold the institutions that are receiving those payments from the fraudsters more responsible for reimbursing consumers that are harmed.

Senator WARNOCK. So in that regard, are there additional authorities and resources that the Federal Government needs in order to protect Americans from financial fraud?

Ms. SANCHEZ-ADAMS. Yes. I mean, I think you could pass legislation, as I mentioned, in the EFTA to hold those institutions that are receiving the payments responsible, to have them bear some liability. The CFPB can do things through regulation. And certainly I agree that we should have the task force to get more information and more people at the table to talk about this and come up with solutions.

Senator WARNOCK. So there is more work to be done, and our rulemaking and legislation has not kept pace with the reality on the ground. Is that a fair assessment?

Ms. SANCHEZ-ADAMS. That is correct.

Senator WARNOCK. Now, my home State of Georgia is a hub for financial technology and payment processing. In fact, Georgia-

based payment processing firms handle about 70 percent of U.S. transactions. Many fintech and payment companies are focusing on activities that traditionally were handled by consumer banking, including digital payment apps and wallets.

When consumers transfer money using traditional financial tools there are financial protection laws in place for these traditional tools that protect their money. But since many of these digital payment systems are owned by large, nonbank financial companies, they may not carry the same safeguards as financial institutions or debit and credit cards. Last November, the CFPB proposed a rule that would ensure that certain nonbank digital wallets and digital payments apps are subject to the same supervisory oversight as banks and credit unions, again, keeping pace with the reality on the ground.

How would the CFPB's proposed rule provide additional protections to consumers who rely on these payment apps?

Ms. SANCHEZ-ADAMS. They would have supervision authority, meaning that they can go in and examine the books. They can talk to them to see the policies and procedures for them protecting consumers from both unauthorized transactions, to see if they are actually reimbursing consumers, doing reasonable investigations, or what they are doing to protect fraudulently induced scams, especially things like Cash App and Venmo, who have access to both accounts and are seeing those that are receiving the fraudulent payments and where it is going, that they can freeze them, stop them, investigate them, and try to make consumers whole.

Senator WARNOCK. There is no question that consumers deserve to know that their funds are protected by consumer protection laws, regardless of their payment method. We cannot have one set of guardrails for one sector and not have the same guardrails for another sector, as we see increasing digital operations in the banking sector or the financial sector.

What other steps can be taken to protect consumers?

Ms. SANCHEZ-ADAMS. So one thing is to make sure that consumers are reimbursed for fraudulently induced transactions, or scams as people talk about that. Full stop. And then hold those financial institutions that are receiving fraudulent payments responsible, and make sure that payment systems are doing more to protect consumers as well.

Senator WARNOCK. Great. Thank you so very much.

Ms. SANCHEZ-ADAMS. Thank you.

Chair BROWN. Thank you, Senator Warnock.

Senator Warren, of Massachusetts, is recognized.

Senator WARREN. Thank you, Mr. Chairman, and thank you for holding this hearing.

So cyber criminals are exploiting cryptocurrency to scam American consumers out of billions of dollars every year. According to the FBI, Americans are reporting losing more money to crypto-related investment fraud than any other kind of investment scam. In 2022, that amounted to reported losses of more than \$2.5 billion, and that was up 183 percent in just 1 year.

Now according to the Federal Trade Commission, since 2021, crypto has accounted for about 1 in every 4 dollars that consumers

report losing to fraudulent schemes, more than any other payment method out there.

So let's focus today on one type of cryptocurrency—stablecoins. Stablecoins, like Tether and USDC, are supposedly pegged to the dollar or other assets that are relatively stable, and this is supposed to make stablecoins safer and less volatile than other tokens, kind of the responsible big brother of crypto.

But new data show that stablecoins are now used in the majority of illicit crypto transactions, especially in the scams. Last year, more than 70 percent of the crypto scams that we know about involve stablecoins.

So Ms. Sanchez-Adams, as a consumer protection expert does it surprise you that stablecoins are increasingly being used to scam customers?

Ms. SANCHEZ-ADAMS. No. As you said, stablecoins are not as stable as they claim, and they really are primarily a gateway to support unsafe and dangerous crypto assets. So it is to get them into the door to do the crypto.

Senator WARREN. Right. So crypto scams, as you know, take a variety of different kinds of forms—pig butchering, a kind of romance scam, where criminals build up a personal relationship with their targets online and then convince them to invest money in fake crypto platforms before stealing the money. Many of these scams are perpetrated by sophisticated criminal organizations based in Asia, including North Korea.

Mr. Benda, you are an expert on cybersecurity. What is it about crypto that makes it such a good tool to scam people out of their money?

Mr. BENDA. So the challenge we have is that these cryptocurrencies operate outside the banking system, operate outside of regulation, operate outside of BSA/AML. Additionally, the technology is there that allows you to mix and hide transactions. So you can go into that crypto ecosystem and you can actually obfuscate where that money goes after that. And additionally, you can put together what are called “cold wallets.” So you can download millions, hundreds of millions of dollars onto a single USB and transfer that internationally without anyone knowing anymore.

Senator WARREN. Well, that is a lot to be able to hide.

You know, we cannot keep making it easy for criminals and for countries like North Korea to defraud Americans out of their hard-earned money. Twenty Senators, both Democrats and Republicans, are sponsoring the Digital Asset Anti-Money Laundering Act. This bill would plug the holes in our anti-money laundering rules to make it easier for financial regulators to track suspicious crypto activity, to make it more visible, and to shut down the scammers.

So Mr. Breyault, your organization, the National Consumers League, has been protecting consumers for over 100 years. Would this bill help protect American consumers from crypto fraud?

Mr. BREYAULT. Absolutely, yes, Senator.

Senator WARREN. Want to say a word more?

Mr. BREYAULT. So cryptocurrency is certainly the next frontier when it comes to payment scams. It offers a scammer's dream—anonymity, immediacy, and irrevocability. And because of the avail-

ability now of cryptocurrency kiosks in convenience stores, grocery stores, smoke shops—I mentioned earlier that by one estimate there are more than 34,000 of these kiosks across the country—the ability to send cryptocurrency to scammers is usually just down the block for the vast majority of Americans. So yes, your bill would do much to protect consumers.

Senator WARREN. Well, thank you, Mr. Breyault, and thank you to the National Consumers League. We are very grateful to have your endorsement from your organization. I also want to say thank you to the National Consumer Law Center, Ms. Sanchez-Adams.

Our bill will help protect consumers and protect our national security, and I look forward to working with my colleagues on this Committee so that we can get it passed. Thank you. Thank you, Mr. Chairman.

Chair BROWN. Thank you, Senator Warren.

Senator FETTERMAN, from Pennsylvania, is recognized.

Senator FETTERMAN. Well, thank you. I hate to have to follow my colleague, Senator Warren, and talk about crypto because she is, of course, the expert on that. But here into it.

Now it turns out that scammers, hackers, and terrorists now have chosen to use crypto. I mean, it is a shock, right? And it makes you wonder why that. Now do you think the terrorists and those folks are using crypto for the airlines' mileage points, or is it because it is untraceable and they are engaging in illegal kinds of things? Is that a fair statement?

Mr. BREYALT. Yes, Senator.

Senator FETTERMAN. So now, of course, we have the bank meltdowns and crypto funding from Hamas, and now we have scammers and hackers using crypto to steal people's money, of course, as will too.

Now again, directly, Mr. Breyault, can you speak to how people have now fallen prey to these kinds of crypto scams? And my real question is, now is that redundant to have the term of "crypto scam"? Crypto is one gigantic scam, really, on that. So, Mr. Breyault.

Mr. BREYALT. Yes, I would say that crypto is the next payment method of choice for scammers. They recognize that your average everyday consumers is probably not familiar with how it works, and yet, as I just mentioned to Senator Warren, the ability to give your cash to buy crypto and send it to a scammer is usually as close as your closest grocery store.

Cryptocurrency, we believe, for people who want to use it, it is a sophisticated investor who should be looking at cryptocurrency, not my grandmother. And scammers prey on that. They prey on the fact that consumers are not familiar with how it works, and they use that to defraud them out of billions of dollars, and growing.

Senator FETTERMAN. Well, and investor—and again, to me that is kind of a paradox, too, crypto investors. Because really, I know somebody once said that they would not buy up every cryptocurrency for I think it was a quarter. And, you know, really, so why would you invest in crypto for a quarter unless you could sell all of it for 50 cents? You know, kind of like the greater fool kind of thing. Is that really what underpins it, or is there any kind

of inherent value on that, that really, why does it seem to be so open to scams? Is there a connection?

Mr. BREYALT. Well, Senator, thank you for the question. Personally, I would never invest in crypto, for all the reasons that you just discussed. But for scammers it is incredibly appealing because it offers what they are after, which is the ability to get their funds quickly, anonymously, and in a way that is practically impossible to reverse, even when the——

Senator FETTERMAN. Anonymously. Anonymously, right?

Mr. BREYALT. Yes.

Senator FETTERMAN. So it is untraceable and anonymous.

Ms. SANCHEZ-ADAMS. If I may, one of the things that, when we are talking about crypto and scams, is to take into consideration how the money is actually going into crypto first. We hear a lot of stories that it is actually unauthorized or even fraudulently induced through wire transfer, and then there are no protections for the consumer there. If it was sent through, like an electronic funds transfer that is covered by the EFTA, they would have protections, but we have heard of it coming either from HELOC accounts or from wire transfers. And so initially, even that transfer out has no protections for the consumer.

Senator FETTERMAN. Oh my gosh. That is amazing, because I literally was going to pivot to you for the next question, and that is really about that. My staff is much smarter than I am, and I was not really aware of this, but they brought it to my attention, is that true bank customers, they aren't protected from hackers if they initiate a wire transfer. Right. I mean, like that is outrageous. I did not even know that myself.

And is there a fix for that or anything that you would recommend, because again, if I was not aware of that, and I am on the Banking Committee, so think of the millions of Americans that are not aware of this.

Ms. SANCHEZ-ADAMS. Yes, absolutely. We get interviewed all the time, even by "Good Morning America", about this very same question. So yes, make it be covered by the Electronic Funds Transfer Act.

There was an exclusion when it was originally written in the 1970s and wire transfers were really business-to-business and consumers were not doing it, and it was in person. Now you are doing it online through mobile and digital applications, and so it is, in essence, an electronic funds transfer now. And even the New York AGs have argued, in a suit they filed against Citi, that it actually is an electronic funds transfer when it is unauthorized or requested from someone who is not the consumer to send it somewhere else.

So it can be included in the EFTA, and of course, we should not forget the fraudulently induced transactions. Those should also be included in the EFTA.

Senator FETTERMAN. So I guess you are saying, so really the banks, I mean, they are the experts and they are professionals, they should be held accountable, not then a customer, that may not have any kind of idea on the level of what is going on. Is that a fair statement again?

Ms. SANCHEZ-ADAMS. Right. Again, if it was unauthorized and the consumer did not do it, then yes, they should be reimbursed.

Senator FETTERMAN. OK. Mr. Chairman.

Chair BROWN. Thank you, Senator Fetterman, for your incisive questions.

It is my turn. I think I will be the last questioner.

Ms. Sanchez-Adams, like an hour ago, an hour-and-a-half ago, you gave your six recommendations. The CFPB, as you know, last year proposed a rule that would allow the consumer agency to supervise larger payment apps. Just walk through, if you would, what this proposed rule means for large payment apps like Venmo and Cash App and Zelle and the consumers, what it means to the consumers who use these platforms. Sort of give us a synopsis of what this rule is actually going to mean for sort of all the players.

Ms. SANCHEZ-ADAMS. One thing is that nobody actually knew what was happening on these platforms until this Committee sent a letter, right, asking for that information of how many people are actually getting reimbursed for unauthorized transactions and how many people are not being reimbursed when they are scammed. Nobody had access to that information because they were not supervised. So the CFPB being able to go in and supervise that means that you will actually know if they are following the law.

So unless you are a private attorney who is suing them because a consumer came and told you a story, there was really no way to know what was happening behind the scenes. So that is why this rule is so important, and again, it is not just Venmo, PayPal, and Cash App, but it is other players as well.

Chair BROWN. Thank you. And, I mean, that really is the work this Committee can do. We do oversight. We sometimes just inform the public and can ask questions like that. And the larger participant rule, as you point out, will allow the agency to supervise these apps, ensuring that they follow consumer protection laws, and why we need a strong, independent CFPB. That has been said many, many, many times from this dais, from a whole bunch of my colleagues.

I would also point out that this attendance—attendance is sometimes spotty in this Committee, sometimes not—this is such an important issue to so many that at least on our side of the aisle all but one Member showed up and a number of Members on the other side, too, and that is a good sign.

Ms. Sanchez-Adams, you discussed the differences between unauthorized transactions and fraudulently induced transactions, with the major difference being that financial institutions are legally required to reimburse consumers for the unauthorized transactions. Does the same hold true for unauthorized transactions using wire fraud? Are consumers and their money really protected from scammers there?

Ms. SANCHEZ-ADAMS. No. As I had mentioned in detail and, I think, in my written testimony is the Uniform Commercial Code (UCC) is the State law that applies to wire transfers, excluding international remittances. And it was not designed to be a consumer protection statute. It was designed for banks to know the procedures when using these.

And so right now it essentially says if there was a security procedure that the consumer and the bank agreed to, and the consumer does not really agree to it when it is in the fine print of something

they are clicking to agree to be able to have an account, or often those terms say that we may choose one. We may call you or we may not call you. So if the banks use that procedure then they argue that they do not have any liability, and it is pushed onto the consumer. This is why we really need wires to be covered by the EFTA.

Chair BROWN. Thank you. Mr. Breyault, we are hearing more and more anecdotes about how scammers are using AI to create personalized attack. For example, scammers, as you know, can use a consumer's voice from a social media post and use AI to replicate that consumer's voice to gain access to account information. How do Congress and regulators get ahead of these problems?

Mr. BREYAUULT. Thank you for the question, Mr. Chairman. I certainly think that AI has the potential to be as big an accelerant of fraud as the internet was 30 years ago. And in addition to the voice-cloning technology that you talked about, we are also very concerned that AI can be used by criminal scammers to basically supercharge the ability to identify the most vulnerable consumer. So we know that criminal gangs will fight over lists of potential victims in the United States that they want to use for many different kinds of scams. With AI, they can target, with laser-like precision, the consumers that they think are most vulnerable to these scams. So even if they do not need to use voice cloning, just being able to know the right people to contact, how to contact them, and the types of words to use to get them on the hook for these frauds is one way that we are really concerned about how AI is going to be used.

I think we are still developing sort of specific policy proposals that Congress could take, but I appreciate what we heard earlier about triple damages, again, scammers using AI in this way. I think that is one area that this Committee should consider, and we are happy to get back to you with additional policy proposals for how to start to tackle the threat that AI poses.

Chair BROWN. That would be helpful. Thank you.

Last question, and be as brief as you can. I am over my time. But this is the end, so that is fine.

Mr. Benda, my colleagues and I wrote to your organization, the ABA, expressing concerns about the alarming increase in check fraud scams. Your organization created an information directory, providing contact information for banks to resolve check fraud claims. That is good as far as it went.

Has this directory improved the timeliness with which defrauded customers get their money back? It seems that bank customers are all too often waiting too long for their money, not something that people often could afford when it is thousands of dollars. So assure me that it is more timely than that and that you are working to make it even more timely.

Mr. BENDA. Thank you, Mr. Chairman, and I appreciate you recognizing the efforts we have made on this.

So the directory now encompasses almost 1,700 banks, and we have heard from many banks at how much better it has made their lives because they can actually file these claims faster. Are we where we want to be? No, we are not, and that is why we are continuing our efforts, reaching out to banks to try and expedite those

processes, make sure they are more streamlined, make sure that we have better and more industry baseline in terms of the requirements to submit these claims so they can be processed faster.

Chair BROWN. OK. Someone from the Richmond Fed told me once, "Watch us and make sure you let us know that we are watching you." So we are in this case, so thank you.

Thanks to the three of you. Really good hearing. Really informative. Great interest from this Committee.

Senators who wish to submit questions for the hearing record, we have notified them they are due 1 week from today, the 8th of February. To the witnesses, please submit responses to any and all of those questions within 45 days from the day we get them to you.

Thank you very much. The hearing is adjourned.

[Whereupon, at 11:57 a.m., the hearing was adjourned.]

[Prepared statements, responses to written questions, and additional material supplied for the record follow:]

PREPARED STATEMENT OF CHAIR SHERROD BROWN

When consumers send money through an app or send a check in the mail, they are supposed to be able to trust that financial companies are protecting their money and will help them if something goes wrong.

Yet that's not what we see.

Scammers and fraudsters have ramped up their efforts to take people's money. Banks and payment apps have stood on the sidelines while the problem has only gotten worse.

Pretty much everyone has either been scammed, or knows someone who has been scammed, when trying to use a financial service.

Today one of the most popular ways people send money is through so-called peer-to-peer apps like PayPal, Venmo, Cash App, and Zelle.

These apps are now part of most Americans' day-to-day lives. Seventy-five percent of adults have used at least one of them. Forty percent of Americans report using them at least once a month.

Where consumers see convenience and accessibility, scammers see an opportunity. In 2022, one major payment app had more than \$100 million in "unauthorized transactions." Another had almost \$60 million.

Of course, it's not just new technology or payment methods that scammers target. Check fraud is as old as our banking system.

They'll steal a check from the mail, use chemicals to wash off the key details, then fill it in with the details they want and deposit it.

You might think that more people using apps would make checks less of a target, but it's the opposite—check fraud is getting worse, too.

Last year, the Financial Crimes Enforcement Network noticed a rise in check fraud so drastic that they issued a public alert.

My colleagues and I wrote to the American Bankers Association expressing our concerns on the issue, and they created an information directory providing contact information for banks to resolve check fraud claims.

By the end of 2022, depository institutions had reported more than 500,000 incidents of check fraud—more than double the year before. Scammers broke their record again in 2023.

The same goes for wire transfers. Scammers target wire transfers because they can steal a larger portion of consumers' savings through wire transfers.

Americans will often use wire transfers when they want to send large amounts of money, like when buying a house.

Imagine a family in the process of trying to buy a home, juggling all the details of the process, along with the excitement of reaching a major life milestone.

On top of everything else they have to worry about, they have to defend against scammers posing as a real estate agent or title company targeting the family's downpayment.

In 2023, consumers lost at least \$270 million to wire fraud.

And now we're faced with the possibility that artificial intelligence will make these problems worse.

As just one example, scammers can now use AI to clone a person's voice to bypass voice authentication procedures.

Banks, payment apps, and other financial institutions are not doing nearly enough to prepare for the threat AI poses in increasing the scale and impact of scams.

All of these problems with scams are rampant.

In Dublin, Ohio, a retired FBI agent, wrote a check for less than \$200.

Someone stole that check from a mailbox right in front of a post office, changed the number to \$8,590 and cashed in.

In another case, a 17-year-old student in Ohio received an acceptance letter from her dream college.

Someone posing as another admitted student reached out and scammed her out of almost \$3,000 of her own money through Zelle.

That \$3,000 was three-quarters of her college money she saved up working at a discount drugstore.

None of this mattered to the bank. As far as the bank was concerned, this young woman was responsible for the money and additional fees for depositing bad checks.

In the end, she got her money back, but only after the efforts of her tenacious mother, who tracked down the local executive of the bank.

No one should have to go to those lengths because banks, payment apps, and other financial institutions can't get their act together to protect their customers.

When these incidents happen, people lose their hard-earned money.

And they're often made to feel ashamed and embarrassed.

No one ever tells a victim of a hold-up that they were stupid or should have known better than to be robbed. But that's exactly what consumers who are scammed hear.

Let's be clear, being scammed has nothing to do with intelligence, savviness, or education.

Just last year, a retired White House scientist was scammed out of \$655,000 of her retirement savings.

Those scammers were organized. They sent her a pop-up message on her computer, rerouted a phone call she meant for her bank, and kept her on the phone for days on end.

She still wonders about what she could have done differently. But no one should have to think about that question.

And to be clear: the answer to these types of stories isn't to warn people to be better prepared or put millions of consumers through a so-called "financial education" course.

Americans do not have time for that. They have jobs and kids and bills to worry about. It's not on them—it's on the companies. People should be able to have an expectation their money is safe when they have a reputable bank.

People lose their money because payment apps and banks don't put enough measures in place to protect their customers.

For example, among the peer-to-peer companies, Cash App refunded just 16 percent of unauthorized transactions in 2022.

Zelle claims they reimburse consumers who have been victims of imposter scams. But their website states that since the consumer, "authorized the payment, you may not be able to get your money back." It is unclear whether Zelle will actually reimburse victims of imposter scams. They need to clarify their reimbursement policy.

These companies need to step up, and they apparently need rules to make them do it. These banks, payment apps, and other financial services companies have shown us they need, shall we say, encouragement.

The Consumer Financial Protection Bureau has a proposed rule that is one strong first step. It would help ensure that companies like Venmo, Cash App, and Zelle follow Federal consumer protection laws.

This is what the CFPB does—protect consumers and their hard-earned money. When the CFPB is empowered, it ensures that the financial system works for consumers, not just corporations.

With millions of users, it only makes sense that these companies do more to protect consumers' money.

Because, as we've seen in previous hearings, frauds and scams are not unique in consumer finance, they are also common within cryptocurrency. We will keep pushing to make our financial system safer—whether its stopping rampant frauds and scams in cryptocurrency or in apps and check fraud.

I hope we can discuss more today about how banks, payment apps and other financial service companies can step up for their consumers and earn their trust back.

PREPARED STATEMENT OF SENATOR TIM SCOTT

I'll start off by saying, I guess Steven Spielberg was on to something when he named the movie "Catch Me If You Can".

Recently, I saw a movie called "The Beekeeper", which starts off about financial scams that led to the grandmother's suicide. Now financial scams may not today lead to suicide, but without any question, they certainly kill your hopes, your dreams, and your sense of financial security.

The impact of financial scams—especially on our senior citizens—is undeniable. Having been the Ranking Member on the Aging Committee, we've had many, many hearings about the devastation of retirement savings lost. Lives changed. Grandmothers looking for a place to call home—moving back in with their kids or their grandkids.

The devastation is so real—and so often—goes unreported in some instances. And certainly, the investigations leave many wanting.

Even in a largely digital age, more traditional forms of fraud continue to flourish.

We think about the fact that whether it's check fraud, wire fraud, or mail fraud, we've seen a resurgence of criminal activity in these spaces—in addition to of course the new types of fraud that comes along with the technological advancements that we've seen around our country—and certainly the innovations around the world.

Not only do I think of my own mother—who celebrates a birthday this weekend as a senior citizen—I think of every single South Carolinian who trusts that their

money is safe when they write a check and place it in the mail, or transfer money to their grandkids.

Mr. Benda, I thank you for bringing your expertise and talking about the different kinds of fraud that can impact American consumers.

Protecting consumers and preventing fraud are critical pillars of our financial system and, frankly, what our society deserves.

For many families, becoming a victim to these scams is equivalent to wiping out a lifetime of savings.

And not just the dollars in the account, but the thought that you are no longer safe to transact business anywhere, in any form.

For many, it is the worry that their identity is compromised, that their credit score is impacted, and they struggle to realize just how will they survive and afford—whether it's their rent, or mortgage, or even simply groceries.

Which in today's inflationary economy is even harder than it was before.

Speaking of dollars, let's just count the costs—\$9 billion in 2022 is the cost of financial fraud. A staggering number.

Unfortunately, these criminal acts of fraud and theft are not new, and criminals like these continue to prey on the vulnerable.

This is precisely why our financial institutions and financial industry participants should—and do—spend billions of dollars developing and implementing innovative technologies to strengthen security that will protect families and businesses from fraud.

But on the other side of the coin, we haven't seen the same commitment from our Federal regulators.

Recently, our regulators seem to be more focused on political grandstanding than promoting innovative solutions, protecting consumers, and increasing efforts that support financial education.

And instead of focusing on real crimes and holding criminals responsible, this Administration seems intent on tying up financial institutions with ever increasing amounts of Washington red tape.

Recently, the CFPB has continued its deceptively named “junk fee” campaign, targeting legitimate, contractually agreed upon payment incentives.

In its latest proposals, the CFPB uses legal gymnastics to turn penalty fees into loans while slapping the label “abusive” on any practice it just doesn't like.

The CFPB is sending a clear message: it is willing to stretch the law beyond its limits to suit Director Chopra's political agenda.

And every dollar spent navigating Washington red tape is a dollar less on initiatives that actually help families and protect businesses.

It's a dollar less for bolstering a firm's cyber defenses in the investment world that may prevent or even catch fraud before it happens.

Unfounded, bureaucratic regulations take resources away from financial innovation and education, both of which can help lift up the underserved and minority communities.

What concerns me even more than all of this, is recent allegations that suggest that Federal law enforcement and financial regulators may be expending their resources to target Americans for their political and religious beliefs.

Instead of targeting Americans for purchasing Bibles or shopping at the Bass Pro Shops, our Government should focus on doing its job—protecting our families and prosecuting actual criminals, including those behind financial scams.

Unfortunately, these examples are part of a larger trend we have seen from this Administration of putting politics first.

For example, banking regulators were so focused on climate change, that they failed to identify the key risk factors leading to the second, third, and fourth largest bank failures in our Nation's history last spring.

And again, if the CFPB wasn't so focused on building a public pressure campaign against so-called “junk fees,” maybe it could do its job and actually protect consumers from the real harm that comes from being a victim of financial crime.

One of the best tools any of us have to fight back against financial crimes is to become better educated, both about the financial products and protections that are available to us and about the scams and methods criminals are using against us.

In fact, I have long championed the idea that financial education and financial literacy is one of the most important and most critical tools for climbing the ladder of success in America.

It's why I've worked so hard to incorporate financial literacy in my work here on this Committee, and financial literacy is a core pillar of two of my initiatives—both the ROAD to Housing and Capital Markets framework.

And I was so proud to work across the aisle with Senator Reed last spring to pass a resolution declaring April financial literacy month.

As we discuss the very real issues of financial fraud and crime, we must take a holistic approach.

Our financial institutions must do their part to protect, to serve, and educate customers.

And our regulators must do their job and implement the law Congress enacted, not their political wish list.

We must all work together to gain a better understanding of the options before us so that we are able to best serve our communities, our constituents, and our Nation.

I look forward to hearing from each of the three witnesses.

PREPARED STATEMENT OF CARLA SANCHEZ-ADAMS
 SENIOR ATTORNEY, NATIONAL CONSUMER LAW CENTER
 FEBRUARY 1, 2024

Chairman Brown, Ranking Member Scott, and Members of the Committee, thank you for inviting me to testify today regarding scams and fraud in the banking system and their impact on consumers. I am Carla Sanchez-Adams, a senior attorney at the National Consumer Law Center. I offer my testimony on behalf of NCLC's low-income clients.

Since 1969, the nonprofit National Consumer Law Center® (NCLC®) has used its expertise in consumer law and energy policy to work for consumer justice and economic security for low-income and other disadvantaged people in the United States. NCLC's expertise includes policy analysis and advocacy; consumer law and energy publications; litigation; expert witness services; and training and advice for advocates. NCLC works with nonprofit and legal services organizations, private attorneys, policymakers, and federal and state government and courts across the nation to stop exploitative practices, help financially stressed families build and retain wealth, and advance economic fairness. NCLC has long advocated for stronger laws, regulation, and enforcement to ensure that consumers' funds and payments are safe and to prevent and remedy fraud.

I am one of the co-authors of NCLC's treatise, *Consumer Banking and Payments Law*. My colleagues and I interact with legal services, government, and private attorneys, as well as community groups and organizations from all over the country who represent low-income and vulnerable individuals on consumer issues. As a result of our daily contact with these advocates, we have seen many examples of the damage wrought by payment fraud from every part of the nation. It is from this vantage point that I supply this testimony.

NCLC has previously provided testimony before Congress on the need to address payment fraud.¹ Additionally, NCLC has provided feedback to various regulatory agencies on the same issue.² I reiterate and incorporate those comments here as well.

Payment fraud impacts all Americans across many communities— young, old, those highly educated, and those that are not. But the impacts of fraud are most keenly felt by certain vulnerable populations such as older Americans, low-income consumers, and minorities.

Consumers are plagued by problems with unauthorized transactions as well as fraudulently induced transactions over peer-to-peer payment applications, bank-to-bank wire transfers, check alterations and forgeries, and Electronic Benefits Transfer card skimming. The increasing ease

¹ See NCLC *et al.*, Statement for the Record, “*What’s in Your Digital Wallet? A Review of Recent Trends in Mobile Banking and Payments*,” Hearing Before the House Financial Services Taskforce on Financial Technology at 10-11 (April 28, 2022), available at <https://www.govinfo.gov/content/pkg/CHRG-117/hr47649/pdf/CHRG-117/hr47649.pdf>; Testimony of Odette Williamson, NCLC “*Fraud, Scams and COVID-19: How Con Artists Have Targeted Older Americans During the Pandemic*,” Hearing Before the U.S. Senate Special Committee on Aging (Sept. 23, 2021) available at https://www.nclc.org/wp-content/uploads/2022/08/Testimony_Covid_Aging-1.pdf.

² See NCLC *et al.*, Comments regarding the FTC Collaboration Act of 2021, (Aug. 14, 2023) available at https://www.nclc.org/wp-content/uploads/2023/08/FTC_AG-Fraud-Collaboration-consumer-comments-8-14-23-final3-Lauren-Saunders.pdf; NCLC *et al.*, Letter Urging Federal Reserve Board to Prevent FedNow Errors and Fraud, (Aug. 10, 2022) available at https://www.nclc.org/wp-content/uploads/2022/09/FedNow_fraud_ltr.pdf; Comments of 43 consumer, small business, civil rights, community and legal service groups to Federal Reserve Board Re: Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire, Docket No. R-1750; RIN 7100-AG16 (Sept. 9, 2021), <https://bit.ly/FedNowCoalitionComments> (“FedNow Comments”).

and use of mobile and online banking through technological advancement have also simultaneously provided opportunities for scammers to exploit newer payment technologies. However, obtaining a complete and holistic picture of the volume, loss, and threat of payment fraud is difficult because of the fragmented way we collect this data.

The financial institutions that design and run these payment systems, including the financial institutions that hold the accounts of scammers and money mules that receive fraudulent payments, need to take more responsibility for making these systems safe and protecting consumers. Given the increasing sophistication of fraud schemes, warnings to consumers are insufficient. If payment system participants take responsibility for protecting consumers, as they are doing in the United Kingdom, they will have the incentive to leverage the latest innovative technologies to prevent and detect fraud, making the entire system safe. At the same time, any attempts to combat fraud must also be tempered with policies and procedures that protect innocent consumers who do not engage in payment fraud but whose funds might be frozen for extended periods of time.

To combat payment fraud, we recommend addressing the current gaps and ambiguities in the Electronic Funds Transfer Act that leave consumers unprotected. These include:

- Ensuring consumers are protected from liability when they are defrauded into initiating a transfer;
- Allowing the consumer's financial institution, after crediting the consumer for a fraudulent transfer, to be reimbursed by the financial institution that allowed the scammer to receive the fraudulent payment;
- Eliminating the exemption for bank wire transfers and electronic transfers authorized by telephone call, bringing those transfers within the EFTA and its protections against unauthorized transfers and errors;
- Eliminating the exclusion of Electronic Benefit Transfer cards from the EFTA, bringing those transfers within the EFTA and its protections against unauthorized transfers and errors;
- Clarifying that the EFTA's error resolution procedures apply when the consumer makes a mistake, such as in amount or recipient;
- Clarifying that the error resolution duties under the EFTA apply if a consumer's account is frozen or closed or the consumer is otherwise unable to access their funds, with an exception if the consumer was denied access due to a court order or law enforcement or the consumer obtained the funds through unlawful or fraudulent means; and
- Considering whether consumer protections for checks should be included in the EFTA.

Federal regulators should also take additional steps to address fraud and protect innocent consumers who are harmed by aggressive fraud reporting. For example, federal regulators should:

- Devote more attention to the responsibilities of institutions that receive fraudulent payments, including stepping up enforcement of Bank Secrecy Act / Anti-Money Laundering obligations;

- Establish interagency collaboration to assist consumers with reporting fraud, collecting data on fraud, and establishing systems; and
- Provide guidance to financial institutions about the timelines and procedures for consumers to regain access to improperly frozen funds and clarify what information can and should be given to account holders regarding account closures and freezes.

I. Fraud is Exploding and Affects Everyone.

Fraud continues to climb and devastates millions of consumers across the country each year. In 2022, the Federal Trade Commission (FTC) received over 2.5 million reports of fraud with reported losses totaling almost \$9 billion (\$8,996,000). Those losses are up a shocking 46.7% over 2021. Losses for 2023, which have not yet been fully reported, are on track to exceed 2022.

Additionally, the FTC numbers reflect only fraud cases reported to the FTC. Fraud is substantially underreported; only an estimated 15% of U.S. fraud victims report the fraud to law enforcement.³

As AARP noted:

“While nearly nine in 10 respondents (87%) feel people should report incidents of fraud, only an estimated 15% contact law enforcement. The gap may be tied to attitudes and awareness about fraud. Sometimes those who have been victimized by a scam feel embarrassed, guilty, or believe there is nothing police can do.”⁴

Fraud impacts all of us, across every community—the young and the old, those highly educated and those that are not.⁵ While the common belief is that older consumers are more likely to be susceptible, in fact younger people are significantly more likely to experience fraud. But when older people suffer fraud, they lose far more money, as shown by the following FTC chart:⁶

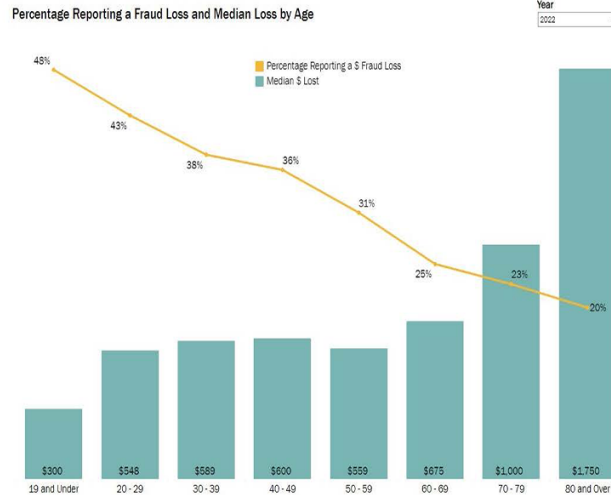
³ Department of Justice, U.S. District Attorney’s Office, District of Alaska, Financial Crime Fraud Victims (2020), <https://www.justice.gov/usao-ak/financial-fraud-crimes>.

⁴ Williams, Alicia R., “Americans Are Aware of Fraud’s Pervasiveness but Remain Vulnerable,” AARP Research (May 17, 2023); see Department of Justice, U.S. District Attorney’s Office, District of Alaska, Financial Crime Fraud Victims (2020), <https://www.justice.gov/usao-ak/financial-fraud-crimes>.

⁵ Levinthal, Dave, “Cyberthieves stole \$186,000 from a Republican member of Congress as fraud epidemic plagues political committees,” Business Insider (Nov. 29, 2022) available at <https://www.businessinsider.com/online-fraud-congress-diana-harshbarger-cybertheft-2022-11>.

⁶ FTC, Percentage Reporting a Fraud Loss and Median Loss by Age (2022), available at <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudLosses>.

FTC CONSUMER SENTINEL NETWORK

Published November 1, 2023
(data as of September 30, 2023)

Fraud has a particularly harsh impact on low-income families and communities of color, who have fewer resources to help them recover. Fraudsters often take the last dollar from those least able to afford it, and often target older adults, immigrants, and other communities of color.

II. Payment Systems Play an Important Role in Enabling or Preventing Fraud and in Protecting Consumers.

Criminals who steal money through fraud schemes need a way to obtain a victim's money. They use a variety of payment systems to receive that money, including person-to-person (P2P) transfer services, wire transfers, checks, and gift cards. Each of those payment systems has a role to play in keeping criminals out, preventing fraud, and protecting consumers. Fraud does not succeed if the fraudster cannot receive the money.

Fraud may result in unauthorized transactions or fraudulently induced transactions, each with different protections. After obtaining information through phishing schemes, fraud schemes, or data breaches, criminals may make unauthorized transactions for which consumers generally have protection (though, in some cases, imperfect protection, as discussed below). Checks can also be stolen and altered, another form of unauthorized transaction. Or criminals can defraud a consumer into making a fraudulently induced transaction where protection is sorely lacking.

As discussed in more detail below, payment fraud usually involves two institutions – the institution that holds the consumer's account (the consumer's institution) and the institution that

receives the stolen funds and holds the account of the fraudster or money mule (the receiving institution). When seeking to prevent and remedy fraud, it is important to focus on the responsibilities of both the consumer's institution and the receiving institution as well as the payment system itself, regardless of whether the fraud is unauthorized or fraudulently induced. When consumers are protected, these institutions and systems will have incentives to use their resources and technological innovations to prevent fraud and make everyone safer.

In the testimony below I will focus on four payment vehicles that have seen increasing fraud: person-to-person payments, bank-to-bank wire transfers, check alterations, and Electronic Benefit Transfer cards. I will discuss how these payment frauds impact consumers and how protections can be improved. I will also discuss the need for more data sharing in the effort to combat fraud.

III. Person-to-Person (P2P) Payment Fraud.

A. The prevalence of P2P use and the incidence of fraud on these platforms.

Person-to-person (P2P) payment apps have become increasingly popular among consumers. Seventy-six percent of households use Venmo or Cash App.⁷ In addition to P2P payment services, consumers are also increasingly adopting other forms of technology to make payments.⁸

According to the FTC,⁹ "payment app or service" is the third largest category of payment method specified by fraud victims in terms of number of reports (after credit cards and debit cards), and the dollar volume of losses by payment app or service increased 25% from 2021 to 2022.¹⁰ Though the final figures of fraud reports are unavailable for 2023, the FTC received reports during the first three quarters of 2023 that are on path for another 25% increase by dollar amount of losses.¹¹ The Consumer Financial Protection Bureau (CFPB) has also seen high growth in complaints about fraud in P2P apps and digital wallets.¹²

As consumer, small business, civil rights, community, and legal service groups described at greater length in comments submitted to the Federal Reserve Board (FRB) and the CFPB, the existing P2P payment systems of large technology companies and financial institutions simply

⁷ Anderson, Monica, "Payment Apps like Venmo and Cash App Bring Convenience – and Security Concerns – to Some Users," Pew Research Center (blog), (Sept. 8, 2022), available at <https://www.pewresearch.org/short-reads/2022/09/08/payment-apps-like-venmo-and-cash-app-bring-convenience-and-security-concerns-to-some-users/>.

⁸ Chen, Jane, Deepa Mahajan, Marie-Claude Nadeau, and Roshan Varadarajan, "Consumer Digital Payments: Already Mainstream, Increasingly Embedded, Still Evolving," Digital Payments Consumer Survey, (Oct. 20, 2023), available at <https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/consumer-digital-payments-already-mainstream-increasingly-embedded-still-evolving>.

⁹ Reports of fraud to the FTC do not always specify the payment method utilized to perpetuate the fraud, however, the FTC does collect and report data on payment method when available.

¹⁰ FTC fraud reports by payment method available at <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods>. Only 429,264 (17%) of 2,563,959 fraud reports received by the FTC specified the payment method.

¹¹ *Id.*

¹² U.S. PIRG Educ. Fund, *Virtual Wallets, Real Complaints*, at 2, (June 2021), available at https://uspirg.org/sites/pirg/files/reports/VirtualWallets/Virtualwallets_USP_V3.pdf.

are not safe for consumers to use.¹³

P2P fraud has a particularly harsh impact on low-income families and communities of color. These communities, already struggling and often pushed out of the traditional banking system, can least afford to lose money to scams and errors. Because many minorities are also unbanked or underbanked,¹⁴ they are the target audience for use of many of the P2P apps. For example, a September 2022 Pew Research Center survey shows that 59% of Cash App users are Black and 37% are Hispanic.¹⁵ Yet Cash App has also been subject to reports of widespread fraud,¹⁶ failing to protect the very vulnerable populations it targets.

The news media has reported many of the fraudulent schemes enabled by the P2P systems. Generally, these scams and theft would not have been possible without the payment apps.

- Manhattan District Attorney Alvin Bragg explains how criminals have utilized deception, violence, or threat of violence to steal funds from consumers through payment apps like Cash App.¹⁷
- Mary Jones of Kansas City paid \$1,700 through Venmo in "rent" to a man who claimed to own the house she wanted to move into. He even gave them access to tour the house before she signed the lease. After she saw a "For Lease" sign in the front yard, she called the rental company and discovered that she had paid a scammer. She filed a police report but has not been able to retrieve her money.¹⁸
- In a similar fraud scheme, a single mom in South Carolina looking for housing paid a deposit, cleaning fee, and first month's rent on a condo listed on Redfin.com through a payment app and lost \$2,600.¹⁹

¹³ See Comments of 65 Consumer, Civil Rights, Faith, Legal Services and Community Groups to CFPB on Big Tech Payment Platforms at 4-5, Docket No. CFPB-2021-0017 (Dec. 21, 2021), <https://bit.ly/CFPB-BTPS-comment> ("CFPB Big Tech Payment Platform Comments"); Comments of 43 consumer, small business, civil rights, community and legal service groups to Federal Reserve Board Re: Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire, Docket No. R-1750; RIN 7100-AG16 (Sept. 9, 2021), <https://bit.ly/FedNowCoalitionComments> (FedNow Comments).

¹⁴ 11.3 percent of Black and 9.3 percent of Latino households are unbanked compared to only 2.1% of white households. See FDIC, *2021 FDIC National Survey of Unbanked and Underbanked Households*, at 2, <https://www.fdic.gov/analysis/household-survey/2021report.pdf> (last updated July 24, 2023).

¹⁵ Anderson, Monica, "Payment apps like Venmo and Cash App bring convenience – and security concerns – to some users," Pew Research Center (Sept. 8, 2022) available at <https://www.pewresearch.org/short-reads/2022/09/08/payment-apps-like-venmo-and-cash-app-bring-convenience-and-security-concerns-to-some-users/>.

¹⁶ Hindenburg Research, "Block: How Inflated User Metrics and 'Frictionless' Fraud Facilitation Enabled Insiders To Cash Out Over \$1 Billion," (Mar. 23, 2023), available at <https://hindenburesearch.com/block/>. ("Former employees estimated that 40%-75% of accounts they reviewed were fake, involved in fraud, or were additional accounts tied to a single individual").

¹⁷ Morales, Mark, "Venmo and other payment app theft is 'skyrocketing,' Manhattan DA warns," CNN (Jan. 23, 2024), available at https://www.cnn.com/2024/01/23/business/venmo-payment-app-theft?cid=ios_app.

¹⁸ Johnson, Tia, "Kansas City woman warns others after losing nearly \$2,000 in rental home scam," Fox4 (May 3, 2021), available at <https://fox4kc.com/news/kansas-city-woman-warns-others-after-losing-nearly-2000-in-rental-home-scam/>.

¹⁹ Cioppa, Jordan, "James Island woman says rental scam cost her \$2,600," WCBD News2 (Jan. 10, 2023), available at <https://www.wcbl.com/news/james-island-woman-says-rental-scam-cost-her-2600/>.

Zelle is another popular P2P payment service, but users transfer funds between bank accounts directly.²⁰ As more and more consumers use Zelle, the service has also become popular among criminals.²¹ For example:

- Maria Glover from Philadelphia had thousands of dollars stolen from her Citibank account via Zelle. She was contacted by the fraudsters through texts though she never provided any password or personal information to them. She further explains that the transactions stolen were for more than her \$2,500 daily withdrawal limit, and Citibank could not even explain how the fraud occurred.²²
- Luke Krafka, a professional musician in Long Island, lost almost \$1,000 dollars through Zelle when a fake client “hired” him to play at a wedding. The man sent him a large check and asked him to pay part of the money back through Zelle. The check bounced after Krafka had already sent the money. His bank refused to refund his payment.²³

P2P payment systems, if properly designed, can provide broad benefits to consumers. But those benefits will only be realized if the systems are safe to use.

B. How technology perpetuates P2P fraud and theft.

Fraudsters have extraordinary creativity;²⁴ they are constantly developing creative ways to steal people’s money by setting up increasingly sophisticated schemes to obtain access to accounts or to fraudulently induce consumers into payment transactions.²⁵ The Federal Communication

²⁰ The FTC designates Zelle transfers as part of the “bank transfer or payment” category, which also includes bank-to-bank wire transfers. See Section IV.A of this testimony for FTC statistics on “bank transfer or payment,” also available at

<https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods>.

²¹ Cowley, Stacy and Nguyen, Lananh, “Senators question Zelle over how it is responding to reports of rising fraud,” New York Times (Apr. 26, 2022), available at <https://www.nytimes.com/2022/04/26/business/zelle-fraud.html>.

²² Pradelli, Chad, “I still don’t know how they got access: Woman loses thousands after thief targets her Zelle app,” ABC Action News, WMPVI-TV Philadelphia, PA (Jun. 2, 2023), available at <https://6abc.com/zelle-peer-to-peer-payment-apps-theft-auto-payments/13335405/>.

²³ See CBS This Morning, “Complaints against mobile payment apps like Zelle, Venmo surge 300% as consumers fall victim to more money scams,” CBS News (June 23, 2021), available at <https://www.cbsnews.com/news/venmo-payal-zelle-cashapp-scams-mobile-payment-apps/>.

²⁴ See NCLC, EPIC report *Scam Robocalls: Telecom Providers Profit*, at 6-10 (Jun. 2022) available at <https://www.nclc.org/wp-content/uploads/2023/02/Robocall-Rpt-23.pdf> for examples of the types of scams utilized by robocalls and scam texts; see also Testimony of Margot Saunders, NCLC “Protecting Americans from Robocalls,” Hearing Before the U.S. Senate Committee on Commerce, Science & Transportation (Oct. 24, 2023) available at <https://www.nclc.org/wp-content/uploads/2023/10/Testimony-of-NCLC-on-Robocalls-2023.pdf>.

²⁵ See the latest scam warning below which also involves impersonation of law enforcement.

SCAM OF THE WEEK:
This Fake App Takes the Cake

Commission's (FCC) website includes a Scam Glossary detailing dozens of different ways individuals and small businesses have lost money to these schemes,²⁶ and the FCC specifically identified P2P apps as a primary means for executing scams and fraud.²⁷ Clearly, the warnings provided by the payment apps themselves to beware of scams and fraud are not adequate to protect consumers from the losses.

This recent scam is impressively complex. The cybercriminals start by impersonating law enforcement officers. They contact you, claiming that your bank account may have been involved in financial fraud. You're then asked to download a mobile app to help them investigate further. If you download the app, the cybercriminal walks you through the steps to set this scam in motion.

First, you are given a case number. When you search for that number in the app, you'll find legal-looking documents with your name on them. These documents make the scam feel more legitimate. Once your guard is down, the app asks you to select your bank from a list and then enter your account number and other personal information.

The most clever part of this scam is what the app does in the background. When you first install the app, it blocks all incoming calls and text messages. That way, you won't be alerted if your bank attempts to contact you about unusual behavior on your account. If all goes as planned, the cybercriminals will steal your money and sensitive information before you know what happened.

No matter how advanced the app is, you can stay safe from scams like this by following the tips below.

- Only download apps from trusted publishers. Anyone can publish an app on official app stores or sites—including cybercriminals.
- Be cautious of scare tactics that play with your emotions. Cyberattacks are designed to catch you off guard and trigger you to reveal sensitive information.
- If you're contacted by someone claiming to be in a position of authority, like law enforcement, ask them to confirm their identity. Real officials will understand your concerns and can provide information that doesn't require you to download an app.

The KnowBe4 Security Team
KnowBe4.com

²⁶ Federal Commc'ns Comm'n, Scam Glossary, available at <https://www.fcc.gov/scam-glossary>.

²⁷ Federal Commc'ns Comm'n, *As More Consumers Adopt Payment Apps, Scammers Follow* (updated Feb. 25, 2021), available at <https://www.fcc.gov/more-consumers-adopt-payment-apps-scammers-follow>.

Additionally, with imposter scams topping the FTC's category of fraud type in 2022,²⁸ the use of deep fakes generated by artificial intelligence (AI) to perpetuate payment fraud is disconcerting.²⁹ NCLC joined numerous nationwide and state advocacy organizations in sending a letter to the FTC and the CFPB on the threat of AI-generated deep fakes used for financial fraud.³⁰

C. Current ambiguity in the law leaves consumers insufficiently protected from P2P fraud.

The Electronic Fund Transfer Act (EFTA) and its implementing Regulation E protect consumers when problems with electronic funds transfers, such as P2P transactions, occur. The law provides consumers with remedies for P2P fraud when it is unauthorized, such as when a criminal defrauds a person into turning over account credentials and then the criminal commits an unauthorized transfer. The definition of "unauthorized transfer" under Regulation E is a 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."³¹

However, the response to consumer complaints about unauthorized payments by some of the largest players in the P2P market is inconsistent at best and possibly non-compliant.³² It is unfortunately too common for financial institutions to fail to comply with the unauthorized use protections of the EFTA and deny reimbursement on improper grounds.³³

The response to P2P payment fraud becomes even more problematic when it involves claims of

²⁸ See Federal Trade Commission, *New FTC Data Show Consumers Reported Losing Nearly \$8.8 Billion to Scams in 2022*, (press release) (Feb. 23, 2023), available at <https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022>.

²⁹ See U.S. Department of Homeland Security, *Increasing Threat from Deepfake Identities*, 2021, available at https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf; Schwartz, Christopher and Wright, Matthew, "Voice Deepfakes Are Calling, Here's How to Avoid Them," Gizmodo (March 24, 2023) available at <https://gizmodo.com/ai-deepfake-voice-how-to-avoid-spam-phone-calls-1850245346>.

³⁰ NCLC *et al.*, Letter to CFPB and FTC on Threat of AI-Generated Deep Fakes Used for Financial Fraud, available at <https://www.nclc.org/wp-content/uploads/2023/10/Deepfake-based-financial-fraud-letter-to-CFPB-and-FTC.pdf>.

³¹ 12 C.F.R. § 1005.2(m) (emphasis added).

³² Brown, Sherrod, Elizabeth Warren, and Jake Reed, "Brown, Reed, Warren Urge Venmo, Cash App to Reimburse Victims of Fraud and Scams | United States Committee on Banking, Housing, and Urban Affairs," (Dec. 14, 2023) available at <https://www.banking.senate.gov/newsroom/majority/brown-reed-warren-urge-venmo-cash-app-to-reimburse-victims-of-fraud-and-scams>. See also Hindenburg Research Report, "Block: How Inflated User Metrics and 'Frictionless' Fraud Facilitation Enabled Insiders to Cash Out Over \$1 Billion," (March 23, 2023), available at <https://hindenburgenresearch.com/block/>.

³³ See, e.g., CFPB, Supervisory Highlights at 17 (Summer 2022) ("Examiners continued to find issues with financial institutions failing to follow Regulation E error resolution procedures.... A financial institution cannot require a consumer to file a police or other documentation as a condition of initiating or completing an error investigation."); CFPB, Supervisory Highlights at 15 (Summer 2021), available at www.consumerfinance.gov (stating that "Supervision continues to find violations of EFTA and Regulation E that it previously discussed in the Fall 2014, Summer 2017, and Summer 2020 editions of Supervisory Highlights, respectively," (Listing several violations)); Sonbuchner, Scott, Examiner, Fed. Reserve Bank of Minneapolis, Consumer Compliance Outlook, Error Resolution and Liability Limitations Under Regulations E and Z; Regulatory Requirements, Common Violations, and Sound Practices (2d issue 2021), available at www.consumercomplianceoutlook.org.

fraudulently induced payments. P2P apps disclaim responsibility to protect consumers from fraudulently induced transactions, even though those payments go to accounts held at the same P2P app. Similarly, most banks will deny a claim of error for a fraudulently induced transaction, though Zelle has begun reimbursing consumers for some fraudulently induced transactions resulting from certain types of imposter scams.³⁴

The definition of “unauthorized transfer” under Regulation E as described above contemplates a transaction that was not initiated by the consumer. If the consumer initiated the transfer, even if the consumer was defrauded into initiating the payment, financial institutions are likely to dispute their liability and may even refuse to help.

Nevertheless, some fraudulently induced transactions may fall under Regulation E’s separate error protections, such as the protection against incorrect transactions – i.e., a payment that went to an imposter – or the right to obtain information.³⁵ The CFPB also has authority to define additional categories of error.³⁶

The disparity of treatment between unauthorized and fraudulently induced payments under Regulation E is made clear in the following two scenarios:

- *Scenario A: Laurie receives a call from a person claiming to be with the IRS. The caller threatens to arrest her if she does not make a payment. Laurie gives the caller her bank account number and routing number, and the caller uses that information to initiate a preauthorized ACH debit against her account.*
- *Scenario B: Laurie receives a call from a person claiming to be with the IRS. The caller threatens to arrest her if she does not make a payment. Laurie takes out her smartphone and sends a P2P payment to the number or email given by the caller.*

Though there is very little difference in these two scenarios, Regulation E protects Laurie in Scenario A where she can contest the debit as unauthorized. In Scenario B, financial institutions will take the position that Laurie is unprotected because she initiated the payment. The difference between how the payment was initiated in Scenario A and B does not make a scammer any more entitled to the money or make the scammer’s bank any less responsible for banking a scammer.

D. Responsibility of receiving institutions.

As discussed earlier, payments often involve two institutions: the one that sent the payment (the consumer’s institution in the P2P context) and the one that received it. While the EFTA governs only the responsibilities of the consumer’s institution, other laws and network rules give the receiving institution obligations to prevent fraud.

Scenario A described above is unlikely to occur because scammers like the fake IRS caller would be deterred from using the ACH system. The ACH system vets and monitors who is

³⁴ Campisi, Natalie, “*Scammed Out Of Money On Zelle? You Might Be Able To Get It Back*,” *Forbes* (Nov. 13, 2023), available at <https://www.forbes.com/advisor/money-transfer/zelle-users-refunded-after-scams/>.

³⁵ 15 U.S.C. § 1693f(f)(2), (6); 12 C.F.R. § 1005.11(a)(1)(ii), (vii).

³⁶ 15 U.S.C. § 1693f(f)(7).

allowed to initiate ACH payments, and the liability of a bank that initiates and receives fraudulent debit payments under both Regulation E and Nacha rules leads to stronger controls that are more likely to keep the scammer from having an account or having access to the ACH system.

But with the growth of payment apps, online bank account opening, and identity theft, it is easier for scammers to obtain accounts – potentially using stolen or synthetic identities – that they can then use to receive payments (directly or through money mules). Yet at present, the payment service or bank receiving the fraudulent payment on behalf of the scammer has no direct liability for enabling the scammer to receive the payment. As a result, that institution has less incentive to prevent the scammer from obtaining an account, put a hold on access to suspicious payments, or shut down the account quickly.

If consumers had more remedies against fraudulently induced transactions, payment network rules could pass liability in whole or in part back to the institution that holds the fraudster or money mule account, which would help to correct these incentives. This is what the United Kingdom has done, as discussed below.

Consumer complaints of P2P fraud will continue to escalate because the current systems impose insufficient responsibility on system operators and financial institutions to protect consumers against fraudulent schemes. Given what we know about how fraudsters target opportunities with the least resistance, it stands to reason that fraudulently induced payment fraud will continue to plague P2P systems if payment systems and financial institutions are allowed to operate under the assumption that they are not liable.

E. Problems with P2P apps when consumers make mistakes.

Beyond fraudulently induced payments and unauthorized payments, P2P payment apps and financial institutions typically refuse to help consumers who accidentally send money to the wrong person or the wrong account – mistakes that are easy to make in payment services designed for convenience and speed over safety. For example, consumers can send money through P2P systems using nothing more than a cell phone number to identify the recipient.

Here are other examples:

- An employee of NCLC unexpectedly saw \$1,000 arrive in his bank account through Zelle. A few minutes later, he received a frantic phone call from a man telling him that he had put in the wrong cell phone number and asking for the money back. The NCLC employee wanted to return the money but asked his bank for assurances that it was not a scam. The man also called his bank. Both banks (each large top-10 institutions) refused to help correct the error. After weeks of getting nowhere, the NCLC employee returned the funds on faith.
- Arthur Walzer of New York City tried to send his granddaughter \$100 through Venmo as a birthday present, but instead sent it to a woman with the same first and last name. When he discovered the error, he told his bank to refuse payment of the \$100, and in response

Venmo froze his account and demanded that he pay them. Venmo eventually refunded him, but only after a journalist contacted the company on his behalf. It was the first time he had ever used Venmo – he set up an account specifically to give his granddaughter the gift.³⁷

Regulation E imposes the duty to investigate and resolve “errors,” which includes “an incorrect electronic fund transfer to or from the consumer’s account.”³⁸ Nothing in the EFTA excludes consumer errors, and Regulation E should be interpreted to cover them. When a payment is sent to the wrong person or in the wrong amount, the person receiving the payment is not more entitled to the payment because the error was caused by the sender. But today, most consumers are out of luck in this situation unless their bank decides to help and the receiving bank or payee is cooperative.

F. Potential remedies to address P2P payment fraud.

1. Update the Electronic Funds Transfer Act.

The EFTA was enacted 43 years ago and as described above does not directly address many of the most important issues in the current consumer payment ecosystem. The statute was initially adopted at a time when consumers were conducting business with their own financial institutions and were using payment systems that did not lead to the same types of problems that plague today’s P2P systems.

We support legislative efforts to address the many gaps and ambiguities in the Electronic Fund Transfer Act that leave consumers unprotected. Some of these problems could also be addressed by rulemaking or guidance from the CFPB, though Congressional action would be faster and less subject to challenge.

The problem of fraudulently induced electronic transfers in P2P payments could be addressed by amending the EFTA to protect consumers from liability when they are defrauded into initiating a transfer and allow the consumer’s financial institution, after crediting the consumer for a fraudulent transfer, to be reimbursed by the financial institution that allowed the scammer to receive the fraudulent payment.

Problems when consumers make mistakes could also be addressed by clarifying that the EFTA’s error resolution procedures apply when the consumer makes a mistake, such as in amount or recipient.

2. Consider the United Kingdom as an example.

The United Kingdom (UK) was early to launch real time payments, and fraudulently induced payment fraud (what the UK calls authorized push payment or APP fraud) immediately

³⁷ See Elliott, Christopher, “*A Venmo user sent \$100 to the wrong person. Then the payment service froze his account.*” *Seattle Times* (Nov. 2, 2020), available at <https://www.seattletimes.com/life/travel/a-venmo-user-sent-100-to-the-wrong-person-then-the-payment-service-froze-his-account-travel-troubleshooter/>.

³⁸ 15 U.S.C. § 1683f(f)(2); 12 C.F.R. § 1005.11(a)(1)(ii).

followed. The UK has been formally considering how to tackle the problem of P2P fraud since 2016, when the consumers association “Which?” submitted a “super-complaint”³⁹ to the United Kingdom’s Payments Systems Regulator (PSR).⁴⁰ The complaint identified the problem of APP fraud, which happens when scammers deceive consumers or individuals at a business to send them payment under false pretenses to an account controlled by the scammer. Which? also identified the lack of consumer protection for victims of APP fraud.

In response, a steering group was formed, comprised of regulators, consumer advocates, financial services providers and industry representatives.⁴¹ The result was the creation of an industry code called the Contingent Reimbursement Model (CRM) Code, launched in 2019. The CRM Code required signatories to reimburse consumers who were the victims of APP fraud under certain circumstances.⁴² The CRM Code was voluntary and existed to help financial institutions in the UK, “detect, prevent and respond to APP scams.”⁴³

The voluntary decision of the leading UK payment industry players to develop a system to reimburse fraud victims shows the consensus that protecting consumers benefits industry players and the payment systems as a whole, not merely consumers. But the uneven implementation of the system – and the growing calls to make it mandatory – also show the limits of voluntary measures.

As reported in September 2021, very few victims of APP fraud were reimbursed under the CRM Code: “banks found victims at least partly responsible in 77% of cases assessed in the first 14 months following the introduction of a Contingent Reimbursement Model and voluntary code.”⁴⁴ Two banks found the customer fully liable in 90% of their decisions.⁴⁵

Under the CRM code, consumers who were unhappy with their bank’s refusal to compensate them could appeal to the Financial Ombudsman Service, which reviewed denials of reimbursement requests for APP fraud. Data obtained by Which? found that in 73% of the complaints the ombudsman received about APP fraud from 2020-2021, the ombudsman concluded that banks were getting the decisions wrong, reversed the banks’ denials, and found in

³⁹ A super-complaint may be made by a designated consumer body where the body considers features of a market in the United Kingdom for payment systems that are or which may be significantly damaging to the interests of consumers. <https://www.gov.uk/government/publications/super-complainants-for-the-payment-systems-regulator>.

⁴⁰ As part of the Financial Services (Banking Reform) Act of 2013, the Payment Systems Regulator (PSR) was established to promote competition, innovation, and responsiveness of payment systems and to receive and respond to super-complaints. <https://www.gov.uk/government/publications/super-complainants-for-the-payment-systems-regulator>.

⁴¹ Speech by the Lending Standards Board Chief Executive, Emma Lovell, “*International Perspective-Scams: Looking Forward: Priorities and opportunities*,” (Mar. 15, 2022) available at <https://www.lendingstandardsboard.org.uk/scams-looking-forward-priorities-and-opportunities-international-perspective-speech/>.

⁴² *Id.*

⁴³ *Id.*

⁴⁴ “Banks called to account over ‘shockingly low’ rate of reimbursements for APP fraud,” Finextra (Sept. 15, 2021) available at <https://www.finextra.com/newsarticle/38832/banks-called-to-account-over-shockingly-low-rate-of-reimbursements-for-app-fraud>.

⁴⁵ *Id.*

favor of the consumer.⁴⁶ This level of reversals suggests that the banks' high rate of denials was inconsistent with both the letter and the spirit of the Code.⁴⁷

The Contingent Reimbursement Model as an industry response, though laudable and necessary, proved insufficient to address the growing number of scams and fraud. In the first half of 2021, APP fraud cases in the UK outnumbered credit card fraud for the first time.⁴⁸

Consequently, the UK Parliament's Treasury Committee recommended "mandatory refunds" to victims of APP fraud and discussion about whether to make "big technology companies liable to pay compensation when people are tricked by con-artists using their platforms."⁴⁹ As a result, the Payment Systems Regulator (PSR) undertook rulemaking, subject to a period of open comment ("consultation").

In June 2023, the PSR finalized a rule that requires mandatory reimbursement to victims of APP fraud.⁵⁰ Under the finalized rule, the victim's financial institution and the recipient's financial institution split the cost of reimbursement 50:50.⁵¹

3. When liability is split between sending and receiving institutions and not pushed onto consumers, more will be done to protect consumers.

P2P apps must take more responsibility to protect consumers from the fraud committed on their platforms and from the scammers they allow to open accounts where they can receive stolen funds.⁵² While consumer education is important and necessary, payment system providers' primary response to fraud and errors in P2P systems should not be to use old-fashioned disclosures and warnings to consumers to "be careful" and not to send payments to people they do not know—all while promoting their systems for broad use. Scammers prey on consumers' trust, and warnings are far less effective than sophisticated systems that payment providers can design.

The providers of P2P payment apps and payment systems as well as the financial institutions

⁴⁶ Which?, "Banks wrongly denying fraud victims compensation in up to 8 in 10 cases," (Nov. 11, 2021), available at <https://www.which.co.uk/news/2021/11/banks-wrongly-denying-fraud-victims-compensation-in-up-to-8-in-10-cases/>.

⁴⁷ Contingent Reimbursement Model Code for Authorised Push Payment Scams OPI at 2, (Apr. 20 2021), <https://www.lendingstandardsboard.org.uk/wp-content/uploads/2022/03/CRM-Code-LSB-April-2021.pdf>

⁴⁸ "UK Government to Legislate for Mandatory Reimbursement of App Fraud," (Nov. 18, 2021), available at <https://www.finextra.com/newsarticle/39245/uk-government-to-legislate-for-mandatory-reimbursement-of-app-fraud>

⁴⁹ "Fraud: MPs seek overhaul to tackle financial scammers," (Feb. 2, 2022), available at <https://www.bbc.com/news/business-60216076>

⁵⁰ Press Release: "PSR confirms new requirements for APP fraud reimbursement," available at <https://www.psr.org.uk/news-and-updates/latest-news/news/psr-confirms-new-requirements-for-app-fraud-reimbursement/>.

⁵¹ To view a summary of the new rule and the feedback received during the open consultation, go to <https://www.psr.org.uk/media/101pbw0u/ps23-3-app-fraud-reimbursement-policy-statement-final-june-2023.pdf>

⁵² See Sanchez-Adams, Carla, "It is essential that we protect consumers from fraud over P2P networks," American Banker, Bank Think (Mar. 15, 2023), available at <https://www.americanbanker.com/opinion/it-is-essential-that-we-protect-consumers-from-fraud-over-p2p-networks>.

who utilize these applications make decisions about what safety features to install, when to protect consumers, and how to monitor and react to red flags of potentially fraudulent payments sent and received by their customers. Companies that are incentivized to prevent fraud and errors will use constantly improving technology and innovations to spot potential scams and errors and to aggregate reports of fraud. Because the UK's new rule will require financial institutions to compensate consumers affected by fraudulently induced transfers (APP scams), for example, nine of the UK's biggest banks have signed up to use a new AI-powered tool that helps banks more effectively spot if their customers are sending money to fraudsters.⁵³

Furthermore, financial institutions already have "Know Your Customer" (KYC) and account monitoring obligations under the Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) laws, which should be reflected through their Customer Identification Program (CIP) and Customer Due Diligence (CDD) policies. Even P2P payment apps and fintech companies have certain obligations under the BSA. To comply with these laws, the institutions make decisions about who they allow to open an account and how to monitor and react to red flags of potentially fraudulent payments sent and received by their customers. When they fail in those responsibilities and allow a customer to use an account to receive stolen funds, it is appropriate for that institution to bear the costs if the funds cannot be recouped.

If fraud and error rates are low in the aggregate, the system can bear those costs and spread them. If rates are high, then the systems clearly have fundamental problems that must be addressed. But even a single instance of fraud or mistake can be devastating to a consumer. The equities strongly favor protecting consumers with the same type of strong protection they have in the credit card market.

4. Address the lack of oversight for certain parties involved in the payments market.

Newer fintech companies, including technology providers and payment apps, do not receive the same type of supervision as other financial institutions in the United States. But the CFPB has proposed a rule that will enable it to supervise large market participants who provide general-use digital consumer payment applications.⁵⁴ Greater supervision is important because compliance with basic EFTA obligations has been problematic even in supervised financial institutions, as noted above. The CFPB should swiftly finalize that rule and expand it to encompass the larger participants on the debit and prepaid card markets and domestic money transfer markets as well.

⁵³ Solon, Olivia "Nine British Banks Sign Up to New AI Tool for Tackling Scams," Bloomberg (Jul. 25, 2023) available at <https://www.bloomberg.com/news/articles/2023-07-05/mastercard-s-ai-tool-helps-nine-british-banks-tackle-scams>.

⁵⁴ The CFPB issued a proposed rule to define larger participants of a market for general-use digital consumer payment applications which closed on January 8, 2024. The proposed rule may lead to greater supervision of some nonbank payment services, though not all. See NCLC *et al.*, Comments to the CFPB's Proposed Rule Defining Larger Participants of a Market for General-Use Digital Consumer Payment Applications, (Jan. 8, 2024) available at <https://www.nclc.org/wp-content/uploads/2024/01/240108-CFPB-Payments-App-Comment-Final.pdf>.

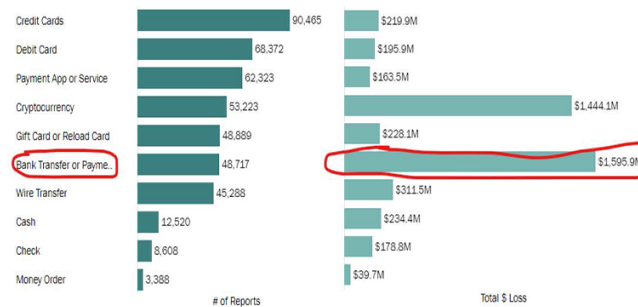
IV. Bank-to-Bank Wire Transfer Fraud.

A. Consumers are devastated by bank-to-bank wire transfer fraud.

The FTC's latest fraud data show that, in terms of dollars lost, "Bank Transfer or Payment" is the largest payment method used by fraudsters.⁵⁵ It also seems safe to assume that the lion's share of those losses by dollar volume are through bank-to-bank wire transfers, which can process very large transfers, rather than through Zelle. (The FTC's "Wire Transfer" category includes only nonbank transfers like Western Union and MoneyGram.)

Cryptocurrency is a close second to bank transfer in total dollar amount of fraud losses reported to the FTC, and some losses through cryptocurrencies may start as bank-to-bank wire transfers to crypto banks or exchanges.⁵⁶ For example, Marjorie Bloom of Chevy Chase, Maryland, a 77-year-old retired civil servant, lost her life savings, \$661,000, through a bank-to-bank wire transfer into cryptocurrency.⁵⁷

2022 Fraud Reports to FTC by Payment Method



Compared to 2019, it is especially dramatic to note how the bank transfer category has overtaken nonbank wire transfers, and how astronomically it has grown – nearly ninefold in five years.⁵⁸

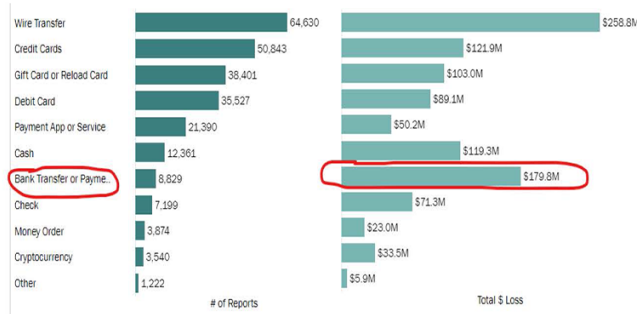
2019 Fraud Reports to FTC by Payment Method

⁵⁵ FTC fraud reports by payment method available at <https://public.tableau.com/app/profile/federal-trade-commission/viz/FraudReports/PaymentContactMethods>.

⁵⁶ See Paluska, Michael, "Cryptocurrency scam drains retired St. Pete victim's life savings How to spot online scams," ABC Action News (Florida) (June 19, 2023), available at <https://www.abcactionnews.com/news/region-pinellas/cryptocurrency-scam-drains-retired-st-pete-victims-life-savings>.

⁵⁷ Iacurci, Greg, "How this 77-year old widow lost \$661,000 in a common tech scam: 'I realized I had been defrauded of everything,'" CNBC (Oct. 8, 2023) available at <https://www.cnbc.com/2023/10/08/how-one-retired-woman-lost-her-life-savings-in-a-common-elder-fraud-scheme.html>.

⁵⁸ The dollar losses in these two charts significantly understate actual losses, as only 12% (2019) to 17% (2022) of reports included information on payment method, and many fraud losses are not reported to the FTC.



For the first three quarters of 2023, the dollar amount of fraud losses due to bank transfer or payment reported to the FTC are on pace to exceed 2022 dollar losses by 14%.⁵⁹

Over the last several years, NCLC has received numerous inquiries on behalf of consumers and heard devastating reports about how criminals have used bank-to-bank wire transfers to take

hundreds of thousands of dollars from people. In one case, an older woman lost her home as a result. Here are other examples:

- A college student lost his entire savings account after someone with two fake identification cards went into a bank and wired \$16,500 to another individual. Busy with college, he did not notice missing money for a month and a half, but the bank refused to return the money.⁶⁰
- After a consumer was the victim of a SIM swap, a wire transfer was used to transfer \$35,000 from his bank account to an account in another state.⁶¹ He is a cancer patient and navigating the bank appeal process has been extremely stressful. These SIM swaps are increasingly common.⁶²
- A low-income consumer in New York lost over \$26,000 – all her savings, which she had carefully saved over many years – after someone transferred money from her savings account to her checking account and then made an outgoing wire transfer to another state.⁶³
- A man lost \$15,000 that was wired to another account by someone who gained access to his account. The bank spotted suspicious activity as the fraud was taking place and

⁵⁹ FTC fraud reports by payment method available at

<https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods>.

⁶⁰ Inquiry received by KPRC (Houston NBC station) reporter Amy Davis.

⁶¹ Email from attorney on file with NCLC.

⁶² See Barr, Luke, ABC News, “‘SIM swap’ scams netted \$68 million in 2021: FBI” (Feb. 15, 2022), available at <https://abcnews.go.com/Politics/sim-swap-scams-netted-68-million-2021-fbi/story?id=82900169>.

⁶³ Email from CAMBDA Legal Services to NCLC, on file with NCLC.

called the man, who alerted them to the fraud, but the bank still refused to return the money claiming that the EFTA did not apply to these fraudulent electronic transactions.

- A fraudster hacked a retiree's online banking account and made a cash advance from the retiree's credit card to his linked bank account. The fraudster then immediately wired that amount from the retiree's bank account to his own. The bank denied any relief.⁶⁴
- A small business had its online banking account hacked and its \$60,000.00 checking account balance emptied over the course of two days and six transactions. The bank denied relief because its banking agreement generally states that customers are responsible for unauthorized transactions.⁶⁵

Wire fraud has become so problematic that even large news outlets like Good Morning America have run stories about the perils and lack of protection available to impacted consumers.⁶⁶

All the examples provided above were for unauthorized wire transfers. However, we have also heard stories where the consumer was fraudulently induced into sending a wire transfer. For example:

- Three Ohio residents were all defrauded into making a bank-to-bank wire transfer by a Chase impersonation scam.
 - Jeff Phipps from Columbus, Ohio lost \$8,500 after the fraudster, impersonating a bank employee, called and convinced the man that his account had been hacked into and he needed to provide login information to protect it. "They asked him if he had authorized a wire transfer and he replied, 'no'. They kept him on the phone for an hour and 47 minutes. They said, 'Well, we want to deactivate your account. Can you send us your username and your passcode?' And he did thinking it was Chase." The fraudster took \$8,500 with this information and Chase refused to refund the victim's money since he had given information to the scammer, "authorizing" it.⁶⁷
 - Kelli Hinton, 7 months pregnant at the time, received a text about a fraudulent wire transfer from her account, then a follow-up call from a fraudster posing as a Chase fraud agent, spoofing Chase's real phone number. The fraudster kept her on the line for an hour and convinced her to change her username and

⁶⁴ Pending arbitration before AAA (Wells Fargo).

⁶⁵ Lawrence and Louis Company d/b/a Hidden Oasis Salon v. Truist Bank, No. 1:22-cv-200-RDA-JFA (E.D. Va.).

⁶⁶ ABC News, Good Morning America "Woman sounds alarm on sophisticated wire transfer fraud," (Jul. 21, 2023), available at <https://abcnews.go.com/GMA/Living/video/woman-sounds-alarm-sophisticated-wire-transfer-fraud-101547100>.

⁶⁷ Gordon, Clay, "Central Ohio man loses \$8,500 in Chase bank impersonation scam," 10 WBNS (Mar. 30, 2023), available at <https://www.10tv.com/article/money/consumer/wire-fraud-scam-warning/530-7af76f5c-cce0-4dce-98a3-5c740a9043bd>.

- password, allowing him to drain \$15,000 from her account.⁶⁸
- Just months after experiencing a near fatal collision that left him in a wheelchair, Todd Evans from West Chester Township was called by a fake Chase fraud protection agent. The fraudster told him about a fraudulent purchase from his account, which Todd confirmed was appearing on his account and which neither he nor his wife had made. The fraudster then mentioned a \$45,000 fraudulent wire transfer from the account. Todd and his wife were nervous about addressing the fraud and asked the caller to verify his identity. He asked the couple to look at the number he was calling from and verify it matched the number on their debit card. Based on this confirmation, the couple allowed the fraudster to guide them through a "wire reversal process". Hours later they were out \$63,000.⁶⁹
 - A couple in South Carolina received an email from their attorney at the time of closing their home purchase with instructions on where to send the down payment via bank-to-bank wire transfer. Their attorney had been the victim of a phishing scam, and the fraudster used a legitimate email copying an actual employee of the attorney. The couple lost \$108,000.⁷⁰

Even in instances where consumers realize they have fallen prey to a fraud scheme, banks are sometimes unwilling or unable to assist consumers or stop a wire transfer. For example, Ann Booras from San Ramon, California received a call from a fraudster impersonating a Wells Fargo employee asking if she had wired \$20,000 from her savings account. In response to the directions provided by the fake employee, Ann wired the \$20,000 sum to the "bank's fraud department" where it would be safe. The fraudster then continued asking about other supposedly fraudulent transactions, and panicking, Ann "drove to the nearest Wells Fargo branch, with the man still on the phone, and told a teller someone was attacking her accounts. Silently, the teller warned her - the thief was actually the man on the phone. 'I had tears running down my face, I was literally shaking because I realized I had just sent \$25,000 to who knows where,'" Ann "pleaded with bank employees to stop those wire transfers -- fast. But to her shock, no one would help." She was told, "I'm sorry we're all busy. We're backed up with appointments back to back. You need to go to another branch, but we can't help you here."⁷¹

B. Technology enables more bank-to-bank wire transfer fraud.

⁶⁸ McCormick, Erin "Gone in seconds: rising text scams are draining US bank accounts," The Guardian (Apr. 22, 2023), available at <https://www.theguardian.com/money/2023/apr/22/robo-texts-scams-bank-accounts>.

⁶⁹ Johnson, Karin "West Chester couple swindled out of thousands of dollars by crooks spoofing bank's phone number," WLWT5 news (Nov. 16, 2023), available at <https://www.wlwt.com/article/west-chester-chase-bank-spoofing-phone-number/45866051>.

⁷⁰ Lee, Diane, "Upstate couple warns of wire fraud that cost them \$108,000," CBS7 News, (May 19, 2023), available at <https://www.wspa.com/news/upstate-couple-warns-of-wire-fraud-that-cost-them-108000/>.

⁷¹ Finney, Michael and Koury, Renee, "Wells Fargo bankers tell East Bay customer they're too busy to stop wire scam," ABC7 (Jun. 21, 2023), available at <https://abc7news.com/bank-impostor-scam-wells-fargo-wire-transfer-fraud-scammer-pretends-to-be/13407340/#:~:text=Wells%20Fargo%20bankers%20tell%20East,busy%20to%20stop%20wire%20scam&text=T he%20victim%20was%20still%20on.SAN%20RAMON%2C%20Calif>.

As the previous stories all illustrate, fraudsters have taken advantage of the technology needed to send texts and make calls to consumers whose information has been obtained through phishing schemes or purchased from the dark web. Technology also enables fraudsters and hackers the ease to take over accounts and initiate transactions through online or mobile banking.

Previously, wire transfers had to be conducted through a cumbersome process of walking into a bank for a time-consuming, in-person transaction. In-person identification would prevent unauthorized transfers, and there were some speed bumps for fraudulently induced transactions as well—the consumer would have time to think about the situation, call a family member, and talk to the bank teller, who could potentially talk them out of it.

But increasingly, bank-to-bank wire transfers are a service offered and permitted through mobile and online banking. As a result, fraudsters have an easy method of using unauthorized or fraudulently induced transfers to steal and send large sums of money, often not possible through P2P apps that set daily transaction limits. The lack of friction that was found in in-person transactions has undoubtedly contributed to the explosion of bank-to-bank wire transfer losses.

C. Bank-to-bank wire transfers are exempt from the EFTA, leaving consumers exposed to losing thousands of dollars.

The EFTA exempts electronic transfers, other than ACH transfers, made “by means of a service that transfers funds held at either Federal Reserve banks or other depository institutions and which is not designed primarily to transfer funds on behalf of a consumer.”⁷² Regulation E and the official interpretations of Regulation E interpret that exemption to cover wire transfers using FedWire, SWIFT, CHIPS, and Telex.⁷³ Thus, even if a criminal impersonates the consumer and makes a completely unauthorized wire transfer, the consumer may have no protection under Regulation E.⁷⁴

At the time the EFTA was written in 1978, bank-to-bank wire transfer services were not viewed as a consumer payment system. That has clearly changed—bank-to-bank wire transfer services are now incorporated into consumer mobile and online banking services and electronic fund transfers are generally far more common among consumers today than in 1978. For large payments, bank-to-bank wire transfers are the primary way consumers can conduct electronic transfers.

Instead of the clear consumer protections provided by the EFTA, which was designed to protect consumers with clear rights and procedures, bank-to-bank wire transfers are covered under state law, more specifically a state’s adopted version of Uniform Commercial Code Article 4A (UCC Article 4A). The UCC was not designed as a consumer protection statute and was instead

⁷² 15 U.S.C. §1693a(7)(B).

⁷³ 12 C.F.R. §1005.3(c)(3) (exempting FedWire or similar systems); Official Interpretation of 3(c)(3)-3 (“Fund transfer systems that are similar to Fedwire include the Clearing House Interbank Payments System (CHIPS), Society for Worldwide Interbank Financial Telecommunication (SWIFT), Telex, and transfers made on the books of correspondent banks.”).

⁷⁴ However, as discussed in FN 77 below, some bank wire transfers may be within the EFTA’s protection.

designed to govern commercial-to-commercial transactions. UCC Article 4A offers very weak or no protection for consumers who have suffered harm due to bank-to-bank wire transfer fraud. In essence, the consumer is deemed to have authorized a wire transfer if the bank utilized a commercially reasonable security procedure that the bank and the consumer agreed to beforehand and if the bank acted in good faith. Yet consumers have no understanding of or control over those security procedures and no choice but to click “I agree” to the fine print of an agreement.

For example, the New York Attorney General recently filed a lawsuit against Citibank alleging it failed to protect and reimburse victims of electronic fraud when it used “poor security and anti-fraud protocols,” that consumers had not negotiated with Citibank.⁷⁵ According to the lawsuit, Citibank connected wire transfer services to consumers’ online and mobile banking apps in recent years—allowing direct electronic access to the wire transfer networks—but employed lax security protocols and procedures; had ineffective monitoring systems; failed to respond in real-time; and failed to properly investigate fraud claims.⁷⁶ As a result, New Yorkers lost millions of dollars in life savings, their children’s college funds, and even money needed to support their day-to-day lives.

I have also heard numerous other reports of banks failing to reimburse unauthorized wire transfers even if the consumer did not agree to any commercially reasonable security procedure. Consumers do not have the resources to fight the bank in court or arbitration to enforce their right to a reimbursement when this occurs.

UCC Article 4A does not provide a consumer with any other remedies besides reimbursement (and possible interest) of the unauthorized wire amount, and the consumer’s attorney is not entitled to recover attorneys’ fees from the bank. As a practical matter, it means that a consumer would have to pay out of pocket to fight in court or in arbitration just to get their money back, while a financial institution with deep pockets can afford to fight a claim. As a result, in most cases financial institutions will reject a consumer’s unauthorized wire transfer claim because the consumer cannot afford to fight the decision.

With respect to fraudulently induced wire transfers, the UCC provides no remedy.

D. Potential remedies to address bank-to-bank wire fraud.

As previously stated, we support legislative efforts to address gaps in the Electronic Fund Transfer Act that leave consumers unprotected.

The EFTA can be amended to address specific problems of unauthorized consumer bank-to-bank

⁷⁵ New York State Attorney General, Press Release, Attorney General James Sues Citibank for Failing to Protect and Reimburse Victims of Electronic Fraud (Jan. 30, 2024), available at <https://ag.ny.gov/press-release/2024/attorney-general-james-sues-citibank-failing-protect-and-reimburse-victims>.

⁷⁶ See Complaint, People of the State of New York v. Citibank, No. 1:24-cv-00659 (S.D.N.Y. filed Jan. 30, 2024), available at <https://ag.ny.gov/sites/default/files/2024-01/citi-complaint.pdf>. The New York AG also alleges that the unauthorized wire transfers that occurred by electronic requests initiated by scammers via online banking or mobile app are covered by the EFTA. They are electronic instructions that do not come from the actual consumers who are Citi account holders and under the EFTA are unauthorized.

wire transfers as well as fraudulently induced consumer bank-to-bank wire transfers by:

- Eliminating the exemption for bank wire transfers and electronic transfers authorized by telephone call, bringing those transfers within the EFTA and its protections against unauthorized transfers and errors;
- Protecting consumers from liability when they are defrauded into initiating a transfer, and
- Allowing the consumer's financial institution, after crediting the consumer for a fraudulent transfer, to be reimbursed by the financial institution that allowed the scammer to receive the fraudulent payment.

The consumer bank-to-bank wire transfer loophole and inclusion of fraudulently induced transfers could also be addressed by rulemaking or guidance from the CFPB, though Congressional action would be faster and less subject to challenge.

V. Check Fraud.

A. Check alteration fraud is on the rise.

Although checks are an old payment system, new technology is leading to a rise in fraud using checks. In particular, new technology makes it easier for criminals who steal checks to engage in “check washing” – changing the payee and payment amount on a check – and harder for banks or consumers to spot those alterations.⁷⁷ Criminals can also create fake checks from stolen account information. These altered or fabricated checks can then be deposited remotely through mobile devices, made easier through the increased ability to open fraudulent accounts into which those checks can be deposited, as described in Section III.D above.

Although checks are near the bottom of payment types in terms of number of fraud reports, the total dollar loss by check fraud reported to the FTC is actually higher than for payment apps and services: \$177.4 million in 2022 for checks compared to \$163.5 million for payment apps and services. But this reported dollar loss is vastly understated;⁷⁸ one report a year ago puts annual check fraud losses at \$815 million.⁷⁹

Check fraud loss reported to the FTC increased by over 15% from 2021 to 2022.⁸⁰ Based on the first three quarters of 2023, check fraud losses are on pace to exceed 2022 numbers by 40%.⁸¹

In February 2023, FinCEN issued an alert about a nationwide surge in mail theft-related check fraud schemes and urged financial institutions to “be vigilant in identifying and reporting such

⁷⁷ DePompa, Rachel, “Check washing’ scams still on the rise,” Fox10 News (Jan. 25, 2024), available at <https://www.fox10tv.com/2024/01/25/check-washing-scams-still-rise/>.

⁷⁸ Of the 2.5 million reports of fraud received by the FTC in 2022, only 17% specified the payment method for the fraud. FTC fraud reports by payment method available at

<https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods>.

⁷⁹ Nadelle, David, “Check Washing Is an \$815M Per Year Scam — How It Works and Ways To Prevent It,” GoBanking Rates, (Feb. 22, 2023), [https://www.nasdaq.com/articles/check-washing-is-an-\\$815m-per-year-scam-how-it-works-and-ways-to-prevent-it](https://www.nasdaq.com/articles/check-washing-is-an-$815m-per-year-scam-how-it-works-and-ways-to-prevent-it).

⁸⁰ *Id.*

⁸¹ *Id.*

activity.”⁸² The report indicated that there were over 680,000 cases of possible check fraud reported to FinCEN in 2022 through the use of SARs (Suspicious Activity Reports), an increase from a little over 350,000 check fraud-related SARs sent to FinCEN in 2021, which itself was a 23% increase from 2020.⁸³ The statistics for check-fraud related SARs were not specific to mail-theft related check fraud.⁸⁴

Technology also enables criminal organizations to traffic stolen checks. As a recent New York Times article⁸⁵ conveyed:

“The cons may start with stealing pieces of paper, but they leverage technology and social media to commit fraud on a grander scale, banking insiders and fraud experts said. In the past, criminals needed a special internet browser that would grant entry into the dark web marketplace of stolen checks, maybe even someone to vouch for them. Now all they need is an account from Telegram, a messaging app.

“You can buy checks on the internet for \$45, with a perfectly good signature,” said John Ravita, director of business development at SQN Banking Systems, which provides check fraud detection software. “There is one website that offers a money-back guarantee. It’s like Nordstrom.”

NCLC spoke with Larry Smith, an attorney in Chicago, whose clients did not even have checks issued to their associated bank account, yet a fraudster somehow obtained their bank account and routing number and created fake checks.⁸⁶ The fraudster deposited these checks in various bank accounts from December 2021 and January 2022, stealing around \$14,000 from the consumers. Though the consumers disputed the fraudulent checks with their bank and have filed a lawsuit, their bank has not recREDITED their account for the stolen amount.

B. Though some protections exist for consumers harmed by check fraud, they are often left scrambling.

Checks are largely governed by state law through the Uniform Commercial Code (UCC). If a consumer timely reports the problem, the UCC protects them if their checks are altered or if a fraudulent check is presented against their account.⁸⁷

Yet as the previous example demonstrates, consumers are often left scrambling, waiting for their banks to recREDIT their account even when state law provides remedies for the consumer when a

⁸² FIN-2023-Alert003 available at <https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20Check%20Fraud%20FINAL%20508.pdf>

⁸³ *Id.* citing FinCEN SAR Stats available at <https://www.fincen.gov/reports/sar-stats>

⁸⁴ *Id.* See FN 10.

⁸⁵ Barnard, Tara Seigel, “We Can’t Stop Writing Paper Checks. Thieves Love That,” (Dec. 9, 2023) available at https://www.nytimes.com/2023/12/09/business/check-fraud.html?unlocked_article_code=1.QU0.08_m.7j3dyrD0mzvX&smid=url-share

⁸⁶ Arroyo and Ramos v. Fifth Third Bank, N.A., Cause No. 2023L004163, Cook County, IL.

⁸⁷ See U.C.C. §§ 3-407(b), (c) cmt. 2, 4-401(d)(1) for a consumer’s rights when a check is altered; see U.C.C. §§ 4-401; 4-406(f) for a consumer’s rights when a check is forged.

check is altered or forged. One consumer in Los Angeles was unable to get his account recredited for over two years. The consumer had written a check to the IRS and sent it by mail. The check was stolen from the mail and deposited into an account that was not the U.S. Treasury.⁸⁸ The consumer's bank kept insisting it would not recredit his account until the fraudster's bank sent them reimbursement.

While a bank's obligation to reimburse a consumer for an altered check is not dependent on the bank's ability to be repaid by the depository bank, the failure to timely resolve check fraud between institutions has also been the subject of complaint by community banks against their large-bank counterparts.⁸⁹ Consumers turn to their own bank for reimbursement when a check is altered or forged, and that bank in turn will request reimbursement from the bank into which the check was fraudulently deposited. As previously described in more detail in Section III. F. 3., the depository bank has "know-your-customer" responsibilities that are important to prevent fraud, but there is insufficient incentive to be diligent if there is no liability. As Steven Gonzalo, president and CEO of American Commercial Bank & Trust, stated: "From a deposit perspective, some banks do not perform the same level of due diligence because the bank assumes the risk of loss to them is zero or minimal, and fails to consider losses due to fraud incurred by the counterparty banks. And therein lies the failure."⁹⁰

Furthermore, even though the UCC provides consumers up to a year to inform their bank of a fraudulent or altered check, it allows banks to shorten that notification time in the fine print of account agreements. Many bank account agreements shorten that time for notification to anywhere between 14 and 30 days.

Yet check alterations can be hard to spot. If the payee has been changed but not the amount, the consumer might have no reason to think that anything is amiss. For example, one consumer reported to NCLC that he had no idea his check had been altered until his landlord – a family friend – eventually told him months later that he had not received the rent.

Most banks no longer return physical checks to consumers and have also engaged in an aggressive push to eliminate paper statements. Bank websites and mobile apps focus on listing transactions but make it more cumbersome to review actual statements. The grainy photocopies of checks included with statements can be hard to read, consumers may not expect to have any reason to look at them, and those images are not even available to review on some mobile banking apps.

But if the consumer does not inform their bank about the check fraud before the end of the 14- to 30-day time period, they may be left with absolutely no recourse at all.

C. Potential remedies to address check fraud.

⁸⁸ See Lazar, Kristine, "On Your Side: Check fraud is on the rise - here's how to protect your money," CBS News Story, KCAL News (Apr. 17, 2023), available at <https://www.cbsnews.com/losangeles/news/on-your-side-check-fraud-is-on-the-rise-heres-how-to-protect-your-money/>.

⁸⁹ Berry, Kate, "Small banks urge crackdown on big banks with lax check-fraud controls," American Banker (Feb. 9, 2023), available at <https://www.americanbanker.com/news/small-banks-urge-crackdown-on-big-banks-with-lax-check-fraud-controls>

⁹⁰ *Id.*

To protect consumers from check fraud:

- Federal bank regulators should examine institutions to ensure that they are complying with their responsibility to reimburse consumers for altered or forged checks.
- Federal bank regulators should step up enforcement of BSA/AML obligations and scrutinize the institutions into which fraudulent checks are deposited.
- States should amend their UCC laws to remove the ability of banks to shorten the time period provided by the UCC to report altered or forged checks.
- Improvements in the protections for P2P payments would also give consumers more confidence in using those systems instead of checks.

We should also give consideration to moving consumer protections for checks within the EFTA, which provides a clearer framework than the UCC for consumer protection including error resolution timelines and procedures and consumer rights.

The Federal Reserve Banks should also explore collecting information on check fraud, which may help to identify institutions that need to do a better job with their BSA/AML obligations.

VI. Electronic Benefit Transfer (EBT) Card Fraud.

A. EBT card skimming and theft leave cardholders without any protections.

Supplemental Nutrition Assistance Program (SNAP) benefits are distributed and administered through the Electronic Benefit Transfer (EBT) system to eligible participants. EBT has been the sole method of SNAP issuance in all states since June of 2004,⁹¹ and some states also use EBT cards to issue Temporary Assistance for Needy Families (TANF) or other state administered financial assistance.⁹² EBT accounts perform the same function for low-income households as do checking accounts—the accounts power daily, or near daily, transactions. People who receive these benefits typically spend down the account balance to \$0 each month.

In 2020, about 39.9 million people across the country received SNAP benefits;⁹³ 38% of whom were white, 25.5% Black, and 15% Hispanic.⁹⁴ As of 2022, nearly 2 million Americans receive Temporary Assistance for Needy Families (“TANF”) benefits to support their families.⁹⁵ In FY

⁹¹ <https://www.fns.usda.gov/snap/ebt>

⁹² <https://fns-prod.azureedge.us/sites/default/files/resource-files/ebt-contract-procurement-summary-20221215.pdf>

⁹³ U.S. Department of Agriculture, Food and Nutrition Service “*Characteristics of SNAP Households: FY 2020 and Early Months of the Covid-19 Pandemic: Characteristics of SNAP Households*,” available at <https://www.fns.usda.gov/snap/characteristics-snap-households-fy-2020-and-early-months-covid-19-pandemic-characteristics>

⁹⁴ Cronquist, Kathryn and Eiffes, Brett, “*Characteristics of Supplemental Nutrition Assistance Program Households: Fiscal Year 2020, Table B.4.b. Distribution of participating households by shelter-related characteristics and by State, waiver period*” (Washington: U.S. Department of Agriculture, 2022), available at <https://fns-prod.azureedge.us/sites/default/files/resource-files/Characteristics2020.pdf>; 7 C.F.R. § 273.10(c)(2)(i).

⁹⁵ Office of Family Administration, Administration for Children and Families, “TANF Caseload Data 2022,” August 2022, <https://www.acf.hhs.gov/ofa/data/tanf-caseload-data-2022>.

2021, 35% of TANF recipients were Hispanic, 29% were Black, and 27% were white.⁹⁶ These public benefit programs are focused entirely on low-income families.

During the past two years, EBT cardholders have been targeted by criminals who “skim” account information and PINs and then deplete the accounts of all funds belonging to the recipients. This problem is so endemic that even the USDA issued a policy memo on EBT card skimming prevention with tools and resources to prevent and identify the fraud,⁹⁷ and Congress recently provided for reimbursement of these stolen funds for the period of October 1, 2022, to September 30, 2024.⁹⁸

However, while other consumers have also been victimized by skimming, EBT consumers are particularly vulnerable and left with little to no recourse. Unlike other cardholders whose funds may be stolen in the same way, EBT cardholders – the lowest-income and most vulnerable consumers – do not have protections afforded to other consumers by the Electronic Funds Transfer Act or Regulation E. Even if the consumer did not lose their card, was not responsible for providing card information to the criminal, and immediately reported missing funds, they are completely out of luck. These lost funds come out of the pockets of the poorest families who cannot afford to lose a single dollar.

B. Potential remedy to address EBT card fraud.

We support legislative efforts to address gaps in the Electronic Fund Transfer Act that leave consumers unprotected. The EFTA and SNAP statute can be amended to address the specific problem of EBT card fraud by eliminating the exclusion of EBT cards from the EFTA and providing protection against unauthorized transfers. As a result, consumers who are impacted by EBT card theft will be able to avail themselves of the EFTA unauthorized use provision and error resolution procedures.

VII. Problems with the collection of accurate payment fraud data create an additional barrier in addressing payment fraud.

A. The problem of fragmented data collection on payment fraud.

In the United States, regulatory oversight and supervision of actors in the payments space depends on several factors including the size, type, and nature of a financial institution,⁹⁹ as well

⁹⁶ U.S. Department of Health and Human Services, Office of Family Assistance, “*Characteristics and Financial Circumstances of TANF Recipients, Fiscal Year 2021*,” updated February 2023, available at <https://www.acf.hhs.gov/ofa/data/characteristics-and-financial-circumstances-tanf-recipients-fiscal-year-2021>.

⁹⁷ <https://www.fns.usda.gov/snap/snap-tanf-ebt-card-skimming-prevention>

⁹⁸ See the Consolidated Appropriations Act (CAA) of 2023, Title IV, Section 501.

⁹⁹ Depending on the size and activity, a financial institution engaging in payment activity could be subject to supervision by the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and/or the Consumer Financial Protection Bureau. Otherwise, the institution could be subject to state regulatory supervision under a state bank charter or money transmitter license. Some payment actors may not be subject to any supervision, though they are still required to comply with all laws.

as the extent to which the activities¹⁰⁰ undertaken by an institution are covered by existing law. As a result, no centralized federal agency receives or collects all data about payment fraud.¹⁰¹ Additionally, defrauded consumers may report fraud to the Federal Trade Commission, the FBI's internet crimes division, and/or the Consumer Financial Protection Bureau, among other local law enforcement agencies, leading to differing and incomplete snapshots of payment fraud. Although these agencies may share fraud data with each other or the general public, there is no mandate to do so.¹⁰²

Furthermore, financial institutions, payment processors, and payment operators are not required to report the incidents of payment fraud experienced by their customers/consumers to any federal agency. The institutions are required to file a Suspicious Activity Report (SAR) for large transactions in certain circumstances if they suspect their customer is engaged in fraudulent activity, but they are not required to report smaller fraudulent transactions or instances where their clients have been victimized by fraud.¹⁰³ Even with SARs mandatory reporting, the information collected by FinCEN relies heavily on the discretion of a financial institution, whether the fraud or potential fraud is discovered/flagged by the reporting institution, and if the transaction is large enough to warrant reporting.¹⁰⁴

Players in the payment industry have recognized the need for fraud information sharing, and some payment operators do collect data about fraud. The Federal Reserve Board collects reports of fraud on FedNow as specified under Regulation J, Subpart C and keeps a "Negative List" of suspicious accounts that is shared with its participants.¹⁰⁵ The Clearing House also collects fraud reports for RTP® (their real time payments platform) and Early Warning Systems (EWS), owner of Zelle, collects reports of fraud occurring on Zelle, though it is unclear if this information is

¹⁰⁰ Though not covered by this testimony, institutions engaged in payments through cryptocurrency and/or stablecoin face the possibility of oversight by the prudential regulators as well as Commodities Futures Trading Commission, the Securities and Exchange Commission, and/or the Consumer Financial Protection Bureau.

¹⁰¹ Of any type, including fraud through P2P apps, bank-to-bank transfers, or check fraud.

¹⁰² Though certain fraudulent activity is required to be reported to FinCEN, and the Federal Reserve Board will collect fraud data through FedNow. However, FinCEN does not publicly share the data it collects, and it is unclear how the Federal Reserve Board will utilize and disseminate the data it will collect for FedNow.

¹⁰³ "Dollar Amount Thresholds- Banks are required to file a SAR in the following circumstances: insider abuse involving any amount; transactions aggregating \$5,000 or more where a suspect can be identified; transactions aggregating \$25,000 or more regardless of potential suspects; and transactions aggregating \$5,000 or more that involve potential money laundering or violations of the BSA. It is recognized, however, that with respect to instances of possible terrorism, identity theft, and computer intrusions, the dollar thresholds for filing may not always be met. Financial institutions are encouraged to file nonetheless in appropriate situations involving these matters, based on the potential harm that such crimes can produce. Even when the dollar thresholds of the regulations are not met, financial institutions have the discretion to file a SAR and are protected by the safe harbor provided for in the statute." From FDIC "Connecting the Dots... The Important of Timely and Effective Suspicious Activity Reports" Supervisory Insights (Updated Jul. 10, 2023), available at <https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin07/siwin07winter2007-article03.html#:~:text=Dollar%20Amount%20Thresholds%20%E2%80%93%20Banks%20are,and%20transactions%20aggregating%20%24%20or%20or>.

¹⁰⁴ See Mansfield, Cathy, "It Takes a Thief... and a Bank: Protecting Consumers From Fraud and Scams on P2P Payment Platforms," 57 U. Mich. J.L. Reform (2024).

¹⁰⁵ See Operating Circular 8: Funds Transfers through the FedNow Service (Sept. 21, 2022) available at <https://www.frb-services.org/binaries/content/assets/crsooms/resources/rules-regulations/operating-circular-8.pdf>.

shared widely among users.¹⁰⁶ Even initiatives such as SardineX¹⁰⁷ and Beacon¹⁰⁸ were launched in response to increased fraud in digital payments and real-time payment systems. However, the information shared is not available to the public and may be industry or payment specific. For example, if a bad actor is flagged in one payment system (i.e. Zelle), that does not mean a financial institution will have that bad actor flagged when allowing a fraudulent wire transfer to be released.¹⁰⁹

The fragmentation described above prevents a clear and cohesive picture of the payment fraud landscape, actors, and trends and poses a barrier to forming effective strategies to combat fraud.

B. Potential remedies to address the problem of fragmented payment fraud data collection.

1. Interagency collaboration.

The importance of information sharing and collaboration between state and federal law enforcement agencies charged with protecting the public from fraud and other unfair, deceptive, and abusive business practices cannot be overstated. Collaboration is essential not only to identify illegal practices that harm consumers, but to facilitate a comprehensive and effective strategy to stop fraudsters before they have stolen money from individuals and families. Criminals know no boundaries; they leverage technology to perpetrate their schemes quickly and are oftentimes unknown until it is too late. Staying ahead of these players requires rigorous and easy lines of communication between partners—including private attorneys and non-profit organizations—who are often the first to hear about scams on the ground.

Indeed, NCLC provided many of the recommendations that follow in comments to the FTC Collaboration Act of 2021.¹¹⁰ One of these recommendations is that the FTC develop a Fraud Task Force to ensure more regular information sharing and cooperation among all the various agencies that see and deal with individual pieces of the fraud landscape.

¹⁰⁶ See *Faster Payments Fraud Trends and Mitigation Opportunities*, Faster Payments Council, Fraud Work Group Bulletin.01 at 5 (Jan 2024), available at https://fasterpaymentscouncil.org/userfiles/2080/files/FPC%20Fraud%20Bulletin_01_01-24-2024_Final.pdf.

¹⁰⁷ Join sardineX, Sardine, available at <https://go.sardine.ai/sardineX>. SardineX is intended as a real-time fraud detection network made up of a consortium of financial institutions and fintech organizations, including banks, card networks, payment processors, and fintechs, which will include a shared database where participants can access fraud data on entities transacting across the network.

¹⁰⁸ Meier, Alain “Introducing Beacon, the Anti-Fraud Network,” Plaid (June 22, 2023), available at <https://plaid.com/blog/introducing-plaid-beacon/>. Beacon, launched by Plaid, is intended as an anti-fraud network enabling financial institutions and fintech companies to share critical fraud intelligence via API across Plaid. Members contribute by reporting instances of fraud and can use the network to detect if a specific identity has already been associated with fraud.

¹⁰⁹ Any private database of suspected fraud actors could be considered a “consumer reporting agency” (CRA) under the Fair Credit Reporting Act (FCRA). Early Warning Services already acknowledges it is a CRA. See CFPB, List of Consumer Reporting Companies, 2023, at 28, https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-companies-list_2023.pdf. As such, these databases would be subject to the file disclosure, accuracy, and dispute resolution rights under the FCRA.

¹¹⁰ See NCLC *et al.*, Comments regarding the FTC Collaboration Act of 2021, (Aug. 14, 2023) available at https://www.nclc.org/wp-content/uploads/2023/08/FTC_AG-Fraud-Collaboration-consumer-comments-8-14-23-final3-Lauren-Saunders.pdf.

Since reportfraud.ftc.gov and ic3.gov are two of the most used sites to report fraud, the FTC and the FBI should work with the CFPB, banking regulators, and state Attorneys General (AGs) and local law enforcement to simplify fraud reporting for consumers. Consumers may report fraud to many different places – the local police department, the FBI, an AG, the CFPB, or the FTC. Sometimes police refuse to take fraud reports, viewing fraud as a civil matter. Once a consumer is turned away once place, they may give up. We advise consumers to file a complaint in as many places as possible, but that is cumbersome and not always realistic. Consumers may also find that they are asked for the same information multiple times from different agencies. We urge these agencies to:

- Develop standardized complaint intake forms that can be used by many different agencies.
- Provide a range of easily accessible channels (e.g. in person, phone, e-mail, web, mobile app) for consumers to submit complaints and grievances.
- Include options to report fraud and other complaints in multiple languages.

Fraud reporting must be as simple and universal as possible to be effective.

We also support the provision in Title I of the Senate Appropriation Committee’s Financial Services and General Government bill on financial fraud, which directs the Treasury Department to “facilitate a public-private partnership to enhance Americans’ financial security and prevent the proliferation of financial fraud and scam schemes... (including) the relevant Federal and State financial regulators, consumer protection agencies, law enforcement, financial institutions, trade associations, consumer and privacy advocates, and other stakeholders.”¹¹¹ That partnership would “encourage information sharing among participants, develop best practices for relevant stakeholders, including the larger public, develop educational materials to enhance awareness of financial fraud schemes across sectors, share leading practices and tools, and encourage innovations in counter-fraud technologies, data-analytics, and approaches.”¹¹²

2. Require fraud reporting within payment systems.

As previously mentioned, the operators of FedNow, RTP®, and Zelle already collect reports of fraud, and they should analyze those reports, follow up on patterns, and develop preventive measures if they are not already doing so.

But we especially urge the Federal Reserve Board, the operators of other wire transfer services, and other bank regulators to devote attention to bank-to-bank wire transfers. While there is a fair amount of knowledge about how consumers are defrauded into sending funds through wire transfers, no one seems to be collecting or analyzing information about the accounts into which funds are sent. Some of these questions can only be answered by the banks, bank regulators, or wire transfer operators. We understand that the Federal Reserve Board does not receive fraud

¹¹¹ Financial Services and General Government Appropriations Bill, 2024. (S. 2309), Title I. Department of the Treasury, “Financial Fraud” at 10, available at https://www.appropriations.senate.gov/imo/media/doc/fv24_fsgg_report.pdf.

¹¹² *Id.*

reports from institutions utilizing Fedwire, though it may be exploring doing so. We do not know what fraud information is collected on other wire transfer services, such as The Clearing House's CHIPS system.

As previously mentioned, the Federal Reserve Banks should also explore collecting information on check fraud.

The more information law enforcement, payment system operators, and regulators have about fraud committed through these platforms, and the more that agencies work together to identify trends, the more avenues there will be for stopping fraud.

VIII. The use of AI and automated tools to combat payment fraud is important, but consumers need clear rights when innocent consumers are negatively impacted.

A. Overaggressive algorithms can shut out innocent consumers from access to their accounts and funds.

Most parties who engage in payments, (financial institutions, payment processors, card networks, money service businesses, and fintechs) utilize tools to combat payment fraud, including AI and machine learning technologies. Financial institutions who hold consumer deposits may also utilize these same kinds of technologies to comply with their BSA/AML obligations. However, these tools may harm innocent consumers if not utilized properly and if institutions do not have clear procedures and timelines in place to restore access to funds that are improperly frozen.

Sometimes the appropriate response by a company who suspects its customer is engaging in fraudulent activity is to freeze a transaction or close an account that is being used to receive fraudulent funds before the funds are gone and more consumers can be defrauded. However, no law requires the company to take these actions; it is up to the risk tolerance of the company and the internal policies set in place by the company. The only required responses to potential fraud a company may need to undertake under BSA/AML law is to file a Suspicious Activity Report (SAR) if the transaction is large enough to meet the threshold reporting requirements and update their customer risk profile.¹¹³

According to the Bank Policy Institute, "a sample of the largest banks reviewed approximately 16 million alerts, filed over 640,000 SARs, and received feedback from law enforcement on a median of 4% of those SARs. Ultimately, this means that 90-95% of the individuals that banks report on were likely innocent."¹¹⁴ As a result, even the filing of a SAR alone should not automatically trigger an account closure.

¹¹³ Financial Crimes Enforcement Network, Customer Due Diligence Requirements for Financial Institutions, Final Rule, 81 Fed. Reg. 29398 (May 11, 2016); 31 C.F.R. 1020.210(b)(i); Office of the Comptroller of the Currency, *Bank Secrecy Act (BSA)*, available at <https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html/>.

¹¹⁴ Bank Policy Institute "The Truth About Suspicious Activity Reports," (Sept. 22, 2020) available at <https://bpi.com/the-truth-about-suspicious-activity-reports/>; and citing to, "Getting to Effectiveness—Report on U.S. Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance," Bank Policy Institute (Oct. 29, 2018) available at https://bpi.com/wp-content/uploads/2018/10/BPI_AML_Sanctions_Study_vF.pdf.

But financial institutions have broad discretion in how they respond to perceived risk threats and have sometimes overreacted to fraud waves, catching innocent consumers in the process. Often, the most vulnerable people have been denied access to their money.

After Chime embarked on a marketing campaign to convince people to open Chime accounts to receive their stimulus payments, its inadequate identity verification led to a wave of fraud. Chime then froze numerous accounts, leaving some people without their money for months on end:

- “Chime stole my entire unemployment backpay.... I’m a single mom of 4 kids and they stolen \$1400 from me and refuse to give it back and now we are about to be evicted.”¹¹⁵

Similarly, Bank of America froze 350,000 unemployment debit cards in California after extensive fraud reports. But the freezes caught many legitimately unemployed workers, and the bank failed to respond in a timely fashion to their complaints:

- “Heather Hauri got a text from Bank of America that suggested her debit card may have been compromised too. When she responded that she had not made the transactions in question, she was locked out of her account. ‘The whole account is frozen,’ she said. ‘You can’t get your own money.’”¹¹⁶

Months later, after a lawsuit was filed, a judge prohibited the bank from freezing accounts for California unemployment benefits based solely on an automated fraud filter and required it to do a better job of responding when jobless people say their benefits were stolen.¹¹⁷ The CFPB ultimately brought an enforcement action against Bank of America,¹¹⁸ and also against U.S. Bank¹¹⁹ for similar conduct in indiscriminately freezing accounts and leaving them frozen for long periods of time. This conduct harmed the most vulnerable consumers – those who had lost their jobs and were relying on unemployment benefits.

The amount of accountholders who have complained about checking and savings account closures to the CFPB more than doubled since 2017,¹²⁰ and in 2022 the CFPB ordered Wells

¹¹⁵ Kessler, Carson, “A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers’ Money,” ProPublica (July 6, 2021), available at <https://www.propublica.org/article/chime>.

¹¹⁶ KCAL News, “Bank Of America Freezes EDD Accounts Of Nearly 350,000 Unemployed Californians For Suspected Fraud,” (Oct. 29, 2020), available at <https://www.cbsnews.com/losangeles/news/bank-of-america-freezes-edd-accounts-of-nearly-350000-unemployed-californians-for-suspected-fraud/>.

¹¹⁷ McGreevy, Patrick, “Bank of America must provide more proof of fraud before freezing EDD accounts, court orders,” Los Angeles Times (Jun. 1, 2021), available at <https://www.latimes.com/california/story/2021-06-01/bank-of-america-ordered-to-unfreeze-unemployment-benefit-cards-in-california>.

¹¹⁸ CFPB, “Federal Regulators Fine Bank of America \$225 Million Over Botched Disbursement of State Unemployment Benefits at Height of Pandemic,” (Press Release) (July 14, 2022), available at <https://www.consumerfinance.gov/about-us/newsroom/federal-regulators-fine-bank-of-america-225-million-over-botched-disbursement-of-state-unemployment-benefits-at-height-of-pandemic/>.

¹¹⁹ CFPB, “CFPB Orders U.S. Bank to Pay \$21 Million for Illegal Conduct During COVID-19 Pandemic,” (Press Release) (Dec. 19, 2023), available at [https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-us-bank-to-pay-21-million-for-illegal-conduct-during-covid-19-pandemic/#:~:text=The%20CFPB%20and%20OCC%20together,411%20DCFPB%20\(2372\)](https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-us-bank-to-pay-21-million-for-illegal-conduct-during-covid-19-pandemic/#:~:text=The%20CFPB%20and%20OCC%20together,411%20DCFPB%20(2372).).

¹²⁰ CFPB Consumer Complaint Database trends data for complaints received due to checking or savings account

Fargo to pay \$160 million to over one million people for improperly freezing or closing bank accounts from 2011 to 2016 when it “believed that a fraudulent deposit had been made into a consumer deposit account based largely on an automated fraud detection system.”¹²¹

There have been other stories featured by reporters detailing the devastating impact sudden account closures and freezes can have on consumers, especially when they are deprived access to their funds, are not provided with any information about the reason for the institution’s actions, and are not provided an opportunity to address any perceived risk.

Following are a few examples from a New York Times article detailing the responses consumers received after discovering their accounts were either frozen or closed and the attempts to communicate with their financial institutions about it:¹²²

- Naafeh Dhillon, 28 from Brooklyn, NY, learned his account had been closed after his debit card and credit card were declined. He was later told by a Chase representative that the “bank’s global security and investigation team had ultimately made the decision. Would the representative transfer him to that department? Nope... Since he wasn’t given a specific reason for the closure, he couldn’t disprove whatever raised suspicions in the first place.”
- Todd Zolecki, 47 of Media, PA, did not have his account closed, but they did lock him out of access to his account. “They said your account has been suspended for further review,” Why? “We can’t tell you that. The only thing we can tell you is it can take up to 60 days for this review.”

When people cannot access money they need based on red flags triggered by automated fraud tracking systems alone, that problem is compounded when a consumer’s complaint is not followed up with any reasonable investigation by the financial institution involving any discussion with the accountholder or any clear timeline to unfreeze their money.

The EFTA has clear error resolution timelines and procedures, and those should be used when consumers cannot access their funds. If a consumer is unable to make an electronic withdrawal or transfer because of an account closure or freeze based on suspected fraud, that action should be viewed as an error – an incorrect transfer of zero instead of the requested amount – triggering the error resolution rights, duties, timelines and investigation procedures of the EFTA. But financial institutions and payment apps seem to believe the EFTA does not apply in this

closure available at https://www.consumerfinance.gov/data-research/consumer-complaints/search/?chartType=line&dateInterval=Month&dateRange=All&date_received_max=2024-01-27&date_received_min=2011-12-01&has_narrative=true&issue=Closing%20an%20account%E2%80%A2Company%20closed%20your%20account&lens=Product&product=Checking%20or%20savings%20account&searchField=all&sublens=sub_product&tab=Trends

¹²¹ *In the Matter of Wells Fargo Bank, N.A.*, CFPB No. 2022-CFPB-0011 (Dec. 20, 2022) (consent order), available at https://files.consumerfinance.gov/f/documents/cfpb_wells-fargo-na-2022_consent-order_2022-12.pdf

¹²² Barnard, Tara Siegel and Lieber, Ron, “Banks Are Closing Customer Accounts, With Little Explanation,” New York Times (Apr. 8, 2023) available at https://www.nytimes.com/2023/04/08/your-money/bank-account-suspicious-activity.html?unlocked_article_code=1.QU0.szRm.kfoZRQd7-O6&smid=url-share.

situation.

B. Potential remedies to address improper freezes or account closures due to the use of automated fraud detection.

We support legislative efforts to address the many gaps and ambiguities in the Electronic Fund Transfer Act that leave consumers unprotected. The EFTA can be amended to address the specific problem of improper freezes and account closures by clarifying that the error resolution duties under the EFTA apply if a consumer's account is frozen or closed or the consumer is otherwise unable to access their funds. When a consumer contacts their financial institution complaining about the inability to access funds or an account closure, the institution would have to perform a reasonable investigation and provide a resolution to the consumer within 10 days or provide a provisional, unfrozen, credit pending a longer investigation. After a reasonable investigation, the consumer's financial institution would have to release the frozen funds or reopen a closed account if it was done in error—except in cases where the consumer obtained the funds through unlawful or fraudulent means or was denied access due to a court order or as directed by law enforcement.

The EFTA's error resolution procedures allow financial institutions to continue using automated fraud detection systems while ensuring that consumers have remedies when those systems get it wrong. This would ensure a consumer receives information about why their account was frozen or closed and get more timely access to their funds if the bank was in error.

The problem with account closures and freezes could also be addressed by rulemaking or guidance from the CFPB.

FinCEN and bank regulators should also provide guidance to financial institutions about what information they may and should provide to accountholders regarding freezes and account closures while still complying with the BSA. For example, they could clarify in a FAQ that, while financial institutions are not allowed to disclose that a SAR was filed, they are allowed to disclose that an account was frozen or closed due to suspicious activity and/or describe the specific activities that raised concerns.

As shown by the CFPB's recent enforcement actions and in light of risks of unfair, deceptive, or abusive practices when consumers' funds are held indefinitely, the CFPB and bank regulators should also provide guidance to financial institutions about the importance of having clear procedures to enable consumers to quickly regain access to their funds when they are frozen due to concerns of suspicious activity and provide guidance as to the timeliness of returning an accountholder's funds after account closure.

IX. Conclusion

Payment fraud is a pervasive problem impacting U.S. consumers, especially those most vulnerable to the loss of income caused by unauthorized and fraudulently induced transactions. However, Congress can take steps to address these problems by utilizing a holistic approach to the problems caused by fraud and scams instead of just relying on consumer education and information dissemination.

With any questions, please contact Carla Sanchez-Adams, Senior Attorney at the National Consumer Law Center, at csanchezadams@nclc.org.

Thank you for the opportunity to provide this statement for the record.

Yours very truly,

National Consumer Law Center (on behalf of its low-income clients)

PREPARED STATEMENT OF PAUL BENDA

EXECUTIVE VICE PRESIDENT, RISK, FRAUD AND CYBERSECURITY, AMERICAN BANKERS ASSOCIATION

FEBRUARY 1, 2024

Chairman Brown, Ranking Member Scott, and Members of the Committee, thank you for the opportunity to testify today for a hearing “Examining Scams and Fraud in the Banking System and Their Impact on Consumers”. My name is Paul Benda, and I serve as Executive Vice President, Risk, Fraud and Cybersecurity for the American Bankers Association (ABA). The American Bankers Association is the voice of the Nation’s \$23.4 trillion banking industry, which is composed of small, regional, and large banks that together employ approximately 2.1 million people, safeguard \$18.6 trillion in deposits, and extend \$12.3 trillion in loans. Our members know that fraud takes a financial and emotional toll on their customers and banks of all sizes are making extraordinary efforts to protect and safeguard customer accounts as fraud has become more sophisticated.

Introduction

From using breakthrough technologies such as generative artificial intelligence (AI) to old fashioned theft of checks out of mailboxes, criminals are relentlessly pursuing new ways to scam consumers and small businesses and steal money from their bank accounts. Banks have a long history of improving and innovating to protect their customers—from the adoption of chip-enabled credit cards to multifactor authentication to protect user accounts to the use of advanced AI tools to warn customers about potentially fraudulent transactions—banks have been on the front lines of innovation and deploying advanced capabilities to protect their customers. Unfortunately, however, the fight against these criminals is one that banks cannot win on their own.

A recent example of widespread fraud efforts occurred when criminals took advantage of the economic devastation of COVID-19 and the unprecedented Government response to support small businesses and out-of-work Americans. By the Government’s own estimate over \$300B^{1 2} was lost, fueling the growth of more organized and sophisticated networks of financial criminals who continue to look for new ways to keep the illicit funds flowing. The criminals are now using the tools and networks they built during the pandemic, along with secure messaging technology, to share tactics, techniques and procedures to expand their reach, finding new people to cash stolen checks and provide “mule” bank accounts³ to receive and move the funds. They are also becoming more sophisticated, using new advanced deepfake technologies to change their voice and appearance in real-time video calls to execute romance and impersonation scams. A significant portion of the \$300B that was stolen during the pandemic has been reinvested by these criminals to create a highly advanced and sophisticated adversary who is a far departure from the basic phishing scams of yesteryear.

These criminals can’t be stopped by banks alone, and we support law enforcement as they combat this scourge. While banks need to have the technology and infrastructure in place to defend themselves and their customers, they can only provide the leads necessary for law enforcement to track down the perpetrators. Banks also need the telecom companies and their regulators to close regulatory loopholes that allow criminals to spoof legitimate names and phone numbers to convince customers they are speaking with a bank. Banks need social media companies to proactively root out accounts pretending to be bank employees or financial advisors to convince people to put their money into their investment scams. Banks need the postal service to improve the security of the mail system so that when someone mails a check, it won’t get intercepted, stolen, altered and cashed by the criminal. Most importantly, banks need strong partnerships with law enforcement, so the resources to combat these crimes match the amount of money being stolen from consumers. And when these criminals are caught, the punishments must match the crime, so these offenders won’t continue to steal from American consumers and businesses. Banks also welcome the chance to partner with community-based organizations that are doing critical work in this area, as they are trusted voices in many underrepresented communities.

¹ See: <https://www.sba.gov/sites/sbagov/files/2023-06/SBA%20OIG%20Report%2023-09.pdf>.

² <https://www.sba.gov/sites/sbagov/files/2023-06/SBA%20OIG%20Report%2023-09.pdf>

³ Money mules are people who, at someone else’s direction, receive and move money obtained from victims of fraud.

Banks clearly play a key role in fighting fraud, but unless every player in the ecosystem joins the fight, criminals will continue to steal at a scale we've never witnessed before.

State of Fraud Today

Banks have made significant progress in protecting themselves and their customers from being hacked. One recent industry analysis found that Financial Services, which is a category that includes more than just banks, account for only 5.4 percent of ransomware attacks in Q3 2023.⁴ Unfortunately, bank customer losses from scams and fraud have been increasing significantly. Reliable data on consumer fraud is scarce, but the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) is the Nation's hub for businesses and consumers to report cybercrime and elder fraud.⁵ This data is limited to certain types of fraud, and therefore underreports the true dollar amount of fraud perpetrated, but it is still a useful proxy to identify trends and compare the number of different internet-based scams.

In the IC3's 2022 *Internet Crime Report* (the Report), released in March 2023, data showed a nearly 50 percent increase in losses reported by consumers and businesses from 2021 to 2022



Figure 1. Complaints to IC3 over the last five years⁶

According to the Report, the top three categories of scams in order of victim losses were investment scams, business email compromise, and technical support scams. The rise of investment scams was especially pronounced with an increase of 127 percent from 2021 of \$1.45B to \$3.31B lost.

While the top three scams rely on different mechanisms, impersonation is the common enabling factor. Impersonation scams can take many different forms, including a criminal pretending to be a financial advisor or romantic partner to convince someone to invest in the next “can’t miss” opportunity, or a criminal who has hacked a realtor’s email account and then convinces the buyer to change the wiring instructions for the home-closing costs.

⁴<https://www.coverware.com/blog/2023/10/27/scattered-ransomware-attribution-blurs-focus-on-ir-fundamentals>

⁵www.ic3.gov

⁶https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Impersonation scams directly affect banks and their customers. In June 2023, the Federal Trade Commission (FTC) published a Data Spotlight⁷ that identified the top text messaging scams of 2022. The top scam was an impersonation scam—which is often in the form of a fake fraud alert from a bank:

Reports about texts impersonating banks are up nearly twentyfold since 2019. You might get a fake number to call about supposed suspicious activity. Or they might say to reply “yes or no” to verify a large transaction (that you didn’t make). If you reply, you’ll get a call from the (fake) fraud department. People say they thought the bank was helping them get their money back. Instead, money was transferred out of their account. This scam’s median reported loss was a whopping \$3,000 last year.

It’s not just the private sector that is being impersonated. Just this year the Consumer Financial Protection Bureau (CFPB) became the victim of an imposter scam, confirming that “scammers are using CFPB employees’ names to try to defraud members of the public. We’ve heard from people, specifically older adults, who received phone or video calls.”⁸ Unfortunately, many times these types of scams impersonating public and private entities are aided by inadequate technology controls that allow the criminals to show a legitimate business or agency phone number and name on caller ID giving an air of authenticity to the criminal.

Though losses from the internet and impersonation-based scams are most prominent, check fraud has become one of the fastest-growing categories of fraud impacting consumers across the country. However, as noted above, it is extremely difficult to gather the actual volume of check fraud being perpetrated as there is no central repository of data. The IC3 does provide some data, but it combines check and credit card fraud for a value of \$264M for 2022. Judging by what we are hearing from our members, this very likely underrepresents the actual volumes of check fraud; one bank alone has reported losses of over \$100M in a single quarter due to check fraud.

In order to determine if the anecdotal growth being reported is accurate, we must cross reference it with trend data. Treasury’s Financial Crimes Enforcement Network (FinCEN)—charged with collecting and analyzing information about financial transactions to combat money laundering and financial crimes, including confidential Suspicious Activity Reports (SARs) banks are legally required to file—provides one such source. FinCEN categorizes and tracks the types of SARs being filed and the growth of check fraud-related reports by banks and other financial institutions has become so substantial that early last year FinCEN published an alert on the “Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail”. The alert states:

In 2021, financial institutions filed more than 350,000 SARs to FinCEN to report potential check fraud, a 23 percent increase over the number of check fraud-related SARs filed in 2020. This upward trend continued into 2022, when the number of SARs related to check fraud reached over 680,000, nearly double the previous year’s amount of filings.⁹

Even though the exact dollar value of fraud being committed can’t be determined, the trends are clear and troubling. Fraud is increasing across all channels. Banks are investing heavily in new technologies and capabilities to try to stop it, but when customers are duped into giving their money to criminals or mail gets stolen from a post office, there are limits to what banks can do. Attacking these trends requires work in the following areas:

- *Continue To Enhance Banks’ Anti-Fraud Operations*—The scale of fraud being experienced may make existing procedures and policies obsolete and banks must continue to look for ways to improve bank to bank recoveries and customer experiences.
- *Increase Consumer Education*—Securing someone’s account doesn’t help if they can be convinced to willingly hand over their money or their login credentials.
- *Close Loopholes To Stop Impersonation Scams*—Too many loopholes, such as phone number spoofing, exist allowing criminals to impersonate legitimate businesses and agencies.

⁷ <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/06/iykyk-top-text-scams-2022>

⁸ <https://www.consumerfinance.gov/about-us/blog/beware-of-new-cfpb-imposter-scams/>

⁹ <https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20Check%20Fraud%20FINAL%20508.pdf>

- *Improve Information-Sharing*—Criminals have an active information-sharing ecosystem that banks and the public sector must match to try to slow the flow of illicit funds.
- *Enhance Collaboration With Law Enforcement and Regulators*—Law enforcement plays a critical role in stopping fraud and ensuring perpetrators are prosecuted and prevented from further activity.

Banks Are Continually Improving Anti-Fraud Operations

The rise in fraud has not only impacted consumers but banks as well. The rise in the volume of cases, the complexity of processing check fraud claims, and the significant churn in personnel that occurred as a result of the pandemic created very significant operational challenges for banks, resulting in processing delays for check fraud claims.

Banks are working diligently to reduce current timelines and improve the overall experience for customers. In the majority of instances, and assuming a customer reports the fraud promptly, they are not liable for a fraudulent check and the bank will make them whole. The process requires the bank that accepted the check for deposit (bank of deposit) and the bank that issued the check (the paying bank) to work out liability under applicable State law and contractual agreements. This is achieved in a number of ways, depending on the reason the check is unpayable. For certain claims, the paying bank whose customer has notified them of a fraudulent check will file a check warranty breach claim with the bank of deposit. Given the wide range of banks involved, one of the biggest challenges is determining a point of contact with which to exchange a claim.

Recognizing this challenge, in 2023 ABA worked collaboratively with other industry groups to establish a check fraud working group focused on expediting the processing of check fraud claims. Among other things, the working group exchanged points of contact and documentation requirements to process a claim. And while the working group focused on the banks handling the vast majority of claims, its success has resulted in ABA developing an online check fraud directory that any bank—whether an ABA member or not—can access for free as long as they reciprocate and provide their contact information. In just over 6 months the directory has grown to nearly 1,700 banks, and we have heard from banks how invaluable this resource is in speeding up the claim processing timeline. Our job is not done yet, and we continue efforts to expand the number of participating banks in the directory.

In addition to the directory, the check fraud working group has undertaken efforts to improve the overall claims process for banks and customers alike, including:

- Drafting a Universal Warranty Breach Claim form to help standardize the required information for a claim, reducing duplicative submissions.
- Reducing burdensome documentation hurdles by encouraging banks to drop notarization requirements.
- Making it easier to file a claim if a customer's stolen check was going to pay a recurring bill to a large company (e.g., an electric utility) by not requiring the normally standard affidavit from the utility, which can be very difficult for the consumer to obtain.
- Developing industry baselines for notifying the paying bank when a claim was received, assigning it a claim number, and providing an estimated time for processing.
- Attempting to standardize the time after a claim has been adjudicated and paid out, which can vary significantly.

The processing of check warranty breach claims is surprisingly complex and difficult, but banks and the ABA are committed to improving the system.

Banks Provide Extensive Consumer Education

Consumers are on the front lines of this fight, and we need to do all we can to ensure they have the tools and knowledge they need to protect themselves. Many banks have significantly increased their education of customers. For example, many provide tips for spotting scams in branches, customer communications, and websites and provide timely warnings that customers not share passcodes or send money to people they do not know, in addition to participating in ABA's cross-industry consumer education efforts.

However, while banks can help to keep customers' accounts secure, these controls can be defeated if a criminal convinces the customer to let them into the customer's account or to send them money. Ultimately, banks have little power to stop customers from withdrawing their own money, and indeed victims often are coached to ignore the bank employees who warn them not to withdraw or send the money.

People need to hear from other sources as well, and ABA encourages other trusted sources, such as Government actors or nonprofits, to partner with us to amplify the important work banks are doing to educate consumers on fraud.

Stopping Phishing

One of ABA's most important consumer protection initiatives is our #BanksNeverAskThat¹⁰ anti-phishing campaign. Since its launch in October 2020, we have helped educate millions of consumers on how to spot common scams from bad actors posing as their bank.

The public awareness campaign, developed with input from banks of all sizes across the country, educates consumers by posing ridiculous questions banks would never ask a customer. Using humor and bold graphics, we hope to drive home the message that your bank will also never ask for your password, pin, or Social Security number. ABA provides all of the campaign materials free of charge to any bank in the country interested in participating, so they can deliver the #BanksNeverAskThat messaging in their local markets.

The campaign has increased in size and scope each year. To date, more than 2,300 banks have participated in #BanksNeverAskThat and spread its educational content to millions of Americans through social media, bank websites, ATM screens, and bank branches across the country. ABA has promoted the campaign nationally and anyone who has been to a Capitals, Wizards, or Nationals game has probably seen its education message.

In 2023, ABA launched a Spanish language version of the campaign, available at www.BancosNuncaPidenEso.com. This year's campaign also features an interactive quiz, an educational video game and short entertaining videos. The campaign has been recognized by Federal, State, and local officials for its consumer protection message, and it has received numerous national awards for its creative approach. We've briefed other industry trade groups interested in launching something similar and are already planning for next year's campaign.

Combating Elder Fraud

In addition to its public outreach campaign, ABA through the ABA Foundation has active programs to protect seniors from scams. Given the seriousness of the issues facing older customers, ABA works through its nonprofit foundation to ensure that all banks, irrespective of membership status, can access tools and resources to prevent, detect, and combat elder financial exploitation.

The ABA Community Engagement Foundation, known as the ABA Foundation, is a 501(c)3 corporation that helps banks and bankers make their communities better. Through its leadership, partnerships and national programs, the Foundation supports bankers as they provide financial education to individuals at every age, elevate issues around affordable housing and community development and achieve corporate social responsibility objectives to improve the well-being of their customers and communities.

The ABA Foundation offers banks a free toolkit on "Protecting the Financial Security of Older Americans". This three-part resource is designed to help banks develop a framework on educating and engaging their communities on preventing elder financial exploitation.

Since 2016, more than 1,850 banks have participated in the ABA Foundation's Safe Banking for Seniors program.¹¹ Through the free initiative, participating banks have access to turnkey materials to inform their communities about avoiding scams, choosing executors, financial caregiving, preventing identity theft, known perpetrator fraud, and understanding powers of attorney. Banks use the materials to help empower their communities and lead a combination of in-person and virtual workshops, post videos and other content on social media, and share vital information during one-on-one conversations at teller stations. All the resources are available at no cost to ABA member and nonmember banks.

Through a prior partnership with the FTC, the ABA Foundation also developed infographics to raise awareness about scams that disproportionately affect older customers. Banks and nonbanks alike can freely access and disseminate materials on: Fake Check Scams, Government Imposter Scams, Imposter Scams, Money Mule Scams, Online Dating Scams, Phishing Scams, and Peer to Payments.¹²

While ABA's campaigns have been instrumental in educating the public, we are just one voice. We need a nationwide message coordinated among multiple agencies

¹⁰ www.banksneveraskthat.com

¹¹ <https://www.aba.com/seniors>

¹² <https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money>

(including the CFPB and FTC), nonprofits, and private companies to promote a simple and memorable action plan for people of all ages facing scams. The campaign should also focus on dispelling the behavioral techniques scammers use in impersonating authorities, indicating urgency, requiring secrecy, and manipulating people into action.

Changes Are Needed To Stop Impersonation Scams

Criminals' ability to impersonate legitimate businesses or Government agencies is a major challenge that needs to be addressed to reduce the amount of fraud Americans experience. The challenge can be made more difficult when criminals are able to misrepresent themselves either through a spoofed caller ID that shows a legitimate business name and business' phone number, or through stolen or copycat social media accounts that are indistinguishable from real accounts.

Currently technology can help criminals impersonate legitimate actors through three primary channels:

- *Spoofing of Caller ID*—Criminals have figured out loopholes that allow them to “spoof” the numbers and names of legitimate businesses with intent to defraud the call recipient. For example, banks have reported that customers have received calls that show they are coming from the 1-800 number listed on the back of their debit card. When a customer is presented with what they believe is technologically validated information, it significantly aids the criminal in convincing the customer that they are from their bank.
- *Impersonation Text Messages*—Criminals can use email-to-text tools to create text messages that look like they come from a bank or simply use similar numbers and formats to pretend they're from a bank. These can include links to fake bank websites, call-back numbers, or prompts that cause the criminal to call the customer to socially engineer them to give up security credentials or send money from their accounts.
- *Stolen or Spoofed Social Media Accounts*—The FBI reported that investment scams had the highest losses in dollars. There are many ways these scams can be perpetrated but one recent example is the unknowing takeover of actual bank employees' social media accounts, which were then used to reach out to their connections to convince them to invest in fraudulent investment scams.

Spoofing of Caller ID Information

The Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) caller ID authentication framework established by the Federal Communications Commission (FCC) is meant to help protect consumers from illegally spoofed robocalls by verifying that the caller ID information transmitted with a particular call matches the caller's telephone number.¹³ Unfortunately, technical limitations of existing networks used, particularly non-IP networks, and calls originating from overseas communications providers have hampered the effectiveness of the framework, leaving loopholes that criminals can exploit to spoof the data (i.e., phone number) shown on a consumer's caller ID. We appreciate that the FCC continues to make progress in fully implementing STIR/SHAKEN across all networks. Nonetheless, ABA strongly believes that more needs to be done. Only callers whose calls are fully authenticated—signed at origination and attested throughout the call's pathway—should be able to display data in the recipient's caller ID display. If at any point the authentication cannot be validated, the caller ID should simply display “unknown caller.” We recognize that due to technical limitations some legitimate callers may have their caller ID data dropped, but we believe erring on the side of caution is the best course due to the vast scale of impersonation fraud being committed.

Additionally, we believe that telecommunications providers who enable criminals to impersonate legitimate numbers and incorrectly authenticate their calls with impersonated numbers and company names should be held to account. We have expressed strong support¹⁴ for the FTC's proposal to prohibit entities from providing the “means and instrumentalities” for another to impersonate a Government or business.¹⁵ We agree with the statement made by the National Association of Attorneys General in that proceeding that “when an entity provides substantial assistance or support to impersonators and knows or should have known that their

¹³<https://www.fcc.gov/call-authentication>

¹⁴Letter from Am. Bankers Ass'n, et al., to Lina Khan, Chair, Fed. Trade Comm'n (Dec. 16, 2022), <https://www.aba.com/advocacy/policy-analysis/impersonation-proposal-comment-letter/>.

¹⁵Notice of Proposed Rulemaking and Request for Public Comment, Trade Regulation Rule on Impersonation of Government and Businesses, 87 FR 62,741, 62,751 (Oct. 17, 2022).

products [or] services are being used in a fraudulent impersonation scheme, that company could also be held liable under the proposed impersonation rule.”¹⁶

The vast majority of telecommunications providers follow the law, but those who know or should know that they are enabling criminals to steal from Americans should be held accountable and be liable for the harms they enable.

Impersonation Text Messages

Texting has become a primary method of communication for Americans and criminals have shifted their tactics to “meet their customers where they are.” ABA has focused on ensuring that banks have the tools to identify fraudulent texting trends quickly enough to prevent or mitigate customer harm. Unfortunately, banks are still encountering barriers as they seek to prevent fraudulent texts from reaching customers.

ABA has supported the FCC’s efforts to combat illegal text messages, but we believe more needs to be done. With ABA’s support, the FCC now requires “terminating mobile wireless providers” (providers that deliver calls to recipients) to investigate and potentially block texts from a sender after they are on notice from the agency that the sender is transmitting suspected illegal texts.¹⁷ We have urged the FCC to apply this requirement to entities that originate text messages, as these entities are best positioned to stop illegal texts from being sent in the first place. Last spring, ABA identified “email-to-text” as a common method by which bad actors send large numbers of phishing or otherwise fraudulent messages because the bad actor can load consumers’ cell phone numbers into an email application to send these texts.¹⁸ We support the FCC’s December 2023 statement encouraging providers to make email-to-text an opt-in service—whereby consumers have the option whether they receive text messages that originated through an email platform.¹⁹

We also have urged the FCC to finalize a requirement that text messages be authenticated and set a deadline for the development and mandatory implementation of a text message authentication solution.²⁰ As described earlier, bad actors use numerous approaches to impersonate legitimate companies in text messages sent to consumers. The FCC should work with mobile wireless providers and other entities involved in the texting ecosystem to design an authentication framework that prevents bad actors from sending to consumers text messages that impersonate legitimate companies, while at the same time ensuring that text messages from legitimate companies are not blocked.²¹

Beyond creating an authentication regime for text messages, the FCC should provide banks with access to the information necessary to protect their customers from fraudulent texts. Currently, the telecommunications industry asks that the public forward scam texts to the short code 7726, which spells “SPAM” on your phone. It would be very helpful for banks to have access to the spam messages in order to identify those impersonating their bank and the fake phone numbers and links they are trying to get consumers to use. In fact, one bank worked with telecommunications companies to establish a pilot program whereby the bank gained access to and reviewed reported SPAM data. The bank then used that data to actively issue take-down requests to the relevant phone numbers and internet links that were in the messages so that they no longer functioned. Unfortunately, this program was

¹⁶ Comments of Nat’l Ass’n of Attorneys General 10 (Feb. 23, 2022), <https://www.regulations.gov/comment/FTC-2021-0077-0164>.

¹⁷ In the Matter of Targeting and Eliminating Unlawful Text Messages, CG Docket No. 21–402, Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02–278, Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17–59, Second Report and Order, Second Further Notice of Proposed Rulemaking in CG Docket Nos. 02–278 and 21–402, and Waiver Order in CG Docket No. 17–59, para. 16–25 (released Dec. 18, 2023) [hereinafter, Second Report and Order].

¹⁸ Reply Comments of Am. Bankers Ass’n, et al., In the Matter of Targeting and Eliminating Unlawful Text Messages, CG Docket No. 21–402, Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02–278, at 8 (filed June 6, 2023), <https://www.aba.com/advocacy/policy-analysis/joint-ltr-txt-msgs-lead-generators> [hereinafter, ABA Reply Comments].

¹⁹ Second Report and Order, *supra* note 17, at para. 86.

²⁰ ABA Reply Comments, *supra* note 18, at 10–11.

²¹ In designing an authentication framework, however, the Commission should recognize that legitimate companies frequently send text messages through “short code” text messages—a five- or six-digit number registered through CTIA’s short-code registry that businesses use to send and receive text messages—or through a 10-digit number that is registered with a third-party aggregator. Short Code Registry, Frequently Asked Questions, <https://www.usshortcodes.com/learn-more/faq> (last visited May 2, 2023). The FCC should ensure that the framework adopted does not interfere unduly with these texts.

discontinued because the telecommunication companies revoked the bank's access to the data.

We strongly urge policymakers ensure banks and other legitimate businesses are allowed to access, with appropriate privacy safeguards, data from scam/spam reporting services, whether it is the 7726 data, the "Report Junk" data in Apple's iMessage application, or other similar scam/spam reporting features in other closed messaging applications. Additionally, consideration should be given to requiring all significant messaging services to operate a "Report Spam" feature and be required to share that data so that businesses can protect their customers even if these messaging providers are unwilling to do so.

Stolen or Spoofed Social Media Accounts

Criminals also target consumers by stealing personal social media accounts of employees of legitimate businesses or building fake accounts that portray them as working for that business. In both instances, the brand of the company, often a bank, is used to grant legitimacy to the criminal's posts or messages. While this is a complex problem to combat and prevent, once these "impersonation accounts" are identified there should be a simple, quick, and free method to request that they be taken down. Unfortunately, no major social media company offers such a method.

ABA strongly urges policymakers to ensure that social media companies provide a method to report impersonation accounts that is free to access and to use, and that results in an expedited removal of the offending account. Additionally, we recommend that if the hosting company refuses to take down the impersonation account, they then may be held liable for any fraud committed by that account as they are clearly providing the "means and instrumentalities" and have knowledge that the account is engaged in fraud.

Banks are committed to protecting their customers' data and money. Our goal is to provide a safe and sound financial system that allows our customers to achieve their financial goals. Banks spend billions of dollars a year on cybersecurity and antifraud measures to provide one of the most secure banking systems in the world, but banks can't do it alone. The technology companies that enable criminals to pose as trusted agents must help as well. The criminals have realized the challenges in directly hacking someone's bank account, so instead they focus on convincing customers to give them that access. This is made easier when a phone, text message, or social media site tells a consumer they are speaking with a banker and not the criminal behind the screen.

Improve Information-Sharing To Combat Fraud

Given the massive scale and global reach of fraud, it is simply not possible for one bank to fight back alone; collaboration is required to ensure success. One of the most important tools banks have in combating financial crimes is shared information. However, due to inconsistencies across financial institutions, among other reasons, there are challenges in accessing actionable information in a timely manner.

That is why ABA has been working to establish a program to help banks share information that identifies activity that may involve terrorist financing or money laundering, and predicate crimes like fraud. ABA formed an association of banks to design and develop this new information-sharing exchange, which ABA will manage. The goal is to encourage the sharing of information in real-time so it can reduce the flow of funds to criminals' accounts and improve the quality of banks' reporting. We believe this effort can make a real difference in fighting fraud and other financial crime.

Partnership With Law Enforcement and Regulators

As I have discussed, the rising tide of fraud cannot be fixed by banks or technology alone. At some point, the criminals executing this fraud need to be caught, prosecuted, and sentenced so that they no longer commit these crimes. ABA has a history of partnering with law enforcement and the public sector on education and outreach activities along with identifying potential improvements in addressing fraud.

For example, ABA and the U.S. Postal Inspection Service (USPIS) are entering into a formal partnership to combat check fraud. It is often publicized that the increase in check fraud is partly due to criminals targeting the U.S. mail infrastructure by stealing mailed checks and altering (washing) them, leading to fraudulent transactions at banks.

This agreement builds on our current partnership—dating back to early 2022—when we began joint training initiatives to proactively address fraud: USPIS briefings for ABA-hosted fraud information-sharing groups, participation in ABA webinars, and platforms at ABA conferences. Drawing on USPIS and ABA's respec-

tive resources and reach allows us to educate the public and bank and Postal employees with joint training and red flag alerts at a greater scale.

ABA and USPIS will kick off this new partnership by hosting a free webinar for banks with the USPIS on ways they can collect evidence and support criminal investigations. Following this webinar, ABA and USPIS will distribute co-branded materials to educate bank customers and consumers on how to spot and report on common check fraud activity.

ABA also applauds efforts by other agencies to educate the public regarding fraud and scams. We lead a committee on the FTC's Stop Senior Scams Advisory Group focused on the freezing and recovery of fraudulent transfers, are active in the Federal Reserve Bank of Boston's Scams Definition and Information-Sharing Working Group and have worked with CFPB on elder fraud prevention tools such as trusted contacts adoption among depository institutions and powers of attorney.²²

There are more opportunities for agencies to improve consumer education about scams. For example, Congress established a Financial Education Office in the Consumer Financial Protection Bureau with a statutory mandate to "be responsible for developing and implementing initiatives intended to educate and empower consumers to make better informed financial decisions."²³ We encourage the CFPB to prioritize using this office's resources to help consumers detect and avoid scams and would welcome an opportunity to work collaboratively, as we have done with the FCC, FTC, FBI, and USPIS.

While agencies can also effect fraud prevention through their regulatory actions, we urge them to take care not to impede or inhibit banks' fraud prevention efforts. For example, recently the CFPB outlined changes it is considering to regulations implementing the Fair Credit Reporting Act (FCRA), which could have a significant impact on banks' work to detect and prevent fraud, identity theft, and other financial crimes.²⁴ Among these, the CFPB is contemplating narrowing the permissible purposes for which information can be used under the FCRA, treating consumer-identifying information (including name, address, and Social Security number) as a consumer report subject to the FCRA, while expanding who could be considered a consumer reporting agency to potentially include vendors banks rely on to assist with fraud prevention. Doing so could create new legal, practical, and procedural difficulties for banks that use this information to detect and prevent fraud and crime. Indeed, a Small Business Regulatory Enforcement Fairness Act (SBREFA) that reviewed the CFPB's potential policies for their impact on small entities specifically recommended that the CFPB carefully consider the impacts on fraud prevention and detection, identity verification, and law enforcement and "consider . . . ways to mitigate any negative effects."²⁵ It is important that the CFPB and other regulators consistently evaluate how each policy they consider may impact banks' efforts to detect and prevent fraud.

Law enforcement is a critical force in preventing and detecting fraud, and ABA applauds work by the FBI, United States Secret Service, and FinCEN to try and freeze funds that have been transferred fraudulently. The FBI IC3 Recovery Asset Teams have been great partners, but we are concerned that they may lack capacity to engage on lower-dollar frauds that are reported to the IC3 portal. We would welcome a partnership with them to identify those cases that may not be pursued in a timely manner to determine whether a public-private partnership could be created to pursue those cases and result in more funds being returned to consumers. Congress has recommended similar efforts by the Treasury Department, as seen in a report accompanying a bipartisan Senate Appropriations bill approved by the Committee unanimously, last year, which urged the facilitation of a public-private partnership on fraud prevention.²⁶

Americans are losing billions of dollars to fraud annually. Yet, amid resource constraints and competing demands, local law enforcement struggle to devote appropriate time and attention to these cases. Given the levels of fraud taking place against Americans, police departments and sheriff's offices should not have to choose between dedicating personnel to violent crimes and financial fraud cases.

²² https://files.consumerfinance.gov/f/documents/cfpb_trusted-contacts-fis_2021-11.pdf

²³ Dodd-Frank Act Wall Street Reform and Consumer Protection Act, 12 U.S.C. 5493 §1013(d).

²⁴ CFPB, Small Business Advisory Review Panel for Consumer Reporting Rulemaking Outline of Proposals and Alternatives Under Consideration (Sept. 15, 2023), https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-rule-sbreffa_outline-of-proposals.pdf

²⁵ Final Report of the Small Business Review Panel on the CFPB's Proposals and Alternatives Under Consideration for the Consumer Reporting Rulemaking (Dec. 15, 2023) at 47–48, https://files.consumerfinance.gov/f/documents/cfpb_sbrefa-final-report_consumer-reporting-rule-making_2024-01.pdf.

²⁶ See p. 10; https://www.appropriations.senate.gov/imo/media/doc/fy24_fsgg_report.pdf.

Additionally, law enforcement personnel need more effective training on addressing and responding to fraud allegations. Fraud is a continually evolving landscape and new fraud typologies develop each day. Enforcing the law and responding to these cases requires understanding the multifaceted strategies criminals employ to defraud Americans, particularly with respect to cybercrime. As such, we recommend strengthening the relationship between local law enforcement and Federal agencies.

Moreover, while the losses Americans experience goes to U.S.-based criminals, large amounts are being transferred overseas and potentially by and to those who threaten our national security. The lack of a centralized fraud response and tracking capability within the U.S. Government hinders the ability to spot trends, track tactics, techniques and procedures, and the ability to recover funds for Americans when fraud has been identified. Additionally, there is no central agency with which banks can work on innovative programs to defeat fraud and recover funds.

Conclusion

Banks are working every day to protect their customers from fraud by investing in new technologies, deploying public relations campaigns to educate consumers and small businesses about old and new scams, and partnering with law enforcement and other Federal agencies on new initiatives to combat fraud. Yet our industry recognizes that there is more work to do, and banks can't stop criminals by themselves. Every player in the fraud ecosystem must play a role; from the telecommunications firms to the social media companies to the postal service. And we would welcome collaboration with community groups who have the trust of consumers across the country. The goal of all banks is to help their customers have a safe and secure financial future, and ABA and America's banks are ready to help protect our customers from fraud. I look forward to answering your questions.

PREPARED STATEMENT OF JOHN BREYAULT

VICE PRESIDENT OF PUBLIC POLICY, TELECOMMUNICATIONS, AND FRAUD,
NATIONAL CONSUMERS LEAGUE

FEBRUARY 1, 2024

Introduction

The National Consumers League appreciates the opportunity to provide the Committee with our views on protecting consumers from fraud involving misuse of the banking system.

Founded in 1899, the National Consumers League (NCL) is the Nation's pioneering consumer and worker advocacy organization. Our nonprofit mission is to advocate on behalf of consumers and workers in the United States and abroad.¹ For more than 25 years, NCL has worked, via our Fraud.org campaign, to educate consumers about the warning signs of fraud and promote public policies that protect the American public from scams of all kinds.

Fraud Involving Peer-to-Peer Platforms, Gift Cards, and Cryptocurrency Is Getting Dramatically Worse

There is an epidemic of fraud and identity theft in the United States. While the number of complaints received by the Federal Trade Commission (FTC) has leveled off since hitting a record of 5.96 million in 2021 during the height of the COVID-19 pandemic, complaint levels remain unacceptably high. Nearly 5.2 million consumers submitted complaints in 2022, according to the FTC.² And while fewer complaints may suggest that the situation is improving somewhat, scammers are getting better at extracting more money from their victims. From 2020–2022, fraud losses increased from \$3.3 billion to a staggering \$8.8 billion. Median fraud losses more than doubled from \$311 to \$650.

When NCL last testified before this Committee in 2021, we warned that peer-to-peer (P2P) payment platforms such as Zelle, Venmo, Cash App, and PayPal had become “payment methods of choice for scammers.” Unfortunately, the problem has only worsened since then. In 2020, the FTC received 62,000 complaints where payment apps were the method of payment, with total reported losses of \$87

¹For more information, visit www.nclnet.org.

²Federal Trade Commission. Consumer Sentinel Data Book 2022 (February 2023) p. 6. Online: <https://www.ftc.gov/system/files/ftc-gov/pdf/CSN-Data-Book-2022.pdf>.

million.³ By 2022, reported losses from fraud involving payment apps had grown to \$163 million.⁴ We anticipate that when the FTC reports its 2023 fraud data, this regrettable trend will only continue.

The situation is similarly dismal when it comes to fraud involving one of scammers' other favorite payment methods: gift cards. In 2020, the FTC received 43,242 complaints where a gift card was the method of payment, with reported losses of \$124 million.⁵ In 2022, complaints rose to 48,800 with losses nearly doubling to \$228 million.⁶ Even NCL itself was recently targeted by scammers who tried to get our staff to purchase gift cards by impersonating our CEO. Despite the relative savvy of our staff, several considered going out and buying gift cards, scratching off the back and sending the codes as the scammers asked.

An explosion in the fraudulent use of cryptocurrency as a payment method should be of particular concern to the Committee. Since the FTC first began tracking it as a payment method in 2020, losses involving cryptocurrency payments have ballooned from \$129 million to \$1.59 billion in 2022—a tenfold increase in just 2 years. Complaints received at NCL's Fraud.org website last year were littered with references to fraudulent cryptocurrency investment schemes, and such scams were by far the costliest type of fraud for their victims.⁷ Law enforcement agencies—like the Federal Bureau of Investigation—have reported similar spikes in cryptocurrency scam losses.⁸

All consumers, of every age, income, and education level are vulnerable to falling victim to professional criminal fraudsters. Unfortunately, fraud is a chronically underreported crime due in part to the stigma too often directed at fraud victims.⁹ While these numbers are sobering, they are almost certainly a significant undercount of the true scope of the fraud.

Consumers Should Not Shoulder the Costs of Financial Fraud Alone

This data makes clear that we are not winning the fight against fraud. A common thread running through P2P, gift cards, and cryptocurrency is that once funds are sent, they are available to scammers on the other end of the transaction nearly instantaneously. And when a victim discovers the fraud, it is extremely difficult to recover lost funds. From a scammer's point of view, this is exactly why payment methods like these are so attractive in the first place. Through NCL's Fraud.org campaign, we know that consumers are not only bewildered at becoming a victim of fraud, but also outraged that the companies to whom they entrusted their money do so little to protect their customers' interests or help make them whole.

While P2P platforms, banks, and cryptocurrency trading platforms profit from ever-increasing transaction volumes, they bear little of the costs of fraud that occur on their systems. Instead, the liability for fraud falls on those who can least afford to absorb the losses—individual consumers. The costs of fraud to individual victims can be life-altering. Nearly every day, NCL's fraud counselors hear stories from consumers of how scams erased victims' life savings and caused deep trauma. We clearly need better solutions.

No amount of consumer education, better disclosure, or “friction” put into payment flows will solve this problem alone. We believe the payment platforms where fraud occurs must have a bigger financial incentive to stop scams before they happen. By spreading risk across all the participants in this system, the costs can be better absorbed, resulting in a safer and more secure payments marketplace.

A model for consumer protection for P2P apps and gift cards should be credit and debit cards. Thanks to the Electronic Funds Transfer Act (EFTA) and Fair Credit Billing Act (FCBA), consumers typically shoulder none of the risk when there is unauthorized use on their credit or debit cards. Instead, fraud risks are shared across issuing and receiving banks, card networks, and merchants. As a result, card

³ Federal Trade Commission. “Consumer Sentinel Network Data Book 2020”. (February 2021) p. 11. Online: https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-databook-2020/csn_annual_data_book_2020.pdf.

⁴ Federal Trade Commission. “Consumer Sentinel Data Book 2022”. (February 2023) p. 11. Online: https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf.

⁵ Federal Trade Commission. “Consumer Sentinel Network Data Book 2020”. (February 2021) p. 11. Online: https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-databook-2020/csn_annual_data_book_2020.pdf.

⁶ Federal Trade Commission. “Consumer Sentinel Data Book 2022”. (February 2023) p. 11. Online: https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf.

⁷ National Consumers League. “2024 Top Ten Scams Report”. (Forthcoming, February 2024).

⁸ Lyngaas, Sean, and Rabinowitz, Hannah. “FBI Says \$10 Billion Lost to Online Fraud in 2022 as Crypto Investment Scams Surged”, *CNN.com*. (March 13, 2023) Online: <https://www.cnn.com/2023/03/13/politics/fbi-online-fraud-report/index.html>.

⁹ Ianzito, Christina. “Let's Stop Blaming Scam Victims, New AARP Report Says”. AARP. (July 21, 2022) Online: <https://www.aarp.org/money/scams-fraud/info-2022/victim-blaming.html>.

networks are protected by 24/7 fraud monitoring, with more secure payment technologies such as chip-and-PIN and tap-to-pay regularly replacing older, out of date technology.

From a consumer's perspective this works well. Consumers typically first become aware that fraud has occurred on their credit or debit cards when they receive communication from their bank letting them know that their card has been compromised and will need to be replaced. Unfortunately, because many of the scams involving P2P apps and gift cards involve consumers being induced into authorizing a transaction, banks and payment platforms usually refuse to bear liability for this fraud, resulting in a far less secure payment system.¹⁰

Fixing the "Unauthorized Transactions" Loophole in EFTA Should Be a Priority

To meaningfully reduce fraud on P2P apps and gift cards, a multifaceted approach will be required, including better information-sharing among stakeholders in the payments ecosystem and more fraud-fighting resources and authorities for law enforcement agencies. Congress can and should play a leading role in this effort by strengthening EFTA so that it protects consumers who are victims of induced fraud. Already, pressure from Congress has led Zelle to take some initial steps to protect victims of impersonation scams.¹¹ However, voluntary actions by one actor in the payments ecosystem is no substitute for robust safeguards that protect consumers no matter what payment technology they use. Congressional action is urgently needed to address the rising costs of fraud to consumers.

NCL supports the legislative policy proposals that the National Consumer Law Center included in their written testimony for this hearing. We urge Congress to give special priority to passing legislation, such as the Protecting Consumers From Payment Scams Act,¹² to expand the definition of "unauthorized electronic fund transfer" in the Electronic Funds Transfer Act to cover fraudulently induced payments. This simple fix would address fraudulently induced payments on all payment platforms covered by EFTA, including P2P apps and gift cards. Recently enacted rules in the United Kingdom require banks to reimburse victims of fraud in the inducement, with issuing and receiving banks sharing liability for making victims whole.¹³ The U.K.'s rules should serve as a model for U.S. law in this area.

The Explosion in Cryptocurrency-Related Scams Must Be Addressed

Cryptocurrency will soon become, and by some estimates already is, the payment method of choice for criminal scammers. Driven by the mania for Bitcoin and other cryptocurrencies, as many as 34,000 cryptocurrency kiosks (also known as "BTMs") have been placed in convenience stores, malls, smoke shops, laundromats, and grocery stores around the country.¹⁴

The proliferation of the kiosks in relatively insecure retail locations has made them a favorite tool of scammers.¹⁵ At Fraud.org we often see complaints where scammers direct victims to their closest convenience store to deposit cash into the criminals' cryptocurrency wallets. Kiosk operators, one of whom was reportedly making a 20 percent commission on every transaction,¹⁶ lack sufficient incentives to crack down on these scams.

More must be done to protect consumers from scammers using BTMs. Simply relying on better disclosures or undertrained retail employees will not meaningfully reduce fraud rates. Congress must act. To this end, NCL supports policies that:

¹⁰ Mierzwinski, Ed, et al. "Virtual Wallets, Real Complaints". MASSPIRG Education Fund. June 2021. p. 9. Online: https://masspirg.org/sites/pirg/files/reports/MA_wallets.pdf.

¹¹ Lang, Hannah. "Payments App Zelle Begins Refunds for Imposter Scams After Washington Pressure", Reuters. (November 13, 2023) Online: <https://www.reuters.com/technology/cybersecurity/payments-app-zelle-begins-refunds-imposter-scams-after-washington-pressure-2023-11-13/>.

¹² Online: <https://democrats-financialservices.house.gov/UploadedFiles/BILLS-117pih-ProtectingConsumersFromPaym-U1.pdf>.

¹³ Payment Systems Regulator (U.K.). "PSR Confirms New Requirements for APP Fraud Reimbursement". Press release. (July 6, 2023) Online: <https://www.psr.org.uk/news-and-updates/latest-news/news/psr-confirms-new-requirements-for-app-fraud-reimbursement/>.

¹⁴ Oguz, Kaan. "Why Bitcoin ATMs Are Taking Over Malls and Gas Stations Across the U.S." CNBC.com. (November 7, 2023) Online: <https://www.cnbc.com/video/2023/11/07/why-bitcoin-atms-are-taking-over-malls-and-gas-stations-across-the-us.html>.

¹⁵ Duncan, Jericka, et al. "Unregulated Crypto ATMs Give Criminals a Loophole To Prey on Unsuspecting Victims", CBS News. (March 22, 2023) Online: <https://www.cbsnews.com/news/crypto-atm-scams-unregulated-machines/>.

¹⁶ Anderson, Zach. "Bitcoin of America Indicted for Operating Unlicensed Kiosks", Blockchain News. (March 7, 2023) Online: <https://blockchain.news/news/bitcoin-of-america-indicted-for-operating-unlicensed-kiosks>.

- Require cryptocurrency kiosk operators to provide regulators the physical addresses of any crypto BTM's they operate;
- Require cryptocurrency kiosk operators to abide by longstanding anti-money laundering and know-your-customer requirements, including ID verification for parties involved in a transaction;
- Require businesses that host cryptocurrency kiosks to provide training to their employees on how to spot and intervene in likely fraud involving crypto ATMs; and
- Require businesses that host cryptocurrency kiosks to prominently display warnings about the risks associated with depositing cash into crypto ATMs, especially when the funds will go to digital wallets the consumer does not own.

Senator Warren's Digital Asset Anti-Money Laundering Act of 2023 includes many of these protections and would do much to begin cracking down on the use of cryptocurrency as a payment method for fraudsters.¹⁷ Her bill has NCL's full support and we urge the Committee to approve it.

Conclusion

Chairman Brown, Ranking Member Scott, and the Members of the Committee, we thank you for your continuing work to protect consumers and for holding this hearing. On behalf of the National Consumers League, thank you for including the consumer perspective as you consider these important issues.

¹⁷ Senator Elizabeth Warren, "Warren Expands Coalition of Banking Committee Support for Bill Cracking Down on Crypto's Use in Money Laundering, Drug Trafficking, Sanctions Evasion". Press release. (December 11, 2023) Online: <https://www.warren.senate.gov/newsroom/press-releases/warren-expands-coalition-of-banking-committee-support-for-bill-cracking-down-on-cryptos-use-in-money-laundering-drug-trafficking-sanctions-evasion>.

**RESPONSE TO WRITTEN QUESTION OF SENATOR BUTLER
FROM CARLA SANCHEZ-ADAMS**

Q.1. Ann Booras, a teacher from East Bay had \$20,000 snatched from her by a scammer who called her, pretending to be from her bank, Wells Fargo, and claimed to be investigating fraud. She was asked to wire \$20,000 and \$5,000 from her account; the wire for transfer for \$5,000 was recovered but the larger sum was not. Sadly, Ann’s story of wiring her hard-earned money to criminals is not an isolated one. When she received the scam call, her caller ID even said Wells Fargo bank. Ann realized what had happened and contacted Wells Fargo, her request for reimbursement was denied on the grounds that she had authorized the transaction.

Ms. Sanchez-Adams, what can be done to help steer financial institutions to refund unauthorized transactions and ensure that funds are returned to customers in a timelier manner?

A.1. The transactions described in this story are examples of fraudulently induced transfers through bank-to-bank wire transfer. I have heard of so many stories with the same type of fraudulently induced transfers, often referred to by the payment industry as “imposter” scams, where a fraudster poses as a customer’s own bank and even spoofs the bank’s own phone number to deceive and manipulate a consumer into initiating a transfer. Because the consumer initiates the transaction, it is considered to be “authorized” by the consumer, even though the consumer only initiated the transfer based on the deception and manipulation of the fraudster. Currently, there are no clear protections for fraudulently induced transfers under Federal law.

Even if the transfer had been unauthorized, where the consumer did not know of the transaction and did not initiate it, bank-to-bank wire transfers also have very little protection under the law. Instead of the clear consumer protections provided by the Electronic Funds Transfer Act (EFTA), which was designed to protect consumers with clear rights and procedures, bank-to-bank wire transfers are covered under State law, more specifically a State’s adopted version of Uniform Commercial Code Article 4A (UCC Article 4A). The UCC was not designed as a consumer protection statute and was instead designed to govern commercial-to-commercial transactions. UCC Article 4A offers very weak or no protection for consumers who have suffered harm due to bank-to-bank wire transfer fraud. In essence, the consumer is deemed to have authorized a wire transfer if the bank utilized a commercially reasonable security procedure that the bank and the consumer agreed to beforehand and if the bank acted in good faith. Yet consumers have no understanding of or control over those security procedures and no choice but to click “I agree” to the fine print of an agreement.

For example, the New York Attorney General recently filed a lawsuit against Citibank alleging it failed to protect and reimburse victims of electronic fraud when it used “poor security and anti-fraud protocols” that consumers had not negotiated with Citibank.¹

¹New York State Attorney General, Press Release, “Attorney General James Sues Citibank for Failing To Protect and Reimburse Victims of Electronic Fraud” (Jan. 30, 2024), available at <https://ag.ny.gov/press-release/2024/attorney-general-james-sues-citibank-failing-protect-and-reimburse-victims>.

According to the lawsuit, Citibank connected wire transfer services to consumers' online and mobile banking apps in recent years—allowing direct electronic access to the wire transfer networks—but employed lax security protocols and procedures; had ineffective monitoring systems; failed to respond in real-time; and failed to properly investigate fraud claims.² As a result, New Yorkers lost millions of dollars in life savings, their children's college funds, and even money needed to support their day-to-day lives.

I have also heard numerous other reports of banks failing to reimburse unauthorized wire transfers even if the consumer did not agree to any commercially reasonable security procedure. Consumers do not have the resources to fight the bank in court or arbitration to enforce their right to a reimbursement when this occurs.

UCC Article 4A does not provide a consumer with any remedies besides reimbursement of (and possibly interest on) the unauthorized wire amount, and the consumer's attorney is not entitled to recover attorneys' fees from the bank. As a practical matter, it means that a consumer would have to pay out of pocket to fight in court or in arbitration just to get their money back, while a financial institution with deep pockets can afford to fight a claim. As a result, in most cases financial institutions will reject a consumer's unauthorized wire transfer claim because the consumer cannot afford to fight the decision.

With respect to fraudulently induced wire transfers like those in the story you shared above, the UCC provides no remedy.

You asked me what could be done to help steer financial institutions to refund unauthorized transactions and ensure that funds are returned to customers in a timelier manner. If the definition of unauthorized use in the EFTA was amended to include fraudulently induced transfers and if the EFTA was amended to include bank-to-bank wire transfers, then consumers like Ms. Booras would be entitled to timely refunds of unauthorized transactions.

Congress can and should amend the EFTA to address the problems of unauthorized consumer bank-to-bank wire transfers as well as fraudulently induced consumer bank-to-bank wire transfers by:

- Eliminating the exemption for bank wire transfers, bringing those transfers within the EFTA and its protections against unauthorized transfers and errors;
- Protecting consumers from liability when they are defrauded into initiating a transfer; and
- Allowing the consumer's financial institution, after crediting the consumer for a fraudulent transfer, to be reimbursed by the financial institution that allowed the scammer to receive the fraudulent payment.

The consumer bank-to-bank wire transfer loophole and inclusion of fraudulently induced transfers could also be addressed by rule-

² See Complaint, People of the State of New York v. Citibank, No. 1:24-cv-00659 (S.D.N.Y. filed Jan. 30, 2024), available at <https://ag.ny.gov/sites/default/files/2024-01/citi-complaint.pdf>. The New York AG also alleges that the unauthorized wire transfers that occurred by electronic requests initiated by scammers via online banking or mobile app are covered by the EFTA. They are electronic instructions that do not come from the actual consumers who are Citi account holders and under the EFTA are unauthorized.

making or guidance from the CFPB, though Congressional action would be faster and less subject to challenge.

**RESPONSE TO WRITTEN QUESTION OF SENATOR BRITT
FROM PAUL BENDA**

Q.1. As part of the bipartisan Taxpayer First Act of 2019, Congress required the Internal Revenue Service (IRS) to implement updates to modernize its Income Verification Express Service (IVES). The IVES system permits financial services providers to submit Form 4506-C to verify a credit applicant's income, helping to prevent fraud and ensure accurate underwriting.

On January 2, 2024, the IRS issued a notice that it intends to limit the use of the entire IVES system to only mortgage loan applications. Given that the IVES has been a useful tool in combating fraud, including in helping to identify whether a credit card applicant is a legitimate person, it seems short-sighted to restrict access to this tool for financial institutions working to combat fraud. The IRS was directed by Congress to modernize the system so that it would no longer be fax machine-based and instead could be accessed electronically. However, the IRS decided to also limit access to this useful system. This is counterintuitive, financial systems should have every possible tool at their disposal to fight fraud.

Could you share your thoughts on this decision by the IRS to limit financial services providers' access to a useful and effective fraud prevention tool?

A.1. ABA appreciates your attention to this important matter. The use of tax transcripts as a mechanism to obtain income and asset information from consumers is crucial to bank efforts on multiple fronts, including accurate income verification, fraud detection and continued efforts to propel real-time application innovation programs that benefit consumers and are desired by the industry.

The Income Verification Express Service (IVES) program provides financial institutions direct access to tax transcripts and is currently used by consumer and commercial lenders and Government agencies such as the Small Business Administration (SBA) to confirm the income of a borrower during the processing of a loan application. Lenders request tax transcripts from borrowers for various reasons:

- *Income Verification:* Tax transcripts provide an official record of the borrower's income, helping lenders verify the accuracy of income stated on loan applications.
- *Accuracy and Consistency:* Comparing loan application data with tax transcripts ensures income consistency and accuracy.
- *Fraud Prevention:* Tax transcripts aid in detecting and preventing income fraud by confirming reported income matches IRS records.
- *Regulatory Compliance:* Obtaining tax transcripts may be mandated by regulatory authorities to ensure compliance with lending regulations and guidelines.

- *Risk Assessment*: Reviewing tax transcripts helps assess a borrower's financial stability and ability to repay loans, indicating consistent income over time.

A most important benefit of the IVES program is that it guarantees direct access to a primary source document—the tax transcript—and such access is crucial in validating the legitimacy of information received. For instance, IVES will be used to verify a consumer's W2 form electronically when making a loan, allowing the bank to verify a consumer's self-reported income. Using primary sources such as IVES serves as a highly effective disincentive to fraudulent behavior because: (a) applicants cannot access documents that can be potentially altered, and (b) bank staff are able to immediately review and recognize inconsistencies in documents that are standardized and therefore easily reviewed for inconsistencies or defects. Our bank operations professionals stress that the absence of current abilities to verify tax returns in commercial and residential lending originations would affirmatively invite illicit actors to commit financial crimes—in short, if potential fraudsters know that application submissions cannot be verified with primary sources, it will trigger new avenues for illicit schemes.

The most important types of information that would be denied to financial institutions if IRS were to limit financial services providers' access to IVES include the following:

- *Gross Income*: The total income reported by the taxpayer, including wages, salaries, tips, and other sources of income. This information is crucial for income verification and assessing the borrower's ability to repay the loan.
- *Adjusted Gross Income (AGI)*: AGI represents gross income minus specific deductions, providing a more accurate reflection of the borrower's financial situation. Lenders often use AGI for income verification and regulatory compliance purposes.
- *Taxable Income*: Taxable income is the amount of income subject to taxation after deductions and exemptions. It helps lenders assess the borrower's financial stability and repayment capacity.
- *Tax Filing Status*: The taxpayer's filing status (e.g., single, married filing jointly, married filing separately) provides context for interpreting income information and ensures regulatory compliance.
- *Tax Year*: The tax year for which the transcript is issued is essential for lenders to match the income information with the borrower's application timeline and verify recent financial status.

These are key pieces of information that enable lenders to conduct essential income verification, fraud prevention, and regulatory compliance checks while still maintaining the integrity of the lending process.

**RESPONSE TO WRITTEN QUESTION OF SENATOR BUTLER
FROM JOHN BREYALT**

Q.1. Ann Booras, a teacher from East Bay had \$20,000 snatched from her by a scammer who called her, pretending to be from her bank, Wells Fargo, and claimed to be investigating fraud. She was asked to wire \$20,000 and \$5,000 from her account; the wire for transfer for \$5,000 was recovered but the larger sum was not. Sadly, Ann’s story of wiring her hard-earned money to criminals is not an isolated one. When she received the scam call, her caller ID even said Wells Fargo bank. Ann realized what had happened and contacted Wells Fargo, her request for reimbursement was denied on the grounds that she had authorized the transaction.

Mr. Breyalt, as scammers use technology to fool consumers, what are financial institutions doing to inform their customers about these scams?

A.1. Financial institutions typically do try to put in place procedures and educational materials to mitigate these scams. For example, the American Bankers Association has their #BanksNeverAskThat campaign.¹ Many banks also train their tellers to spot potential red flags for fraud and put warnings on their websites, materials, and payment apps. However, at the National Consumers League we have limited insight into the full extent of measures banks may take to inform their customers about scams.

Consumer education alone will not make a meaningful impact in preventing the tens of billions of dollars lost to fraud each year. We have found that scammers quickly recognize and adapt to the warnings that banks put in place. Many victims report that the criminals coached them through the process, guiding them to ignore and bypass the banks’ advisories. Any strategy to eliminate fraud will be ineffective if it relies on educational programming while failing to establish incentives for financial institutions to implement greater antifraud measures. We must stop scams before they can be executed in the first place. Banks are the parties in the financial system best positioned to accomplish this.

¹American Bankers Association. “ABA and America’s Banks Launch 4th Annual #BanksNeverAskThat Consumer Awareness Campaign”, Press release. (October 2, 2023) Online: <https://www.aba.com/about-us/press-room/press-releases/banksneveraskthat-2023-launch>.

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

Statement for the Record

Bank Policy Institute

Senate Committee on Banking, Housing and Urban Affairs Hearing: “Examining Scams and Fraud in the Banking System and Their Impact on Consumers”

February 1, 2024

The Bank Policy Institute welcomes the opportunity to provide input on today’s Senate Banking Committee hearing on “Examining Scams and Fraud in the Banking System and Their Impact on Consumers.” Today’s hearing examines a critical issue for the U.S. banking system and its customers. Addressing fraud and scams in the financial system has taken on increasing urgency as threats proliferate and scam tactics become more sophisticated. While banks already employ some of the most robust defenses among critical infrastructure sectors, they are constantly innovating to protect their customers from fraudulent activity.

Fraud management is an important priority for all participants in the global financial system, as well as a concern for the customers the financial system serves. The Bank Policy Institute – along with its technology policy division BITS, which has been working with banks for nearly three decades on critical fraud challenges – has facilitated efforts by stakeholders from industry and government to combat fraud. For example, BPI-led groups tackle challenges and help advance the industry’s efforts to combat fraud; examples of this work include developing customer education programs on fraud, identifying effective practices for detecting fraud, partnering to implement fraud intelligence sharing services and strategies to mitigating check fraud, among many other actions.

The issue of combating scams and fraud is a nationwide challenge, one in which banks invest substantial resources to protect their customers and their customers’ money. Such a far-reaching challenge demands comprehensive, multi-dimensional solutions. Collaboration across the private and public sectors is crucial to help protect American consumers from criminals who seek to defraud them.

In recent years, the financial system has experienced a rise in fraud attacks due to the proliferation of real-time digital payments, increased availability of stolen access credentials, increased instances of identity theft, a substantial increase in the sophistication of scams and social engineering, and a surge in check fraud. Banks continue to invest in protecting their customers, including extensive investment in staff and technology to bolster their fraud defenses. A Juniper Research report on online payment fraud found merchants and financial services organizations were expected to spend \$9.3 billion per year on fraud detection and prevention tools by 2022¹.

Criminals have increased the speed and sophistication of their attacks. Fraud losses for banks and consumers are also increasing. Consumers reported losing almost \$8.8 billion to scams and fraud in 2022, up 30 percent over 2021’s losses, according to data from the Federal Trade Commission. The rising cost of these crimes is staggering; as a comparison, in 2020 Americans lost \$3.5 billion to fraud, including identity theft².

¹ [The banking industry’s multi-billion dollar fraud problem—and how to solve it \(bpi.org\)](https://www.bpi.org/the-banking-industry-s-multi-billion-dollar-fraud-problem-and-how-to-solve-it)

² [New FTC Data Show Consumers Reported Losing Nearly \\$8.8 Billion to Scams in 2022 | Federal Trade Commission](https://www.ftc.gov/news-events/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-to-scams-in-2022)

Fraud and its impact on consumers will continue to grow in the absence of a more strategic, coordinated partnership between the public and private sectors. To better address the issues, some key policy solutions should be pursued:

1. Appoint a federal director to take ownership on fraud and appoint a single federal agency as the national champion to lead and coordinate the fight against fraud.

Currently there is no single leader or agency explicitly responsible for addressing the growing fraud issues across the nation; therefore, there is no singular, coordinated effort or national strategy targeting this issue. There are pockets of work occurring in various agencies, including the Federal Trade Commission, the Consumer Protection Financial Bureau, and the Department of Treasury, but due to this fragmentation and lack of a holistic approach, none is comprehensively tackling the issue.

This agency would need to establish a cross-sector task force to facilitate a public-private partnership to pursue these goals. This multisectoral effort should include the relevant federal and state financial regulators, consumer protection agencies, law enforcement, financial institutions, telecoms, trade associations, consumer and privacy advocates, and other stakeholders.

2. Equip the U.S. government to play a leading role in helping educate consumers on how to protect themselves.

Equipping consumers with the knowledge to recognize scams is pivotal, and in many ways the true first line of defense. Banks have consistently focused on educating their customers about the evolving fraud landscape and the importance of vigilance. This work, often done with other organizations such as AARP, could still benefit from public sector partnership to reach an even larger audience. Collaborative private sector education efforts include providing information on common fraud schemes, safe online practices, and guidance on recognizing suspicious activities.

A government-led national public awareness campaign, in partnership with industry, to educate consumers on emerging scams and fraud activity proactively and persistently has proven effective in other countries. By raising public awareness and promoting collective responsibility in the fight against fraud, banks and regulatory bodies can better shield the financial ecosystem from threats.

3. Promote and enable data and intelligence sharing between institutions and ensure laws are in place that support sharing of information.

Sharing of intelligence, fraud-related data and key indicators of fraud plays a crucial role in reducing fraud by facilitating the exchange of relevant information among different entities, such as government agencies, financial institutions, businesses, and law enforcement, that may otherwise be siloed from each other. This collaborative approach enhances the ability to identify, prevent and respond to fraud more effectively. Ensuring that banks and government have the means to share intelligence without hindrance is critical to addressing fraud events in a timely manner.

An example of effective efforts to improve collaboration is the Bank Policy Institute | BITS strategy on fraud intelligence, which has established a three-pillar strategy to advance fraud sharing across the industry. The objective of this initiative is to enhance the financial industry's intelligence and information sharing capabilities through the strategic development of three key pillars:

- 1) **Fraud Data Sharing:** Near-real-time fraud information sharing of account and transaction data associated with bad actors and/or fraudulent accounts.
- 2) **Fraud Intelligence Sharing:** Industry-wide timely sharing of fraud types, trends, and major changes in fraud tactics – at scale – from an authoritative source.
- 3) **Law Enforcement Collaboration:** Aggregation, analysis and packaging of cases and coordination with law enforcement against large-scale or organized fraud actors.

This aims to create a resilient, integrated, and effective strategy for managing and preventing financial fraud. This strategy includes engagement with BPI's member banks, the American Bankers Association, the FS-ISAC, and Early Warning Systems (the operator of Zelle instant payments) to deliver upon this strategy over a multi-year basis. A key deliverable of the fraud data sharing pillar is the American Bankers Association's work to share bad beneficiary data to help identify possible fraudulent beneficiaries across financial institutions. This solution is set to pilot with an initial group of banks in the first half of 2024. In addition, as part of the fraud intelligence pillar, the FS-ISAC is building out its capabilities for better and more actionable sharing of fraud intelligence to gather fraud schemes, analyze systematic and qualitative input from member institutions and develop actionable advisories.

4. **Ensure all sectors are properly held accountable to help mitigate fraud and scams.**

Cross-sector involvement, including the telecom industry and social media platforms, is necessary to properly fight digital fraud. A digital fraud scheme is usually complex and coordinated, spanning a large ecosystem of cross-sector players who all have an opportunity to detect and prevent attacks from occurring. To effectively address this fraud, multiple sectors must participate in cross-sector initiatives aimed at preventing attacks against consumers. It is critical that all participating sectors feel compelled and accountable to help protect customers. Banks alone cannot address the problem without collaboration from other industries.

According to the U.S. Federal Trade Commission, in 2022 there were 2.4 million consumers who reported being a victim of fraud. It was also reported that consumers lost \$1.2 billion because of fraudulent scam activity involving social media. When scammers contacted users by phone, the average loss was \$1,400 per user. This data highlights the importance of cross-sector collaboration in addressing growing digital fraud trends, along with importance of mitigating the threat as close to the initiation of a call from a scam "center" as possible.

It is imperative to encourage the telecom industry, the social media industry, and Big Tech platforms to continue to participate in partnership with the banking industry to help address the scams and social engineering threats facing American consumers.

5. **Increase law enforcement resources needed to prosecute fraudsters and ensure the sentences for fraud are effective deterrents.**

Much of the fraud being committed today is a result of organized groups: large-scale rings, organized crime, gangs, and nation-state-sponsored attackers. To effectively disrupt the groups committing this fraud, law enforcement agencies need the appropriate fraud-fighting resources. Agencies at all levels need to be provided with the resources needed to investigate and prosecute fraud.

In addition, it is important that the appropriate sentences are in place in fraud prosecutions to ensure criminals are deterred from committing such offenses.

6. Modernize payments by promoting the use of secure electronic payment methods and reduced use of paper checks.

Check fraud has risen at alarming rates over the last few years. In 2022 banks reported about 680,000 cases of check fraud, nearly double what they reported in 2021.³ Experts predicted that check fraud losses would exceed \$24 billion in 2023 and that losses will continue to grow⁴. Legacy payment methods, such as checks, have significantly higher fraud rates than electronic payments. Electronic payments bring opportunities for more controls to be introduced. Electronic payment methods, like Zelle, offer consumers a secure alternative to paper-based payments like checks.

Using Zelle, all funds transferred using Zelle remain in, and are transferred between, insured deposit accounts, as the Zelle Network is a messaging service between participating financial institutions (and does not hold or transfer funds or maintain accounts). More than 99.9 percent of Zelle transactions have been completed without a report of fraud or scam, which is a direct result of the robust array of consumer protection measures Zelle and its financial institution owners utilize (and this rate continues to improve). Zelle enables the use of additional protections that checks cannot employ, such as strong multifactor authentication prior to submitting a payment, real-time transaction limits, real-time communication and customer education, abnormal activity monitoring and real-time alerts or activity notifications.

Additionally, we believe modernizing regulations, such as Regulation CC - Availability of Funds and Collection of Checks will help banks to better mitigate and respond to check fraud. Areas that should be addressed around this regulation include clarification of funds availability and hold time rules along with addressing the exploitation of mandates around check deposits/duplicate presentment especially with the increase in use of remote deposit capture technologies.

7. Eliminate screen scraping as a way for third parties to access banking information.

An additional area that should be considered when discussing fraud control is the growth of open banking and the additional risks it brings to the ecosystem, particularly when third parties continue to use credential-based access and screen scraping to access consumer financial data.

The banking industry has been working for years to develop technical solutions that enable consumer access to financial data while providing sufficient data protection. The financial services industry has collectively advanced the marketplace towards common technical standards for the secure access of consumer-permissioned data. For example, FDX, a cross-section of banks, third-party fintechs, data aggregators, consumer groups, and other financial industry groups have aligned around a common API to standardize the security and authentication for data transfer.⁵ Through the development, adoption and constant improvement of the FDX API, FDX and its members have made

³ [FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail | FinCEN.gov](#)

⁴ [Check Fraud, First Party Fraud to Rise in 2023 \(bankinfosecurity.com\)](#)

⁵ See Financial Data Exchange website at <https://financialdataexchange.org/>.

significant progress transitioning from credential-based screen scraping to this more secure alternative, with over 65 million consumer accounts using the FDX API as of fall 2023.⁶

Despite the industry's progress, screen scraping remains a widely used method for accessing not only payments account data, but also other types of data that are less accessible through a bank account (such as payroll data), thus enabling data harvesting of credentials to continue. BPI has long argued that screen scraping, and credential-based access should be prohibited at a certain future date for the following reasons⁷. Credential-based screen scraping creates opportunities for malicious actors to gain access to a consumer's accounts at a financial institution and commit fraud, or even take over the consumer's account. It also creates unnecessary risk by having authentication information, such as username and password stored in databases by each aggregator company that leverages screen scraping, substantially increasing the attack surface for criminals to try to steal this information.

The Bank Policy institute, along with our member banks, recognizes the importance of combating fraud for consumers and is advocating for changes that protect consumers from fraud, such as secure data-sharing practices, enhanced intelligence-sharing between the public and private sectors and regulatory oversight of nonbank fintechs and aggregators. We are encouraged that the Committee is examining this topic of fraud and look forward to engaging further on this topic.

⁶ See FDX Press Release: "Financial Data Exchange (FDX) Reports 65 Million Consumer Accounts Use FDX API" (October, 5, 2023), available at [https://financialdataexchange.org/FDX/News/Press-Releases/Financial%20Data%20Exchange%20\(FDX\)%20Reports%2065%20Million%20Consumers%20Use%20FDX%20API.aspx](https://financialdataexchange.org/FDX/News/Press-Releases/Financial%20Data%20Exchange%20(FDX)%20Reports%2065%20Million%20Consumers%20Use%20FDX%20API.aspx) (last accessed December 24, 2023). Almost all FDX financial institution members are using or plan to use the FDX API.

⁷ See, e.g., BPI comment in response to the High-Level Summary and Discussion Guide of Outline of Proposals and Alternatives Under Consideration for SBREFA: Required Rulemaking on Personal Financial Data Rights issued by the Consumer Financial Protection Bureau pursuant to Section 1033 of the Dodd-Frank Act (Jan. 25, 2023); See also BPI-TCH response to the Proposed Required Rulemaking on Personal Financial Data Rights issued by the Consumer Financial Protection Bureau pursuant to section 1033 of the Dodd-Frank Act (Dec. 29, 2023).



January 31, 2024

The Honorable Sherrod Brown
Chairman
Senate Banking, Housing and Urban Affairs
Committee
Washington, D.C. 20515

The Honorable Tim Scott
Ranking Member
Senate Banking, Housing and Urban Affairs
Committee
Washington, D.C. 20515

Dear Chairman Brown and Ranking Member Scott:

On behalf of the American Financial Services Association (AFSA)¹, I am writing to commend you for conducting the hearing, “Examining Scams and Fraud in the Banking System and Their Impact on Consumers.”

As fraudulent activities occur within the financial services and banking community, I write regarding the increasing threat credit repair scams pose to consumers and the credit markets. Credit repair organizations exploit the most vulnerable Americans and inundate creditors and credit bureaus with meritless and duplicative claims that information in a credit report is inaccurate. These activities jam the credit reporting system with illegitimate claims that divert resources from authentic consumer disputes and cost Americans exorbitant amounts of money for no actual value.

Before the Senate Banking Committee last year, the Consumer Financial Protection Bureau (CFPB) Director Rohit Chopra testified that the Bureau has taken “a number of enforcement actions” against so-called credit repair services.² Additionally, during a recent hearing before the House Financial Services Committee, Director Chopra voiced concerns about credit repair entities and noted, “They [CROs] might be targeted using very sensitive information about people...” However, legislation is needed to curtail the harm these companies are causing consumers.³

We encourage the committee to introduce bipartisan legislation to modernize the Credit Repair Organizations Act (CROA), which was passed in 1996. Amending the CROA would help to prevent credit repair firms from inducing consumers to pay for services that are not provided and from clogging dispute systems with false claims.

As the Federal Trade Commission and CFPB have warned, CROs take advantage of consumers who are trying to improve their financial situation through potentially misleading messaging. Often without the consumer’s knowledge, these firms use bulk mail to deploy identical form letters that fail to provide a specific explanation of a dispute or supporting documentation. Sometimes it is impossible to tell whether the consumer or the CRO sent the dispute on the consumer’s behalf or even with the consumer’s permission.

¹ Founded in 1916, AFSA is the national trade association for the consumer credit industry, protecting access to credit and consumer choice. AFSA members provide consumers with many kinds of credit, including direct and indirect vehicle financing, traditional installment loans, mortgages, payment cards, and retail sales finance.

² The Senate Banking, Housing, and Urban Affairs Committee: [The Consumer Financial Protection Bureau’s Semi-Annual Report to Congress](#) (June 13, 2023)

³ The House Financial Services Committee: [The Semi-Annual Report of the Bureau of Consumer Financial Protection](#) (November 29, 2023)

Thank you for your attention to this important issue. We welcome the opportunity to further engage on this matter. Please contact me with any questions at 202-776-7300 or cwinslow@afsamail.org.

Sincerely,

A handwritten signature in cursive script that reads "Celia Winslow".

Celia Winslow
Senior Vice President
American Financial Services Association



January 31, 2024

The Honorable Sherrod Brown
Chairman
Senate Committee on Banking, Housing, and
Urban Affairs
534 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Tim Scott
Ranking Member
Senate Committee on Banking, Housing,
and Urban Affairs
534 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Brown and Ranking Member Scott:

The Consumer Bankers Association (CBA) submits the following comments for the hearing titled "Examining Scams and Fraud in the Banking System and Their Impact on Consumers." We appreciate the Committee's attention to these issues. CBA is the voice of the retail banking industry whose products and services provide access to credit to millions of consumers and small businesses. Our members operate in all 50 states, serve more than 150 million Americans, and collectively hold two-thirds of the country's total depository assets.

Some of the most significant threats facing consumers today are peer-to-peer payments (P2P) scams, check fraud, and synthetic identity fraud—but the landscape constantly evolves, and new threats emerge regularly. Over the last several years, the banking industry has undertaken significant steps to identify and counter P2P payments scams in a way that does not chill innovation while simultaneously enhancing the consumer experience. One of the most difficult instances of P2P scams to address are cases when scammers trick consumers into initiating transactions, because unlike credit cards, checks, or traditional bank transfers, the instant, non-revokable nature of these payments makes them very difficult to stop once a transaction is initiated.

While significant progress has been made by banks in addressing P2P payments scams, check fraud and synthetic identity fraud have resurged. According to the Financial Crimes Enforcement Network (FinCEN), instances of check fraud filed by banks nearly doubled from 2021 to 2022. Last year, FinCEN issued an alert highlighting the unique risk of mail theft-related check fraud. One common form of mail theft-related check fraud is check washing, which is when a criminal steals a signed check from a postal box, then uses chemicals to alter the check information before depositing it.¹

The Identity Theft Resource Center (ITRC) predicts that 2024 will experience an increase of identity crimes, especially impersonation and synthetic identity fraud.² The ITRC has noted there has been an unprecedented number of data breaches in 2023, with 733 total data compromises in Q3 2023 alone. Criminals may use compromised information to either open new accounts or gain control over existing accounts. Identity verification efforts will take on an even greater level of importance to counter this type of fraud.

Banks have been on the front lines dedicating enormous resources—billions of dollars and

¹ <https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20Check%20Fraud%20FINAL%20508.pdf>

² <https://www.idtheftcenter.org/post/2024-predictions-more-id-fraud-privacy-laws-ai-concerns/>



thousands of hours by dedicated teams each year– to fight fraud and scams and continue to enhance these efforts in response to increasingly prevalent and sophisticated methods used by criminals, many of whom operate under state sponsored or organized crime rings. Some of these industry efforts include working to prevent, detect, and mitigate scams through education, and deploying advanced technologies to monitor, authenticate, and reduce risk, as well as consistently evolving and adapting customer protection measures, including real-time safety notifications and alerts, to address the continually changing nature of these threats.

But banks cannot wage the battle against fraud and scams alone. CBA calls on the Consumer Financial Protection Bureau (CFPB) to work collaboratively with other financial regulators, law enforcement agencies, and the private sector on a cross-industry basis (including telecommunications, credit reporting, non-bank financial and technology providers, and financial institutions) to educate consumers on fraud and scams and how to avoid them. One of the most meaningful ways the Bureau can partner with the industry is by using the substantial Civil Penalty Fund balance to conduct broader consumer education, which is one of the six “primary functions” of the Bureau and is essential for consumer protection. Aside from these helpful measures, the CFPB should ensure any action it takes would not run contrary to any prudential regulatory requirement and make it more difficult for banks to prevent fraud and scams.

The Senate’s Financial Services and General Government Appropriations bill report contains helpful language on fraud and scams,³ and acknowledges that fraudsters and scammers have become more sophisticated at using both private sector and government systems to harm consumers. The report urges the Treasury Department to engage in a public-private partnership, in coordination with federal and state regulators, law enforcement, financial institutions, trade associations, and consumer advocates to combat fraud and scams. This effort would encourage information sharing, best practices, and education of the general public. CBA supports this report language and urges Congress to maintain it in final appropriations legislation.

Thank you for considering our views. CBA stands ready to work with regulators, legislators, consumers, and the broader industry as a whole to win the battle against fraud and scams.

Sincerely,

A handwritten signature in black ink, appearing to read "L. Johnson".

Lindsey D. Johnson
President and CEO
Consumer Bankers Association

³ <https://www.congress.gov/118/crpt/srpt61/CRPT-118srpt61.pdf#page=10>



Check Fraud: The Community Bank Perspective

The Independent Community Bankers of America, representing community banks across the nation with nearly 50,000 locations, appreciates the opportunity to provide this statement for the record for today's hearing: "Examining Scams and Fraud in the Banking System and Their Impact on Consumers." ICBA would like to use this opportunity to highlight the recent surge in check fraud and its impact on community bank customers.

At the outset, ICBA would like to acknowledge the important work of one of our state affiliate associations, the Community Bankers Association of Illinois (CBAI), who was early in identifying and documenting the increasing occurrences of check fraud and its resulting impact on CBAI members and their customers. In January of 2023, CBAI surveyed its members and found that the scope and cost of the problem to community banks is significant and growing.¹

When a customer falls victim to fraud, a community bank's primary goal is to make the customer whole through recovery of funds. Additionally, community banks conduct thorough investigations on such incidences to ensure the fraud does not continue. Community banks assist law enforcement to identify and understand specific crimes and trends with the hope of protecting all consumers from similar incidents.

Fraud Rooted in Rampant Mail Theft

Check fraud occurs when checks are stolen and the payee and possibly the amount are altered, using advanced "check washing" techniques. The check is cashed or deposited, typically into a fraudulent account created for this purpose. Funds are withdrawn or transferred before the fraud is discovered, and the criminals escape with the proceeds.

Check fraud has become highly sophisticated in recent years with large scale operations, sale of stolen checks and mailbox keys on the dark web, and the recruitment and training of "walkers" who are paid to deposit or cash washed checks using false identification. According to FinCEN, Suspicious Activity Reports (SARs) related to check fraud increased from 350,000 in 2021 to more than 680,000 in 2022.²

By far the biggest source of stolen checks is the United States Postal Service. Checks are stolen from consumer mailboxes as well as from USPS facilities. During the Covid pandemic, USPS became a rich source of checks for criminals as government benefits were distributed through the mail. Effective mail security is a critical, though not exclusive, part of the solution to the problem of check fraud. With better security, check fraud would be significantly reduced.

¹ According to a CBAI survey of its members, 60 percent of respondents said that they had experienced problems obtaining reimbursement for fraudulent returns in the past year. An extrapolation of these results nationwide would suggest that some 2,800 community banks are experiencing this problem. The CBAI respondents further indicated that large banks and credit unions were the source of the problem. On average, respondents had five unresolved checks awaiting reimbursement for an average of \$23,000 each, and these checks had been outstanding for an average of five months. A nationwide extrapolation would suggest that 19,600 are unresolved with an estimated total value of \$65 million. 65 percent of respondents said they had had no response from the large banks of first deposit in their efforts to obtain reimbursement. Respondents' losses averaged \$30,000 in 2022. Extrapolation would suggest that nationwide community bank losses are approximately \$94 million.

² <https://www.fincen.gov/news/news-releases/fincen-alert-nationwide-surge-mail-theft-related-check-fraud-schemes-targeting>

Bank Cooperation Is Critical to Consumer Reimbursement

Check fraud typically involves two banks: the drawee bank on which the check is issued and at which the customer's funds ultimately reside, and the "bank of first deposit" at which the criminal deposits or cashes the fraudulent check. Following deposit, the bank of first deposit requests a transfer of funds from the drawee bank to cover the deposit.

The fraud is usually discovered when the owner of the stolen check, be it a consumer or a business, flags the check as fraudulent and requests reimbursement. The drawee bank reimburses its customer and seeks reimbursement from the bank of first deposit, where liability for the fraud resides.

The Uniform Commercial Code (UCC) provides that the bank of first deposit is liable. This makes sense because that bank is the entry point of the fraud and is in the best position to prevent it by screening out the deposit, or better yet, deterring the creation of a fraudulent account to accept a deposit. Liability creates an incentive for the party that is best positioned to prevent the fraud to do so. Though liability is unambiguous, there is no effective enforcement mechanism outside of costly litigation. Resolution depends on willing cooperation between the banks.

Community banks are frustrated because large banks or credit unions of first deposit are often nonresponsive when fraud is discovered by a community bank. Coordination between banks is an important step for quickly understanding and resolving instances of check fraud. Any lack of consistent and timely cooperation slows the investigation and can lead to additional instances of fraud.

Opening of Fraudulent Accounts Deserves More Scrutiny

Check fraud is frequently enabled by fraudulent accounts opened at large banks and credit unions with stolen credentials. These accounts are used for the deposit of fraudulent or altered checks. Account opening at all financial institutions is subject to the Bank Secrecy Act's (BSA) Know Your Customer (KYC), and Customer Identification Program (CIP) rules, which are expressly designed to prevent the use of assumed identities to open accounts. Because community banks exercise due diligence and do not rely on generic and anonymous account opening processes that are easily manipulated by fraudsters, they are less vulnerable to account opening fraud.

Community Banks Are Part of the Solution

Community banks are uniquely positioned to prevent, detect, and mitigate customer fraud. They take this role very seriously. As relationship bankers, community banks know their customers in real and meaningful ways. These relationships promote access to services, prevent fraud on the front lines, and give customers a personal resource when they fall victim to fraud or scams.

Recently, a community bank member told us of a customer that had been tricked into wiring a significant amount of money to a fraudster. Upon realizing they were scammed, the customer contacted the community bank for help. The community bank, which employs former police officers with expertise in financial crime, acted immediately and was able to recover the money for the customer. This could only have been achieved by a financial institution that knows its customers, prioritizes needs, and is willing to act rapidly.

Customer education, whether in person, at branches, or online is a critical component of fraud prevention and mitigation. The most vulnerable customers benefit the most from the face-to-face interactions they find in a community bank. When fraud occurs, preexisting relationships allow for an immediate response.

Under certain circumstances, a community bank may take steps to make defrauded customers whole before the bank of first deposit has reimbursed the customer for the loss. Community banks often choose to absorb these costs because they prioritize long-term customer relationships.

While community banks are a critical part of the solution, they cannot do it alone. USPS must do more to prevent mail theft. Cooperation among financial institutions is needed to prevent the opening of fraudulent accounts, mitigate fraud, and promptly reimburse victims, and the largest institutions of first deposit must take steps to promptly respond and be held accountable.

ICBA Supports and Partners with Community Banks and other Stakeholders

ICBA leads an industry fraud work group comprised of regulators, law enforcement, trade associations, and other government stakeholders such as the U.S. Postal Inspection Service to share information, identify best practices, and discuss emerging approaches to combatting check and other types of fraud. This group has built a considerable record of success in creating cooperation among entities.

ICBA continues to engage with its members to explore different mechanisms for collaborating to prevent, detect, and mitigate fraud. ICBA also values its ongoing work and relationships with members of Congress and federal agencies. We will continue to partner with these important stakeholders as we collectively work to reduce the burden of check fraud.

Thank you for convening today's hearing to examine fraud in the banking system and its impact on consumers. We appreciate the opportunity to provide community bank perspectives and hope to provide ongoing input as solutions are developed.