

FOLLOWING THE MONEY: TOOLS AND TECHNIQUES TO COMBAT FRAUD

HEARING BEFORE THE SUBCOMMITTEE ON NATIONAL SECURITY, ILLICIT FINANCE, AND INTERNATIONAL FINANCIAL INSTITUTIONS OF THE COMMITTEE ON FINANCIAL SERVICES U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

APRIL 1, 2025

Serial No. 119–12

Printed for the use of the Committee on Financial Services



www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

59–941 PDF

WASHINGTON : 2025

HOUSE COMMITTEE ON FINANCIAL SERVICES

FRENCH HILL, Arkansas, *Chairman*

BILL HUIZENGA, Michigan, <i>Vice Chairman</i>	MAXINE WATERS, California, <i>Ranking Member</i>
FRANK D. LUCAS, Oklahoma	SYLVIA R. GARCIA, Texas, <i>Vice Ranking Member</i>
PETE SESSIONS, Texas	NYDIA M. VELÁZQUEZ, New York
ANN WAGNER, Missouri	BRAD SHERMAN, California
ANDY BARR, Kentucky	GREGORY W. MEEKS, New York
ROGER WILLIAMS, Texas	DAVID SCOTT, Georgia
TOM EMMER, Minnesota	STEPHEN F. LYNCH, Massachusetts
BARRY LOUDERMILK, Georgia	AL GREEN, Texas
WARREN DAVIDSON, Ohio	EMANUEL CLEAVER, Missouri
JOHN W. ROSE, Tennessee	JAMES A. HIMES, Connecticut
BRYAN STEIL, Wisconsin	BILL FOSTER, Illinois
WILLIAM R. TIMMONS, IV, South Carolina	JOYCE BEATTY, Ohio
MARLIN STUTZMAN, Indiana	JUAN VARGAS, California
RALPH NORMAN, South Carolina	JOSH GOTTHEIMER, New Jersey
DANIEL MEUSER, Pennsylvania	VICENTE GONZALEZ, Texas
YOUNG KIM, California	SEAN CASTEN, Illinois
BYRON DONALDS, Florida	AYANNA PRESSLEY, Massachusetts
ANDREW R. GARBARINO, New York	RASHIDA TLAIB, Michigan
SCOTT FITZGERALD, Wisconsin	RITCHIE TORRES, New York
MIKE FLOOD, Nebraska	NIKEMA WILLIAMS, Georgia
MICHAEL LAWLER, New York	BRITTANY PETTERSEN, Colorado
MONICA DE LA CRUZ, Texas	CLEO FIELDS, Louisiana
ANDREW OGLES, Tennessee	JANELLE BYNUM, Oregon
ZACHARY NUNN, Iowa	SAM LICCARDO, California
LISA McCLAIN, Michigan	
MARIA SALAZAR, Florida	
TROY DOWNING, Montana	
MIKE HARIDOPOLOS, Florida	
TIM MOORE, North Carolina	

Ben Johnson, *Staff Director*

SUBCOMMITTEE ON NATIONAL SECURITY, ILLICIT FINANCE, AND INTERNATIONAL FINANCIAL INSTITUTIONS

WARREN DAVIDSON, Ohio, *Chairman*

ZACHARY NUNN, Iowa, <i>Vice Chairman</i>	JOYCE BEATTY, Ohio, <i>Ranking Member</i>
FRANK D. LUCAS, Oklahoma	JOSH GOTTHEIMER, New Jersey
PETE SESSIONS, Texas	JUAN VARGAS, California
ANDY BARR, Kentucky	BILL FOSTER, Illinois
ROGER WILLIAMS, Texas	VICENTE GONZALEZ, Texas
YOUNG KIM, California	RITCHIE TORRES, New York
ANDREW OGLES, Tennessee	SEAN CASTEN, Illinois
LISA McCLAIN, Michigan	SAM LICCARDO, California
MARIA SALAZAR, Florida	

C O N T E N T S

Tuesday, April 1, 2025

OPENING STATEMENTS

	Page
Hon. Warren Davidson, Chairman of the Subcommittee on National Security, Illicit Finance and International Financial Institutions, a U.S. Representative from Ohio	1
Hon. Joyce Beatty, Ranking Member of the Subcommittee on National Security, Illicit Finance and International Financial Institutions, a U.S. Representative from Ohio	3

STATEMENTS

Hon. Maxine Waters, Ranking Member of the Financial Services Committee, a U.S. Representative from California	4
---	---

WITNESSES

Mr. Darrin McLaughlin, Executive Vice President and Chief BSA/AML & Sanctions Officer, Flagstar Bank, on behalf of the American Bankers Association (ABA)	5
Prepared statement	7
Ms. Jacqueline Burns Koven, Head of Cyber Threat Intelligence, Chainalysis ..	17
Prepared statement	19
Mr. Jeff Brabant, Vice President, Federal Government Relations, National Federation of Independent Business (NFIB)	30
Prepared statement	32
Ms. Kathy Stokes, Director, Fraud Prevention Programs, on behalf of the American Association of Retired Persons (AARP)	38
Prepared statement	40

APPENDIX

MATERIALS SUBMITTED FOR THE RECORD

Hon. Maxine Waters:	
Financial Accountability and Corporate Transparency (Fact) Coalition	76
CFP Submissions:	
CFP Board Letter	79
How to Protect Yourself Against Scams	81
Protecting Your Elderly Parent from Financial Fraud	85

RESPONSES TO QUESTIONS FOR THE RECORD

Written responses to questions for the record from Representative Maxine Waters	
Ms. Jacqueline Burns Koven	88
Ms. Kathy Stokes	90

LEGISLATION

H.R. 1799, the Financial Reporting Threshold Modernization Act	93
H.R. 425, the Repealing Big Brother Overreach Act	96
H.R. ———, the Repealing Big Brother Overreach Act	99

IV

	Page
H.R. ———, the Guarding Unprotected Aging Retirees from Deception (GUARD) Act	101
H.R. ———, the Stop Foreign Scammers Act of 2025	112
H.R. ———, the Accountability through Confirmation Act	115
H.R. ———, the Bringing Real Accountability Via Enforcement (BRAVE) in Burma Act	117
H.R. ———, the Financial Access Improvements Act	124
H.R. ———, the Foreign Affiliates Sharing Pilot Program Extension Act	128
H.R. ———, the Kleptocracy Asset Recovery Rewards Program Act	130

FOLLOWING THE MONEY: TOOLS AND TECHNIQUES TO COMBAT FRAUD

Tuesday, April 1, 2025

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY,
ILLICIT FINANCE, AND
INTERNATIONAL FINANCIAL INSTITUTIONS,
COMMITTEE ON FINANCIAL SERVICES,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:04 a.m., in room 2128, Rayburn House Office Building, Hon. Warren Davidson [chairman of the subcommittee] presiding.

Present: Representatives Davidson, Lucas, Sessions, Williams of Texas, Kim, Ogles, McClain, Salazar, Beatty, Vargas, Foster, Gonzalez, Casten, Liccardo, and Waters.

Chairman DAVIDSON. The Subcommittee on National Security, Illicit Finance, and International Financial Institutions will come to order.

Without objection, the chairman is authorized to declare a recess of the committee at any time.

The hearing is titled “Following the Money: Tools and Techniques to Combat Fraud.”

Without objection, all members will have 5 legislative days within which to submit extraneous materials to the chairman for inclusion in the record.

I now recognize myself for 5 minutes for an opening statement.

OPENING STATEMENT OF HON. WARREN DAVIDSON, CHAIRMAN OF THE SUBCOMMITTEE ON NATIONAL SECURITY, ILLICIT FINANCE AND INTERNATIONAL FINANCIAL INSTITUTIONS, A U.S. REPRESENTATIVE FROM OHIO

I want to welcome our witnesses. Thank you for participating in our hearing today. It is devoted to analyzing investment fraud in the United States and reassessing the effectiveness of tools used to combat fraud in our financial system.

Earlier this month, the Federal Trade Commission reported that U.S. consumers lost \$5.7 billion to investment scams in 2024. Criminals are increasingly finding ways to bypass U.S. financial regulations in order to scam Americans into draining their life savings for the sake of the criminal’s illicit gain.

This type of organized fraud transcends both State lines and political divides. These scammers prey on everyday Americans, often our most vulnerable senior citizens.

The United States is supposed to have the world's most capable financial intelligence capabilities. We are focused in this committee, on national security issues, but we also need to use these resources and capabilities we have more effectively to protect our own citizens.

Safety and soundness are essential to preserving our own financial well-being. Beyond our own population, America's capital markets are home to more than half of the world's invested capital. The U.S. dollar is the world's reserve currency.

Since its enactment in 1970, the Bank Secrecy Act has served as the cornerstone for U.S. anti-money laundering, counterterrorism, financing, and Know Your Customer compliance measures for U.S. financial institutions. The Bank Secrecy Act's regulatory framework is intended to defend and secure our financial system from crime.

However, considering the ever-changing landscape of technology and financial crime, we must continually assess the effectiveness of the tools and techniques traditionally used to secure the financial system.

Today we will take time to learn more about investment fraud and how financial institutions, including blockchain analytics firms, contribute to combatting this pervasive issue.

Investment fraud, as these losses grow in the United States, it is important to consider changes that can be made to enhance the effectiveness of our reporting.

Suspicious activity reports, or SARs, and currency transaction reports, CTRs, are tools used by financial institutions to flag transactions over a certain monetary value that could be related to illicit activities. These reports are filed by financial institutions and maintained by FinCEN, the Financial Crimes Enforcement Network, and used by law enforcement agencies over the course of their investigations.

The SAR is filed when a financial institution has a transaction over \$5,000, and a CTR is filed on cash transactions involving more than \$10,000.

Based on consumer price index (CPI) inflation, \$10,000 in 1970 would be more than \$81,000 today. These numbers in the reporting requirements have never been adjusted for inflation, so the reporting burden keeps growing with no obvious improvement on the effectiveness of the reports.

FinCEN estimated that an average total of 12,600 SARs and 57,000 CTRs were filed each day. This is 2023 data.

According to a December 2024 Government Accountability Officer (GAO) report, law enforcement agencies accessed only 5.4 percent of those CTRs filed between 2014 and 2013—or 2023. You have a 10-year period there with data and only 5.4 percent. That is not very efficient.

It is long overdue for Congress to consider these clearly outdated thresholds and frameworks so that we can protect our people and our financial institutions.

Even as we update old laws, it is important to consider other updates. Thankfully, the Trump Administration has mooted the disastrous and unconstitutional Corporate Transparency Act requiring businesses to report the beneficial ownership to FinCEN.

Presumably, by the law's framework, operating a business or even a homeowners association means you are engaged in illicit finance, but our Constitution says that, when the government wants to know private information, they need probable cause, at least reasonable suspicion, to get a warrant or subpoena.

Surely, we can minimize the financial harm suffered by Americans exploited by scammers without infringing on their civil liberties or adding ways to make ordinary citizens criminals.

As we consider legislative solutions to maximize the effectiveness of our financial intelligence architecture, I am hopeful that we will increase and improve nationwide education on investment scams. I am also hopeful that we will equip law enforcement agencies with better tools to go after criminals that are continually operating unseen.

I look forward to the insights gained on this issue from today's hearing.

I yield back.

The chairman now recognizes the ranking member of the committee, Ms. Beatty, for 4 minutes for an opening statement.

OPENING STATEMENT OF HON. JOYCE BEATTY, RANKING MEMBER OF THE SUBCOMMITTEE ON NATIONAL SECURITY, ILLICIT FINANCE AND INTERNATIONAL FINANCIAL INSTITUTIONS, A U.S. REPRESENTATIVE FROM OHIO

Mrs. BEATTY. Thank you, Mr. Chairman and Ranking Member.

Good morning and thank you to our witnesses who are here today and for holding this hearing.

I want to make sure that we understand today that we really need to have this discussion to combat financial fraud, and it is no secret. We have heard comments from our chair that fraud schemes are on the rise, and the bad actors are now finding new and creative ways to defraud consumers.

For example, the Federal Trade Commission data showed us that, in 2024, American consumers lost more than 12.5 million—billion dollars to fraud, a 25 percent increase from the previous year.

Our constituents in red and blue districts alike are being robbed of their hard-earned savings, and I am eager to work with my Republican colleagues to develop sharper tools to deter fraud, folks, and protect American consumers, starting with today's hearing.

Although I appreciate the bipartisan approach to tackling this matter, we cannot ignore the stark contradictions between the goal of today's hearing and the Trump Administration's roll back of key financial crime measures that would help us detect and deter fraud.

The President, along with Elon Musk's Department of Government Efficiency (DODGE) is trying to unlawfully eliminate the Consumer Financial Protection Bureau (CFPB), the agency, as you know, that is responsible for protecting Americans from fraud and abuse. The President announced that the United States will no longer enforce Foreign Corrupt Policy Practices Act—the Foreign Corrupt Practices Act (FCPPA), which prohibits Americans from bribing foreign officials. Also, the Treasury Secretary, Scott Bessent, unilaterally announced that the Department will not be

enforcing the bipartisan Corporate Transparency Act (CTA), which President Trump signed into law during his first term, against U.S. persons exempting over 99 percent of the companies Congress intended the law to cover.

Gutting the CTA eliminates a critical tool for law enforcement to detect and deter fraud cases that involve anonymous shell companies, effectively making the United States a haven for money launderers, traffickers, and fraudsters.

Let me just give you an example. In 2022, six individuals were charged with scamming over 20,000 victims by tricking them into paying for tech repair services. Victims paid more than \$10 million. I am going to say that again: Victims paid more than \$10 million to bank accounts tied to a network of shell companies.

While I join my colleagues on the other side in calling out the need for key beneficial ownership reforms, the administration repeatedly chooses to gut the law entirely instead of working in a bipartisan manner to ease small business compliance burdens.

In just 2 months, President Trump has made it easier for financial fraud to devastate hardworking families, particularly older adults, by unlawfully dismantling the pillars of our financial crime regulatory regime.

While I, again, appreciate this hearing, I hope the discussion only underscores the vital significance of this regime and the need to preserve it if we were truly, truly to prevent fraud and protect our constituents.

Once again, to our witnesses, I hope that you can shed some light on this, and I yield back.

Chairman DAVIDSON. I thank the gentlewoman.

I now recognize the ranking member of the full committee, Ms. Waters, for 1 minute.

STATEMENT OF HON. MAXINE WATERS, RANKING MEMBER OF THE FINANCIAL SERVICES COMMITTEE, A U.S. REPRESENTATIVE FROM CALIFORNIA

Ms. WATERS. Thank you, Chairman Davidson and Ranking Member Beatty for convening this hearing on fraud.

U.S. fraud losses were estimated at nearly \$13 billion in 2023, but many think the actual amount is much higher. Especially for the 100 million Americans over age 50, fraud is a serious threat to their secure retirement and well-being.

Congress must take financial crime seriously. It must stand up for the tools it has enacted, like the Bank Secrecy Act and Corporate Transparency Act, to detect fraud and hold fraudsters accountable.

Congress must stand up for the bank examiners, investigators, prosecutors, agencies, and consumers that are under attack by the Trump regime and his billionaire cabinet, and we must end Trump's own schemes to defraud the American public using his meme coin and stablecoin.

I thank you and I yield back.

Chairman DAVIDSON. I thank the Ranking Member.

Today we welcome the testimony of: Mr. Darren McLaughlin, he is the Executive Vice President and Chief BSA/AML (Bank Secrecy Act/Anit-Money Laundering) and Sanctions Officer for Flagstar

Bank in Michigan and is testifying on behalf of the American Bankers Association (ABA); Ms. Jacqueline Burns Koven is the Head of Cyber Threat Intelligence at Chainalysis; Mr. Jeff Brabant is the Vice President for Federal Government Relations at the National Federation of Independent Businesses (NFIB); and Ms. Kathy Stokes is the Director of Fraud Prevention for the American Association of Retired Persons (AARP).

We thank each of you for taking time to be here. Each of you will be recognized for 5 minutes to give an oral presentation of your testimony.

Without objection, your written statements will be made part of the record.

Mr. McLaughlin, you are now recognized for 5 minutes for your oral statement.

STATEMENT OF DARRIN MCLAUGHLIN, EXECUTIVE VICE PRESIDENT AND CHIEF BSA/AML & SANCTIONS OFFICER, ON BEHALF OF THE AMERICAN BANKERS ASSOCIATION

Mr. MCLAUGHLIN. Thank you, sir.

Thank you Chairman Davidson, Ranking Member Beatty, Ranking Member Waters, and members of the subcommittee. Thank you for the opportunity to testify.

My name is Darren McLaughlin, and I am the Executive Vice President (EVP) and Chief BSA/AML Officer for Flagstar Bank based in New York. I am testifying today on behalf of the American Bankers Association. These views are my own and do not necessarily reflect the views of my employer.

Criminal enterprises are targeting all Americans. One in three adults have experienced financial fraud or a scam in just the last 12 months, while nearly two in five have experienced a financial loss.

Bad actors have leveraged cutting-edge technology, social media, and telecommunications to target American's life savings. Through increasingly sophisticated techniques, bad actors make false promises of huge financial returns on fictitious investment opportunities.

I represent the thousands of talented BSA and anti-fraud professionals across the country who have dedicated their entire careers to protecting our customers and the U.S. financial system, but our customers are still under attack.

To succeed, we need a more strategic approach that includes the government, the banking industry, and other industries across the economy. It is critical that the banking industry receive transparent and actionable feedback from the government and important regulatory reforms to let us focus on the real threats.

I would like to emphasize three things today. First, banks are doing important work to combat fraud, including leveraging technology, continuously improving anti-fraud operations, and investing in customer anti-fraud education, but a whole-of-government approach is needed.

Financial institutions across the country have implemented rigorous risk-based AML compliance and anti-fraud programs that alert us to signs that customers have started to send money in un-

usual patterns. Unfortunately, these customers sometimes fall victim to those overseas characters.

We can share heartbreaking stories across the industry about innocent customers who have lost their lifetime savings to investment scams. As hard as we try, sometimes we cannot convince our customers that they are the victim of a scam in progress.

Although we file suspicious activity reports with the Treasury's Financial Crimes Enforcement Network, by the time law enforcement receives the report, it is often too late.

A major part of this threat comes from overseas, and these bad actors are using new generative artificial intelligence (AI) tools to increase the sophistication and effectiveness of their outreach. There must be a better approach to tackling this grave problem. Greater involvement by and coordination with the government is essential.

Second, banks need timely, actionable and feedback from—actionable data and feedback from the government on priority threats. The Federal Government has a database bursting with threat information, which should be shared with the private sector.

Although thousands of SARs are filed, they may not actually reflect criminal or other illicit acts. It would help banks to see analysis of these reports and other information the government may have about this illicit activity.

Finally, we need meaningful reforms of the BSA rules, including creating a true risk-based approach to BSA/AML compliance, providing transparent government feedback to banks regarding priority threats, reform of outdated currency transaction reporting, streamline and update the suspicious activity and other reporting forums that we must complete, and increase collaboration between bank regulators and the banks.

In conclusion, banks are working hard to combat fraud, but it is clear our customers are still under attack. To fight back and succeed, we need a whole-of-government approach that includes greater transparency and actionable feedback from the government. We need other sectors to do their part, and we need important regulatory reforms to let us focus on the real threats.

Chairman Davidson, Ranking Member Beatty, and Ranking Member Waters, and members of the subcommittee, we are grateful for your leadership and holding this hearing to highlight the extraordinary and growing financial fraud problem that is plaguing our country.

We look forward to working with you and your colleagues to explore what Congress, the regulatory agencies, and the Federal Government can do to help.

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

[The prepared statement of Mr. McLaughlin follows:]

April 2025

Testimony of
Darrin McLaughlin
On Behalf of the
American Bankers Association
Before the
**Subcommittee on National Security, Illicit Finance, and International
Financial Institutions**
Of the
House Financial Services Committee
April 1, 2025



Testimony of
Darrin McLaughlin
On Behalf of the
American Bankers Association
Before the
Subcommittee on National Security, Illicit Finance, and International Financial Institutions
 Of the
House Financial Services Committee
April 1, 2025

Chairman Davidson, Ranking Member Beatty, and members of the Subcommittee, thank you for the opportunity to offer testimony for today's Hearing: "Following the Money: Tools and Techniques to Combat Fraud." My name is Darrin McLaughlin, and I am Executive Vice President and Chief AML and Sanctions Officer for Flagstar Bank, which is headquartered in Hicksville, New York. I am testifying today on behalf of the American Bankers Association (ABA). ¹ These views are my own and don't necessarily reflect the views of my employer.

Bad Actors Continue to Aggressively Target Bank Customers

There are thousands of talented Bank Secrecy Act (BSA) and anti-fraud professionals across the country who have dedicated their entire careers to protecting their customers and the U.S. financial system. We want nothing more than to accomplish that critical mission – and it is clear, despite all our efforts, there is more work to be done. Effectively combatting these attacks by bad actors requires proactive steps from both the federal government and other industries. We need transparency and actionable feedback from the government, and we need important regulatory reforms to let us focus on the real threats.

Criminal enterprises are targeting all Americans. Bankrate's latest Financial Fraud Survey found that about one in three adults have experienced a financial fraud or scam in just the last 12 months, while nearly two in five among them have experienced a financial loss. ²

Bad actors have leveraged cutting edge technology, social media, and telecommunications to mask their true location and identity and to target Americans' life savings. Through increasingly

¹ The American Bankers Association is the voice of the nation's \$24.1 trillion banking industry, which is composed of small, regional, and large banks that together employ approximately 2.1 million people, safeguard \$19.2 trillion in deposits, and extend \$12.7 trillion in loans.

² <https://www.bankrate.com/credit-cards/news/financial-fraud-survey/#:~:text=More%20than%20in%203,sent%20funds%20to%20a%20scammer>

sophisticated techniques, bad actors make false promises of huge financial returns on fictitious investment opportunities. The latest Federal Trade Commission (FTC) Consumer Sentinel 2024 Databook indicates that the greatest median losses are from investment, business/job opportunity, and debt management scams.³ The scale of the problem is so vast that comprehensive numbers are difficult to ascertain. However, we have snapshots of how this epidemic is shattering lives. In 2023, the FTC estimated fraud losses to be as high as \$158.3 billion,⁴ which is roughly the size of Kuwait's gross domestic product (GDP).⁵ That same year, FTC estimated elder fraud losses to be as high as \$61.5 billion.⁶ AARP estimates that on average, elder financial exploitation victims lose up to \$120,000.⁷

Banks are Doing Important Work to Combat Fraud, But A Whole-of-Government Approach is Needed

Banks strive to follow all applicable BSA and compliance rules, educate our customers, train our employees, and invest in sensitive detection and compliance systems. But banks are in a difficult position with only limited tools to address this growing problem. The federal government and other private sector industries, including telecommunications and social media, must do their part. Combating fraud requires a whole-of-government approach, partnered with the private sector.

Last year, ABA's Paul Benda made this point when he testified to the Senate Banking Committee about the important work banks do to combat fraud, including leveraging technology, continuously improving anti-fraud operations, and investing in customer anti-fraud education.⁸ But bad actors continue to impersonate government officials, banks, and other trusted companies to defraud innocent Americans. Bad actors hide their true identities, trade in the good names and reputations of banks and other responsible companies, and abuse shell corporations to facilitate the flow of their ill-gotten gains away from their victims.

Banks have adapted to this sad reality by warning our customers that danger can lurk behind any call, text, or email the customer has not initiated. Banks will rarely ask for your account number, PIN, or password during a phone call — and will never ask for a one-time login code. Banks

³ https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf

⁴ https://www.ftc.gov/system/files/ftc_gov/pdf/federal-trade-commission-protecting-older-adults-report_102024.pdf ("In 2023, the FTC estimates the overall loss, adjusted for underreporting, was \$158.3 billion or \$23.7 billion for consumers of all ages and \$61.5 billion or \$7.1 billion for older adults. These estimates are based on two different assumptions about the degree of underreporting for high dollar losses.")

⁵ https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=true

⁶ <https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-issues-annual-report-congress-agencys-actions-protect-older-adults>

⁷ <https://www.aarp.org/pri/topics/work-finance-retirement/fraud-consumer-protection/the-thief-who-knows-you-the-cost-of-elder-exploitation-examined/>

⁸ <https://www.aba.com/advocacy/policy-analysis/aba-testimony-on-scams-and-frauds-in-banking-system>

advise customers never to share such confidential personal information unless the customer called the number on the back of their bank card. The banking industry cautions customers to be skeptical of every email, be wary of incoming calls, never click on a text link, and delete unexpected texts. Criminals frequently raid mailboxes, and snatch checks to steal customer funds. We communicate to customers that if they are contacted and asked to provide sensitive financial or personal information – assume it is a scam.

ABA is proud of its award-winning anti-phishing campaign, Banks Never Ask That,⁹ our new Practice Safe Checks¹⁰ initiative, as well as the critical work of ABA's non-profit subsidiary, the ABA Foundation.¹¹ These tools educate customers and help banks support the financial well-being of their communities. Members of this committee may have received warning emails, texts or letters from their banks, and may have seen ABA's campaigns. But the need, driven by fraudsters' deception, to educate customers to disregard unsolicited outreach from banks and other trusted companies also creates a new challenge. Banks still need reliable ways to exchange essential communications with our customers.

Financial institutions across the country have rigorous, risk-based BSA compliance and anti-fraud programs that alert us to signs customers have started to send money in unusual patterns, including to high-risk individuals, entities, and jurisdictions. When we investigate these unusual transactions, we often need our customers to tell us what is going on. But if our customers — whom we rightly train to be suspicious of incoming calls, emails, texts, and letters — simply give up and stop answering communications, they miss our legitimate outreach and cannot immediately give us critical information necessary to protect them. This leads to the terrible outcome where bad actors, who can assume any disguise, and tell any manipulative lie, have better access to our customers to defraud them than banks do to protect them.

The banking industry has seen heartbreaking stories about innocent customers who have been preyed on by investment schemes, losing the money they have spent a lifetime saving, and as hard as we try, we cannot convince them of the scam in progress. We warn our customers, but very often, our warnings cannot break the spell of psychological manipulation tactics deployed by experienced fraudsters. In addition to warning customers, we also submit confidential reports through appropriate channels, including Suspicious Activity Reports (SARs) filed with Treasury's Financial Crimes Enforcement Network (FinCEN). However, by the time law enforcement receives the information, it is generally too late. As recently reported by the New York Times, money is moved quickly, often into the hands of professional international money launderers.¹²

⁹ <https://www.banksneveraskthat.com>

¹⁰ <https://practicesafechecks.com>

¹¹ <https://aba.com/Foundation>

¹² <https://www.nytimes.com/2025/03/23/world/asia/takeaways-money-laundering-investigation.html>

In such cases, banks face the impossible choice – should the bank continue to process transactions that could possibly harm their customer and help the bad actors, or does the bank close the account to avoid inadvertently facilitating the on-going fraud? Reluctantly, sometimes banks must close these accounts as a last resort. But even this measure cannot always end the harm. When that happens, the customer often takes the account closure check and deposits it at another bank that is unaware of the ongoing fraud. The customer continues to be exploited, and the new bank is left managing the old risk.

A major part of this threat comes from overseas, so we strongly encourage the federal government to do more. The Center for Strategic and International Studies reports that cyber scams often originate from other countries, especially from China and Southeast Asia.¹³ When the Covid-19 pandemic brought lockdowns and strict border controls, preventing gamblers from traveling, criminal groups sought new sources of profit.¹⁴ Overseas scam compounds, rooted in the collapse of Southeast Asia's gambling industry, are closely tied to Chinese criminal groups. Many repurposed the facilities into cyber-scramming compounds where victims of human trafficking are forced to scam victims out of billions of dollars.¹⁵ Working under threat to their lives, these human trafficking victims are coerced to befriend and entice innocent Americans into fraudulent investment schemes.

These deceptive relationships can be built using new generative artificial intelligence (AI) tools exploited by bad actors to increase the sophistication and effectiveness of their outreach. Research published last year by the Institute of Electrical and Electronics Engineers noted that AI large language models that generate realistic text, converse coherently, and perform linguistic tasks at superhuman levels can create content that appears uniquely crafted for individual targets, sometimes even mimicking the linguistic style of a close acquaintance.¹⁶ Bad actors can therefore use AI to cheaply produce credible, compatible (or relevant), and customized phishing attempts¹⁷ that have been used to successfully target Americans. Banks and other industries cannot combat this problem alone—greater involvement by and coordination with the government is essential.

Banks Need Timely, Actionable Data and Feedback from the Government on Priority Threats

¹³ <https://www.csis.org/analysis/cyber-scramming-goes-global-unveiling-southeast-asias-high-tech-fraud-factories>

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Devising and Detecting Phishing Emails Using Large Language Models*; IEEE Access; Fredrik Heiding, Bruce Schneier, Arun Vishwanath, Jeremy Bernstein, Peter S. Park (March 11, 2024); <https://ieeexplore.ieee.org/document/10466545>.

¹⁷ *Id.*

Protecting customers and the U.S. financial system is a calling for me and thousands of my counterparts, the dedicated professionals who do this important work. We do our jobs, not for recognition, but to advance the mission. However, despite our best efforts, every bank cannot be an expert in global fraud trends or the illicit finance threats prioritized by the government. Furthermore, each bank often only has a single piece of the puzzle. In contrast, the government has a comprehensive database BSA reporting and needs to tell banks where to look. To stay on top of the problem, banks need real, actionable, up-to-date information on the typologies, patterns, and characteristics of the illicit financial transactions that harm customers. Improving feedback loops to banks was one of the important reforms Congress included in the Anti-Money Laundering Act.¹⁸ The initiative just announced by Internal Revenue Service – Criminal Investigation on March 28 to provide quantifiable results to financial institutions on IRS-CI’s use of SARs¹⁹ is positive development.

But we need more of this to be implemented. When a bank files a SAR, it is very often the end of the story. Banks receive no further information on the vast majority of potentially suspicious acts the rules require them to report to FinCEN. Banks rarely know whether they have identified a significant crime or whether the bank is wasting resources reporting transactions of limited or no value to law enforcement. It is critical for banks to know whether they’re on the right track, or whether the bank needs to be looking elsewhere. Only then can banks tune our internal monitoring and reallocate resources to fend off the real threats.

Banks require actionable feedback to continuously improve several existing and important anti-fraud functions, such as:

- Evolving bank training to recognize, respond to, and report fraud;
- Educating consumers on how to avoid scams;
- Partnering with law enforcement and other appropriate agencies to help investigate and prosecute fraud; and
- Leveraging technology to identify fraud and irregular patterns of behavior.

It is important that banks evolve our detection capabilities when criminals change tactics and develop new tactics to operate under the radar. They may tell victims to open different kinds of accounts at different banks to ensure that no one bank has all the puzzle pieces or even suspect that there are other puzzle pieces to find. Bad actors may coach their victims to provide plausible explanations to bank officials when the bank asks about unusual transactions (although some customers, unfortunately, ignore the bank’s outreach altogether).

¹⁸ See AMLA, Public Law 116-283, Div. F § 6002.

¹⁹ <https://www.irs.gov/compliance/criminal-investigation/irs-ci-releases-fy24-bsa-metrics-announces-ci-first-initiative>

Once the customer has withdrawn cash or other funds, a bank has no way of knowing what will happen next. The customer may be coached to deposit cash in a crypto ATM in order to “invest” it or use another financial institution to “buy” convertible virtual currency through a scammer-controlled exchange. But these are today’s methods – and they are rapidly evolving every day.

Banks need information only the government can provide to stay abreast of changes. Banks also need feedback about whether banks’ BSA reporting is highly useful to the government to detect fraud, financial crime, and counter terrorism funding. ABA has called for this feedback, and for bank regulators, FinCEN and government agencies to work together to ensure regional federal law enforcement priorities and trends are shared with banks, while encouraging state and local law enforcement to do the same.²⁰ Since SARs represent a bank’s best efforts to identify suspicious activity—but may not actually reflect criminal or other illicit acts— it would help banks to see analysis of their reported SAR information incorporated with reported crime statistics and other information the government may have about illicit activity. In short, the federal government needs to tell banks whether they are hot or cold.

ABA Recommendations on BSA Regulatory Reforms

Regulatory improvements would help banks better protect their customers. Congress has reformed BSA laws, but we need further action by FinCEN and the banking agencies to amend the BSA rules. These regulatory changes would be consistent with this administration’s directive to clarify regulatory expectations and reduce regulatory burden on businesses,²¹ and they would allow banks to focus on critical anti-fraud work. ABA renews calls for the following reforms:

Focus on Higher-Risk Activities and Customers. Allow banks to focus on the real threats and reinforce a true, risk-based approach to BSA compliance.²² Just as Congress stated in the Anti-Money Laundering Act of 2020, banks must be allowed to redirect important compliance resources toward higher-risk customers and activity and away from lower risk-customers and activity. Banks’ BSA program rules should be amended to explicitly allow this reallocation of resources away from lower-risk and toward higher-risk customers and activities.

Improve Threat Feedback and Update FinCEN Alerts and Advisories. Provide transparent government feedback to banks regarding priority threats. Banks cannot effectively identify evolving threats to their customers and the U.S. financial system without feedback, information, and assistance, including from federal law enforcement. State governments should also be encouraged to participate. FinCEN alerts and advisories should reflect current priorities, and

²⁰ <https://www.aba.com/advocacy/policy-analysis/letter-to-the-agencies-on-the-aml-program-rule-nprm>.

²¹ <https://www.federalregister.gov/documents/2025/02/06/2025-02345/unleashing-prosperity-through-deregulation>

²² See <https://www.aba.com/advocacy/policy-analysis/letter-to-fincen-on-aml-nprm>; see also <https://www.aba.com/advocacy/policy-analysis/letter-to-the-agencies-on-the-aml-program-rule-nprm>.

correlate with the Anti-Money Laundering/Countering the Financing of Terrorism Priorities the guidance is designed to address. Some FinCEN alerts and advisories have been in effect since 1996 without change.²³ FinCEN should re-examine existing advisories to reaffirm, update, or phase them out consistent with the current threat environment.²⁴ This would also allow banks to minimize threat-based outreach to their customers, who are justifiably wary of unsolicited communications. Banks should be regularly alerted to the latest evolving fraud trends.

Reform CTR Reporting. Reform outdated currency transaction reporting (CTR) rules to allow banks to focus resources on actual and emerging threats and away from collecting, documenting, and reporting non-suspicious currency transactions.²⁵ We need smart, data-driven reforms so banks can put their compliance resources to their highest and best use. FinCEN reports that banks filed over 20.5 million CTRs in 2022 alone—nearly 5 times the number of SARs filed that same year—but these reports are no longer inherently tied to combating financial crime.²⁶ 80 years after Treasury first established a currency reporting requirement at this same threshold,²⁷ \$10,000 is no longer an unusually large sum of money,²⁸ and existing rules oblige banks to spend disproportionate resources on CTR reporting. In a 2023 survey of ABA members, a quarter of respondents reported spending between 25% and 50% of *all their BSA compliance costs* on CTR filings.²⁹ If a cash transaction is suspicious, banks are also required to file a SAR, in addition to the CTR, which does not flag the suspicious behavior. Some smaller dollar cash transactions involve illicit behavior: IRS-CI just reported that over 67% of their opened cases in FY24 had a subject with a CTR below \$40,000, with 50% involving less than \$22,230.³⁰ Data-driven CTR reform should allow banks to focus their compliance resources on reporting suspicious cash transactions, rather than requiring banks to report on cash transactions banks understand, made by their law-abiding customers.

Update BSA Reporting Forms. Streamline and update BSA reporting forms, so banks do not need to fill out endless boxes that do not benefit law enforcement. For example, CTR Form 112 includes requests for information that exceeds BSA program and CTR regulatory requirements,

²³ *Id.*

²⁴ *Id.*

²⁵ <https://www.aba.com/advocacy/policy-analysis/letter-to-fincen-on-ctr-pra-2024>.

²⁶ *Id.*

²⁷ The first currency transaction reporting requirement was promulgated by Treasury in 1945, under the Trading with the Enemy Act, directing banks to report transactions that “exceed those commensurate with the legitimate and customary conduct” of bank customers. 10 Fed. Reg. 6547, 6556 (June 5, 1945). This new rule established a \$10,000 reporting threshold, directing banks to report cash transactions that exceeded this amount, unless banks knew the transactions to be legitimate and customary.

²⁸ <https://www.aba.com/advocacy/policy-analysis/letter-to-fincen-on-ctr-pra-2024>.

²⁹ *Id.*

³⁰ <https://www.irs.gov/compliance/criminal-investigation/irs-ci-releases-fy24-bsa-metrics-announces-ci-first-initiative>

are burdensome for banks to collect and report, and may even conflict with other legal requirements.³¹

Reduce Focus on Mere Technical Compliance. Release banks from check-the-box compliance obligations.³² The rules, and bank examiners, must reduce excessive focus on mere technical compliance at the expense of effective BSA program operations. Even strong programs do not, and cannot, avoid all technical failures, especially at the expense of a risk-based approach. Focusing on minor issues that have no measurable effect on the quality of a bank's program materially interferes with a risk-based approach.³³

Increase Collaboration Between Bank Regulators and Banks and Enhance Information Sharing. Increase collaboration between banking regulators and banks to ensure examinations credit the important work banks are doing to fight fraud, financial crime, and terrorism funding. Further, ABA supports the Foreign Affiliates Sharing Pilot Program Extension Act, which is led by Rep. Sylvia Garcia (D-TX). This legislation would extend the deadline for the pilot program authorizing SAR sharing with foreign affiliates, passed as part of the AMLA, to three years after the date the program begins. This bill would realize Congress' objective in authorizing this program, and ensure the clock starts when the program does, allowing a fair assessment of its value.

Conclusion

Banks employ thousands of talented anti-fraud and BSA professionals across the country who have dedicated their entire careers to protecting their customers and the U.S. financial system. But it is clear, in spite of all our efforts, our customers are still under attack by bad actors. To fight back and succeed, everyone must do their part. We need a whole-of-government approach that includes greater transparency and actionable feedback from the government, we need other sectors to do their part, and we need important regulatory reforms to let us focus on the real threats.

We are grateful for the leadership being shown by Chairman Davidson, Ranking Member Beatty, and members of the Subcommittee in holding this hearing to highlight the extraordinary and growing financial fraud problem that is plaguing the country. We look forward to working with

³¹ *Id.*

³² See <https://www.aba.com/advocacy/policy-analysis/letter-to-fincen-on-aml-nprm>; see also <https://www.aba.com/advocacy/policy-analysis/letter-to-the-agencies-on-the-aml-program-rule-nprm>.

³³ See <https://www.aba.com/advocacy/policy-analysis/letter-to-fincen-on-aml-nprm>; see also <https://www.aba.com/advocacy/policy-analysis/letter-to-the-agencies-on-the-aml-program-rule-nprm>.

you and your colleagues to explore what Congress, the regulatory agencies and the federal government can do to help.

Thank you once again for the opportunity to testify. I look forward to answering your questions.

Chairman DAVIDSON. Thank you, Mr. McLaughlin.

Ms. Burns Koven, you are now recognized for 5 minutes for your oral statement.

**STATEMENT OF JACQUELINE BURNS KOVEN, HEAD OF CYBER
THREAT INTELLIGENCE, CHAINALYSIS**

Ms. BURNS KOVEN. Chairman Davidson, Ranking Member Beatty, Ranking Member Waters, and distinguished members of the subcommittee, thank you for inviting me to testify before you today on the pressing issue of fraud targeting Americans.

My name is Jacqueline Burns Koven, and I am the Head of Cyber Threat Intelligence for the blockchain data platform Chainalysis where we help make blockchain safer and more secure so that financial institutions, businesses, and government can engage cryptocurrency with confidence.

Leveraging the blockchain's inherent transparency, we track cryptocurrency activity by illicit actors, such as those engaged in scams, and provide data on their financial activity to private and public sector customers.

Today's hearing shines an important spotlight on scams facing the American people as a matter of national security, most notably, so-called pig butchering scams, also referred to as investment or confidence scams, that target and build relationships with individuals, convincing them to invest in fraudulent opportunities.

Scam syndicates are well-resourced. According to Chainalysis data, for each of the past 4 years, scam operators received over \$10 billion in cryptocurrency payments, with 2024 estimated as a record year.

It has never been easier for scammers to access tools to make the con more convincing and scalable. The peer-to-peer marketplace, Huione Guarantee, for example, has become a one stop shop for the scam supply chain.

As we highlighted in our annual crypto crime report, Huione has processed more than \$70 billion in crypto transactions, and its infrastructure facilitates laundering services, as well as the sale of contact information for outreach to potential scam victims, web-hosting services, social media accounts, and AI software.

Fraudsters can always be counted on to abuse novel technologies for their aims, but the utilization of cryptocurrency should fundamentally place scammers at a disadvantage.

Cryptocurrency transactions are inherently public, and the data from those transactions is preserved on a transparent, immutable ledger. In fact, Stablecoins, in particular, are freezable midstream, which has led to spectacular seizures of scammed funds.

Blockchain intelligence provides insight into the entire scam supply chain, laundering patterns, and even to scale at a level unparalleled to traditional finance. Indeed, a single cryptocurrency payment to a scam can often lead to identifying hundreds of other victim payments of a multimillion dollar fraud scheme, allowing for a more effective disruption and restitution efforts rather than just one-off criminal investigations.

However, the current reality is that scammers are exploiting the siloed nature of how the public and private sector identify and re-

spond to these schemes. Scammer syndicates are organized and agile, and they are capitalizing on our visibility gaps.

Today scam victims have multiple State, local, and Federal agencies they can report to, yet there is no easy mechanism for these agencies to share with each other, let alone with the private sector best positioned to prevent additional victims.

Financial institutions reporting on scams have no visibility into the scams reported by their peers, leaving them unable to protect their customers from scams known to the government or to the financial institution next door.

At the same time, private sector entities outside of financial institutions on the frontline of scams lack the structures to comprehensively share and receive information from the public sector about scam activity that would allow them to take more proactive measures.

It is essential to modernize and streamline bidirectional scam reporting and response between public and private sectors to facilitate restitution and the prevention of additional victims.

Furthermore, too often scam victims are turned away from local authorities who are ill-equipped to properly assess crypto cases. We must ensure law enforcement's access to blockchain analysis and training and invest in tech-driven efficiency to swiftly take action with intelligence and seize funds.

Over the past 10 years, Chainalysis has supported hundreds of cases involving the freezing of assets in partnership with government agencies worldwide, helping to secure at least \$12.6 billion worth of illicit crypto. It is imperative that we develop strategies to prevent Americans from falling prey to scams altogether.

Chainalysis acquired Alteryx, which utilizes artificial intelligence to identify early stage scam activities, enabling financial institutions large-scale upstream detection. We further support a regulatory framework that clearly delineates responsibility for oversight of businesses offering Stablecoins and trading services.

Finally, we need to close gaps in AML/Countering the Financing of Terrorism (CFT) standards implementation. In the absence of cooperation, more pressure is needed to disrupt financial networks, define laws, and regulatory norms.

Thank you again for the opportunity to provide testimony on this important topic. I am encouraged by the subcommittee's interest, and to that end, we invite Congress' continued engagement on this topic to combat scams and better protect Americans.

I look forward to your questions.

[The prepared statement of Ms. Burns Koven follows:]



Written Testimony of Jacqueline Burns Koven
Head of Cyber Threat Intelligence
Chainalysis Inc.

Before the
House Financial Services Committee,
Subcommittee on National Security, Illicit Finance, and International Financial Institutions

Hearing on
Following the Money: Tools and Techniques to Combat Fraud

April 1, 2025

Chairman Davidson, Ranking Member Beatty, and distinguished members of the Subcommittee: Thank you for inviting me to testify before you today on the pressing issue of fraud targeting Americans.

My name is Jacqueline Burns Koven, and I am the Head of Cyber Threat Intelligence for the blockchain data platform Chainalysis, where we help make blockchains safer and more secure so that banks, businesses, and governments have the confidence and knowledge they need to help this new digital economy thrive. Leveraging the blockchain's inherent transparency, we track cryptocurrency activity by illicit actors, such as those perpetrating investment and confidence scams and provide data on their financial activity to private and public sector customers, including the federal government.

The intersection of scams and cryptocurrencies

This hearing could not be more timely. Americans are facing a growing threat by scammers and fraudsters as a result of numerous factors, including the convergence of technological developments such as social media, cryptocurrencies, and artificial intelligence. Of particular focus, cryptocurrency adoption and the application of blockchain technologies has expanded into a vibrant, innovative ecosystem, but fraudsters can always be counted on to abuse novel technologies and are leveraging cryptocurrency as a tool in a broader, more diverse set of criminal activity. Cryptocurrencies are increasingly a part of virtually every type of illicit activity, from scams targeting vulnerable US citizens to complex national security challenges driven by the most persistent foreign adversaries and nation states.¹

Today's hearing shines an important spotlight on the pervasive issue of fraud and scams, including their connection to cryptocurrencies. Over the years, the prevalence and sophistication of scams involving cryptocurrencies has increased, and now there are classes of scams that are almost exclusively associated with cryptocurrencies – most notably, so-called “pig butchering” – which refers to

¹ “2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized,” *Chainalysis*, Jan. 15, 2025, <https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/>.



investment or confidence scams that target and build relationships with individuals, convincing them to invest in fraudulent opportunities.

The utilization of cryptocurrency should fundamentally place scammers at a disadvantage due to the traceable nature of these assets. Cryptocurrency transactions are inherently public and the data from those transactions is preserved on a transparent, immutable ledger. At Chainalysis, we analyze the transaction data from blockchain networks in conjunction with open source intelligence information and proprietary data to map the ecosystem of benign as well as illicit participants in these networks. Blockchain investigations and transaction monitoring leveraging Chainalysis software and data provides a clear and visual representation of potential scam networks and laundering activities, a level of transparency that is unparalleled in traditional financial institutions. Indeed, identifying a single cryptocurrency payment to a scam enterprise can often lead to identifying hundreds of other victim payments, even revealing in some cases the scam compound from which the scammers are operating from, allowing for more effective disruption and restitution efforts rather than just one-off criminal investigations.

However, the current reality is that scammers are exploiting the disjointed and siloed nature of how the public and private sector respond to their schemes. Today, scam victims have multiple state, local, and federal agencies they can report to, yet there is no easy mechanism or obligation for these agencies to share reported information with each other or those in the private sector. Cryptocurrency businesses and financial institutions reporting scam information through Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs) have no visibility into the scam indicators and cryptocurrency wallet addresses submitted by their peers and are unable to protect their customers from scams known to the government or the financial institution next door. At the same time, private sector actors outside of financial institutions, like blockchain forensics companies, lack the structures to comprehensively share and receive information from the public sector about scam activity that would allow them to take more proactive measures. More broadly, the cryptocurrency industry as a whole lacks a unified regulatory framework that clearly delineates which regulator has frontline responsibility for oversight of businesses offering stablecoins and trading services. This fragmentation allows scammers to operate with impunity, often due to the lack of communication and information flow between different entities and regulatory bodies.

We are encouraged that this subcommittee is interested in learning more about the impact of scams and fraud involving cryptocurrency on victims in the United States and globally. We strongly believe that blockchain intelligence solutions like Chainalysis are key to helping fight back against this growing form of criminal activity. To that end, we invite Congress' continued engagement on this topic, as addressing this issue requires an all-of-government approach in collaboration with the private sector, and we



recommend that Congress ensure that state and local as well as federal law enforcement and other federal agencies have the resources necessary to comprehensively combat this issue.

Chainalysis data and insights on scam activity

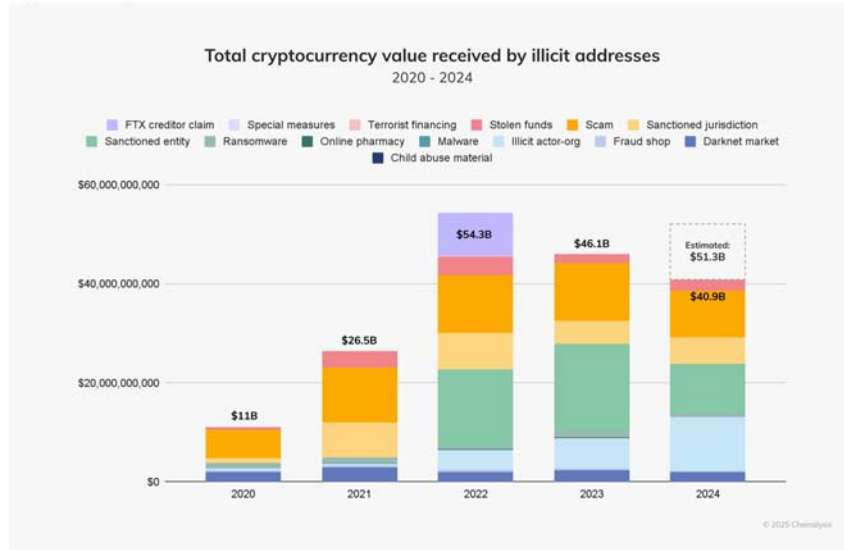
Chainalysis publishes an annual Crypto Crime Report that provides a detailed survey of the various types of illicit activity involving cryptocurrencies.² As cryptocurrency adoption accelerates and the broader crypto economy grows in size, cryptocurrency transactions are now frequently observed as part of activities as disparate as the manufacturing of fentanyl precursors supplied to Mexican drug cartels, the financing of entities affiliated with designated terrorist organizations, and the laundering of proceeds from cyberattacks conducted by hacking groups connected with the Democratic People's Republic of Korea (DPRK).

In 2024, we estimate that the total amount of cryptocurrency received by illicit actors will be over \$51 billion. Our current data reflects over \$40 billion received by illicit actors which, based on historical trends, will invariably increase as we identify more illicit transactions associated with activity in 2024. Scams as a class of illicit activity is one of the largest we track, accounting for approximately 25% of all illicit cryptocurrency proceeds that we trace. For each of the past four years, scam operators received

² "The Chainalysis 2025 Crypto Crime Report," *Chainalysis*, <https://go.chainalysis.com/2025-Crypto-Crime-Report.html>.



over \$10 billion in cryptocurrency payments, and 2024 is estimated to be a record year in terms of cryptocurrency scam revenue.³

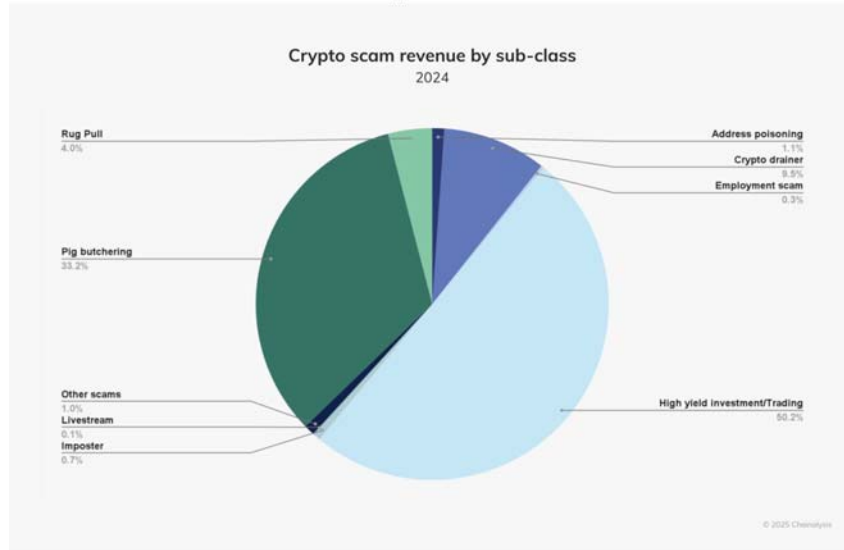


In 2024, over 80% of total crypto scam profits can be attributed to pig butchering and high-yield investment scams. Pig butchering - also referred to as investment, confidence, or romance scams - target and build relationships with individuals, convincing them to invest in fraudulent opportunities. This subclass of scam activity grew over 40% in 2024 based on total crypto funds received by wallets identified as belonging to entities operating pig butchering schemes. The other major subcategory of

³ "Crypto Scam Revenue 2024: Pig Butchering Grows Nearly 40% YoY as Fraud Industry Leverages AI and Increases in Sophistication," *Chainalysis*, Feb. 13, 2025, <https://www.chainalysis.com/blog/2024-pig-butchering-scam-revenue-grows-yoy/>.



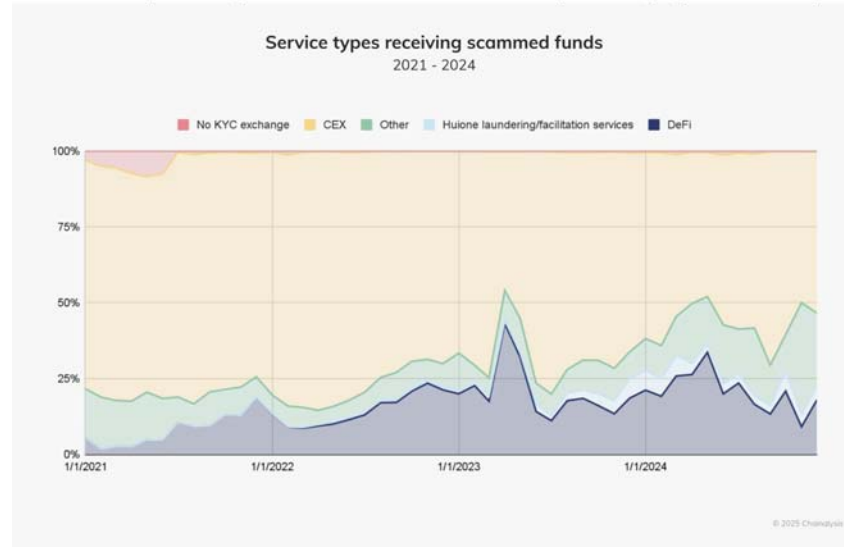
scams, high-yield investment scams, generally include Ponzi schemes and other get-rich-quick schemes. A more detailed breakdown of different scam types can be observed in the chart below.



We not only track the amount of cryptocurrency funds received by scam operators but also where those funds are directed for purposes of laundering or cashing-out to fiat currency. In the last few years, laundering destinations for scammed funds have remained relatively constant, with most funds going to



centralized exchanges (CEXs). It is important to note that scam proceeds are largely laundered through overseas entities, reinforcing the effectiveness of the US anti-money laundering regime domestically.



One example of an offshore institution playing a large role in facilitating scams is the Cambodian service Huione Guarantee. Huione Guarantee has become a one-stop shop for illicit actors needing the technology, infrastructure, and resources to conduct scams. As we have highlighted in our annual Crypto Crime report, Huione and all vendors operating on their platform have processed more than \$70 billion in crypto transactions since 2021.⁴ This platform has provided infrastructure that facilitates the sale of scam technology and processed on-chain transactions for pig butchering and other fraud and scams, addresses reported as stolen funds, sanctioned entities such as the Russian exchange Garantex, fraud shops, child sexual abuse material, and Chinese-language gambling sites and casinos, among others. Many merchants on Huione Guarantee put little effort into masking their illicit activities, advertising the types of services they look for using thinly-veiled code words.

Other vendors on Huione catering to the scam ecosystem offer technology for facial recognition or facial alteration, targeted data lists for outreach to potential victims, web hosting services, social media accounts and content creation, orchestration of pig butchering and Ponzi schemes, and global passports, visas, and purportedly assisting with applications, and AI software. While generative AI can accelerate

⁴ "Crypto Scam Revenue 2024: Pig Butchering Grows Nearly 40% YoY as Fraud Industry Leverages AI and Increases in Sophistication," *Chainalysis*, Feb. 13, 2025, <https://www.chainalysis.com/blog/2024-pig-butchering-scam-revenue-grows-yoy/>.



legitimate innovation, it can also make scams more scalable and affordable for bad actors to conduct. Generative AI is amplifying scams, the leading threat to financial institutions, by enabling high-fidelity, low-cost, and highly scalable fraud that exploits human vulnerabilities. It facilitates the creation of synthetic and fake identities, allowing fraudsters to impersonate real users and bypass identity verification controls.

In fact, Chainalysis recently acquired a company, Alteryx, that found that 85% of scams involve fully verified accounts that are not detected by traditional identity-based fraud prevention solutions. Additionally, GenAI enables the generation of realistic fake content, including websites and listings, to power investment scams, purchase scams, and more, making these attacks easier and cheaper to deploy at scale, and more convincing and harder to detect. With this technology, scammers can deceive targets into authorizing payments under false pretenses, often known as authorized push payment (APP) fraud. The Huione Guarantee platform hosts dozens of software vendors that provide generative AI technology to facilitate scams.

Chainalysis solutions and the power of blockchain intelligence

The data and insights above barely scratch the surface of the type of intelligence that Chainalysis has developed on scammers, as well as numerous other types of illicit actors exploiting cryptocurrency networks. This is because the uniquely transparent manner in which cryptocurrency networks operate opens up powerful opportunities to gain invaluable insights into illicit activity occurring on these networks. Since all crypto transactions occur on a public and immutable ledger, detailed data is accessible for all transaction activity occurring on permissionless crypto networks.

Over ten years ago, Chainalysis pioneered the field of blockchain analytics by combining this publicly available data with proprietary data and intelligence to ascertain the underlying identities of the entities conducting on-chain transactions. Building on top of this foundation, we have developed custom-made products to map the blockchain in order to identify potential suspicious activity, trace fund movements, and disrupt illicit activity across crypto networks. Over the past ten years, our tools and data have become indispensable to the workflows of law enforcement and intelligence agencies in the US and globally, as well as to corporate compliance and risk departments.

The most demonstrable result from this work is Chainalysis' support of hundreds of cryptocurrency cases involving seizures and freezing of assets in partnership with government agencies worldwide, helping secure an estimated \$12.6 billion dollars worth of illicit crypto with a median seizure size of \$5.9 million per action.⁵ Recent reports point to approximately 198,000 bitcoin currently under U.S. government custody. Chainalysis has supported much of the recovery of these seized funds, providing

⁵ "Asset Seizure and Cryptocurrency: How Chainalysis Creates Opportunities for Self-Sustaining Law Enforcement," *Chainalysis*, Mar. 26, 2025, <https://www.chainalysis.com/blog/cryptocurrency-asset-seizure/>.



the most comprehensive blockchain tooling and training to enforcement agencies and regulatory bodies across the world.

The following notable scam-related crypto seizures were only possible due to the transparency of the blockchain and the availability of state-of-the-art Chainalysis tools and data. They are also a reflection of the significant ability to disrupt illicit activity possible when the US government is willing to responsibly integrate private sector software and services into novel workflows.

- Stablecoin issuer Tether and the cryptocurrency exchange OKX announced that they collaborated with the United States Department of Justice in an investigation that led to Tether freezing approximately \$225 million in USDT tokens linked to an international human trafficking syndicate in Southeast Asia responsible for romance scams, helped in part by Chainalysis solutions.⁶
- In 2023, a South Korea-led Interpol operation saw authorities arrest 3,500 cybercriminals associated with online scamming and seize \$300 million in funds, \$100 million of which was made up of digital assets.⁷

Beyond these specific law enforcement examples, last year, Chainalysis launched Operation Spincaster designed to disrupt and prevent scams through public-private collaboration.⁸ Leveraging the transparency of the blockchain, Chainalysis proactively identified thousands of compromised wallets. This actionable intelligence formed the basis of a series of operational sprints across six countries (US, UK, Canada, Spain, Netherlands, and Australia) with over 100 attendees, including 12 public sector agencies and 17 crypto exchanges. The operational sprints featured training in identifying compromised wallets and tracing the stolen funds using Chainalysis Crypto Investigations solutions. Over 7,000 leads were disseminated during these sprints relating to approximately USD \$162 million of losses. These leads were used to close accounts, seize funds and build intelligence to prevent future scams. In fact, in one of the sprints, participants were able to contact a victim directly to warn them of an ongoing scam,

⁶ "Following Investigations by Tether, OKX, and the U.S. Department of Justice, Tether Voluntarily Freezes 225M in Stolen USDT Linked to International Crime Syndicate," *Tether and OKX*, Nov. 20, 2023, <https://www.okx.com/en-eu/learn/tether-okx-investigation> and <https://tether.io/news/following-investigations-by-tether-okx-and-the-us-department-of-justice-tether-voluntarily-freezes-225m-in-stolen-usdt-linked-to-international-crime-syndicate/>.

⁷ Toulas, Bill, "Interpol operation arrests 3,500 cybercriminals, seizes \$300 million," *BleepingComputer*, Dec. 19, 2023, <https://www.bleepingcomputer.com/news/security/interpol-operation-arrests-3-500-cybercriminals-seizes-300-million/>.

⁸ "Introducing Chainalysis Operation Spincaster: An Ecosystem-Wide Initiative To Disrupt and Prevent Billions in Losses to Crypto Scams," *Chainalysis*, Jul. 18, 2024, <https://www.chainalysis.com/blog/operation-spincaster/>.



prompting the victim to take preventative action on-chain by revoking the approval before the scammer was able to steal a six-figure sum.

AML compliance and the need for prevention

Chainalysis data and tools are not only integral to public sector operations and seizures but also play an important role in the AML programs of financial institutions, crypto businesses, and the broad swath of private sector businesses motivated to stop scam activity. Chainalysis data is leveraged by financial institutions for transaction monitoring, enhanced due diligence, and when appropriate, enhancing SAR filings. Our data serves as the intelligence driving blockchain transaction monitoring alerts for exposure to suspicious funds coming onto their platforms or customers attempting to send funds to illicit entities from their platforms.

At Chainalysis, we also think it is imperative to move past reactive compliance and fraud workflows at financial institutions and to start developing processes to prevent Americans from falling prey to scams altogether. Chainalysis' acquisition of Alteryx enables financial institutions to map the entire lifecycle of fraudulent operations, from initial online scam campaigns and money muling to monetization within financial services and subsequent money laundering and cash-out processes through proactive AI-driven scam detection, financial data, and infrastructure mapping. We utilize artificial intelligence and other advanced techniques to identify scam activities across various online sources, enabling large-scale early "upstream" detection. We construct a comprehensive scam social graph that interconnects fraudulent activities across various platforms, payment systems, and blockchains. Our adversaries are leveraging AI to rob Americans of their life savings, and we must leverage that very technology to beat them at their own game. This is what the future of combatting scams looks like.

Recommendations

1. Modernize and streamline scam reporting and response with the ability to efficiently share information on scams between the public and private sector.

Today scam victims in America have multiple options in federal and local law enforcement where they can report their crime. This has greatly contributed to a fragmented approach to combatting scams and reduces our visibility into the true scale of this war on potential victims both in the US and abroad. A centralized reporting database feeding from state, local, and federal reporting is critical to enhancing efficiency and actionable intelligence for cases leading to the recovery of funds, restitution, and the prevention of additional victims.

Similarly, Suspicious Activity Reports (SARs) are filed by financial institutions but the crucial information contained within these reports about particular scams is not accessible to other financial institutions or the other entities supporting scam prevention. This lack of information sharing creates blind spots and



delays in response, enabling scammers to continue their illicit activities unabated. Singapore's [Anti-Scam Command \(ASCom\)](#) is a great model for combatting scams efficiently by eliminating silos and working constructively with over 80 private sector partners. It is imperative that the industry and regulatory bodies work together to break down these information silos and create a more cohesive and collaborative approach to combating cryptocurrency-related scams. This will ensure that the inherent advantages of blockchain technology in tracing and combating financial crime are fully leveraged, and that scammers are not able to exploit the system due to gaps in communication and information sharing.

2. Ensure broad education and training about crypto networks and blockchain intelligence and invest in tech-driven efficiency by leveraging third-party blockchain analysis software and data to swiftly action intelligence and seize funds.

With the broader adoption of cryptocurrency on the rise, including by illicit actors, it is no longer sufficient to isolate knowledge about crypto networks to a small group of technical experts. Rather, government agencies and departments must ensure that a broad spectrum of personnel receive the latest training on how crypto networks operate, how blockchain analysis can supplement traditional analytical and operational workflows, and what actions can be taken to quickly disrupt illicit fund movements through crypto networks. Too often, victims are turned away from local authorities who are ill-equipped or even uninformed as to how to take on crypto cases. Other times, an individual complaint might not get prioritized if law enforcement doesn't have the analytic tools it needs to connect a low-value scam payment to a bigger scam conglomerate netting tens or hundreds of millions of dollars.

Particular offices within agencies that have invested in integrating blockchain analytics into their workflows have achieved massive successes - such as IRS Criminal Investigations and FBI's Virtual Asset Unit. However, the extensive overlap of crypto in all parts of many agencies' missions necessitates a broader cohort of staff to understand the underlying technology and how it is used.

We strongly recommend that US agencies invest in the training and tools to stay on top of the latest scam trends, enhance their visibility into their case to cover the full expanse of the scheme, and empower them to potentially seize illicit fund movements yielding huge dividends back to the US government in the form of billions of dollars of forfeited cryptocurrency.

3. Enact legislation that ensures a unified federal regulatory framework for cryptocurrency businesses.

Chainalysis is encouraged by the momentum within Congress to pass legislation that would create federal regulatory frameworks for stablecoin issuers and cryptocurrency trading businesses. From the perspective of mitigating scam activity, it is important to have a dedicated regulator that can understand



the unique operations of the business that they oversee and ensure that processes are in place to best disrupt bad actors and prevent illicit activity.

4. Close gaps of AML/CFT standards implementation for FATF members, especially countries that scammers rely on to launder funds defrauded from Americans.

More capacity building is needed in jurisdictions with weak AML and CFT policies that are providing havens for laundering the proceeds of scams defrauding Americans. In the absence of cooperation, more pressure is needed to disrupt the financial networks and the digital asset services flagrantly abusing laws and regulatory norms. Sanctions have proven to be an effective tool, and sustained enforcement actions targeting every facet of the scam supply chain – especially the offshore institutions defying international norms and AML/CFT processes and standards – would help cut scam perpetrators and their facilitators off from the global financial system.

-

Thank you again for the opportunity to provide testimony on this important topic. At Chainalysis, we continue to support the bipartisan efforts of the Committee, such as the recent passage of the OFAC Licensure for Investigators Act. We hope we can continue to be a partner on helpful initiatives by Congress to better protect against scams and fraud.

Chairman DAVIDSON. Thank you for that.

Mr. Brabant, you are now recognized for 5 minutes for your oral statement.

STATEMENT OF JEFF BRABANT, VICE PRESIDENT, FEDERAL GOVERNMENT RELATIONS, NATIONAL FEDERATION OF INDEPENDENT BUSINESS

Mr. BRABANT. Chairman Davidson, Ranking Member Beatty, Ranking Member Waters, and the members of the House Committee on Financial Services, thank you for allowing me to testify before the committee today.

My name is Jeff Brabant, and I am the Vice President of Federal Government Relations for the National Federation of Independent Business.

NFIB is the voice of small business in Washington, DC, all 50 State capitals, and our Nation's courts. We represent about 300,000 small business owners with the average NFIB member employing about seven to eight people.

Data privacy is a significant concern for small business owners. A prime example of this is the Corporate Transparency Act. Under the CTA, small businesses with fewer than 20 employees and 5 million in revenue are required to report their beneficial ownership information to the Financial Crimes Enforcement Network. This includes a scanned copy of a driver's license or passport of every beneficial owner.

Federal, State, local and international law enforcement and intelligence agencies can access this information without a subpoena or warrant. Small businesses fear their information will be targeted by criminals, politically motivated individuals, or subject to cyberattacks by our Nation's adversaries that could expose their personal information to actual criminals and nefarious actors.

Some small businesses have fallen victim to companies, which may be scam operators, offering to file beneficial ownership information (BOI) data. A recent search of "CTA BOI filing" on Google demonstrates this problem.

Three sponsored BOI companies appear before the official FinCEN result. One of these companies in particular, BOIR.org, even uses an imitation government seal with an eagle on it to appear like an official seal that the U.S. Government would use.

Recently, an Indiana farmer contacted NFIB regarding one of these scam companies. This farmer had begun the process to file through a scam company but did not complete the filing. Still, this farmer had \$249 charged to his credit card. Now the farmer is searching for a refund but likely will not get one.

Small businesses overwhelmingly oppose the CTA. Thankfully, President Trump recognized the absurdity of beneficial ownership information reporting requirements. He called the law invasive, outrageous, and an economic menace. He could not be more right.

The ultimate irony is that a law that supporters claim is for national security has likely opened the U.S. economy, American citizens, and small business owners to more data and privacy risk. The Federal database will be breached. It will be hacked, and private information will leak.

This is why Congress and Treasury must immediately and permanently delete the records of the millions of U.S. small business owners who already filed their BOI with FinCEN. This is non-negotiable. It has to be destroyed.

Let me be clear. The CTA is unconstitutional and should be overturned by the courts. Absent intervention from the courts, Congress can clean this mess up by passing Chairman Davidson's Repealing Big Brother Overreach Act. This legislation will repeal the CTA so a future administration could not revive or expand the statute.

Congress could also exempt law-abiding U.S. small businesses from the CTA, as the Trump Administration has proposed.

Before I close, I would like to draw attention to the issue of internet protocol (IP) and identity theft by fraudulent, as well as legitimate Chinese businesses, such as Temu.

NFIB members have shared stories of how their popular American-made products are being stolen and ripped off by Chinese companies. One of the more egregious examples is of the Illinois-based and American-made Power Planter. Power Planter is a garden auger manufacturer that works in standard cordless drills.

This small business has been the target of nonstop IP and identity theft by Chinese scammer companies. These companies will copy and paste Power Planter's copywritten images, verbiage, and advertising imagery, including their Made in America claim, and sell from China at a lower cost.

The Chinese product is of inferior quality, and, when it breaks, consumers do not even realize it is from China and often complain directly to Power Planter, even leaving negative comments on their social media pages.

Power Planter has dedicated significant resources to try and stop these scammers, but it is a full-time job. In fact, this small business has been forced to retain counsel, whose job is to track rip-off companies on sites like Amazon, Alibaba, and eBay, and report them to the appropriate company for removal.

There have been instances where Power Planter's counsel has removed several thousand such imposters in a single month. The process of getting the scam company taken down often takes several attempts, and even then, there is often a remedial process where they are allowed to begin selling again or another company pops right back up. It is an endless game of Whac-A-Mole.

These fraudulent companies are taking money out of the pockets of American businesses and workers.

Thank you for the opportunity to discuss the impact of scams and fraud on small businesses, and I look forward to your questions.

[The prepared statement of Mr. Brabant follows:]

TESTIMONY BEFORE THE UNITED STATES CONGRESS
ON BEHALF OF THE

NATIONAL FEDERATION OF INDEPENDENT BUSINESS



Statement of Jeff Brabant
Vice President, Federal Government Relations

**United States House of Representatives
Committee on Financial Services
Subcommittee on National Security, Illicit
Finance, and International Financial
Institutions**

Following the Money: Tools and Techniques to Combat Fraud

April 1, 2025

National Federation of Independent Business
555 12th Street NW, Suite 1001
Washington, DC 20004

Chairman Davidson, Ranking Member Beatty, and members of the House Financial Services Committee,

On behalf of the National Federation of Independent Business (NFIB), I appreciate the opportunity to participate in today's hearing on efforts to limit the impact of fraud on small businesses.

My name is Jeff Brabant, and I am the Vice President of Federal Government Relations for NFIB. NFIB is the nation's leading small business advocacy organization, advocating on behalf of nearly 300,000 small business owner members in Washington, DC, all 50 state capitals, and in our nation's courts. NFIB's mission is to promote and protect the right of our members to own, operate, and grow their businesses. NFIB is proud to represent small businesses nationwide from every industry and sector.

In recent years, small businesses have been through a lot. They have faced government-imposed COVID shutdowns, supply chain disruption, historic inflation, \$1.8 trillion of new regulatory costs, and systemic workforce shortages. Small businesses have largely weathered these storms, but many threats remain.

One constant threat is the reality that a single computer click can open a business up to targeted scams and fraud. As technology advances, small businesses must adapt to the everyday changes of a digitized economy. With those technological advances, the threat of protecting business data and customers is constantly on the minds of small business owners.

It is especially frustrating for small businesses when congressionally mandated reporting requirements open their businesses up to data privacy threats. A prime example of this is the Corporate Transparency Act (CTA). Under the CTA, small businesses with fewer than 20 employees and \$5 million in revenue are required to report their beneficial ownership information (BOI) to the Financial Crimes Enforcement Network (FinCEN).

The CTA has opened 32.6 million law-abiding small business owners to countless threats. For one, state, federal, and international law enforcement can access this

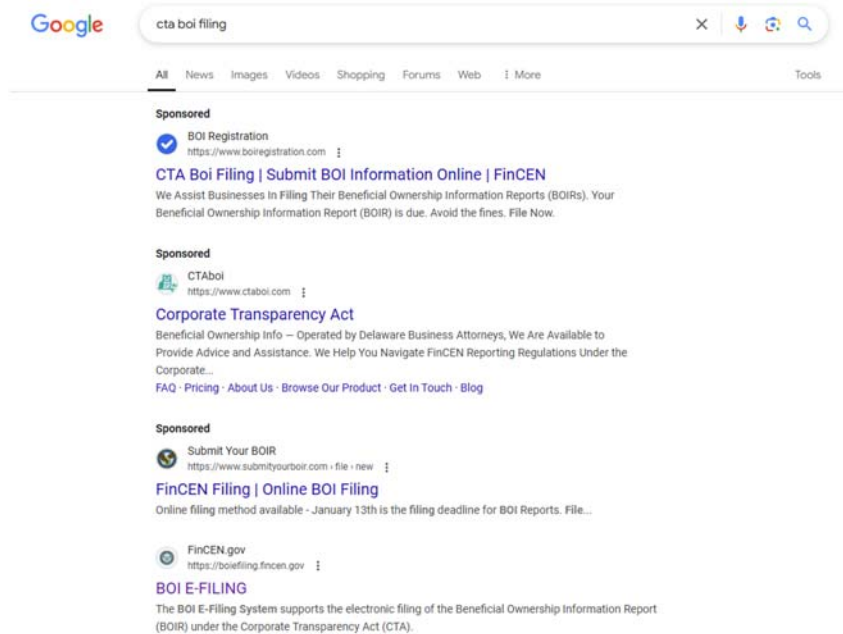
information without a subpoena or warrant. Small businesses fear their information will be targeted by criminals, politically motivated individuals, or subject to cyber-attacks by our nation's adversaries, that could expose their personal information to actual criminals and nefarious actors.

Small businesses have also faced other forms of phishing and scams from the CTA. I have heard from many small business owners who have sought assistance to file their BOI. Many have had to pay their CPAs or hire an outside counsel to assist with their filings. This is an unnecessary added cost that has increased red tape and compliance burdens for small businesses.

Others have fallen prey to profit companies, which may be scam operators, offering to file BOI data. A recent search of "CTA BOI Filing" on Google demonstrates this problem. As you can see in the image below, the search resulted in three "sponsored" BOI companies before the official FinCEN result. One of these companies in particular "BOIR.org" even uses an imitation government seal with an eagle on it to appear like an official seal the U.S. government would use.



BOIR E-Filing System



Just last week, an Indiana farmer contacted NFIB regarding one of these scam companies. This farmer had begun the process to file through a scam company but did not complete the filing. Still, this farmer had \$249 charged to his credit card. Now, the farmer is searching for a refund but will likely be without redress.

How many small businesses have fallen prey to these scam BOI companies? How many small businesses wasted hours and sunk significant resources into complying with the CTA? These resources are now unavailable to small businesses as they contemplate opportunities to expand, invest, hire new employees, or increase employee compensation.

It did not have to be this way. Congress should have written the CTA to be more targeted, prioritize small business data protection, and not treat over 32 million law-biding small business owners as criminals.

Small businesses overwhelmingly oppose the CTA. Thankfully, President Trump recognized the absurdity of BOI. He called the law invasive, outrageous, and an economic menace.¹ He could not be more right.

The ultimate irony is that a law that supporters claim is for “national security” has likely opened the U.S. economy, American citizens, and small business owners to more data and privacy risk. The federal database will be breached. It will be hacked, and private information will leak. This is why Congress and Treasury must immediately and permanently delete the records of US small business owners who filed their BOI with FinCEN. This is non-negotiable, it has to be destroyed.

Congress can also clean this mess up by passing Chairman Davidson’s H.R. 425, the *Repealing Big Brother Overreach Act*. This legislation has 133 cosponsors and would repeal the CTA so a future administration could not revive or expand the statute. I urge members of Congress to cosponsor and enact this legislation immediately. Congress could also exempt law-abiding US small businesses from the CTA, as the Trump administration has proposed.

Small businesses are very concerned with the privacy and security of their information. I think we can all agree with the need to protect data and information from nefarious actors. The question is how we do this.

I believe a starting point is to recognize what is working and what isn’t, and to correct the course. One way to do so is to stop doing economic harm. Congress must recognize that well-intentioned laws like the CTA are not working. The CTA is unlikely to achieve its goals because criminals will not file, but law-abiding small business owners will. All the CTA has done is increased red tape and compliance burdens, while missing the intended targets. Congress must recognize the law is burdensome, intrusive, duplicative, unnecessary, and unconstitutional.

Small businesses are optimistic that the Trump administration and 119th Congress will provide certainty for small businesses to grow, invest, and hire new employees. But doing so requires Congress to roll up its sleeves and get busy providing tax certainty, reducing regulatory burdens, and eliminating overly broad statutes like the CTA. A great starting point for this Committee to protect small businesses from fraud would be to require FinCEN to delete all BOI of US businesses and to repeal the CTA.

¹ @realDonaldTrump, Truth Social, March 2, 2025, <https://truthsocial.com/@realDonaldTrump/posts/114096106742782827>.

Thank you for the opportunity to discuss the impact of scams and fraud on small businesses and I look forward to your questions.

Chairman DAVIDSON. Thank you, Mr. Brabant.

Ms. Stokes, you are now recognized for 5 minutes for your oral statement.

STATEMENT OF KATHY STOKES, DIRECTOR OF FRAUD PREVENTION PROGRAMS, AMERICAN ASSOCIATION OF RETIRED PERSONS

Ms. STOKES. Thank you and good morning.

My name is Kathy Stokes, and I am the Director of Fraud Prevention Programs for AARP. Thanks for inviting me to testify on behalf of AARP at this important hearing.

This morning I am going to shed light on the true impact of fraud, its potential to victimize anyone, and its significant threat to national security.

Through the Fraud Watch Network, AARP educates older adults on the risk that fraud poses to their financial security, meeting them where they are. We have hundreds of volunteers that work with our State offices and communities all over the country to help older Americans avoid fraud.

We share information online, through newsletters, and to podcasts, and we cover fraud in most editions of our publications that tens of millions of Americans receive.

Our victim support program, including a help line receiving 500 calls daily, and support groups that address fraud's emotional impact helps people like Dave, who lost family and friends and contemplated suicide after having his home and his business stolen from him through a romance scam.

The recent growth in fraud has been meteoric, but the Federal Trade Commission (FTC) estimates underreporting, suggesting real fraud losses in 2023 were not the reported \$10.4 billion but \$158.3 billion.

Criminals do not discriminate on who they target, but when older adults are victimized, the financial impact can be catastrophic. These people are financially ruined. They experience emotional and health impacts. Often their families are torn apart, and many once financially secure Americans who did the right thing and saved for a comfortable retirement are left to rely on government safety nets.

In my written testimony, I describe how the sophistication and scale of today's transnational crime rings have led to them becoming a national security threat. These enterprises leverage a vast array of tools to commit their crimes, including all methods of communication and forms of payment, complex impersonation schemes, anonymous shell companies, human trafficking, and more.

Take the Jalisco New Generation Cartel in Mexico. It is using scams to fund things like sending meth and fentanyl across our southern border or take the massive explosion of financial grooming schemes, the origins of which are Chinese organized crime in Southeast Asia. Their goal is to cripple the U.S. economy.

The reason scams succeed beyond sophistication and scale relies on how our brains work. Criminals know that they can force our brains to bypass logic by getting targets into a heightened emotional state. Criminals call it getting targets under the ether, and academics have shed light on the actual science behind it.

Linda, a professor, shared her story with AARP about the day her life was turned upside down when a tech support scam that started with a fear-inducing computer pop-up message led to a 4 and a half month nightmare that forced her retirement and saw her buying gold bars and putting them into a stranger's car. When she realized the crime, she said it was like the walls of her house blew down.

Now, there is no single solution to the fraud crisis. It will take a whole-of-society approach. For individuals, it is things like better protecting ourselves, freezing our credit, using password managers and multifactor authentication.

For educators, it is focusing on the red flags that are important but so is training on how most scams come at to us and what to do when they do.

For industry, financial institutions must continue to innovate on fraud mitigation. Tech companies must build safety and security into product design and manufacturing.

Telcos must find a way for stopping the scams over the networks from reaching Americans, and industry and law enforcement must work together.

AARP is a founder of a new public-private partnership called The National Elder Fraud Coordination Center, and we will enhance the ability for private industry and the public space to work together to begin to solve elder fraud crimes.

At AARP, we are looking forward to working with policymakers to address fraud by supporting resources for State and local law enforcement: to hire and train staff and secure tools that combat the fraud crimes; to improve fraud reporting systems so law enforcement can prioritize cases; to reinstate the casualty and theft loss deduction to address the taxation of stolen assets; support legislation to limit the damage of crypto ATMs; and support the National Elder Fraud Coordination Center. You can learn more about that at fightelderfraud.org.

Thank you.

[The prepared statement of Ms. Stokes follows:]



Testimony of

Kathy Stokes
Director of Fraud Prevention Programs
AARP Fraud Watch Network

on

Following the Money: Tools and Techniques to Combat Fraud

before the

U.S. House Financial Services Committee
Subcommittee on National Security, Illicit Finance, and International Financial Institutions

April 1, 2025

AARP Point of Contact:
Clark Flynt-Barr
Director of Government Affairs, Financial Security
(cflyntbarr@aarp.org)

My name is Kathy Stokes, and I am the Director of Fraud Prevention Programs for the AARP Fraud Watch Network. I am honored to be here to testify on behalf of AARP, which advocates for the more than 100 million Americans age 50 and older. I would like to thank you and the members of the House Financial Services Committee for holding this important hearing, “Following the Money: Tools and Techniques to Combat Fraud.” AARP has long worked to educate consumers, support fraud victims, and improve fraud detection and prevention across industries, and we look forward to working with you towards policy solutions to prevent fraud and protect fraud victims.

AARP Fraud Prevention Work

The Fraud Watch Network is AARP’s program focused on helping our nation’s older adults understand the very real threat to their financial security that fraud represents.

We show up in communities around the country through all our state offices and their trained volunteer fraud fighters spreading the message of fraud prevention. We share robust information online at aarp.org/fraudwatchnetwork; we cover the issue in *AARP the Magazine* and the *AARP Bulletin* – which reach tens of millions of readers with each edition; we offer a biweekly email or text ‘watchdog alert’ newsletter and we produce an award-winning podcast, AARP’s [The Perfect Scam](#) – in the true crime genre but focused on the impact of this type of crime on victims and their families. We also offer a variety of virtual educational events, from member teletown halls to webinars and Facebook live events.

Beyond education, AARP is unique in its focus on supporting victims of fraud and their families. Our [Fraud Watch Network Helpline](#) receives around 500 calls a day. These calls can be from people who simply want to report a scam they’ve encountered but didn’t engage with, from people who aren’t sure whether that Publishers Clearing House letter claiming they’ve won \$1 million and a Mercedes is legitimate (it’s not), and too often, from victims and their family members in the aftermath of the crime. We also offer an online victim support group program, through which trained facilitators run small group sessions to begin to address the emotional impact of fraud victimization—helping older Americans rebuild their lives.

AARP has also been leading an effort to reframe the narrative on fraud victimization. Our society tends to treat fraud victims differently than other crime victims. We often blame them with the language we use: they’ve been tricked, or duped, or fooled, rather than stating that a criminal has stolen from them. We tend to believe that there’s nothing law enforcement can do because the criminals are abroad. Our narrative change movement is [rooted in research](#) that shows how our tendency to blame fraud victims has served to deprioritize fraud as a crime. This must change if we are to meaningfully combat this insidious and devastating crime.

Additionally, AARP is proud to be among the founders of the new nonprofit National Elder Fraud Coordination Center (or NEFCC) which formally launches this month. Similar to the National Center for Missing and Exploited Children, this private/public partnership will aggregate and analyze private and public sector fraud data through an organized crime lens, tying cases together to produce data-rich packages for federal law enforcement investigation and prosecution.

The Fraud Crisis

The growth in fraud crimes over the past five years has been meteoric. For example, published report data from the [Federal Trade Commission \(FTC\)](#) shows a reported \$12.5 billion stolen in 2024. But this number doesn't begin to tell the true story. In a [2024 report](#) the FTC submitted to Congress, the agency acknowledged the significant problem of under-reporting. Using its own estimates of under-reporting, the agency extrapolated that money stolen from fraud in 2023 was not the reported \$10.4 billion, but more like \$158.3 billion. And the agency pegged fraud losses among older adults at \$61.5 billion.

Fraud criminals know no demographic bounds. They seek to steal money and sensitive information from targets regardless of age, educational attainment, or socioeconomic status. But when they victimize our nation's older adults, the financial impact is too often profound and life altering. This stands to reason, as older adults are more likely to have accumulated a lifetime of savings and are more likely to have housing wealth. And, too often, the criminals steal everything. The victims are emotionally and financially ruined, often their families are torn apart, and many victims who were financially prepared for a secure retirement are instead left to rely on already strained local, state and federal safety nets.

The Criminals Behind Fraud

The driver of fraud's expansion since 2019 has been the growth of transnational criminal organizations behind most of the fraud we see today. Importantly, the funds they amass by stealing billions of dollars through fraud represents a national security threat.

For example, we know that the Jalisco New Generation Cartel in Mexico is a major contributor to fentanyl and meth crossing our southern border. They are now [known](#) also to run [timeshare resale scams](#) targeting timeshare owners in the United States, which helps fund their illicit activities. Last summer, FinCEN put out an [alert](#) on this alarming new trend together with OFAC and the FBI. We also know that illicit funds pulled in through ransomware and other attacks by the North Korea-backed [Lazarus Group](#) support the country's missile and nuclear programs.

In a highly sophisticated financial grooming scam with its origins in Southeast Asia, Chinese organized crime rings are stealing hundreds of millions of dollars from American targets. The [Economist](#) recently reported the experience of an individual who through human trafficking was enslaved to serve as a front-line scammer. He recalled the morning ritual where they all chanted things like "Death to the American Economy." This victim is but one of potentially hundreds of thousands of people who are victims of human trafficking that fuels this crime.

Why Scams Succeed

The days of snake oil salesmen and lone grifters have given way to transnational organized crime rings with corporate offices, employees (often enslaved prisoners forced by physical threat to be frontline scammers), lead lists, personally identifiable information (PII) from data hacks and breaches, scripts, and a playbook of how to turn a fraud target into a fraud victim. These criminal enterprises leverage a vast array of tools to commit their crimes, including all methods of

communication and forms of payment, complex impersonation schemes, anonymous shell companies, and human trafficking.

But sophistication and scale alone aren't the reasons they succeed. The reason scams are successful is largely because of how the human brain functions. AARP's own research beginning decades ago unveiled what criminal scammers refer to as getting their targets "under the ether." They have known since the beginning of time that to trigger a heightened emotional state is to bypass logical thinking – it is how our brains work.

What criminals call getting the target "under the ether, academics refer to as an "amygdala hijack." The amygdala is the part of our brain that processes emotions. When the amygdala is hijacked, the part of our brain responsible for logic – the prefrontal cortex, is bypassed. It's important to recognize that becoming a fraud victim is not the victim's fault. They didn't become a victim because of their age, educational level or cognitive impairment. They became a victim because of how our brains function.

This message is critical if we are ever to marshal a meaningful response to the fraud crisis. Until we all understand that fraud victims are crime victims and that they aren't responsible for becoming victims, we will fail to address this crime for the scourge it is.

Concerning Fraud Trends

The tactics of fraud criminals range from old school (stealing your mail) to high tech (hacks of banks, retail chains and other companies that stockpile consumer data). They might pretend to be from the government, utility companies, banks or big tech firms in order to steal sensitive personal information, or they send phishing emails with links that can infect devices with data-harvesting malware. Sensitive information is bought and sold among criminals on the dark web and via apps, which other criminals then use to better target their victims.

Methods of attack by these criminals span across communication channels: phone calls, emails, text messages, social media, online ads and other pop-up messages, fraudulent apps, mail and at times, in person. In other words, there is no form of communication that fraud criminals have not made dangerous.

Of the hundreds of fraud types in play, three are of particular concern: the tech support scam, the bank impostor scam, and financial grooming.

Tech Support Scams

A [tech support scam](#) may originate with a call from someone claiming to be with Microsoft or Windows tech support, or via a pop-up window on your device screen. The target is warned that a virus has been detected, and to protect their data, they must go to a web address or call a provided phone number. Inevitably, the "tech support" person convinces the target to allow them to remotely access their device, leading often to even more complexity to the scam and massive financial losses.

Helen, from Southern California, told AARP's Fraud Watch Helpline that she received a pop-up message on her computer screen along with a loud voice warning: "Do not turn off your computer!" Helen was instructed to call the phone number on her screen, and she soon found herself talking to someone who claimed to be a tech support staffer from Microsoft. The fake tech support staffer told her that her computer was under attack and convinced her to download software that gave him access to her computer and its data.

Helen didn't realize that the "helpful" technician was part of a fraud ring, and that the pop-up on her computer was a fake. He offered to put her through to the security department, where someone posing as a bank official told her that hackers already were stealing from her account, and she needed to quickly move her funds to a new, safe account. Helen followed his instructions, withdrawing cash and buying gift cards and sending wire transfers and cashier's checks to addresses in other cities. Most of her retirement nest egg was stolen before a bank fraud investigator intervened, convincing her to speak to her family about what was happening.

Bank Impostor Scams

In this [growing scam](#), a target receives a text message from what appears to be their bank, asking them if a certain transaction made on their account is legitimate, typically requesting a Yes or No response. The target sees a transaction they didn't make and responds No.

A phone call immediately follows, ostensibly from their bank. The caller explains that they are their bank's fraud investigator, and their accounts are actively being hacked. The fake bank investigator then helps the target transfer their assets to keep them safe. The ending is always the same; it wasn't the person's actual bank and the victim's assets have been stolen with little chance of recovery.

Magis, who reached out to AARP's Fraud Watch Network Helpline, experienced this scheme. She was made to believe that her bank's fraud investigators were seeking to help her address fraud in her accounts. They told her that her stolen identity was being used by foreign cybercriminals who used it to buy child sexual exploitation materials, murder people, and sell body parts. The impact grew to affect her retirement account, and more than \$1 million was stolen throughout the scam. Magis has suffered significant stress and faces the possibility of being forced to sell her home and face homelessness.

Financial Grooming

Romance scams are sadly common, where a victim is manipulated over time to believe they are in a deep love affair with someone they've met online, only to be crushed when they learn it was all a lie and their savings had been wiped out as well.

A [more recent form of this scam](#) typically begins with what seems like an errant text message such as, "Hey Bob, are we still on for dinner at 7?" The recipient kindly responds to tell the sender they have the wrong person. And that is all it takes to build out a conversation, that turns into a friendship that becomes a trusted relationship, that leads to a devastating investment fraud that destroys victims emotionally and financially.

In this particular scam, there are victims on [both ends of the crime](#). Southeast Asian organized crime groups lure frontline scammers with fake job offers. Once they arrive, the criminals take their passports and force them to phish for potential scam victims for endless hours a day under threat of violence and even death. This crime is dubbed by the criminals who came up with it, Pig Butchering – where they fatten the victim before slaughter. The term is so loaded with victim blaming that many in this space refer to it instead as financial grooming. Through an in-depth investigative report from [The Economist](#) published in February, readers learned that a stated goal of this crime is to “cripple the US economy.”

Their targets are groomed over weeks or months and at some point, the scammer explains that they have such a great life with cars and homes and jewelry because of their investments in cryptocurrency – and they can show the target how to trade. The scammer convinces the target to access an online or app-based crypto exchange and encourages small investments at first. The returns entice the target to invest larger amounts, and the returns continue to grow. When the victim decides it’s time to cash out, they are told they first have to pay thousands in taxes. The victim may even cash out other accounts to pay the taxes, only to find that the entire ordeal was built on a brutal lie.

While these cases typically focus on fake investments in cryptocurrency, sometimes the commodity is precious metals.

Cryptocurrency ATM Scams

AARP has seen an alarming increase in criminals using cryptocurrency kiosks to steal hardworking Americans money. Cryptocurrency kiosks, also known as “crypto ATMs,” “BTMs,” or “virtual currency kiosks,” can be found in supermarkets, convenience stores, gas stations, bars, and restaurants. Crypto kiosks look like bank ATMs and allow people to conduct legitimate cryptocurrency transactions, such as sending money to digital wallets. Today, there are more than 45,000 crypto ATMs nationwide. However, because crypto ATMs are largely unregulated at the state level compared to traditional financial institutions, such as banks and other money service businesses, they lack similar fraud protections. As a result, criminals are using crypto ATMs to steal hundreds of millions of dollars from Americans each year through fraudulent schemes.

The way these scams work is that criminals – often impersonating government officials or businesses – convince individuals that they must address an urgent financial matter, directing them to withdraw large amounts of cash and put that money into a crypto ATM. It is then transferred to a digital wallet controlled by the criminal.

Older adults are disproportionately affected by fraud and scams using cryptocurrency ATMs. In 2023, the FBI received [over 5,500 complaints](#) involving crypto kiosks, and Americans reported over \$189 million in stolen funds. Over 65% of the theft losses in cryptocurrency kiosk fraud were experienced by adults 60+. AARP is advocating for important consumer protections that will deter criminals from leveraging cryptocurrency kiosks in their schemes. Our state-level advocacy recently led to the passage of a bill in Nebraska to put important consumer protections, including fee and exchange rate transparency, fraud warnings, and transaction limits in place.

This will help prevent older Americans from losing their retirement savings they worked so hard to amass.

A Path Forward

It may seem that we are in a fraud quagmire with little hope of getting out. There is no single solution, but there are roles for each sector of our society that will go a long way to turning the tide on the fraud tsunami.

For individuals, it's taking steps to better protect ourselves and our loved ones from fraud attacks. Such actions include freezing our credit, using a password manager and multifactor authentication, shredding documents, keeping our device operating systems updated to protect against known vulnerabilities and not engaging with incoming messages from unknown persons. And share what we know. Each of us should make it a point to talk about the latest we've heard about fraud with our family members and friends. The more we talk about these scams, the better protected we will be.

For educators, it is important that we tell consumers about the signs of the latest scams and their red flags. But what if we are able to come up with something simpler? If we can train our brains on how most scams come at us and what to do when they do, we could probably thwart a great deal of crime before it happens. Most scams come as a communication out of the blue that gets us immediately into a heightened emotional state and contains urgency. If we could train consumers that this scenario is likely a scam, we can train them how to react. AARP has been working on this concept with input from people around the globe and are hopeful something can be accomplished.

Industry has a critical role to play as well. Financial institutions must continue to innovate on fraud controls and mitigation. Tech companies must build security into the design and manufacture of technology products, so that products come to market secure by design and safe by default.

From a public policy perspective, there are many actions Congress can take to address the fraud crisis.

For example, we are very pleased that Representative Zach Nunn (R-IA) has reintroduced legislation, the GUARD Act, which would direct federal funding to state and local law enforcement agencies to hire personnel, train staff, and secure tools to fight these crimes, empowering them to combat fraud committed against Americans. With new technology now playing a role in many forms of financial crime, law enforcement must have the right tools and training to unravel complex investigations and give victims the justice they deserve.

AARP has also urged Congress to improve fraud reporting systems to ensure that law enforcement can adequately prioritize cases. The Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) is the central site for reporting cyber-enabled crimes. Currently the FBI generally does not have advanced analytics capacity or interoperability across FBI systems. The result is that the FBI cannot identify commonalities between reported crimes

and cannot search these reports to compare with information in other systems. Without the ability to analyze information to identify the most commonly reported identifiers or between systems, the FBI cannot easily find potential links between cases. Ultimately this could lead to a situation in which the severity or extent of a crime is not recognized and perhaps not properly reviewed because it appears to be under a threshold for investigation. We are advocating for the FBI to prioritize enhancements to its data systems so that IC3 reports can be easily searchable and analyzed for potential links.

AARP is also advocating for the reinstatement of the casualty and theft loss deduction. The impact of fraud often goes beyond the theft of funds – if a criminal has stolen funds from a victim's 401(k) or other taxable account, this is considered a taxable event and the victim will likely owe taxes on the funds withdrawn from the account, and often end up in a higher tax bracket, compounding the loss. This is an insurmountable burden for many victims, many of whom no longer have the ability to pay this tax bill due to the fraud loss. It can also impact a victim's eligibility for public benefits based on income. As of 2018, theft losses are no longer covered under the tax code and casualty losses are only covered if the loss is due to a major disaster as declared by a Presidential disaster declaration. There have been several pieces of legislation introduced in Congress to reinstate the casualty and theft loss deduction and AARP urges Congress to restore the deduction in any upcoming tax package.

Industry and law enforcement should champion the success of the new National Elder Fraud Coordination Center (NEFCC), noted earlier. Even with underreporting, law enforcement is swimming in a sea of elder fraud reports. Scarce resources make it difficult for investigators to link cases. Jurisdictional challenges that come with transnational organized crime investigations limit prosecutions. Developing high-priority, high-impact cases takes time, labor, and analysis. A national coordination center like NEFCC -- with the leads, the data analysts, and the combined resources of the private and public sector -- can overcome these obstacles. In addition to the ability to create rich law enforcement investigative packages, incoming data from members could offer opportunities to neutralize known fraud vectors.

Indeed, [in a commentary piece](#) for *Fortune*, Nasdaq Chair and CEO Adena Friedman unveiled research that shows that annual GDP growth in the US would be 0.5% larger without fraud. Friedman says fraudulent acts too often go unnoticed but can be mitigated by better communication between the public and private sector. NEFCC marks an important and imminent means of producing this coordination.

Policymakers have an important role to help victims and bring the fight to fraud crime rings, including legislative solutions such as: providing more resources to train state and local law enforcement to investigate fraud crimes; reinstating the casualty loss deduction to address the significant tax burden that fraud victims face having to also pay taxes on the assets that were stolen; limiting the damage of fraud involving cryptocurrency ATMs; improving staffing of DOJ's Elder Justice Strike Forces; and enhanced efforts such as the National Elder Fraud Coordination Center to bring the public and private sectors together to build cases for investigation and prosecution.

Conclusion

Addressing fraud requires more than piecemeal solutions; it demands a whole-of-society approach. We cannot educate our way out of the fraud crisis. Industry cannot mitigate and engineer our way out of it. Policymakers cannot regulate our way out of it. And law enforcement cannot arrest our way out of it.

But, together, educators, policymakers, law enforcement and industry can turn the tide against the vicious crime gangs who hold the power right now. Together, we can disrupt their business model, protect millions of consumers, and safeguard billions of dollars in savings and retirement accounts and in our economy.

We thank this Committee for bringing attention to this important issue and look forward to working with you to turn the tide on criminals committing fraud.

Chairman DAVIDSON. Thank you.

I really appreciate all our witnesses. We learned a lot just from your opening statements, and, wow, what a challenge.

We will now turn to member questions.

I now recognize myself for 5 minutes of questioning.

Mr. McLaughlin, based on your 27 years of experience, have you seen an expansion in the efforts to stop fraud?

Mr. McLAUGHLIN. Thank you for your question, Chairman.

Over 27 years, yes, there has been a huge, huge, emphasis on protecting our customers in the industry. We have tackled this via enhancing our education programs, via workshops in our branches, educational material posted on our websites——

Chairman DAVIDSON. So your own efforts in the industry, but also you have seen more regulatory pressure to disclose and report, correct?

Mr. McLAUGHLIN. Correct, yes. The increased significance or pressure placed on financial institutions to identify and report suspicious activity and fraud has grown over the course of the last 27 years.

Chairman DAVIDSON. Has the number of fraud cases and the size and scope of the fraud also increased?

Mr. McLAUGHLIN. Yes, sir.

Chairman DAVIDSON. In a way, it is like, well, in spite of our effort, we have not really stopped it. We have not necessarily shrunk it either.

Some would say, “Well, gosh, imagine how bad it would be if we had not been doing these things.” On the other hand, maybe the way we are going about it is not working.

Could you highlight what you think works and what maybe could be done more effectively from your experience.

Mr. McLAUGHLIN. Thank you again.

From my experience, what has been working is the increased investment within the public sector in education, in advanced technologies to catch the fraud at the front door, as we call it, before they are able to transact with the institutions. Also, advancements in the models and scenarios for which we monitor customer behavior once that account is established.

What we could be doing better, I would say, is establishing that relationship, that public-private relationship, where there is a flow of information back and between the government and the regulated financial institutions that I represent.

The government sits on a mountain of data from the hundreds of thousands of SARs that are filed and CTRs that are filed, as well as the prosecutions that law enforcement——

Chairman DAVIDSON. Do they normally get back to you? Here is a case: I was working on the Weaponization Committee last Congress. One bank was asked by the Federal Bureau of Investigation (FBI) to report on their customers, and the bank said, “We need a warrant or subpoena.” Then the FBI came back and said, “Well, why do you not generate a suspicious activity report,” where none had previously existed.

Is that kind of interaction with law enforcement normal?

Mr. McLAUGHLIN. Yes. The financial services and the financial institutions that I have had the honor of working for do have good

relationships with law enforcement. However, to protect the laws and the regulations that the financial institutions fall under, we do often, after conversations with law enforcement, request the subpoena to turn over information.

Now, it is unusual to receive that type of conversation where a SAR was not filed, but usually once the SAR is filed, outreach begins, and conversations and flow of data start happening.

Chairman DAVIDSON. Thank you for that.

I look forward to working with you all and my colleagues to make our system more effective.

I just want to highlight Mr. Brabant. I appreciate your testimony because not only are individuals being scammed, but businesses are and especially small businesses.

You referenced a bill, the Repealing Big Brother Overreach Act. It has 133 House cosponsors and identical legislation sponsored by Senator Tuberville in the Senate.

The change that you referenced that the Trump Administration has done by focusing beneficial ownership reporting requirements on foreign entities, is that an improvement for American citizens?

Mr. BRABANT. I think absolutely an improvement for American citizens and an improvement for American small businesses. When you are looking at 32.6 million reports FinCEN was expecting in year one, that is not a risk-based approach, that is a needle-in-a-haystack approach. When you refine it down to a smaller, more risk-based approach, it should be a win.

Chairman DAVIDSON. I appreciate you also referencing to what we need to do with the existing data, so thank you for that.

Ms. Stokes, I really appreciate your emphasis on seniors and the great work you have done to educate seniors.

Working with our county prosecutors, do you have a way to roll that toolkit out through member offices, so we make sure that our county prosecutors who are on the frontlines—they often feel unsupported by Federal resources.

In your experience, in what you are seeing, are these like lone actors trying to scam people or is it sort of an organized crime effort that is hitting individuals and businesses?

Ms. STOKES. Thank you for that question, Representative.

For a long time, we have all held this assumption that the fraudster is some guy in his mom's basement making phone calls and lurking on social media. I am sure those guys are still out there, but they are not the ones that are causing the majority of the problems.

This is transnational—

Chairman DAVIDSON. Thank you. I wish I had longer, but my time has expired. I hope you can respond in writing. Sorry I did not leave you enough time there.

My time has expired, and I now recognize the ranking member of the subcommittee, Ms. Beatty, for 5 minutes for questions.

Mrs. BEATTY. Thank you, Mr. Chairman.

I will continue with Ms. Stokes.

I think we all touched on this earlier, but I would like to go a little deeper into it. The bipartisan Corporate Transparency Act, as you know, was created to prevent bad actors from hiding behind anonymous shell companies. Can you clearly lay out for us how

this relates to fraud prevention and how the CTA and the beneficial ownership database would be a critical fraud prevention tool?

Ms. STOKES. Thank you, Representative Beatty, for that question.

I think that—I have a lot of opportunities to interact with law enforcement, financial crimes investigators, and I understand from them how critical information is and will help them get to the bottom of the cases. Anything that takes away from that would be a challenge.

The tools that criminals use are vast. They are complex impersonation schemes and fake websites, shell companies, and human trafficking. There are so many crimes within this crime.

Mrs. BEATTY. Maybe you can answer this as a follow-up. Can you address how Treasury's recent decision to exempt more than 99 percent of the companies that Congress intended to cover will weaken our fraud prevention efforts?

Ms. STOKES. Thank you, Representative.

I can say that anything that is going to reduce information that can be actionable by law enforcement from our perspective when it comes to fraud that is a crisis, is very problematic.

Mrs. BEATTY. Okay.

Mr. McLaughlin, let me ask you this. It has been mentioned several times already this morning that fraud is rapidly on the rise, by you, by my colleagues. Each year American consumers, as we know, are reporting significantly greater financial losses to scams, and we clearly need to take, I believe, a whole-of-government approach to tackling this problem.

I understand that there are several Federal and State and local organizations that play various roles in addressing fraud, but there is currently no one central location for fraud victims to seek help.

Can you shed some light on or explain the current disjointed framework and any suggestions you would have for us in Congress that we could instate a streamlined, user-friendly process for fraud victims to report these crimes to?

Mr. McLAUGHLIN. Thank you for your question, Ranking Member.

Currently, in the industry, we work with several not-for-profits that focus on this, including AARP and other well-established fraud, anti-fraud groups. At the local, State and Federal law enforcement level, we also interact because we all believe that this is something that is growing and that we need to tackle.

There are working groups that are established. There are conferences that are held where idea-sharing occurs. There is also a greater need for transparency in the actual anti-fraud movement.

When financial institutions in the public sector file suspicious activity reports or file with adult protective services when it comes to elder exploitation, there is very little time we get feedback on the information that we provided to see if it was actionable for those agencies.

The sharing of knowledge back and forth would allow us to actually target specific threats to our customers and our population. Centralizing a fraud group within law enforcement or a regulatory agency would give our customers a central point of contact but also

allow the financial institutions as well to have a central point of contact to continuously build upon the programs that we have.

Ms. BEATTY. Okay.

I might have enough time for either one of you to give us any insight on how fraudsters are using social media platforms to lure victims in.

Ms. Stokes? Mr. McLaughlin? Anything on that?

Ms. STOKES. Thank you for that question.

Yes, social media is one of the biggest vectors for fraud, and we see so much harm coming from them. Yet, we do not see a concerted effort to take down the social media profiles that are there and are known to be related to scams, and a lot more needs to be done by that industry to—

Ms. BEATTY. My time is almost up. Yes, or no? Is that something that Congress should be looking into, you believe?

Ms. STOKES. Yes.

Mrs. BEATTY. Okay. Thank you.

Chairman DAVIDSON. Thank you.

The gentleman from Oklahoma, also the Chairman of the Task Force on Monetary Policy, Mr. Lucas, is now recognized for 5 minutes.

Mr. LUCAS. Thank you for holding this hearing, Mr. Chairman. Thank you to our witnesses for testifying today.

In my regular meetings with bankers across my home State, the issue of fraud is one that often comes up. They are on the ground. They are seeing the people in their community being taken advantage of.

It is unfortunate then that, oftentimes, Federal agencies place reporting burdens on our financial institutions rather than trying to get at the root of the problem.

Mr. McLaughlin, how does it affect your communities, our communities, I should say, when our credit providers have to spend all their time complying with what some might define as burdensome reporting requirements?

Mr. McLAUGHLIN. We have finite resources available to us within the public financial institution sector. When increased burden is placed on us, we have to make certain risk-based decisions as to where to deploy those resources, where to spend money, on our investments in technology and other operational efficiencies that we can garner to continuously focus on the mission of catching as many bad guys as we possibly can.

When we get more burden in terms of more checkbox exercises, that just means we have to expend more resources to tackle the job.

Mr. LUCAS. If I could follow up on that question.

Oftentimes, our credit providers are the first to notice when something goes wrong. I recently met with bankers again in my district that told me countless stories of how they were able to identify fraudulent activities and protect their customers.

Bankers are allies in detecting fraud, but they are not responsible for enforcing the law, and they should not be asked to do so by the Federal Government.

Mr. McLaughlin, could you expand on how we could support our financial institutions that are targeted by these crimes?

Mr. McLAUGHLIN. I am going to go back to—and thank you for your question.

I am going to go back to the transparency between local, State, Federal law enforcement, regulatory agencies, and FinCEN.

The access to data and allowing these smart individuals that we have working for us and data scientists across all sectors, allowing us to analyze the data to focus on the threat at hand instead of having us focus on check-the-box exercises that many financial institutions face today would be a huge step forward.

Mr. LUCAS. Turning to you, Mr. Brabant, I have heard again from a number of my small businesses across Oklahoma that are worried about the increased administrative burden that many reporting requirements place on them.

Small businesses, by definition, have fewer resources to devote to these lengthy and elaborate reporting regimes. Can you talk about the harms of overly broad reporting mechanisms?

How does rulemaking like the previous administration's rule on beneficial ownership, actually hurt our efforts to stop fraud?

Mr. BRABANT. Yes. When something is overly broad, it is extremely challenging. For example, you have the "substantial control" prong in the definition, which is essentially defined as "substantial control."

The previous administration defined it so broadly to be senior staff. If you are a restaurant manager and you have no ownership stake, you probably have substantial control.

One of the challenges when you are a small business owner is, well, what senior staff do I have to put in? FinCEN does not clearly define this. You are worried about going to jail for 10 years because you might not have put enough senior staffers in. It is a real challenge.

Then you have to ask yourself how pertinent is this information that is being reported that has sometimes just staff out there with no ownership control at all.

Mr. LUCAS. Ms. Burns Koven, you have worked in this industry from various vantage points and have seen the ebbs and flows of the financial crime operators. What trends are you seeing today in financial fraud and how can we, perhaps, try to get ahead of this industry, so to speak?

Ms. BURNS KOVEN. Thank you for that question.

I think we have seen broadly that illicit actors of all stripes, whether that be fraudsters, drug traffickers, are using jurisdictions with weak AML/CFT standards. They are looking for those paths of least resistance.

In closing those gaps, in capacity building or even applying pressures to jurisdictions willingly being blind to the use of their platforms for laundering, we can better identify and prevent these illicit actors from reaping the rewards of their activities.

Mr. LUCAS. Mr. Chairman, let me simply say, in closing, customers are feeling it. Financial institutions are feeling it. Fraudsters do not discriminate when it comes to who they steal from, and we need to focus on that problem and give our law enforcement tools it needs to stop these criminals rather than just more paperwork.

Thank you, Mr. Chairman.

I yield back.

Chairman DAVIDSON. I thank the gentleman.

The gentlewoman from California, also the ranking member of the full committee, Ms. Waters, is now recognized for 5 minutes.

Ms. WATERS. Thank you very much, Mr. Chairman, and members.

I am about to ask a question about a particular situation in this country that is hardly believable, but I am pleased that we are here talking about following the money, tools and techniques to combat fraud.

Here is some money I want us to follow.

Ms. Stokes, days before Donald Trump took office, he introduced the meme coin dedicated, of course, to himself. While the entities behind his Trump meme coin earned nearly \$100 million in trading fees in less than 2 weeks, hundreds of thousands of small traders suffered \$2 billion in losses over the same timeframe.

Days after he released his coin, Melania Trump issued her own coin. The many concerns about this are not only that the Trump family profits or how this venture has become the biggest component of the President's personal wealth, more than even the real estate for which he is known. It raises questions about the use of cryptocurrency, including meme coins to entice, to police, to defraud people out of their hard-earned savings.

Further, at the same time that Donald Trump is offering his meme coin and other cryptocurrency products to enrich himself, his regime is considering the rules that will define how cryptocurrency is regulated. They are in charge.

It also comes at a time when Trump and Republicans are working hard to lower, even to remove, barriers to fraud and financial crime.

As an expert in fraud prevention, how do criminals use cryptocurrency to commit fraud, especially that which targets older Americans? Why is cryptocurrency so attractive to bad guys and how do the perpetrators, such as transnational criminal organizations, make crypto appealing to the victim?

By the way, not only has the President created this coin, meme coin, he is also involved with the company on Stablecoins—because we are negotiating Stablecoins right now. In the middle of our negotiations, he is creating his own company on Stablecoins.

What is going on?

Ms. STOKES. Thank you for that question, Representative Waters.

I do know that when cryptocurrency is in the news, the criminals follow. This does create tremendous opportunity because generally everyday Americans do not really understand what crypto is. They do not understand that its value is simply based on supply and demand, so the investments can seem really attractive.

We are seeing two ways that crypto is showing up in the fraud space. One is crypto investment schemes where people are having everything stolen from them. That is the goal of the criminals, to steal every penny from every victim.

The other is the use of crypto ATM machines. You have probably seen 12,000 of them around the country. They are in big businesses and grocery stores. The criminals are convincing the victim of an

urgent matter that they have to address, and they have to go to the bank. They take out wads of cash, then they walk over to these crypto ATM machines, and they put a hundred dollars at a time into these machines, taking sometimes hours, which is a risk in and of itself. Then they send the money to those who they think are going to help them, and it goes into the wallet of a criminal.

Ms. WATERS. Wow. Well, thank you. Let me move on.

We know that anonymous shell companies are common tools used by fraudsters to facilitate their crimes and to launder the proceeds of their bad act.

For example, two Chinese nationals were arrested for allegedly leading a scheme to launder 73 million in proceeds from cryptocurrency investment scams. The victims transferred millions of dollars to U.S. bank accounts opened in the names of over 70 U.S. shell companies whose apparent purpose was to launder the proceeds of the fraud.

Similarly, the leader of a large-scale time share resale scam was sentenced to prison for defrauding more than 1,000 victims, many of them elderly, out of their millions, using a network of fake front companies in cities across the country.

These examples abound, and I would like to submit for the record a fact sheet from the Transparency International U.S. that describes how these corporate entities registered in the United States are abused for a range of fraudulent purposes.

The Trump regime, with the help of my colleagues across the aisle, are trying to make such fraud schemes easier by gutting the Corporate Transparency Act, which helps the government combat who—

Chairman DAVIDSON. The gentlewoman's time has expired.

Ms. WATERS [continuing]. truly owns these shell companies. Enough, enough, enough.

I know I do not have any more time.

I yield back.

Chairman DAVIDSON. Without objection, I will accept the gentlewoman's submission without objection.

[The information referred to can be found in the appendix.]

Chairman DAVIDSON. The gentleman from Texas, Mr. Sessions, is now recognized for 5 minutes.

Mr. SESSIONS. Mr. Chairman, thank you very much.

Before we go too far, I want to acknowledge the gentleman, Hon. Jack Fields, former member of our Texas delegation who was the Ranking Member of Energy and Commerce when he retired in 1996, is with us today.

Mr. Fields, I want to thank you. You have been a guardian of moving America forward for a long time, and I think, as you watch what is going on and have since you have left, you have seen where the things that developed also have a downside to them, an underbelly that we are speaking about today.

I want to, if I can, go to anybody on the panel. I have heard—I have read the testimony and also the things which we have prepared Mr. Davidson's great staff about, the overview. Increasingly, what comes out today is we have a problem, and I think we have seen and heard this.

What has Federal law enforcement done to mirror up to try and stop this?

I know there are working groups. We heard there is a national elder fraud, a task force you are trying to gather together as an industry.

Who is—What agency is the lead that you would look to?

Anybody.

Mr. McLAUGHLIN. I will take the first stab at that.

Thank you for your question, sir.

From a financial institution standpoint, we would interact with local or Federal agencies within the State that we found fraud.

Mr. SESSIONS. Can you name that? In other words, I know that the Securities Exchange Commission (SEC) or Financial Industry Regulatory Authority (FINRA) has jurisdiction over looking at transactions and data information. When you have something that you considered to be a crime, who do you look for? Who is the lead agency?

Mr. McLAUGHLIN. Again, thank you for your question.

It depends on the fraud that we are seeing. If we are seeing checks or financial fraud, we would contact the Secret Service in some cases because they sit within the Department of Treasury and have that exposure.

If we are talking about elder abuse, financial exploitation, we would reach out to Adult Protective Services (APS) and/or the FBI within the city or State that the crime is taking place.

Mr. SESSIONS. Have we, as Members of Congress, through the law, made it clear to not just consumers but really the industry about who—have we streamlined that? Do you know who to go to in a given circumstance?

Ms. BURNS KOVEN. Thank you for the question.

I think more can be done to streamline reporting and modernize it so that we can connect the dots from a one-off investigation to understanding that entire scheme so that we can actually increase recovery and restitution and make more victims whole.

We have had spectacular seizures by U.S. Government of cryptocurrency assets. Chainalysis has worked with governments around the world seizing over \$12.6 billion worth of illicit crypto.

More needs to be done to upskill and train at the State and local level to ensure those departments that are the first line of response oftentimes for victims are well equipped to understand and act quickly to pursue these cases and seize those funds.

Mr. SESSIONS. I am well aware that many U.S. attorneys and other agencies within law enforcement want to look at minimums. It is not big enough for them until it gets to a certain stature, and I have heard testimony, which I believe is true, unless you go and plug a circumstance and challenge someone, they are going to continue these things.

I think that it is important that what the chairman is doing here. That we do pass his piece of legislation that I received yesterday, but we also have to have that translate to the Department of Justice, to law enforcement that actually we honor them and ask them to please understand more about this.

I think, as they look at the crime, they also see what might be called MOs, method of operations, of how people do this. Then the

feedback comes to you, which was talked about. We fill out these reports, and we do not hear anything back. We are not sure whether what we are providing is enough information, whether it was specific information.

I think some success stories would go a long way to do that. I think that I would love to have this subcommittee delve into that angle of what we need to do better to incent law enforcement to want to do that, whether it is us paying attention or gathering things together.

I want to thank you, Warren, for doing this hearing. I think it is most instructive about our job as Members of Congress to warn people, in particular seniors.

I yield back my time, Chairman.

Chairman DAVIDSON. I thank the gentleman.

The gentleman from California, who is also the Ranking Member of the Task Force on Monetary Policy, Mr. Vargas, is now recognized for 5 minutes.

Mr. VARGAS. Thank you very much, Mr. Chairman, and thank you for holding this hearing.

I also thank the ranking member and the witnesses. Thank you for being here. I think it has been very, very informative.

I do have to call out, though, right at the beginning, when a lot of my colleagues on the other side like to talk about unconstitutionality or illegal acts. It is funny that none of them seem to call out the executive orders of President Trump.

In fact, interestingly, a Republican-appointed judge, Judge John Coughenour said this, "that one of the orders is blatantly unconstitutional." He says, "I have a difficulty understanding how a member of the bar could State unequivocally that this is a constitutional order. It boggles the mind."

Again, I think it is important to call that out because I know we have heard time and time again since I have been here the CFPB is an illegal bureau. It went all the way to the Supreme Court. Certainly, the Supreme Court did not agree with my colleagues. I think that has to be called, so I call it out.

I do want to ask this. There seems to be a contradiction in what some of you have been saying today. It is interesting. If you listen to what some of you said, you said, "The government has a whole bunch of information, and they ought to give it to us, and sometimes in real time so we can help them solve this fraud problem."

Then I heard somebody else saying, "The government has too much information, and this information, in fact, could be hacked and then that would be very detrimental to us."

It seems that is what I heard. Did I not hear that?

Let me go first to Mr. Brabant. It sounded to me like you were saying you are not confident with some of the information the government holds.

Mr. BRABANT. Absolutely. If—the beneficial ownership information database going forward have 32—over 32 million driver's license photocopies of small business owners, which would make it a hacker's dream to get that information, from an identify perspective.

Mr. VARGAS. Right. In fact, we see right now a lot of the complaints that we are getting about DOGE is they are trying to get

into people's private information that no one knows why they need it. Then it seems—and not for a negative purpose, you guys want to stop fraud, but it seems like you are saying the Federal Government has a whole bunch of information, and we would like to have it in real time so we can stop this fraud. Well, it seems like it potentially could be a massive invasion of privacy. How do you reconcile that? Yes.

Mr. McLAUGHLIN. Thank you for the question. The folks that I represent, the thousands of dedicated anti-money-laundering and fraud professionals care for our customers' data just as much as everybody else in the industry. However, we have a responsibility to our customers to collect data and collect illicit threats on our customers to do things like transaction monitoring.

Mr. VARGAS. No one disagrees with that, and I have to tell you, I come from the perspective that I think banks try to do the right thing with this information. I do not think they want their clients to be defrauded. I do not believe that at all. I think you guys are trying hard, but I also—I am not one of these guys who think the government is the bad people either. I think the government attempts to do the right things, too. Sometimes it falters like anything else.

It does seem like you are asking for a lot of information, private information that a lot of people would have a problem with you having. In fact, I am kind of surprised my colleagues on the other side did not call that out. They are usually pretty good about this privacy stuff. It seems like you are saying, "Hey, give us a whole bunch of this information back." Is there not a conflict there.

Mr. McLAUGHLIN. Again, thank you for the question. It is not a conflict from the financial crimes' perspective. We as financial institutions collect a lot of sensitive information on our customers already to establish a reasonable belief in that customer's identity.

The information I am looking for, and the folks in my industry are looking to partner with, is a secure transmission of information that has been used in a financial crime outside of the institution that we are employed by.

Mr. VARGAS. No. I get that. I get that. The government has a lot of information, and you would like some of that, too. I do not know, it seems to me that it could be a massive invasion of privacy. I am surprised that my colleagues on the other side have not called it out.

I do want to say one thing. You talked about the financial fraud with the farmer. When the CFPB was still in order, we could still go after that. In fact, right now, when they are calling about fraud, no one answers the damn phone.

We have elderly people, we have people in the military, veterans in San Diego that call the CFPB, and there is nobody on the other side of the line, and that is a problem.

With that, I yield back.

Chairman DAVIDSON. I thank the gentleman.

The gentleman from Texas, also the Chairman of the Small Business Committee, Mr. Williams, is now recognized for 5 minutes.

Mr. WILLIAMS of Texas. Thank you, Mr. Chairman, and thanks to the witnesses for being here.

Ms. Burns Koven, we are seeing an evolution in how fraud is committed and concealed, particularly through the use of emerging technologies like decentralized exchanges and cryptocurrencies. These tools are not only being exploited by traditional scammers behind investment funds and pig butchering schemes but increasingly by sophisticated transnational criminal organizations, including Mexican drug cartels that are adapting their tactics to evade the detection.

In many cases, these groups are bleeding fraud proceeds with other illicit revenue streams and using crypto infrastructure to obscure the origin and flow of funds.

Now, from your vantage, what trends are you seeing in how fraudsters, both individual and organized, are using these technologies to evade AML controls, and how is your organization working with the private sector and law enforcement to stay ahead of these evolving threats and ensure that we can continue to track down these criminals effectively.

MS. BURNS KOVEN. Thank you for the question. We are able to track these cartels purchasing fentanyl precursors from Chinese dealers who are primarily operating in cryptocurrency. We are seeing illicit actors adopt cryptocurrency for the same reason it is being used for legitimate purposes, because it is stable; it is liquid, fast. Any technology, we can count on fraudsters to abuse. Luckily, we have been able to track some of these fentanyl dealers and Mexican cartels, but they are early stage in cryptocurrency, and they are not expert launderers, which provides excellent opportunity for intervention.

I want to highlight the Eastern District of Wisconsin for forfeiting \$5.5 million in cryptocurrency associated with cartels and Chinese fentanyl precursor dealers.

There are a number of cases where we see this over and over at the Federal and State and local level, and we need to make sure that the State and local investigators are equipped to be able to identify and track these payments.

Mr. WILLIAMS of Texas. Thank you. One particular area of concern of mine is how government-related reporting requirements, such as FinCEN's beneficial ownership information rule, may be putting small businesses at, and their owners, at risk.

The rollout of BOI reporting under the Corporate Transparency Act has required millions of small businesses to navigate a complex new Federal compliance system, often for the first time.

Unfortunately, bad actors are using the requirements of the rule to exploit business owners to—emails, fraudulent websites, and scam calls impersonating FinCEN.

I applaud the Trump Administration for scaling back its harmful requirement recognizing this approach a burden and security risk that rule—that this rule has placed on small businesses, but there are still bad actors we must protect small businesses and entrepreneurs from.

Mr. Brabant, how has FinCEN BOI reporting requirements opened up small businesses to the threat of fraud and scams, and how can Congress better protect small business owners from BOI-related fraud.

Mr. BRABANT. Thank you, Congressman.

The first one I discussed earlier is filing scams themselves. When you do a Google search, the first several results are not going to be from FinCEN. They are going to be from BOIR.org, who have what looks like a government seal with an eagle in it.

Some of these sites are charging \$400 to file, and then small business owners have no idea if their information is actually being filed.

Then, of course, there is the question of when you have your—a copy of your driver's license in a data base and there are tens of millions of driver's licenses in there, it is only a matter of time until that information is leaked or hacked, and that opens up significant identity theft risks.

Mr. WILLIAMS of Texas. Thank you. I have limited time but, Mr. McLaughlin, could you elaborate on how the current filing burden of SARs and CTRs are affecting community banks, and how Congress can provide financial institutions with some relief from these burdens while still giving law enforcement the information and tools that they need.

Mr. MCLAUGHLIN. Thank you for your question. I think the burden needs to be shifted to a risk-based approach that is an alignment between regulatory agencies, law enforcement, and then the financial institutions.

Check-the-box exercises are a drain on resources across the industry, and it is demoralizing to the institution, the folks that I represent that we are not focusing on the threat, the real threat to our customers, but, rather, we are taking part in check-the-box exercises to get the machine of filing SARs or CTRs out within the regulatory expected SLEs.

Mr. WILLIAMS of Texas. Thank you. I yield my time back, Mr. Chairman.

Chairman DAVIDSON. Thank you, gentleman.

The gentleman from Illinois, who is the Ranking Member of the Financial Institution Subcommittee, Mr. Foster, is now recognized for 5 minutes.

Mr. FOSTER. Thank you, Mr. Chair and to our witnesses. I would like to talk a little bit about identity fraud and particularly the role of digital identity systems and maybe ameliorating some of that. States like Louisiana are using digital driver's license to keep kids off porn websites, things like that.

I guess my first question, Ms. Stokes, what fraction of the fraud that is really at some point against seniors involve identity fraud, where someone is representing themselves online as someone who they are not?

Ms. STOKES. Thank you for that question, Representative. It kind of goes two ways. Identities that have been stolen and used fraudulently can be used for a whole range of things. When we are talking about what is happening online, people do not need a stolen identity to pretend who they are. I mean, it is too easy. You can create—

Mr. FOSTER. I guess the question is, is that, if it became sort of standard practice when someone contacts you, sends you an email, text message, contacts you on social media, to just give a little token that says, "Here is the proof that I am the legally traceable person."

Ms. STOKES. Thank you, Representative. There are activities underway in the industry to try to come to that, and I would think that would benefit everybody.

Mr. FOSTER. It seems like, when—like one of you mentioned the error message on the screen that sort of triggered a big relationship that turned—that was just completely fraudulent. If that—just it became standard practice, and then you can contact me. Someone can send me an anonymous text, and I will just assume it is coming from some AI-generated trash. If they are willing to identify themselves, then I will pick it up, even if I do not recognize the name. It seems like it is a much healthier way to end up with this wave of identity fraud that we are seeing.

Another thing, a lot of you mentioned the need to catch this at the front door and the use of technology. One of the new pieces of technology that may become important are these AI personal assistants and companions that are really, in some cases even simple robots that seniors fall in love with when they have—get into memory care situations or, just the taxi driver I know spends his day in conversation with an AI asking him questions about sports scores or how the wild fire is doing. It seems like on an entity like that, if properly designed and regulated, could be sort of looking over the shoulder of elders as they are on the internet and saying, hey, you know, this AI personal assistant, which is being rolled out by dozens of AI companies, could, if done right, really be the first line of defense against this. Are you—is anyone aware of something like this that is under development or being marketed that way?

Ms. STOKES. Thank you, Representative. I am not aware of those. I am sure that it is out there, but we have grave concern about the misuse of generative artificial intelligence.

Mr. FOSTER. Well, this would be an AI on your side. This would be a product provided to that person whose job it was to defend that person against the wave of garbage out, AI-generated garbage on the internet. It seems like there may be something there, and it would be an interesting project for a nonprofit, for example, or just a company to think about developing because that—what you would really love is that, if every senior on the planet had a benevolent advisor looking over their shoulder and saying, “You know, I am very familiar with the millions of frauds that exist and what you just are getting here on your screen looks a whole like a fraud I have seen a thousand times before,” and that can be done it seems with properly regulated AI assistance. It seems like that is a real opportunity. Any thoughts you had on that or anything that you are aware of being developed I would be interested in.

Let us see. I guess, Representative Vargas made the point I wanted to make about the tension between knowledge sharing and privacy because, when you are talking about knowledge, you are talking about knowledge of things that, where there is no warrant and no—not necessarily probable cause—but, if you see the whole picture, you can assemble the probable cause. It seems like that is very sensitive legal grounds, legal territory to try to figure out how to strike that balance. I just—we have to make sure that, as politicians, we are not sort of making two inconsistent requests of whatever legal system we set up for that.

Anyway, I guess, that—last quick question. What fraction of the ByBit hack money has been recovered, the \$1.5 billion North Korean—what fraction has been successfully laundered?

Ms. BURNS KOVEN. Thank you for the question. I am not familiar with the current status. This is an ongoing investigation, but Chainalysis has aided the recovery of \$40 million to date of that.

Mr. FOSTER. Okay. At one point—most—a big part of it has been successfully laundered and is lost forever. Is that correct?

Ms. BURNS KOVEN. It is ongoing, sir.

Mr. FOSTER. Thank you. I yield back.

Chairman DAVIDSON. Thank you, gentleman.

The gentlewoman from California, Mrs. Kim, is now recognized for 5 minutes.

Mrs. KIM. Thank you, Mr. Chairman. I want to thank you for holding this hearing, and I want to thank our witnesses for joining us today.

Recently, I have been really concerned about the role that the Huione group plays in cyber scam operations.

Ms. Koven, I know that Chainalysis played a very sizable role in exposing the group's illicit activity. Can you break down what exactly your research found?

Ms. BURNS KOVEN. Thank you for the question. We have been tracking Huione for a long time. Since 2021, Huione has processed \$70 billion worth of cryptocurrency. Huione Guarantee operates as peer-to-peer marketplace allowing venders and buyers to connect. It receives a profit, a fee from those transactions. These vendors are nakedly selling scam material, social media accounts, money meal services. Huione also offers an exchange capacity, and it is a one-stop shop for scammers giving them everything they need to conduct scams at scale for cheap.

Mrs. KIM. Those that are critics of blockchain often paint it as a technology existing primary to launder money or for other illicit activity. However, they fail to realize that the transparency that comes with the digital ledger can make it easier to identify and shut down bad actors.

Ms. Koven, how did you leverage blockchain technology in your investigation in Huione group?

Ms. BURNS KOVEN. The blockchain reveals a very detailed story about Huione, way more granularity than we would ever have from traditional financial institution investigations, and it paints a very vivid picture of its illicit exposure.

We see many of our scams are using Huione as a common denominator, the common place to launder cashout funds, but also reinvest the proceeds of scams for additional materials used to target additional victims.

It provides a very powerful tool for financial institutions that leverage our platform for transaction monitoring, as well as investigative law enforcement to understand its inner workings.

Mrs. KIM. As we try to shut down organizations like the Huione group, do you think sanctions are an effective tool?

Ms. BURNS KOVEN. Sanctions are certainly a powerful tool, one tool in the toolbox. I think more clarity would enable financial institutions and cryptocurrency businesses that leverage our data to understand if and when they have exposure, whether they have

customers sending to or receiving funds from Huione; it essentially cuts Huione off from the mainstream crypto ecosystem.

Mrs. KIM. Could you give us an example of how this was actually used and—it was sanction—was being effective?

Ms. BURNS KOVEN. Sanctions have been most effective when coordinated with law enforcement. That one-two punch of not only designations but also takedowns.

Just last month, Garantex, which is a sanctioned Russian service, persisted despite sanctions. Certainly at any—any cryptocurrency business with receiving from or to Garantex has the ability to block those transactions effectively.

What we are now examining is, because Garantex has been blacklisted, it is potentially rebranded, but it allows us to follow the money trail to identify that next iteration. Even when they are in jurisdictions that are not compliant with Western law enforcement, we can still impose cost; we can inject friction.

Mrs. KIM. Thank you. I want to shift gears now and focus on the burden that suspicious activity reports have become on community financial institutions.

Mr. McLaughlin, I want to ask you the questions. For community banks that have smaller regulatory teams, how much harder is it to complete the SARs with the level of details that is required?

Mr. McLAUGHLIN. Thank you for your question. The burden on a smaller financial institution versus a larger institution is greater. At a larger financial institution, there is an investment in automation and other ways to beat the investigative process and the SAR filing or CTR filing more automative and faster.

At the community bank or smaller financial institution level, the burden is on the person. The person has to basically write the who, what, where, when, how, and why the activity took place, and in great enough detail so that we are turning over SARs to the law enforcement that is considered actionable intelligence. We do not like getting feedback that we need to amend SARs or things like that to provide more data. We look to provide as much data upfront so that law enforcement can take it, but it is a very burdensome process because, at that level of institution, there is not a lot of automation that takes place.

Mrs. KIM. Thank you very much.

I yield back.

Chairman DAVIDSON. Thanks, Mrs. Kim.

The gentleman from Illinois, Mr. Casten, is now recognized for 5 minutes.

Mr. CASTEN. Thank you, Mr. Chairman.

Mr. McLaughlin, first, I just want to State the obvious: You currently have systems in place, right, to block, freeze, reject any transactions and report them to the Office of Foreign Assets Control (OFAC) if they are done by shady characters, sanction evaders, child traffickers? Is that a broad, yes?

Mr. McLAUGHLIN. Yes, sir.

Mr. CASTEN. Okay. I am glad to hear it. You would be in trouble if you said anything else.

Tomorrow, the committee is going to markup stablecoin legislation, which would include language to treat stablecoin issuers as financial institutions under the Bank Secrecy Act, in which case

they would also have to comply with anti-money-laundering, Know Your Customer rules that you comply with as well.

Is it your view that, if—that stablecoin issuers should be subject to those same rules that you comply with, regardless of how those rules may change, the rules should not be different for one financial institution to another?

Mr. McLAUGHLIN. Thank you for your question. Yes, sir, I do believe any product, service, industry, or technology that is responsible for moving funds between customers or citizens has to be subject to regulation to make sure that they are protecting the customers or—

Mr. CASTEN. Okay. Since you have presumably got some experience filing SARs reports and what-have-you, can you speculate on what the bad guys would do if we had a stablecoin regime where all of a sudden, they were not subject to the same rules that a depositor at your institution is subject to.

Mr. McLAUGHLIN. Thank you, again. I can speculate that the bad guys would become even more aggressive in the space in terms of targeting vulnerable individuals to defraud, steal, and abuse the customers of the stablecoin.

Mr. CASTEN. Well, I certainly agree. I am glad to hear you say it. I raise that because some of my colleagues on the other side of the aisle believe that stablecoin issuers should not have to comply with anti-money-laundering rules, and I guess, if you are here to represent our Nation's child traffickers, that is a good position to have. But I think it is important to make sure we keep those protections.

Ms. Koven, I want to move to you just to think about what might happen if we do not have those protections in place. My understanding, from your 2020—from Chainalysis 2025 crime report is that stablecoins account for 63 percent of all illicit transactions that you had tracked and that sanctioned entities are increasingly using stablecoins because of the difficulty of using the U.S. dollar. Do I have that basically right on what your 2025 report said?

Ms. BURNS KOVEN. Yes, sir. Stablecoins have become the currency of blockchains. They are by far the most transacted cryptocurrency today and we support efforts to establish regulatory frameworks across stablecoin issuers. Robust consistent standards across this growing market can ensure—

Mr. CASTEN. I appreciate that, but I just want to focus on that 63 percent of the illicit activity is done on stablecoins, and I want to understand that number because my understanding of how what you can track is that you cannot see the off-chain transactions, right?

Ms. BURNS KOVEN. Correct.

Mr. CASTEN. It is 63 percent of the stuff that is trackable, but, presumably, if the bad guys know what is trackable, there might be some—there might be more than 63 percent if you could track everything.

Ms. BURNS KOVEN. As an investigator, for me personally it is a gift when illicit actors decide to dabble on stablecoins because of the traceability and, also, seizability midstream.

Mr. CASTEN. It is sort of like I love the guy who robs 7-Eleven without a mask and holds his ID up to the camera before he pulls the gun out. Right. Presumably there is more there.

Now, I say that because, if I am a bad guy and we do not regulate stablecoins, I can imagine a scenario where I go on to buy some other kind of crypto. I use that to launder money. I then bring that onto an exchange that is issuing the stablecoin, convert it to stablecoin. Those are all off-chain transactions. You would not see any of that, right, if that was the means of money laundering?

Ms. BURNS KOVEN. We have still had spectacular seizures, including a \$225 million seizure of stablecoins associated with the scam funds. Scammers know it is visible and traceable but are still taking the risk of dabbling in it.

Mr. CASTEN. I am not saying this to criticize Chainalysis. I am just saying that, because you are not tracking the off chain, if I bought another crypto, went onto an exchange where the exchange was issuing this—because the exchanges run their own ledgers, right? That is—you do not see that stuff, right.

That is, like you mentioned Garantex earlier, but my understanding is that Garantex loves Tether because they can do all that sort of stuff and bypass the system. Even though we have, hopefully, we are clamping down on Garantex, you could still do that inside other exchanges and not track that, right?

Ms. BURNS KOVEN. Absolutely. That is why regulatory frameworks that put standards on those cryptocurrency businesses to understand all this swapping that is going on is imperative.

Mr. CASTEN. I really appreciate your expertise. I am out of time. A marker for tomorrow: Let us make sure we do not make things easier for the bad guys.

I yield back.

Chairman DAVIDSON. I thank the gentleman.

The gentleman from Tennessee, Mr. Ogles, is now recognized for 5 minutes.

Mr. OGLES. Thank you, Mr. Chairman.

To the witnesses, a new landscape has developed before us, and the bad actors have clearly figured out a way to thrive in that environment.

I want to go back to Huione. Up until January, Apple and Google users on those two platforms could access—Ms. Koven, when you look forward to Huione, what is currently the accessibility for Americans or Westerners to that platform and other platforms that may pose similar risks?

Ms. BURNS KOVEN. Yes. We are seeing scam syndicates primarily leveraging these compounds. Huione Guarantee continues to be the common denominator for the majority of scams that we see, including the laundering of scammed proceeds, as well as facilitating the tools and services needed to perpetrate the scam, so identities and data to contact and reach out to Americans for targeting of these confidence and pig butchering scams.

Mr. OGLES. If you could wave a magic wand, what would be your fix, what would be the defense, that firewall that we put up here to protect the end user, the Americans, from this type of scamming activity.

Ms. BURNS KOVEN. Chainalysis has flagged Huione in our products so that financial institutions with exposure to Huione can make risk-based decisions on funds going to or coming from that platform.

More regulatory pressure on institutions that are flagrantly abusing or flouting regulatory norms is important. Closing those gaps for AML standards is important because of this jurisdictional arbitrage is certainly occurring.

Mr. OGLES. Obviously, this is focused in China, but what about—are there other nation-states that you have concerns about who are doing similar—or learning from other bad actors and scaling up to, quite frankly, abusing Americans? My apologies.

Ms. BURNS KOVEN. Certainly, if Huione did not exist, there would be other jurisdictions, other services ready to take its place, and so we need to continue to use blockchain analytics to understand where these funds are going and who—where the illicit users wind up having success laundering funds.

Mr. OGLES. Well, back to this platform, when you look at the child trafficking that is taking place and the movement of dollars, there has been—again, the bad actors have leveraged this technology to monetize the abuse of individuals but, in particular, children. Again, what are next steps in to combat that, being more aggressive in that space as we—as this is becoming really a plague of our society?

Ms. BURNS KOVEN. These are—these scams are operated by organized criminal syndicates involved in not only scamming but gambling, child trafficking, and sex trafficking. Being able to find those centers of gravity, inject operational friction, deprive them of funds, so seizing funds, and, also, being able to cause them to be a pariah in the ecosystem is incredibly important. We need that blockchain analytic capability to understand where the funds are going and identify those behind it.

Mr. OGLES. In other words, go after the money at the end of the day, right?

Ms. BURNS KOVEN. Yes.

Mr. OGLES. Mr. Chairman, I would love to get—when you talk about the regulatory regime that our colleague from the other side, I would love to get your thoughts over the next few—my remaining time on what you envision as a regulatory regime for stablecoin and, quite frankly, the caution that we must—how we must proceed with caution so that we do not disrupt our marketplace that can be a benefit to the market but at the same time understanding there are victims in the process.

Chairman DAVIDSON. I think—thanks for the dialog here, but I think Mr. Casten's concerns about illicit finance are well placed, and it highlights that technology is changing. Stablecoins are a little different way, and that is why our witness from Chainalysis, I think you did a great job answering, and we like when things are on chain; we can follow it even easier.

When I am talking about the things in my other committee, in Foreign Affairs, a lot of the things that we are looking at with non-State actors that are circumventing our sanctions, which are things our committee does—doing those kinds of things on chain are more traceable. In a lot of ways, that is exactly what we want.

Sometimes we do not even want to turn off the flow of cash immediately. We want to be able to follow the flow so that we can actually target, in the case of warfare, connect targets.

Then, in the case of going after organized crime, we do not necessarily want the guy working out of mom's basement. We want to know who he is reporting to. The question is, are those tools better? We are going to talk about that in a lot of ways.

Thanks, Mr. Ogles.

Mr. OGLES. I yield back.

Chairman DAVIDSON. The gentleman's time has expired, and he has yielded.

The gentleman from California, Mr. Liccardo, is now recognized for 5 minutes.

Mr. LICCARDI. Thank you, Mr. Chair.

Thank you to our witnesses for all this information. The hearing, of course, is captioned "Follow the Money," and I used to be involved in prosecuting drug traffickers and human trafficking as a Federal prosecutor and later as a District Attorney (DA). Certainly I had plenty of challenges following the money when we knew that there was information being provided by entities that was false, that would conceal who the actors were and who was controlling them, and, most importantly, who was getting the money from the criminal enterprise because we knew those were the folks who were really running the show.

I will give you a quick example. We had, I remember, a Cuban national who was controlling a major human trafficking enterprise in southern California, of course, using entirely U.S. corporations, filed under California and other States' laws, with U.S. citizens essentially, ostensibly being their officers.

I am concerned, as I know the National District Attorneys Association is also concerned, based on what we see from their statement, December 2024, about this legislation that we are currently considering that would exempt every U.S. corporation under a certain threshold, the size, from Corporate Transparency Act's requirements providing basic information—information—I am sorry—basic ownership information to FinCEN.

Let us be clear about what that information is under the law. It is the name of the owner, their date of birth, their address, and some identifying number from a driver's license or passport, or some other government—that is it. Four items.

Now, my experience, certainly trying to get the identity of those individuals controlling these entities that are engaged in criminal activity, was pretty important. I guess I just want to ask, Ms. Stokes, does it help, based on your experience, to be able to have this kind of information if we are trying to combat fraud?

Ms. STOKES. Thank you, Representative. Absolutely the information is critical, and I just want to point out that we have heard a lot about concerns of administrative burden and concerns of data privacy.

I want to turn to the burden of the victim. When you look in the aggregate of how much has been stolen just in 2023, an estimate from the FTC is \$158.3 billion, that is three times the revenue of the Coca Cola company. We have to understand that, yes, there are burdens on businesses, and maybe some could be put together bet-

ter than others, but we cannot be moving away from rules that help protect consumers.

Mr. LICCARDO. I agree, Ms. Stokes. In fact, I believe Mr. Brabant suggested somehow or another that corporations have to hire Certified Public Accountants (CPAs) and other outside counsel to be able to submit this information about the name of the owner, the date of birth, the address, and their basic, I guess, driver's license number. Is that your experience, that you need outside counsel to do such things?

Ms. STOKES. Thank you, Representative. I cannot speak to that because that is not the space I work in, but I hear your point.

Mr. LICCARDO. \$153 billion in losses.

Ms. STOKES. 158 billion.

Mr. LICCARDO. 158 billion. Thank you for that.

Mr. Brabant, you might have guessed, I was going to you next. I am trying to understand why providing these four basic pieces of information, which, by the way, I had to provide when I opened an LLC last year—any bank would require it. It is pretty basic information—what is the extraordinary burden involved here.

Mr. BRABANT. It is also a photocopy of a driver's license, but it is that information that challenges the substantial control prong.

I think one thing that is getting lost here is that every bank already has this. This is a duplication of the customer due diligence role, which already exists. Every single LLC that has a bank, if the bank is doing its job, they have this information. What this is really—

Mr. LICCARDO. What happens if the bank has individuals who are involved in criminal activity? Would you not want that information in the hands of those who are investigating criminal activity, not those who may be—

Mr. BRABANT. Anyone who is investigating could subpoena the bank at any time.

Mr. LICCARDO. What happens if you are just investigating for the first time and you actually need to know who you can subpoena, and you do not know exactly where to go because you do not have ownership information to begin with?

You raise concerns, for example, about criminal threats to these companies, but, in fact, the law is very clear under title 31: Penalties only accrue if you are fraudulently reporting this information, willfully and fraudulently reporting information that is false. Somehow or another you have cast this as some kind of great criminalization of corporate America. How can that be?

Mr. BRABANT. That is a knowing and willing standard, which is usually in the eye of a prosecutor.

Mr. LICCARDO. Not knowingly willing. It says willfully provide false or fraudulent. That is what the statute says. Not knowing; it says willfully. Let us be very clear about what the statute says.

Mr. DAVIDSON. The gentleman's time has expired.

Mr. LICCARDO. Thank you.

Mr. DAVIDSON. The gentlewoman from Florida, Ms. Salazar, is now recognized for 5 minutes.

Ms. SALAZAR. Yes. Thank you, Mr. Chairman, and thank you to the witnesses.

My name is Maria Salazar. I represent District No. 27 in Florida, which includes the city of Miami. For what I have been studying, my hometown was ranked number one in the Nation with the highest per capita fraud in the country. That cost Floridians over \$850 million. That said, Miami is a great place, but this is pretty embarrassing.

I would like to ask, Mr. McLaughlin, if you could please explain to us why, according to the FTC fraud report, Miami is number one in the Nation for reported fraud. Why is that? Thank you, Mr. McLaughlin.

Mr. McLAUGHLIN. Thank you for your question. I cannot really answer as to why Miami in particular is ranked number one, but I can tell you that—I can tell you that the financial institutions today that I have had the honor of working with and partnering with have dedicated time, energy, and, more importantly, resources to developing upfront detection of fraud. However—

Ms. SALAZAR. Is there any specific reason why that area in the country, specifically the city of Miami, is the number one in the country for fraud? What are we attracting?

Mr. McLAUGHLIN. If I would have to take a guess it is the population of the potential vulnerable population that resides within the State of Florida.

Also, the availability of being able to reach Miami from a foreign country also would probably play a part in that.

Having the ability to contact an elder in Miami and talk about the investment opportunities maybe in their home country; it exists greater than in other large areas of the country. Again, that is just me taking a guess using my experience over time, but my fellow witnesses may have a better answer than I do.

Ms. SALAZAR. Maybe, Ms. Koven, would you like to give us maybe your opinion as to why the city that I represent is number one for fraud in the country.

Ms. BURNS KOVEN. I am unfamiliar with Miami in particular, but, from my experience, scammers are targeting Americans indiscriminately and are looking to develop relationships with individuals over text and social media and very happy to have their hands on American data to strike up those conversations because America is a target-rich environment. It is a wealthy country, and it makes it a prime target for these fraudsters.

Ms. SALAZAR. Any additional tools, any of you who would like to share with us—any additional tools or ideas that we should consider in order to stop this or make it a lot harder for these scammers to attack our constituents?

Ms. STOKES. If I may, Representative.

Ms. SALAZAR. Of course.

Ms. STOKES. One of the points that was made a little bit earlier—I think the targeting does have a lot to do with where older populations are. If you broaden your look beyond Miami, you will see probably the top five States where the highest number of older adults live.

It is not that they just target older adults, but when they get older adults there is a much bigger payout because they have the assets, right. That is one thing.

Another thing is that this is organized crime, and our system of law enforcement just is not resourced or is not able, because of other competing demands, to look at these crimes through an organized crime lens. If you did, you would get the \$10,000 grandparent scam in Miami connected to the \$10,000 grandparent scam in Tennessee, and all of a sudden, it is a million-dollar threshold-breaking case.

There is a new initiative underway that will launch in April that is going to do just this, the National Elder Fraud Coordination Center (NEFCC), and I would love to tell you more about that if you are interested.

Ms. SALAZAR. Yes. Basically, what you are telling us is that we are going to be honing and targeting the senior population to explain to them or to send the message to be very careful. That means that our seniors do not understand that they are the number one prey for this type of scammers.

Ms. STOKES. Thank you, Representative. I can tell you my job is to educate older Americans, and within 2 years of doing this, I realized we cannot educate our way out of this and NEFCC is not about educating. It is about pulling data together from the private and public sectors to solve.

Ms. SALAZAR. We cannot educate—I mean, my time is up but just give me 30 seconds. Why do you think education is not the way to go with the senior population?

Ms. STOKES. We have been saying education has been the answer for years, and where are we? You know, the \$158.3 billion, \$61.5 billion of which was stolen from older adults in 2023, it cannot work on its own. Because we relied on that, it served to deprioritize any other activity that could have gone to mitigate the loss that is now growing so meteorically.

Ms. SALAZAR. Thank you. I yield back.

Chairman DAVIDSON. Thank you. I appreciate the dialog there.

The gentlewoman from Michigan, the Chairwoman, also the Chairwoman of the full Republican Conference, Mrs. McClain from Michigan is now recognized.

Mrs. MCCLAIN. Thank you and thank you all for being here. This is a really important topic. I think—and something that I think we really need to figure out how to get our arms around. Again, I appreciate you holding the hearing, as well as talking about this.

I want to start with Ms. Koven. I am trying to understand blockchain, the role it plays, but could blockchain analytics or other technological solutions, so to speak, streamline the filing and analysis of SARs and CTRs? If the answer is yes, which I hope it is, could you expand on that a little bit?

Ms. BURNS KOVEN. Yes. Thank you for the question. Blockchain analytics is already enriching SAR and CTR quality. Our customers from the private sector are leveraging the insights from our data to file their SARs and CTRs today. It paints a very vivid picture of the entire kill chain of events.

If we are talking about scams in particular, you have a much more vivid color of where the funds are going and coming from, counterparties as well, much more so than you would in the traditional financial industry.

Mrs. MCCLAIN. Is the timing a lot quicker as well, I am assuming?

Ms. BURNS KOVEN. Yes, ma'am. That is correct. Cryptocurrency is an attractive asset for legitimate uses, as well as illicit, for its speed.

Mrs. MCCLAIN. In my opinion, we have all these governmental agencies, and we have these rules and regulations, and at times they are so cumbersome and at times overburdening for the businesses where I think the businesses are trying to do the right thing, and people are trying to do the right thing; it is just the volume is so immense, right, that it just takes time to go through that.

One of the biggest advantages I see, and I would like to get your opinion on this, is the time, because, to your point, the timing is crucial on when we find these. Could you talk a little bit about the timing of this and the timeframe, how the timeframe is shortened?

Ms. BURNS KOVEN. Yes. We also provide real time transaction monitoring allowing financial institutions to get alerts on funds incoming or off—going off their platform, and they can be alerted in real time to these funds. Really time is of the essence, and current processes, reporting, and information together sharing is painfully slow. Even though cryptocurrency and the blockchain enable tracing and freezing, time is really of the essence. We have to make sure that those insights are delivered in a timely fashion.

Mrs. MCCLAIN. Do you have any measurables on that?

Ms. BURNS KOVEN. No, ma'am.

Mrs. MCCLAIN. Okay. All right. Just curious. Thank you.

Mr. McLaughlin, how can FinCEN improve its communication and feedback mechanisms with banks and blockchain analytics firms following SARs and CTR submissions? Could you talk a little bit about that?

Mr. McLAUGHLIN. Sure. Thank you for your question. As everybody can probably tell, the point of a lot of the things I have said today is creating an open and transparent two-way communication between the public and private sectors so that we can begin focusing on the resources that we have on the threats that our customers face on a daily basis.

Working with FinCEN to establish a working group or a task force or whatever terminology you want to throw at it would allow us to begin establishing and doing data analytics on what the government is seeing, what law enforcement is seeing and what the private sector is seeing so that we can—so that we can begin putting pen to paper on what a true risk-based approach means for financial crimes across the board, fraud, money laundering, sanctions and terrorism finance.

Mrs. MCCLAIN. Are you getting any pushbacks or running into any roadblocks on that?

Mr. McLAUGHLIN. I would not say roadblocks or pushbacks. I think with the increased scrutiny that all of you are bringing to light today, I do think we are seeing across the industry a knowledge-sharing exercise taking place, whether that be informally or formally, but more work is needed.

I think, when we look at things like the Federal Financial Institutions Examination Council (FFIEC) manual and the revisions

there. I do think a public, private, and law enforcement type engagement would allow us to put down what the actual requirements are so that we can point to the crimes that we are trying to capture.

Mrs. MCCLAIN. Are you getting any pushback on that, public-private partnerships?

Mr. McLAUGHLIN. Personally, with the folks that I work with, no. It is just not official. It is outside the hallways here or at a convention or a conference that knowledge sharing really exists.

Mrs. MCCLAIN. Thank you.

With that, Mr. Chairman, I yield back.

Chairman DAVIDSON. Thank you, gentlewoman.

The gentleman from Iowa, who is also the vice chairman of the committee, Mr. Nunn, is now recognized for 5 minutes.

Mr. NUNN. Mr. Chairman, thank you very much for putting this important hearing together today. We all know that my home State of Iowa, in the heart of the heartland, my senior citizens are probably target number one for the scams. It is happening across not just Iowa but the entire country.

I am proud to say that the United States is also probably the best place for innovators to come to the forefront and really be the superheroes in the story of fighting back.

In November, the Department of Justice used blockchain to freeze approximately \$225 million that were used in a human trafficking scheme. However, even amongst this technological solution situation, we remain challenged for most of our State and local law enforcement entities to get an opportunity to play, as, Mr. McLaughlin, you just highlighted.

One victim back in my hometown in Iowa, 68-year-old veteran, lost over \$100,000 to a scam, and challengingly, local law enforcement could not even begin to help.

That is why today, Mr. Chair, I am introducing the Bipartisan Guard Act to give State and local law enforcement agencies access to the technology they need to combat these financial fraud crimes and pig butchering scams.

Let us get started on this. Ms. Koven, I know that you and I are on the same page here because, in your testimony, you advised the need to train more people on things like blockchain, those digital rails in which the future of technology is going to operate on here in the United States. This is exactly what the Guard Act, my bill, attempts to accomplish.

I understand that your company has trained people in these technologies both on the State and even down to the local level. Can you briefly walk us through some of the examples, and if there have been stories of success here?

Ms. BURNS KOVEN. Yes. Thank you for the question. I am sorry to hear about your constituent being defrauded. It is a story we hear all too often, unfortunately.

At Chainalysis, though, we do work with over 70 State and local governments around the country, and we have seen astounding successes when law enforcement is trained and equipped properly. We have only scratched the surface, unfortunately. Particularly with the proliferation of these types of scams, we need to better equip State and local law enforcement to understand how to handle

these cases and connect a single fraud victim to a wider network and increase chances of disruption and recovery.

Mr. NUNN. Jackie, I think you really highlighted a point here that this has happened in the physical world before, and we have had good game plans to go after it. What our Guard Act bill is aiming to do is to create these fusing centers of best practices at the Federal level, marry them up with local law enforcement agencies and provide those level of resources to really go after that so that an Iowan who loses a hundred thousand, or a New Yorker who loses a million all have the same access to the same resources. Is this what you have seen through your experience to be a successful solution?

Ms. BURNS KOVEN. Yes, sir. We should have every advantage because the scammers are leveraging cryptocurrency, but time is of the essence. What we have seen in working groups and small-scale operations is that, when private and public sector are sharing information dynamically, we can turn that wealth of information into actionable insights quickly and have stunning successes.

Mr. NUNN. Thank you, Ms. Koven.

Ms. Stokes, I want to thank you and your incredible team at AARP. You are on the frontline not only guarding our seniors, but you have helped bridge this to be a bipartisan effort. Our Guard Act is really brought together by Mr. Gottheimer and me, a Republican and Democrat, really working for the best interest of the American people here.

I would like to, one, ask, how could retirees benefit from a local law enforcement that would have access to these greater tools that the Guard Act could provide so they can get to know about blockchain, understand how financial fraud works, and really address the sources of these crimes to stop the number of victims we are seeing?

Ms. STOKES. Thank you, Representative and AARP is very proud to support the Guard Act. I think it is critical.

We talk to probably a hundred thousand victims a year, maybe 500 calls a day, and the vast majority of fraud victims where money has been stolen; they have no recourse. They will call local or State police, and even if police that they talk to understand that it is a crime, they will still say, "There is nothing we can do about it," and sometimes do not even take the report, which is a challenge in and of itself. Anything that we can do to not only provide the tools but, importantly, to train local and State law enforcement on things that they simply do not have the training on right now would be of great benefit to our constituency.

Mr. NUNN. Thank you, Ms. Stokes. I want to, again, say thank you to AARP for helping lead this because it is not only my seniors who want this; it is every American who needs this and no one more so than my local law enforcement, who wants to be able to help our own community get better. This gets us in the right direction.

Mr. Chairman, thank you very much. I yield the remainder of my time.

Chairman DAVIDSON. Thank you very much.

I thank all of our witnesses and our colleagues for a great hearing today. Kind of scary what is going on for the citizens of this country. Hopefully this will help make a difference.

Without objection, all members will have 5 legislative days to submit additional written questions to the witnesses, and to the chairman for questions.

Witnesses, please, if you get those, respond no later than May 6th.

[The information referred to can be found in the appendix.]

This hearing is now adjourned.

[Whereupon, at 11:56 a.m., the subcommittee was adjourned.]

APPENDIX

MATERIALS SUBMITTED FOR THE RECORD



April 1, 2025

The Honorable Warren Davidson
Chairman
Subcommittee on National Security, Illicit
Finance, and International Financial
Institutions
U.S. House of Representatives
Washington, DC 20515

The Honorable Joyce Beatty
Ranking Member
Subcommittee on National Security, Illicit
Finance, and International Financial
Institutions
U.S. House of Representatives
Washington, DC 20515

RE: Hearing Titled, “Following the Money: Tools and Techniques to Combat Fraud”

Dear Chairman Davidson and Ranking Member Beatty,

On behalf of the Financial Accountability and Corporate Transparency (FACT) Coalition, we appreciate the opportunity to comment on your hearing examining tools required by financial investigators to detect and crack down on fraud. The FACT Coalition is a [non-partisan alliance](#) of more than 100 state, national, and international organizations promoting policies to combat the harmful impacts of corrupt financial practices. We have been a leading champion of financial transparency reform in the United States for more than 14 years.

We are writing to reiterate the importance of the Corporate Transparency Act (CTA) to protecting everyday citizens from fraud, defending U.S. national security, and providing investigators tools in the broader fight against financial crime. Any attempt to repeal or otherwise defang the CTA would further enable fraudsters that, [in 2024 alone](#), robbed ordinary Americans of over \$12.5 billion.

Anonymous Companies Are “Getaway Vehicles” for Fraudsters

The Corporate Transparency Act was passed on a bipartisan basis to end the use of anonymous U.S. shell companies by a diverse range of domestic and foreign criminals, including drug traffickers, corrupt foreign officials, and, increasingly, fraudsters. Prior to the passage of the CTA, all 50 states required more information to get a [library card](#) than they did to form an anonymous company. The CTA closed this gaping loophole by requiring certain entities formed or registered in the U.S. to name their true owner to a secure directory housed at Treasury’s Financial Crimes Enforcement Network.

As noted in a [recent report](#) by Transparency International U.S., the U.S. chapter of the world’s largest anti-corruption organization, “The criminals behind consumer scams often employ

anonymous companies to execute their schemes and evade detection. What the getaway car is to a bank heist, the anonymous company often is to a fraud scheme.” The report details 19 cases occurring between 2019 and 2024 in which anonymous companies were allegedly used to enable consumer fraud or launder the proceeds of scams. A brief selection of these cases include:

- The alleged use of shell companies to launder some \$11 million in [fraudulently diverted Medicare, Medicaid, and private insurance payments](#);
- The alleged use of over dozens of shell companies by two Chinese nationals to launder \$73 million in proceeds from [cryptocurrency investment scams](#); and
- The use of shell companies to both execute and launder the proceeds of a [wire fraud scheme](#) that cost Medicare more than \$20 million.

According to small business trades like Small Business Majority, abuse of anonymous shell companies also [harms American small businesses](#) by enabling fraud, promoting unfair competition for contracts, and empowering patent trolls to harass small business owners.

Treasury’s Recent Order Violates the Statute of the CTA

Despite clear evidence of the risks posed by anonymous shell companies to U.S. consumers, small businesses, and national security, on March 21 Treasury issued an [interim final rule](#) (IFR) exempting domestic entities – more than 99 percent of all entities originally covered under the CTA – from reporting requirements. This move flies in the face of more than 10 years of [Treasury National Risk Assessments](#) and Congress’ own findings, which make it clear that domestic anonymous entities represent a significant money laundering risk.

The Corporate Transparency Act, as enacted into law, is the product of 20 years of congressional deliberation, debate, and refinement. At no stage of the legislative process did lawmakers seriously consider exempting domestic entities writ-large from reporting requirements, and under the final statute Treasury only has the authority to make reporting exemptions with concurrence from the Department of Homeland Security and Attorney General that reporting by the entities in question “would not serve the public interest” and “would not be highly useful” to investigators.

It is in this final form – clearly mandating that information required to be reported be “highly useful” to law enforcement – that the Act garnered support from [dozens of stakeholders](#) including [42 states Attorneys General](#), the [Fraternal Order of Police](#), and the [National District Attorneys Association](#). In a statement reacting to the release of the IFR, National District Attorneys Association Executive Director Nelson Bunn said that “Treasury’s interim final rule threatens to deny law enforcement the vital information they need to pursue illegitimate business fronts that jeopardize U.S. national security and public safety.”

CTA Repeal Would Further Benefit Criminals and Undermine National Security

[H.R. 425](#), the Repealing Big Brother Overreach Act, would double down on Treasury's harmful interim rule by fully repealing the Corporate Transparency Act, undoing decades of anti-money laundering progress with a single stroke. This approach would deny investigators even what little information they may still be able to access on foreign entities doing business in the U.S. under Treasury's IFR, further crippling law enforcement's ability to effectively patrol the nation's financial borders.

Repealing the CTA could also have particularly dire consequences for ongoing efforts to combat the illicit flow of narcotics into American communities. According to Eric Brown, President of the National Narcotic Officers' Associations' Coalition (NNOAC), "Following the money is a proven strategy in investigations that involve organized criminal activity, especially fentanyl and other illicit drug trafficking. Law enforcement resources are stretched thin, and the Corporate Transparency Act – if fully implemented – would enable narcotic enforcement officers to be more effective in protecting the public from drug trafficking."

We hope the Committee will refrain from advancing any legislation that hurts current and future victims of fraud, undermines U.S. national security, and ties the hands of law enforcement officials pursuing foreign and domestic financial criminals.

Thank you for the opportunity to comment. If you have questions, you can contact Erica Hanichak (ehanichak@thefactcoalition.org).

Cc: The Honorable French Hill, Chairman, Committee on Financial Services

Cc: The Honorable Maxine Waters, Ranking Member, Committee on Financial Services

CFP BOARD

VIA ELECTRONIC MAIL

April 7, 2025

Chairman Warren Davidson
U.S. House Subcommittee on National
Security, Illicit Finance,
and International Financial Institutions
2129 Rayburn House Office Building
Washington, D.C. 20515

Ranking Member Joyce Beatty
U.S. House Subcommittee on National
Security, Illicit Finance,
and International Financial Institutions
2129 Rayburn House Office Building
Washington, D.C. 20515

Re: April 1, 2025 Hearing: *Following the Money: Tools and Techniques to Combat Fraud*

Dear Chairman Davidson and Ranking Member Beatty:

We write today to thank you for holding the hearing, *Following the Money: Tools and Techniques to Combat Fraud*, on April 1, 2025, and to submit for the record this letter outlining CFP Board's work to combat fraud and financial exploitation. We thank the Subcommittee for its attention to this critical issue. As the certifying body for more than 100,000 CERTIFIED FINANCIAL PLANNER® professionals in the United States, we stand ready to assist your efforts on this issue.

CFP Board, which consists of two affiliated non-profit organizations, the Certified Financial Planner Board of Standards, Inc. and the Certified Financial Planner Board of Standards Center for Financial Planning, Inc. (collectively, "CFP Board"), operates the CERTIFIED FINANCIAL PLANNER® certification program and sets high standards of competency and ethics for financial planning in the United States. Today, more than 103,000 CFP® professionals (or approximately one-third of the country's retail financial professionals) provide essential financial advice and financial planning services to everyday Americans in all 50 states. CFP® professionals stand out because they voluntarily commit to CFP Board - as a part of their certification - to act as a fiduciary and, therefore, to act in the best interests of the client at all times when providing financial advice.

Seniors and other vulnerable Americans are among the most targeted for financial exploitation and fraud. Given their age and retirement status, they are also the most unlikely to recoup their losses. This can have a drastic impact on the quality of retirement and seniors' abilities to afford even the most basic services, such as medical care and

prescription drugs. Losses sometimes force seniors and other vulnerable adults to rely on federal programs to a greater extent than they would have if they had not been victimized, costing the federal government additional dollars. Furthermore, these dollars were likely originally intended to be used for retirement, reinvested in local economies, or saved for various financial milestones that the average American achieves. With the rise of new financial systems and transaction methods, there are new types of fraud and scams every day. The digital age presents new types of challenges, and as technology rapidly evolves, so do the types of fraud.

CFP® professionals are on the frontline against fraud for their clients. CFP® professionals must meet rigorous education, training, and ethical standards and are committed to serving their clients' best interests. While providing financial planning advice and education to clients, CFP® professionals are well-positioned to help prevent fraud or exploitation before it happens and may be the first to detect illicit conduct when it does occur. Furthermore, CFP Board takes steps to monitor compliance with and enforce the *Code of Ethics and Standards of Conduct* — including the release of disciplinary information to the public — when CFP® professionals are alleged to have fallen short of their obligations. CFP Board understands that the public's need for competent and ethical financial planning advice has never been greater.

CFP Board also makes financial resources available to the public through its consumer-facing website, letsmakeaplan.org. On this site, consumers can identify CFP® professionals in their area with various expertise and find resources and tools to support their financial well-being. Some of these resources focus on preventing financial fraud and exploitation, such as the attached articles written by CFP® professional “Ambassadors” entitled ***How to Protect Yourself Against Scams*** and ***Protecting Your Elderly Parent from Financial Fraud***.

CFP Board has engaged in advocacy on the federal and state levels on these issues. For example, in the 118th Congress, CFP Board publicly supported the Empowering States to Protect Seniors Against Bad Actors Act and the Financial Exploitation Prevention Act. See <https://www.cfp.net/news/2023/05/cfp-board-urges-senate-to-pass-bill-to-protect-seniors> and <https://www.cfp.net/news/2024/05/cfp-board-statement-on-empowering-states-to-protect-seniors-against-bad-actors-act>. At the state level, CFP Board supports 'hold and report' legislation, which enables financial firms, such as those that employ CFP® professionals, to 'hold' transactions where illicit behavior is suspected and report any wrongdoing to the relevant legal authorities. CFP Board recently issued a statement in support of such legislation in Idaho, which was recently signed into law by the Governor. See



By CFP Board of Standards, Inc.



HOW TO PROTECT YOURSELF AGAINST SCAMS

By Don Grant, CFP® April 18, 2024

Crooks who want to separate you from your money seem to be everywhere, and they continue to get more adept at pulling off financial scams. It's not just the most vulnerable people in society who fall prey to scams — I have had conversations with educated high-earners conned into sending money to a scammer. To me, that indicates there is no one-size-fits-all set of solutions to keep you safe from a clever scammer. But if we are vigilant, there are ways to protect ourselves against financial scams.

The Federal Trade Commission (FTC) is the government agency tasked with protecting consumers from financial fraud, and it reports that criminals are proactive. That means criminals will generally reach out to their victims first. Whether it's an enticing offer that comes to you in an email, or a threatening phone call seemingly from a government agency, it is the scammer who generally initiates contact.

The first level of protection you have against scams is knowledge. If you know how these shady characters operate, you will be more likely to shut them down right away.

First, familiarize yourself with the many types of scams. [FTC.gov](https://www.ftc.gov) is a great place to learn. Here is a list of just a handful of known scams:

Investment scams appeal to our greed. They present an investment opportunity that may include precious metals, cryptocurrencies or real estate. If they tell you that you need to act quickly or miss out, shut down communication.

IRS scams feed on our potential fear of filing our taxes and the power of the Internal Revenue Service (IRS). The scammer may pose as a tax collector or an IRS agent. Remember that the IRS will never reach out to you for payment through email, social media or text — it generally initiates contact only through the U.S. mail.

Social Security scams often involve messages informing you that your Social Security benefits will get suspended unless you pay a fee.

Romance scams feed on our desire to be with someone we love. Once scammers trick you into falling in love, they begin asking for money. They might say that their family member is sick, that their car broke

down or that they need financial support to travel to visit you. These scams are often developed over months to build trust. The [FTC reports](#) that in 2023, more than \$1 billion was stolen in the name of love.

Job scams often prey on those looking for a job. They may impersonate a job recruiter for a well-known company. After a few interviews, they may tell you that you are the top candidate and even schedule an onboarding interview. Of course, the scammer will say that the Human Resources department needs your Social Security number, bank account information and driver's license to get everything set up.

Debt scams impersonate a debt collection agency to trick you into paying a false debt claim. Alternatively, scammers may ask you to pay an [actual debt you owe](#), but all of the money goes directly to the scammer. The same scam exists for [student loan debt](#).

WHAT CAN YOU DO TO AVOID SCAMS?

Slow down and double-check. If you receive an email from [your bank](#) requesting that you click on a link to verify your account, stop and think about it. Has your bank ever contacted you like this before? Probably not. Look at the return address or the link they provide. Is the financial institution spelled correctly? Is the URL address odd? Does the logo in the email look a bit off? Your intuition is the first line of defense. If it seems odd, it's probably a scam.

Go to the source. If a call or email requests personal and financial information, defer the conversation and go directly to the source. Call the bank or company in question with a number other than the one provided by the suspected scammer. Ask the representative you reach if they need the information that was requested. If it is a legitimate request, inquire as to why they need that information.

Notice the payment method. If you are conned into sending money to a scammer, the manner of payment can be a huge red flag. For example, if they request money sent via wire transfer, Western Union or money order, they are probably attempting to complicate the money trail. A wire transfer will probably go to a bank account that is immediately closed after they receive the money. If they request gift cards of any type, it's probably a scam.

Strengthen your account security. If multi-factor authentication is available, opt in for that service. Check your financial accounts regularly and look for unusual activity or unidentified charges. If you find anything that is questionable, report it immediately to the institution. Just because an unidentified charge is small does not mean it's not a threat. Scammers will often test an account with a small transfer to ensure that the connection is valid. Then, they go in for the big financial score.

Freeze your credit. Another protection is to create a security/credit freeze. You can contact the three credit reporting agencies: Equifax, TransUnion and Experian. For no cost, these agencies will freeze your account and not allow any institution to run a credit check unless you authorize it. This means a scammer will not be able to take out a credit card, open a financial account or borrow money under your name without you knowing about it.

Don't be shy if you get scammed. If you have been scammed, you may be embarrassed to tell anyone that you fell for it. The FTC needs to know so that it can go after the perpetrators and help warn others of the threat. Think about the Bernie Madoff Ponzi scheme. Hundreds of well-known, educated, intelligent people lost millions of dollars to that scam. You are not alone — please report it to the FTC.

A CFP® professional can recommend solid security procedures for your money and can help you navigate any financial fallout if you've been scammed. [Find your CFP® professional today.](#)

Get started on securing your financial future today

FIND A CFP® PROFESSIONAL

TOPICS

Banking Social Security Family Finances

CFP® PROFESSIONALS NEAR YOU

not your location?

MR. M. THOMAS PABLO, II

Chevy Chase, MD

Planning Services Offered

Debt Management, Retirement Planning, Education Planning, Business Succession Planning, Insurance Planning, Tax Planning, Estate Planning, Comprehensive Financial Planning, Investment Planning

MS. ANNMARIE BILGER

Washington, DC

Planning Services Offered

Divorce Planning, Comprehensive Financial Planning, Education Planning, Inheritance, Employee and Employer Plan Benefits, Socially Responsible Investing, Retirement Planning

MR. CHRISTOPHER J. RIVERS

Washington, DC

Planning Services Offered

Investment Planning, Tax Planning, Insurance Planning, Education Planning, Retirement Planning, Estate Planning, Comprehensive Financial Planning

<https://www.cfp.net/news/2025/03/announcements/cfp-board-supports-idaho-legislation-to-protect-seniors-from-financial-exploitation>.

When it comes to combating fraud, it truly takes a village. CFP Board is committed to a comprehensive approach that, among other things, includes financial education, financial planning, and knowing what to do when one identifies any illicit behavior. We are grateful to the Subcommittee for holding this critical hearing. Should you have any questions or if we can be a resource to you on these topics, please do not hesitate to contact me at ekoeppel@cfpboard.org.

Sincerely,

A handwritten signature in cursive script that reads "Erin K. Koepfel".

Erin Koepfel
Managing Director, Government Relations and Public Policy Counsel
CFP Board



By CFP Board of Standards, Inc.



PROTECTING YOUR ELDERLY PARENT FROM FINANCIAL FRAUD

By Laura J. LaTourette, CFP® June 16, 2022

Hearing the words "financial fraud" can often send us into a panic. Last year, a scammer called my mother, claiming to be a tech company employee and offering to help her with upgrades to her computer. She followed their instructions, to the point of providing them with her bank credit card information! Fortunately, I called her, interrupting the conversation, and immediately told her to hang up the phone. She became terrified and confused but followed my instructions to end the scam. I then made a conference call with her and her bank to stop all charges. Once notified, the bank canceled her card, created new bank accounts, and put a red flag on her account. It was a scary event.

Against this growing threat of scammers, you must be ready to safeguard your parents by becoming their trusted advocate. Too many criminals take advantage of our elders, preying on their age and limited technical abilities. Unfortunately, not all older folks have trusted family members or advocates to help them understand these types of situations. Working with a CERTIFIED FINANCIAL PLANNER™ professional is a great start to [safeguarding your elderly parents and yourself from financial fraud](#).

Here are seven steps you can take to begin the process of advocating for your parents and [safeguarding](#) their financial future:

Talk About Money

If you will be the one to help with your parents' financial life as they age, it's time to start thinking about your responsibilities. It is important to start conversations with them now instead of later and explain that having someone younger help with financial decisions can help protect them from fraud. Be sure to ask about their spending, saving, and giving habits. Show that you care about their well-being, not just the numbers. Review their spending, and make sure no one has access to their bank account information.

Gather a Money Team

As we age, we need trusted advocates to assist us with financial issues. It can be uncomfortable to talk with your parents about finances, so adding other members of the family to the team is often helpful

and can make discussions easier. In the LGBT community, many elders have identified formal family arrangements and invite those trusted contacts into meetings with financial advisors to build this relationship. If your parents are working with a CFP® professional, ask them to include you in the meetings. Help your parent identify who they can trust and add those people to their Money Team.

Schedule Regular Check-Ins

As your parents' trusted advocate, I recommend you help them establish online access with their bank so that you can monitor banking and credit activity regularly. Also, set up automatic drafts from their bank account to handle their monthly fixed bills. Many elders still like their bank checking accounts balanced and reconciled monthly. I sit with my mom for dinner each month and review hers; we balance to the penny. This allows me to ask her about any expenses that look out of the ordinary. I keep on top of things, so that I can help build trust with her. I also keep my siblings up to date on a regular basis. This helps to create and maintain trust within the family unit.

Update General Power of Attorney Document

At times, you may find yourself in a situation where you need to talk with your parents' financial services institutions. I try to include my mom when I'm having conversations about her finances, but sometimes with our schedules, I must talk with an institution by myself. Therefore, you want to make sure your parents have an up-to-date financial power of attorney (POA) listing you and other trusted contacts. Most financial institutions like to have this document dated within five years of execution. I also recommend that your parent have more than one person listed on the document to follow in succession. This is in case the first person named predeceases the others or is not able to act as POA. Listing a successor (or two) provides a safeguard that someone will be able to act for your parent when the time comes for advocacy.

Current Healthcare/Medical Power of Attorney Document

A medical power of attorney (MPOA) is equally as important to your parents' financial well-being. Being able to have direct communication with healthcare companies, providers and so on, makes navigating overall care and finances easier. Not all states call this document a MPOA — some include the language in the healthcare directive or living will. These documents spell out the wishes of your parent in certain health events. They name the healthcare agent and guardian as well as your parents' wishes on how and what treatments they would like in case they are not able to communicate at the time. I recommend you have these documents drafted prior to any health issues if possible and give a copy to all doctors as well as the hospital with which the doctors are affiliated. As with the POA, I recommend having more than one person listed in succession for the same reasons.

Shred! Shred! Shred!

The **Federal Trade Commission** is another important site that helps consumers understand scams and ways to prevent them. On its website, you will find a list of documents that are best shredded rather than simply thrown away. Help your parent by going through old files and clean out outdated documents. If you don't have access to a shredder at home, many libraries have annual shredding events. Make it fun and help them organize only the important documents they need to keep, such as birth certificates, marriage/divorce paperwork, taxes, passports and so on.

Monitor Credit Reports

Lastly, make sure to review your parents' **credit report** at least annually. By reviewing and monitoring activity on their credit report, you help ensure that no one has access to their private identification and can open credit in their name. You may also want to consider having your parents freeze their credit, which will limit the exposure of a breach of their identity and lock down the ability for anyone to open new lines of credit.

If you or a loved one experience fraud, contact the [AARP Fraud Watch Network](#), which equips you with reliable, up-to-date insights and offers a free Fraud Network Helpline. The network also advocates at the state, federal and local levels to enact policy changes that protect consumers and enforce laws.

For more information about helping protect your parents from fraud, visit [LetsMakeAPlan.org](#).

Get started on securing your financial future today

FIND A CFP® PROFESSIONAL

TOPICS

Elder Care

CFP® PROFESSIONALS NEAR YOU

not your location?

MS. JOANNE YECIES
Chevy Chase, MD

MRS. ANGELA M. BECKHAM
Washington, DC

Planning Services Offered
Retirement Planning, Comprehensive Financial Planning, Investment Planning

MR. WILLIAM STALEY JEFFERY
Washington, DC

Planning Services Offered
Insurance Planning, Retirement Planning, Investment Planning, Employee and Employer Plan Benefits, Estate Planning

MR. JOHN EDWARD GIROUARD

Questions for the Record - Ms. Burns Koven

1. Which of the following options best describes your self-identified race? (You may choose more than one.)
 - ~~White or Caucasian~~
 - Black or African American
 - Hispanic/Latinx
 - Asian
 - Middle Eastern/North African
 - Choose not to answer
 - Prefer to self-describe (please specify)

2. Which of the following options best describes your gender identity?
 - ~~Woman~~
 - Man
 - Non-binary
 - Transgender Man
 - Transgender Woman
 - Choose not to answer
 - Prefer to self-describe (please specify)

3. We know that fraudsters have turned to cryptocurrency as a primary means of fleecing their victims and for moving and laundering the proceeds of their crimes. Digital identity, know-your-customer requirements, and adoption of the Travel Rule have been proposed as a potential mitigating measures to crypto crime. Can you share how digital identity and some of the novel means of collecting and sharing that information (e.g., zero knowledge proofs) could play a role in the responsible future of crypto? What could Congress do to help government and industry towards adoption of such standards and technologies?

How digital identity can play a role in the responsible future of crypto

Digital identity can be a valuable building block for a responsible and efficient crypto ecosystem. Compared to traditional document-based KYC, digital identity can allow crypto platforms to verify users more effectively using authenticated data sources or verifiable credentials, thereby reducing the risk of synthetic or stolen identities. Besides reducing risk, there can also be strong efficiency gains for businesses and consumers - for businesses, it can reduce onboarding lags and optimise the time and manpower required for know-your-customer processes, while for consumers, the ability to reuse digital identity credentials offers convenience.

Today, there are different ways identity information can be collected and shared. Governments, banks, technology platforms and other institutions already hold information that can underpin digital identity. The challenge, however, is whether we can create a digital identity architecture

that is secure, privacy preserving and inclusive, and that avoids unnecessary concentrations of information or power.

Blockchains offer one such pathway, enabling individuals to store and control their own identity credentials. For instance, institutions or government agencies could issue credentials after verifying a person's identity or attributes off-chain. These credentials could be selectively disclosed by the user.

Additionally, novel technologies such as Zero-Knowledge Proofs (ZKPs) can allow users to prove compliance attributes, such as age, residency or sanction-screening status, without revealing underlying personal information. It can also enable automated compliance in decentralised environments - for instance, programming a protocol to only interact with wallets that hold acceptable KYC credentials, ensuring that they do not facilitate illicit activity by sanctioned entities.

It's important to note that digital identity is not a silver bullet for the prevention of financial crime, because verification of identity does not equate to verification of intent. For instance, wilful and unwitting money mule activity can be undertaken by authenticated account holders. More advanced analytics, driven by artificial intelligence and machine learning, can play a role in identifying such behaviour.

What could Congress do to help government and industry towards adoption of such standards and technologies?

Congress has a critical role to play in accelerating the deployment of digital identity in the crypto ecosystem, while ensuring that civil liberties and innovation are protected. This could include funding work to:

- Develop open, interoperable digital identity standards for decentralised ecosystems, through public-private partnerships that harness the latest technological innovations;
- Conduct research and pilot programmes that test how verifiable credentials and zero-knowledge proofs can be integrated into crypto exchanges workflows, wallets and DeFi protocol in a manner that balances transparency and privacy;
- Clarifying legal or regulatory frameworks around the use of identity attestations or cryptographic proofs to satisfy compliance requirements like KYC obligations and the Travel Rule;
- Incentivise adoption of open-source identity infrastructure, particularly for small businesses; and
- Enhance international cooperation to ensure global acceptance of developed standards.

**Kathy Stokes Response to
Questions for the Record
Subcommittee Hearing, entitled:
“Following the Money: Tools and Techniques to Combat Fraud”
April 01, 2025**

1. Which of the following options best describes your self-identified race? (You may choose more than one.)

Choose not to answer

2. Which of the following options best describes your gender identity?

Choose not to answer

3. In your testimony, you mention the need for more accurate and complete data about scams, victims, bad actors, and trends among all three. Can you please discuss why this is needed, how improved data could be leveraged to help both investigators and victims? What, specifically, you would recommend to Congress to improve the collection and analysis of this data and do you also see a role for financial institutions in that process?

We know that the vast majority of fraud victims do not report to law enforcement. In their 2024 “Protecting Older Consumers 2023–2024” [report](#), the FTC adjusted its 2023 reported losses to account for under-reporting, from \$10.4 billion to as much as \$158.3 billion. This means that law enforcement has incomplete information to rely upon as they attempt to identify trends and prioritize resources. Having more complete and accurate data would allow for better resource allocation, as well as better coordination on priority threats, which could help to stop these crimes from happening in the first place. The US needs a centralized reporting system to aggregate and analyze data as well as to provide consumers an easier path to law enforcement reporting.

4. In your written testimony, you mention the damage of fraud involving cryptocurrency automated teller machines. Can you please discuss why action on this is needed, particularly where Americans age 50 and older are involved, and what, specifically, you would recommend with regard to these financial institutions, regulated as money service businesses and money transmitters under the Bank Secrecy Act?

Fraudulent activity targeting older Americans is on the rise. Cryptocurrency kiosks, also known as “crypto ATMs,” “BTMs,” or “virtual currency kiosks,” can be found in supermarkets, convenience stores, gas stations, bars, and restaurants. Crypto kiosks look like bank ATMs and allow people to conduct legitimate cryptocurrency transactions, such as sending money to digital wallets. Today, there are more than 45,000 crypto ATMs nationwide. However, because crypto ATMs are largely unregulated at the state level compared to traditional financial institutions, like banks and other money service businesses, they lack similar fraud protections. As a result, criminals are using crypto ATMs to steal hundreds of millions of dollars from Americans each year through fraudulent purchase schemes.

These scams work like many other types of scams. Criminals – often impersonating government officials or businesses – convince individuals that they must address an urgent financial matter, directing them to withdraw large amounts of cash and put that money into a crypto ATM. It is then transferred to a digital wallet controlled by the criminal.

Older adults are disproportionately affected by fraud and scams using cryptocurrency ATMs. In 2023, the FBI received 10,956 complaints involving crypto kiosks, and Americans reported over \$246 million in stolen funds. The vast majority (2,674) of the complaints came from adults 60+. Given the aforementioned problem of under-reporting, victims and amounts stolen are likely far higher.

AARP is advocating for important consumer protections that will deter criminals from leveraging cryptocurrency kiosks in their schemes. These include:

- Implementing daily transaction limits to limit the appeal of these machines to criminals
- Posting fraud warning notices and clarify steps people should take if they suspect fraudulent activity
- Clearly displaying the fees and exchange rate charged
- Giving receipts with relevant transactional information, which allow law enforcement to investigate immediately
- Requiring cryptocurrency operators to refund transaction fees for transactions related to fraud

Thus far, California, Connecticut, Minnesota, Vermont, Arizona, Arkansas, Iowa, Maryland, Nebraska, and North Dakota have enacted laws to implement greater cryptocurrency kiosk protections. We hope to see the federal government build upon this work at the federal level.

5. Can you please address how authorized push payment or APP fraud schemes are accomplished and how harmful these schemes can be for the victims of these crimes?

Fraud criminals use social engineering methods to make a target believe something that is not true, and to convince them to make financial transactions to address an urgent matter. The key elements of the majority of fraud crimes is contact from out of the blue that yields a heightened emotional state and contains urgency. Criminals use this combination because it signals to the brain that we must move into action to address the urgent matter, bypassing our logical thought processing. Criminals have referred to this as getting targets “under the ether.” Academics refer to it as an “amygdala hijack.”

This scenario plays out repeatedly, whether it’s a government impersonation scheme (The Social Security Administration warning you that your account has been suspended due to criminal activity you appear to be engaged in); the “grandparent scam” (“Grandma, it’s me and I’m in big trouble! Please don’t tell mom or dad, but I need you help right away!”); the utility scam (“Your account is past due and we are on the way to shut off your power...”) and more. Methods of payment can range from credit cards, peer-to-peer payment apps, or wire transfers to convincing the victim to purchase gift cards and share the activation information or to get cash from their bank and convert it at a crypto ATM machine (as referenced in our response to question 3.)

The harm these crimes cause is profound. Financially, the stolen funds are usually unrecoverable, and especially for older fraud victims, it begins a life of family support (if it's even available) and social safety nets. The emotional impact can surpass the financial, even in instances when a victim has been financially depleted. The shame victims feel because of our societal tendency to blame them, rather than the criminals, can result in suffering in silence and even suicide. Scams that involve making the victim believe they are in a trust relationship are especially difficult to recover from emotionally. The FINRA Investor Education Foundation studied harms and found that two in three fraud victims suffer at least one significant health or emotional impact.

.....
(Original Signature of Member)

119TH CONGRESS
1ST SESSION

H. R. _____

To update thresholds for certain currency transaction reports and suspicious activity reports, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. LOUDERMILK introduced the following bill; which was referred to the Committee on _____

A BILL

To update thresholds for certain currency transaction reports and suspicious activity reports, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Financial Reporting
5 Threshold Modernization Act”.

1 **SEC. 2. UPDATING THRESHOLDS FOR CERTAIN CURRENCY**
2 **TRANSACTION REPORTS AND SUSPICIOUS**
3 **ACTIVITY REPORTS.**

4 (a) THRESHOLDS FOR CERTAIN CURRENCY TRANS-
5 ACTION REPORTS.—

6 (1) CURRENCY TRANSACTION REPORTS.—The
7 Secretary of the Treasury shall—

8 (A) not later than the end of the 180-day
9 period beginning on the date of the enactment
10 of this Act, revise regulations issued with re-
11 spect to section 5313 of title 31, United States
12 Code, to update each \$10,000 threshold amount
13 in such regulations to \$30,000; and

14 (B) every 5 years, update each such
15 threshold amount to reflect the change in the
16 Consumer Price Index for All Urban Con-
17 sumers published by the Bureau of Labor Sta-
18 tistics of the Department of Labor.

19 (2) THRESHOLD FOR REPORTS RELATING TO
20 COINS AND CURRENCY RECEIVED IN NONFINANCIAL
21 TRADE OR BUSINESS.—Section 5331 of title 31,
22 United States Code, is amended—

23 (A) by striking “\$10,000” each place such
24 term appears in heading or text and inserting
25 “\$30,000”; and

26 (B) by adding at the end the following:

1 “(e) UPDATES FOR INFLATION.—Every 5 years, the
2 Secretary of the Treasury shall update each dollar figure
3 under this section to reflect the change in the Consumer
4 Price Index for All Urban Consumers published by the
5 Bureau of Labor Statistics of the Department of Labor.”.

6 (b) THRESHOLDS FOR SUSPICIOUS ACTIVITY RE-
7 PORTS.—Not later than the end of the 180-day period be-
8 ginning on the date of the enactment of this Act, each
9 Federal department or agency that issues regulations with
10 respect to reports on suspicious transactions described
11 under section 5318(g) of title 31, United States Code,
12 shall update each \$5,000 threshold amount in such regula-
13 tions to \$10,000 and each \$2,000 threshold amount in
14 such regulation to \$3,000.

15 (c) UPDATING THE MONEY SERVICES BUSINESS
16 DEFINITION THRESHOLDS.—Not later than the end of the
17 180-day period beginning on the date of the enactment
18 of this Act, the Secretary of the Treasury shall revise sec-
19 tion 1010.100(ff) of title 31, Code of Federal Regulations,
20 to update each \$1,000 threshold amount in such regula-
21 tions to \$3,000.

119TH CONGRESS
1ST SESSION

H. R. 425

To repeal the Corporate Transparency Act.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 15, 2025

Mr. DAVIDSON (for himself, Mr. BALDERSON, Mr. BERGMAN, Mr. BIGGS of Arizona, Mr. BUCHANAN, Mr. BURLISON, Mrs. CAMMACK, Mr. CISCOMANI, Mr. CLOUD, Mr. CLYDE, Mr. CRANE, Mr. DUNN of Florida, Mr. EDWARDS, Mr. ELLZEY, Mr. ESTES, Mr. EZELL, Mr. FINSTAD, Mrs. FISCHBACH, Mr. FLEISCHMANN, Ms. FOXX, Mr. FULCHER, Mr. GRAVES, Ms. GREENE of Georgia, Mr. GROTHMAN, Mr. GUEST, Ms. HAGEMAN, Mr. HERN of Oklahoma, Mrs. HOUCHIN, Mr. HUDSON, Mr. JOHNSON of South Dakota, Mr. LAHOOD, Mr. LANGWORTHY, Ms. LEE of Florida, Ms. MACE, Mr. MOOLENAAR, Mr. MOORE of Alabama, Mr. NORMAN, Mr. OGLES, Mr. PERRY, Mr. PFLUGER, Mr. ROSE, Mr. ROUZER, Mr. ROY, Mr. RULLI, Mr. SCHWEIKERT, Mr. SMITH of Missouri, Mr. SMITH of Nebraska, Mr. STAUBER, Ms. TENNEY, Mr. THOMPSON of Pennsylvania, Mr. TIFFANY, Ms. VAN DUYN, Mr. WEBER of Texas, Mr. ZINKE, Mr. COLLINS, Mr. BOST, Mr. KELLY of Mississippi, Mr. SCOTT FRANKLIN of Florida, Mr. BEAN of Florida, Mr. STUTZMAN, Mr. TAYLOR, Mr. BARRETT, Mr. DOWNING, Mr. GILL of Texas, Mr. YAKYM, Mr. VAN ORDEN, Mrs. BICE, Mr. ONDER, and Mr. GRIFFITH) introduced the following bill; which was referred to the Committee on Financial Services

A BILL

To repeal the Corporate Transparency Act.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Repealing Big Brother
3 Overreach Act”.

4 **SEC. 2. REPEAL.**

5 (a) IN GENERAL.—The Corporate Transparency Act
6 (title LXIV of division F of the William M. (Mac) Thorn-
7 berry National Defense Authorization Act for Fiscal Year
8 2021 (Public Law 116–283; 134 Stat. 4604)) and the
9 amendments made by that Act are repealed.

10 (b) TECHNICAL AND CONFORMING AMENDMENTS.—

11 (1) Title 31, United States Code, is amended—

12 (A) in section 5321(a)—

13 (i) in paragraph (1), by striking “sec-
14 tions 5314, 5315, and 5336” each place
15 the term appears and inserting “sections
16 5314 and 5315”; and

17 (ii) in paragraph (6), by striking “(ex-
18 cept section 5336)” each place the term
19 appears; and

20 (B) in section 5322, by striking “section
21 5315, 5324, or 5336” each place the term ap-
22 pears and inserting “section 5315 or 5324”.

23 (2) Title LXV of the Anti-Money Laundering
24 Act of 2020 (division F of the of the William M.
25 (Mac) Thornberry National Defense Authorization

1 Act for Fiscal Year 2021 (Public Law 116–283; 134
2 Stat. 4604)) is amended—

3 (A) by repealing section 6502 (134 Stat.
4 4626); and

5 (B) in section 6509 (134 Stat. 4633)—

6 (i) by striking “(a) IN GENERAL.—
7 Subsection (l)” and inserting “Subsection
8 (l)”; and

9 (ii) by striking subsection (b).

○

[DISCUSSION DRAFT]

119TH CONGRESS
1ST SESSION

H. R. _____

To amend title 31, United States Code, to limit the beneficial ownership reporting requirements to only require the reporting of beneficial owners who are foreign persons.

IN THE HOUSE OF REPRESENTATIVES

Mr. DAVIDSON introduced the following bill; which was referred to the Committee on _____

A BILL

To amend title 31, United States Code, to limit the beneficial ownership reporting requirements to only require the reporting of beneficial owners who are foreign persons.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Repealing Big Brother
5 Overreach Act”.

1 **SEC. 2. BENEFICIAL FOREIGN OWNERSHIP INFORMATION**
2 **REPORTING REQUIREMENTS.**

3 (a) IN GENERAL.—Section 5336 of title 31, United
4 States Code, is amended—

5 (1) by inserting “foreign” after “Beneficial”
6 each place such term appears in heading or text;

7 (2) by inserting “foreign” after “beneficial”
8 each place such term appears in heading or text; and

9 (3) in subsection (a)(3)(A), by inserting after
10 “individual who” the following: “is a foreign person
11 and”.

12 (b) CLERICAL AMENDMENT.—The table of contents
13 for chapter 53 of title 31, United States Code, is amended,
14 in the item relating to section 5336, by inserting “foreign”
15 after “Beneficial”.

.....
(Original Signature of Member)

119TH CONGRESS
1ST SESSION

H. R. _____

To permit State, local, and Tribal law enforcement agencies that receive eligible Federal grant funds to use such funds for investigating elder financial fraud, pig butchering, and general financial fraud, and to clarify that Federal law enforcement agencies may assist State, local, and Tribal law enforcement agencies in the use of tracing tools for blockchain and related technology, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. NUNN of Iowa introduced the following bill; which was referred to the
Committee on _____

A BILL

To permit State, local, and Tribal law enforcement agencies that receive eligible Federal grant funds to use such funds for investigating elder financial fraud, pig butchering, and general financial fraud, and to clarify that Federal law enforcement agencies may assist State, local, and Tribal law enforcement agencies in the use of tracing tools for blockchain and related technology, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Guarding Unprotected
3 Aging Retirees from Deception Act” or the “GUARD
4 Act”.

5 **SEC. 2. DEFINITIONS.**

6 In this Act:

7 (1) **ELDER FINANCIAL FRAUD.**—The term
8 “elder financial fraud” means the illegal or improper
9 use of an elderly or adult with a disability’s money,
10 property, or other resources for monetary or per-
11 sonal benefit, profit, or gain.

12 (2) **ELIGIBLE FEDERAL GRANT FUNDS.**—The
13 term “eligible Federal grant funds” means funds re-
14 ceived under the following:

15 (A) The Department of Justice Economic,
16 High-Technology, White Collar, and Internet
17 Crime Prevention National Training and Tech-
18 nical Assistance Program.

19 (B) The Department of Justice Informa-
20 tion Sharing Training and Technical Assistance
21 Program.

22 (C) The Department of Justice Internet of
23 Things National Training and Technical Assist-
24 ance Program.

25 (D) Section 1401 of the Violence Against
26 Women Act Reauthorization Act of 2022 (34

1 U.S.C. 30107; relating to Local Law Enforce-
2 ment Grants for Enforcement of Cybercrimes
3 Against Individuals).

4 (E) The Department of Justice COPS
5 Technology and Equipment Program.

6 (3) GENERAL FINANCIAL FRAUD.—The term
7 “general financial fraud” means the intentional mis-
8 representation of information or identity to deceive
9 others, the unlawful use of a credit card, debit card,
10 or automated teller machine or the use of electronic
11 means to transmit deceptive information, in order to
12 obtain money or other things of value.

13 (4) PIG BUTCHERING.—The term “pig butch-
14 ering” means a confidence and investment fraud in
15 which the victim is gradually lured into making in-
16 creasing monetary contributions, generally in the
17 form of cryptocurrency, to a seemingly sound invest-
18 ment before the scammer disappears with the con-
19 tributed monies.

20 (5) SCAM.—The term “scam” means a financial
21 crime undertaken through the use of social engineer-
22 ing that uses deceptive inducement to acquire—

23 (A) authorized access to funds; or

24 (B) personal or sensitive information that
25 can facilitate the theft of financial assets.

1 (6) STATE.—The term “State” means each of
2 the several States, the District of Columbia, and
3 each territory of the United States.

4 **SEC. 3. FEDERAL GRANTS USED FOR INVESTIGATING**
5 **ELDER FINANCIAL FRAUD, PIG BUTCHERING,**
6 **AND GENERAL FINANCIAL FRAUD.**

7 (a) IN GENERAL.—State, local, and Tribal law en-
8 forcement agencies that receive eligible Federal grant
9 funds may use such funds for investigating elder financial
10 fraud, pig butchering, and general financial fraud, includ-
11 ing by—

12 (1) hiring and retaining analysts, agents, ex-
13 perts, and other personnel;

14 (2) providing training specific to complex finan-
15 cial investigations, including training on—

16 (A) coordination and collaboration between
17 State, local, Tribal, and Federal law enforce-
18 ment agencies;

19 (B) assisting victims of financial fraud and
20 exploitation;

21 (C) the use of blockchain intelligence tools
22 and related capabilities related to emerging
23 technologies identified in the February 2024
24 “Critical and Emerging Technology List Up-
25 date” of the Fast Track Action Subcommittee

1 on Critical and Emerging Technologies of the
2 National Science and Technology Council (the
3 “Critical and Emerging Technology List”); and

4 (D) unique aspects of fraud investigations,
5 including transnational financial investigations
6 and emerging technologies identified in the
7 Critical and Emerging Technology List;

8 (3) obtaining software and technical tools to
9 conduct financial fraud and exploitation investiga-
10 tions;

11 (4) encouraging improved data collection and
12 reporting;

13 (5) supporting training and tabletop exercises
14 to enhance coordination and communication between
15 financial institutions and State, local, Tribal and
16 Federal law enforcement agencies for the purpose of
17 stopping fraud and scams; and

18 (6) designating a financial sector liaison to
19 serve as a point of contact for financial institutions
20 to share and exchange with State, local, Tribal and
21 Federal law enforcement agencies information rel-
22 evant to the investigation of fraud and scams.

23 (b) REPORT TO GRANT PROVIDER.—Each law en-
24 forcement agency that makes use of eligible Federal grant
25 funds for a purpose specified under subsection (a) shall,

1 not later than 1 year after making such use of the funds,
2 issue a report to the Federal agency that provided the eli-
3 gible Federal grant funds, containing—

4 (1) an explanation of the amount of funds so
5 used, and the specific purpose for which the funds
6 were used;

7 (2) statistics with respect to elder financial
8 fraud, pig butchering, and general financial fraud in
9 the jurisdiction of the law enforcement agency, along
10 with an analysis of how the use of the funds for a
11 purpose specified under subsection (a) affected such
12 statistics; and

13 (3) an assessment of the ability of the law en-
14 forcement agency to deter elder financial fraud, pig
15 butchering, and general financial fraud.

16 **SEC. 4. REPORT ON GENERAL FINANCIAL FRAUD, PIG**
17 **BUTCHERING, AND ELDER FINANCIAL**
18 **FRAUD.**

19 No later than a year after the date of the enactment
20 of this Act, the Secretary of the Treasury and the Director
21 of the Financial Crimes Enforcement Network in con-
22 sultation with the Attorney General, the Secretary of
23 Homeland Security, and the appropriate Federal banking
24 agencies and Federal functional regulators shall, jointly,
25 submit to Congress a report on efforts and recommenda-

1 tions related to general financial fraud, pig butchering,
2 elder financial fraud, and scams.

3 **SEC. 5. REPORT ON THE STATE OF SCAMS IN THE UNITED**
4 **STATES.**

5 (a) IN GENERAL.—Not later than 2 years after the
6 date of the enactment of this Act, the Secretary of the
7 Treasury and the Director of the Financial Crimes En-
8 forcement Network in consultation with the Attorney Gen-
9 eral, the Secretary of Homeland Security, and the appro-
10 priate Federal banking agencies and Federal functional
11 regulators shall submit a report to the Congress on the
12 state of scams in the United States that—

13 (1) estimates—

14 (A) the number of financial fraud, pig
15 butchering, elder financial fraud, and scams
16 committed against American consumers each
17 year, including—

18 (i) attempted scams, including
19 through social media, online dating serv-
20 ices, email, impersonation of financial in-
21 stitutions and non-bank financial institu-
22 tions;

23 (ii) successful scams, including
24 through social media, online dating serv-
25 ices, email, impersonation of financial in-

1 stitutions and non-bank financial institu-
2 tions;

3 (B) the number of consumers each year
4 that lose money to one or more scams;

5 (C) the dollar amount of consumer losses
6 to scams each year;

7 (D) the percentage of scams each year that
8 can be attributed to—

9 (i) overseas actors; and

10 (ii) organized crime;

11 (E) the number of attempted scams each
12 year that involve the impersonation of phone
13 numbers associated with financial institutions
14 and non-bank financial institutions;

15 (F) an estimate of the number of synthetic
16 identities impersonating American consumers
17 each year;

18 (2) provides an overview of the Federal civil
19 and criminal enforcement actions brought against
20 the recipients of the proceeds of financial fraud, pig
21 butchering, elder financial fraud, and scams in the
22 period covered by the report that includes—

23 (A) the number of such enforcement ac-
24 tions;

1 (B) an evaluation of the effectiveness of
2 such enforcement actions;

3 (C) an identification of the types of claims
4 brought against the recipients the recipients of
5 the proceeds of financial fraud, pig butchering,
6 elder financial fraud, and scams;

7 (D) an identification of the types of pen-
8 alties imposed through such enforcement ac-
9 tions;

10 (E) an identification of the types of relief
11 obtained through such enforcement actions; and

12 (F) the number of such enforcement ac-
13 tions that are connected to a Suspicious Activ-
14 ity Report; and

15 (3) identifies amounts made available and
16 amounts expended to address financial fraud, pig
17 butchering, elder financial fraud, and scams during
18 the period covered by the report by—

19 (A) the Bureau of Consumer Financial
20 Protection;

21 (B) the Department of Justice;

22 (C) the Federal Bureau of Investigation;

23 (D) the Federal Communications Commis-
24 sion;

1 (E) the Board of Governors of the Federal
2 Reserve Board;

3 (F) the Federal Trade Commission;

4 (G) the Financial Crimes Enforcement
5 Network;

6 (H) the Securities and Exchange Commis-
7 sion; and

8 (I) the Social Security Administration.

9 (b) SOLICITATION OF PUBLIC COMMENT.—In car-
10 rying out the report required under subsection (a), the
11 Secretary of the Treasury shall solicit comments from con-
12 sumers, social media companies, email providers, tele-
13 communications companies, financial institutions, non-
14 bank financial institutions.

15 **SEC. 6. REPORT TO CONGRESS.**

16 Each Federal agency that provides eligible Federal
17 grant funds that are used for a purpose specified under
18 section 3(a) shall issue an annual report to the Committee
19 on Financial Services of the House of Representatives and
20 the Committee on Banking, Housing, and Urban Affairs
21 of the Senate containing the information received from law
22 enforcement agencies under section 3(b).

1 **SEC. 7. FEDERAL LAW ENFORCEMENT AGENCIES ASSIST-**
2 **ING STATE, LOCAL, AND TRIBAL LAW EN-**
3 **FORCEMENT AND FUSION CENTERS.**

4 Federal law enforcement agencies may assist State,
5 local, and Tribal law enforcement agencies and fusion cen-
6 ters in the use of tracing tools for blockchain and related
7 technology tools.

[DISCUSSION DRAFT]119TH CONGRESS
1ST SESSION**H. R.** _____

To require the Secretary of the Treasury to submit a report with respect to certain money laundering concerns in Cambodia, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To require the Secretary of the Treasury to submit a report with respect to certain money laundering concerns in Cambodia, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Stop Foreign
5 Scammers Act of 2025”.

1 **SEC. 2. MONEY LAUNDERING CONCERN AND ENGAGEMENT**
2 **WITH NATIONAL BANK OF CAMBODIA RE-**
3 **PORT.**

4 (a) IN GENERAL.—Not later than 180 days after the
5 date of the enactment of this Act, the Secretary of the
6 Treasury (hereafter referred to as the “Secretary”) shall
7 submit to the Committee on Financial Services of the
8 House of Representatives and the Committee on Banking,
9 Housing, and Urban Affairs of the Senate a report in
10 which the Secretary—

11 (1) determines, with respect to each covered en-
12 tity, whether reasonable grounds exist for concluding
13 that the covered entity is of primary money laun-
14 dering concern (as such term is used in section
15 5318A of title 31, United States Code) for the pur-
16 pose of the special measures described in such sec-
17 tion; and

18 (2) describes any engagement by the Secretary
19 with the National Bank of Cambodia, including the
20 provision of any technical assistance by the Sec-
21 retary, for the purpose of strengthening anti-money
22 laundering practices in Cambodia.

23 (b) COVERED ENTITY DEFINED.—In this Act, the
24 term “covered entity” means—

- 25 (1) the Huione Group;
26 (2) the Huione Guarantee;

- 1 (3) the Huione International Pay; and
- 2 (4) any successor of an entity described in
- 3 paragraphs (1) through (3).

[DISCUSSION DRAFT]119TH CONGRESS
1ST SESSION**H. R.** _____

To amend title 31, United States Code, to require the Director of the Financial Crimes Enforcement Network to be appointed by the President and confirmed by the Senate, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M. ____ introduced the following bill; which was referred to the Committee on _____

A BILL

To amend title 31, United States Code, to require the Director of the Financial Crimes Enforcement Network to be appointed by the President and confirmed by the Senate, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Accountability through
5 Confirmation Act”.

1 **SEC. 2. DIRECTOR OF THE FINANCIAL CRIMES ENFORCE-**
2 **MENT NETWORK.**

3 (a) APPOINTMENT OF DIRECTOR.—Section 310(b)(1)
4 of title 31, United States Code, is amended by striking
5 “who shall be appointed by the Secretary of the Treasury”
6 and inserting “who shall be appointed by the President,
7 by and with the advice and consent of the Senate”.

8 (b) PAY OF DIRECTOR.—Section 310(b)(1) of title
9 31, United States Code, is amended by adding at the end
10 the following: “The Director shall be compensated at the
11 rate provided under level IV of the Executive Schedule
12 under section 5315 of title 5”.

13 (c) TRANSITION PROVISION.—The Director of the Fi-
14 nancial Crimes Enforcement Network on the day before
15 the date of enactment of this Act shall continue to serve
16 in such position until the date on which the first Director
17 is confirmed by the Senate pursuant to section 310(b)(1)
18 of title 31, United States Code, as amended by subsection
19 (a).

.....
(Original Signature of Member)

119TH CONGRESS
1ST SESSION

H. R. _____

To amend the Burma Unified through Rigorous Military Accountability Act of 2022 to extend the sunset, to require a determination with respect to the imposition of sanctions on certain persons of Burma, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. HUIZENGHA introduced the following bill; which was referred to the Committee on _____

A BILL

To amend the Burma Unified through Rigorous Military Accountability Act of 2022 to extend the sunset, to require a determination with respect to the imposition of sanctions on certain persons of Burma, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Bringing Real Ac-
5 countability Via Enforcement in Burma Act” or the
6 “BRAVE Burma Act”

1 **SEC. 2. EXTENSION OF SUNSET.**

2 Section 5574 of the Burma Unified through Rigorous
3 Military Accountability Act of 2022 (subtitle E of title LV
4 of division E of the James M. Inhofe National Defense
5 Authorization Act for Fiscal Year 2023; 22 U.S.C. 10225)
6 is amended by striking “8 years” and inserting “10
7 years”.

8 **SEC. 3. MODIFICATIONS TO REPORTING REQUIREMENT.**

9 Section 5571(e) of the James M. Inhofe National De-
10 fense Authorization Act for Fiscal Year 2023 (22 U.S.C.
11 10222(e)) is amended to read as follows:

12 “(e) ASSESSMENT AND REPORT ON SANCTIONS
13 WITH RESPECT TO BURMESE PERSONS.—

14 “(1) IN GENERAL.—Not later than 180 days
15 after the date of the enactment of this Act, and an-
16 nually thereafter for 7 years, the President shall de-
17 termine whether the following persons meet the cri-
18 teria for sanctions described under subsection (a) or
19 under Executive Order 14014 (86 Fed. Reg. 9429;
20 relating to blocking property with respect to the sit-
21 uation in Burma):

22 “(A) Any Burmese state-owned enterprise
23 described in subsection (c)(1).

24 “(B) Myanma Economic Bank.

25 “(C) Any foreign person that the President
26 determines operates in the jet fuel sector of the

1 Burmese economy, including through activities
2 such as the provision of financial services or the
3 importation, exportation, reexportation, sale,
4 supply, trade, storage, or transport, directly or
5 indirectly, of jet fuel in Burma.

6 “(2) REPORT REQUIRED.—Upon making the
7 determination required by paragraph (1), the Presi-
8 dent shall submit to the appropriate congressional
9 committees a report on the assessment.

10 “(3) FORM OF REPORT.—The report required
11 by paragraph (2) shall be submitted in unclassified
12 form but may include a classified annex.”.

13 **SEC. 4. LIMITATION OF SHAREHOLDING BENEFITTING THE**
14 **STATE ADMINISTRATION COUNCIL OF**
15 **BURMA.**

16 (a) IN GENERAL.—The Secretary of the Treasury
17 shall instruct the United States Executive Director at the
18 International Monetary Fund to use the voice and vote
19 of the United States, when assessing potential changes to
20 any shareholding formula in connection with a governance
21 review of the Fund, to limit, as appropriate, an increase
22 to the shareholding of Burma if the country is subject to
23 the rule of the State Administration Council.

24 (b) WAIVER.—The President of the United States
25 may waive the application of subsection (a) upon certifying

1 to the Committee on Financial Services of the House of
2 Representatives and the Committee on Foreign Relations
3 of the Senate that the waiver is important to the national
4 interest of the United States, with a detailed explanation
5 of the reasons therefor.

6 **SEC. 5. UNITED STATES SPECIAL COORDINATOR FOR BUR-**
7 **MESE DEMOCRACY.**

8 (a) IN GENERAL.—There is within the office of the
9 Secretary of State a United States Special Coordinator for
10 Burmese Democracy (in this section referred to as the
11 “Special Coordinator”) who shall be appointed by the
12 President, by and with the advice and consent of the Sen-
13 ate.

14 (b) CENTRAL OBJECTIVE.—The Special Coordinator
15 should develop a comprehensive strategy for the implemen-
16 tation of the full range of United States diplomatic capa-
17 bilities to promote human rights and the restoration of
18 civilian government in Burma.

19 (c) DUTIES AND RESPONSIBILITIES.—The Special
20 Coordinator should, as appropriate, assist in—

21 (1) coordinating the sanctions policies of the
22 United States under the Burma Unified through
23 Rigorous Military Accountability Act of 2022 (22
24 U.S.C. 10201 et seq.) with relevant bureaus and of-

1 fices within the Department of State and other rel-
2 evant United States Government agencies;

3 (2) promoting a comprehensive international ef-
4 fort to impose and enforce multilateral sanctions
5 with respect to Burma;

6 (3) coordinating with and supporting inter-
7 agency United States Government efforts, including
8 efforts of the United States Ambassador to Burma,
9 the United States Ambassador to ASEAN, and the
10 United States Permanent Representative to the
11 United Nations, relating to—

12 (A) identifying opportunities to coordinate
13 with and exert pressure on the governments of
14 the People's Republic of China and the Russian
15 Federation to support multilateral action
16 against the Burmese military;

17 (B) working with like-minded partners to
18 impose a coordinated arms embargo on the
19 Burmese military and targeted sanctions on the
20 economic interests of the Burmese military, in-
21 cluding through the introduction and adoption
22 of a United Nations Security Council resolu-
23 tion;

24 (C) engaging in direct dialogue with Bur-
25 mese civil society, democracy advocates, ethnic

1 minority representative groups, and organiza-
2 tions or groups representing the protest move-
3 ment and the officials elected in 2020, such as
4 the Committee Representing the Pyidaungsu
5 Hluttaw, the National Unity Government, the
6 National Unity Consultative Council, the Ethnic
7 Resistance Revolutionary Organizations, and
8 their designated representatives;

9 (D) encouraging the United Nations Inde-
10 pendent Investigative Mechanism for Myanmar
11 to incorporate accountability mechanisms in re-
12 lation to the atrocities against Rohingya and
13 other ethnic groups, to take further steps to
14 make its leadership and membership ethnically
15 diverse, and to incorporate measures to enhance
16 ethnic reconciliation and national unity into its
17 policy agenda;

18 (E) assisting efforts by the relevant United
19 Nations Special Envoys and Special
20 Rapporteurs to secure the release of all political
21 prisoners in Burma, promote respect for human
22 rights, and encourage dialogue; and

23 (F) supporting nongovernmental organiza-
24 tions operating in Burma and neighboring
25 countries working to restore civilian democratic

1 rule to Burma and to address the urgent hu-
2 manitarian needs of the people of Burma;
3 (4) providing timely input for reporting on the
4 impacts of the implementation of the Burma Unified
5 through Rigorous Military Accountability Act of
6 2022 on the Burmese military and the people of
7 Burma; and
8 (5) reporting to and coordinating with Con-
9 gress.

.....
(Original Signature of Member)

119TH CONGRESS
1ST SESSION

H. R. _____

To amend the Foreign Assistance Act of 1961 to include information in the International Narcotics Control Strategy Report on improvements by countries in combating narcotics-related money laundering, to require a report on the consistency of Bank Secrecy Act examinations, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Ms. WATERS introduced the following bill; which was referred to the
Committee on _____

A BILL

To amend the Foreign Assistance Act of 1961 to include information in the International Narcotics Control Strategy Report on improvements by countries in combating narcotics-related money laundering, to require a report on the consistency of Bank Secrecy Act examinations, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Financial Access Im-
3 provements Act”.

4 **SEC. 2. IMPROVEMENTS BY COUNTRIES IN COMBATING**
5 **NARCOTICS-RELATED MONEY LAUNDERING.**

6 (a) IN GENERAL.—Section 489 of the Foreign Assist-
7 ance Act of 1961 (22 U.S.C. 2291h) is amended—

8 (1) in subsection (a)(7)—

9 (A) in the matter before subparagraph (A),
10 by striking “paragraph (3)(D)” and inserting
11 “paragraph (3)(C)”; and

12 (B) by inserting after subparagraph (C)
13 the following:

14 “(D) Where the information is available,
15 examples of improvements in each country re-
16 lated to the findings described in each of
17 clauses (i) through (viii) of subparagraph (C),
18 such as—

19 “(i) actions taken by the country due
20 to each country’s adoption of law and reg-
21 ulations considered essential to prevent
22 narcotics-related money laundering;

23 “(ii) enhanced enforcement actions
24 taken by the country, such as regulatory
25 penalties, criminal prosecutions and convic-
26 tions, and asset seizures and forfeitures;

1 “(iii) status changes in international
2 financial crime-related evaluations;

3 “(iv) other descriptions that are rep-
4 resentative of efforts to enhance the pre-
5 vention of narcotics-related money laun-
6 dering; and

7 “(v) if applicable, bilateral, multilat-
8 eral, and regional initiatives which have
9 been undertaken to prevent narcotics-re-
10 lated money laundering.”.

11 (b) ADDITIONAL REQUIREMENTS FOR MONEY LAUN-
12 DERING ISSUES.—In making each report required under
13 section 489(a) of the Foreign Assistance Act of 1961 as
14 amended by subsection (a), the President shall—

15 (1) consult with the Secretary of the Treasury
16 on any parts of the report relating to money laun-
17 dering; and

18 (2) prepare a separate volume of the report
19 containing all items relating to money laundering,
20 and submit a copy of such separate volume to the
21 Committee on Financial Services of the House of
22 Representatives and the Committee on Banking,
23 Housing, and Urban Affairs of the Senate.

24 (c) REPORT ON CONSISTENCY OF BSA EXAMINA-
25 TIONS.—

1 (1) IN GENERAL.—The Secretary of the Treas-
2 ury shall, not later than 180 days after the date of
3 the enactment of this section—

4 (A) consult with the Federal banking agen-
5 cies, the Financial Institutions Examination
6 Council, and the Bank Secrecy Act Advisory
7 Group to determine how to build more con-
8 sistent Bank Secrecy Act exams across such
9 agencies; and

10 (B) submit to the Committee on Financial
11 Services of the House of Representatives and
12 the Committee on Banking, Housing, and
13 Urban Affairs of the Senate, a report that de-
14 scribes steps the Secretary of the Treasury is
15 taking to build more consistent Bank Secrecy
16 Act exams across such agencies based on the
17 consultation required under paragraph (1).

18 (2) FEDERAL BANKING AGENCY.—In this sub-
19 section, the term “Federal banking agency” has the
20 meaning given the term in section 3(q) of the Fed-
21 eral Deposit Insurance Act.

.....
(Original Signature of Member)

119TH CONGRESS
1ST SESSION

H. R. _____

To amend the start date of the pilot program on sharing with foreign
branches, subsidiaries and affiliates.

IN THE HOUSE OF REPRESENTATIVES

Ms. GARCIA of Texas introduced the following bill; which was referred to the
Committee on _____

A BILL

To amend the start date of the pilot program on sharing
with foreign branches, subsidiaries and affiliates.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Foreign Affiliates
5 Sharing Pilot Program Extension Act”.

6 **SEC. 2. FOREIGN AFFILIATES SHARING PILOT PROGRAM.**

7 Section 5318(g)(8)(B)(iii) of title 31, United States
8 Code, is amended by striking “3 years after the date of
9 enactment of this paragraph” and inserting “3 years after

- 1 the date on which the Secretary of the Treasury issues
- 2 rules pursuant to subparagraph (A)’’.

[DISCUSSION DRAFT]119TH CONGRESS
1ST SESSION**H. R.** _____

To amend the Kleptocracy Asset Recovery Rewards Act to make the Kleptocracy Asset Recovery Rewards Pilot Program permanent, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M____ introduced the following bill; which was referred to the Committee on _____

A BILL

To amend the Kleptocracy Asset Recovery Rewards Act to make the Kleptocracy Asset Recovery Rewards Pilot Program permanent, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Kleptocracy Asset Re-
5 covery Rewards Program Act”.

1 **SEC. 2. KLEPTOCRACY ASSET RECOVERY REWARDS PRO-**
2 **GRAM.**

3 Section 9703 of the Kleptocracy Asset Recovery Re-
4 wards Act is amended—

5 (1) in the heading, by striking ‘**KLEPTOCRACY**
6 **ASSET RECOVERY REWARDS PILOT PROGRAM**’
7 and inserting “**KLEPTOCRACY ASSET RECOVERY**
8 **PROGRAM**”;

9 (2) in subsection (a)(1), by striking
10 “‘Kleptocracy Asset Recovery Rewards Pilot Pro-
11 gram’” and inserting “‘Kleptocracy Asset Recovery
12 Rewards Program’”;

13 (3) in subsection (g)(1), by striking “for 3
14 years”;

15 (4) striking (i); and

16 (5) by redesignating subsection (j) as sub-
17 section (i).