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

American Bankers Association®

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%202%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-finances-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 Checks[10] 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 dis 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-scamming 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 attempts[17] 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-scamming-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 SARs[19] 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.