**CONSUMER BANKERS ASSOCIATION JULY 17, 2024 FRAUD AND SCAMS ROUNDTABLE**

**SUMMARY AND PROPOSED NEXT STEPS**

The Consumer Bankers Association (CBA) hosted a roundtable (Roundtable) on July 17, 2024, to discuss a white paper the CBA commissioned by outside consultant Nick Bourke[1] entitled "Stopping Scams Against Consumers: Roadmap for a National Strategy" (the Paper).[2]

The Paper is not a CBA publication and does not necessarily represent the perspectives of CBA or our member banks. Rather, the Paper is Bourke's "roadmap" for expert stakeholders across industries and government functions as they work together to develop a national strategy for preventing fraud and scams against consumers and businesses. The Paper offers broad thematic goals for a national strategy, as well as a dozen "critical and cross-cutting" challenges that a national strategy could choose to prioritize.[3]

CBA's Roundtable was the beginning of CBA's efforts to seek cross-industry, public-private feedback on the ideas set forth in the Paper, with the intent to help shape CBA's own policy initiatives and prioritization related to fraud and scams.

During the Roundtable, CBA asked the assembled experts (collectively, the Participants):

- What deliverables or key performance indicators could be used to ensure that a national strategy for preventing fraud and scams would be effective?

- Are there any deliverables that would be both impactful and near-term achievable that CBA, or similarly interested parties, could pursue in parallel to the creation of a broader cross-industry, public-private national strategy?

---

[1] Nick Bourke has over two decades of experience in research, policy, law, banking, and program management. He was previously a founder and head of consumer finance and housing programs at The Pew Charitable Trusts, where he led expert teams of researchers and advocates to produce publications and technical assistance that contributed to substantial policy reforms including credit cards legislation, banking and consumer protection regulations, and major state payday loan reform laws.

[2] Nick Bourke, Stopping Scams Against Consumers: Roadmap for a National Strategy (July 17, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4897644 ("The proposed strategy calls for a broad government mandate, potentially directed at the White House or Congressional level, to facilitate coordination across the banking/financial services, telecommunications, and technology/social media sectors. Drawing on interviews with diverse experts and examples from overseas, the paper outlines the need for a comprehensive approach that focuses on sharing information to better detect and prevent scams that cause economic harm to consumers and businesses. To achieve a national strategy, industry leaders must form a cross-sector campaign using consistent messaging and advocating for strong government leadership.").

[3] These twelve "critical and cross-cutting challenges" include: (i) digital identification, (ii) privacy and data security, (iii) consumer education, (iv) reporting tools for victims, (v) standardize user experiences, (vi) help victims, (vii) include small or resource-poor firms, (viii) accommodate vulnerable consumers within a stronger system, (ix) establish stronger content screening capabilities, (x) address specific issues in the bank / financial institutions sector, (xi) address specific issues in the telecommunications sector, and (xii) address specific issues in the technology/social media sector.

The Roundtable was held under a modified Chatham House Rule: Participants were informed that their attendance at the event and a summary of the discussion would be made public, but no statement or position would be attributed to any specific Participant. Due to this modified Chatham House Rule, this summary of the Roundtable will not indicate "agreement" or "consensus" on any particular matters, so as to not bind any Participant to positions that were even widely agreed upon in the discussion. **Participation in the Roundtable by a person or entity is not an endorsement of the Paper or the positions that CBA will prioritize following the roundtable**.

The Participants included Nick Bourke, who moderated our discussion, and senior representatives from:

- Capital One, which currently Chairs the CBA Fraud Committee;
- the Consumer Bankers Association;
- CTIA, a trade association representing the U.S. wireless communications industry;
- Early Warning Services;
- the Federal Bureau of Investigation;
- Fintech Takes;
- the Identity Theft Resource Center;
- Stripe;
- USTelecom, a trade association representing telecommunications-related businesses based in the United States;
- the White House, National Security Council; and
- One or more additional independent federal agency/agencies that have relevant rulemaking and enforcement authorities, but declined to be identified.

The remainder of this document provides a high-level overview of the roundtable discussion.

***Bad actors scam and defraud consumers across a range of sectors and extract money from the banking system using fast and highly-integrated tactics. In order to combat these evolving tactics, the government must convene and lead a cross-industry public-private national strategy against fraud and scams.***

Participants discussed the need for coordinated government and cross-industry activity, but also the need to help regulators understand the scale of the issues; the need for government leadership; and the importance of tangible paths forward for policymakers to make progress on these issues.

Participants gave clear examples demonstrating the material underreporting of fraud and scams today, raising concerns about factors such as victim reticence (feeling shame or helplessness), lack of sufficient metrics, and lack of effective reporting mechanisms. Participants discussed the need for any national strategy to address each of those issues.

In that regard, Participants noted that conversations with banking regulators, legislators, and government agencies have left some with the impression that some policymakers have not prioritized fraud and scams. For example, Participants explained that currently proposed draft privacy legislation initially did not include exceptions for information-sharing relating to fraud prevention because even progressive legislative officials did not believe government-related data to be accurate. Similarly, Participants noted that states have begun repealing requirements that state law enforcement agencies accept the Federal Trade Commission's identity theft affidavit,

leading to a sense of backsliding and frustration.[4] Participants raised concerns that policymakers may be deterred from prioritizing fraud and scams due to jurisdictional obstacles or the perception of fraud and scams as "unwinnable" issues.

Participants noted that the lack of policymaker prioritization may be due to a lack of clear metrics quantifying both the size and growth of the fraud and scams problem. Government statistics often use overlapping definitions and appear to differ from one another by at least 100 percent or more, when attempting to estimate the prevalence of fraud and scams. For example, the Financial Crimes Enforcement Network's (FinCEN's) *2024 Financial Trends Analysis* noted 42 percent of Suspicious Activity Reports filed in 2021, representing $212 billion in transactions, related to identity issues.[5] FinCEN identified over 14 typologies commonly indicated in identity-related Bank Secrecy Act (BSA) reports, of which fraud was a subset. (The most frequently reported typologies were: fraud, false records, identity theft, third-party money laundering, and circumvention of verification standards, with the top five typologies accounting for 88 percent of identity-related BSA reports and 74 percent of the total identity-related suspicious activity amount reported during calendar year 2021.) In contrast, a 2024 U.S. Government Accountability Office report, released just three months later, estimated that federal government losses due to fraud were $521 billion a year. [6] Presumably fraud against the federal government should be a subset of the FinCEN identity totals – yet GAO's estimates more than twice FinCEN's estimates for the value of all identity-related BSA reports.

Participants noted that fraud and scams appear to be exponentially growing, both in prevalence and severity. Participants expressed that this growth was likely driven by technological advances (e.g., the ubiquity of artificial intelligence tools); the advanced sophistication of international criminal organizations; and the increasing involvement of nation-state actors. The Identity Theft Resource Center has publicly noted "[a] dramatic increase in high-dollar losses impacting victims of identity scams, routinely exceeding six and occasionally seven figures."[7] Participants noted resulting significant, non-financial harm to consumers as well. According to publicly available reports, the number of identity crime victims who have contacted the Identity Theft Resource Center in 2022 that report having considered suicide has risen to 16 percent.[8] For

---

[4] Federal Trade Commission, Federal Trade Commission Announces ID Theft Affidavit (Feb. 5, 2002), https://www.ftc.gov/news-events/news/press-releases/2002/02/federal-trade-commission-announces-id-theft-affidavit. ("The ID Theft Affidavit provides a model form that can be used to report information to many companies, simplifying the process of alerting companies where a new account was opened in the victim's name. Previously, victims of identity theft often had to fill out a separate reporting form for each fraudulent account opened by the identity thief.").

[5] Financial Crimes Enforcement Network, FinCEN Issues Analysis of Identity-Related Suspicious Activity (Jan. 9, 2024), https://www.fincen.gov/news/news-releases/fincen-issues-analysis-identity-related-suspicious-activity.

[6] U.S. Gov't Accountability Office, Fraud Risk Management: 2018-2022 Data Show Federal Government Loses an Estimated $233 Billion to $521 Billion Annually to Fraud, Based on Various Risk Environments, GAO 24-105833 (April 16, 2024), https://www.gao.gov/products/gao-24-105833. ("GAO collected data from three key sources to develop the estimate: investigative data, such as the number of cases sent for prosecution and the dollar value of closed cases; Office of Inspector General (OIG) semiannual report information; and confirmed fraud data reported to the Office of Management and Budget (OMB) by agencies.").

[7] Identity Theft Resource Center, 2023 Annual Report (April 2024), https://www.idtheftcenter.org/wp-content/uploads/2024/04/ITRC-2023-Annual-Report.pdf.

[8] Identity Theft Resource Center, 2023 Consumer Impact Report (Aug. 2023), https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-

comparison, the number of US residents (excluding unsheltered people) who have contemplated taking their own lives for any reason is 5 percent.

Participants expressed that industry needs assistance in emphasizing the need for a government call to action, as well as helping direct areas for policymakers to be more effective. At least one Participant suggested that the White House or Department of Treasury coordination could help cut across various public/private "silos" in both priority and goal setting.

A Participant also emphasized the need for a national strategy to restore consumers' confidence in the broader economy and its respected institutions.

***Strategies may differ based on the stages of fraud and scams, but consumer education is relevant at multiple stages.***

The Paper notes that many consulted experts felt fraud and scams could be stopped earlier in the cycle, before any victims' funds are transmitted. Examples of how fraud and scams could be stopped earlier in the cycle include:

- An online marketplace identifying that the same used car appears to be for sale in all 50 states;

- A dating site recognizing that the same profile or message is sent to thousands of potential suitors; or

- A social media site having an easily accessible way for users to report a "group" page dedicated to teaching people how to conduct fraud or scams.

Accordingly, Participants discussed framing the potential strategy and interventions in three categories:

- *Contact with the consumer before money movement*
    - Participants stressed the importance of education and reporting mechanisms at this stage.

- *The actual transmission of victims' funds*

- *Opportunities for interventions after funds have been transferred to bad actors*
    - Participants expressed the need for effective law enforcement investigation and prosecution of bad actors; and
    - Participants discussed tools, traditionally used for recovery of illicit money laundering proceeds, that could be used to help industry stop or claw back funds.

---

Report_Final-1.pdf ("Regardless of the reasons, there are still far too few resources to assist far too many identity crime victims. Too many victims are shunned by organizations that should support them and ignored by government agencies that are too short-staffed or ill-equipped to help them."). Participants noted these non-financial harms have become increasingly prevalent issues in popular culture and plot points in recent mainstream films. For example, in the action-thriller film *The Beekeeper* (2024) and the spy movie satire *Thelma* (2024), the inciting incidents for each film involve elderly women falling victim to financial scams – with a suicide involved in the former.

***Participants raised the need for effective consumer education throughout the Roundtable.***

One Participant mentioned that many fraud and scam victims do not want to acknowledge that such activities have happened to them. Participants noted that fraud and scam victims may believe that reporting will not help their situation, given the perceived lack of prosecution of bad actors and limited ability to recover funds. Nonetheless, Participants discussed the need for reporting mechanisms for consumers, given the lack of accurate reporting on these issues as well as the opportunity to identify new bad actors or fraudulent tactics as soon as possible. Participants emphasized the critical value consumer education would have on de-stigmatizing the conversation about fraud and scams and how consumer education could give consumers comfort and support during what they believe is an embarrassing event. Participants noted that quicker consumer reporting could also enable quicker law enforcement and/or trend identification to help reduce the risk of additional consumers falling prey to similar tactics.

Participants emphasized consumer education needs to be an ongoing coordinated effort, not just a point-in-time campaign. Additionally, Participants expressed that education needed to come from entities as broad and visible as government agencies, citing the "Smokey the Bear" federal campaign on wildfire suppression education. Participants expressed that consumer education would need to be sufficiently robust to shift consumers towards a new way of life, given the new realities of the digital economy.

Participants noted that federal agencies had ample opportunities and resources to fund such consumer education that, at least with respect to fraud and scam issues, appeared to be relatively untapped. For instance, the Department of Justice was required to establish a Crime Victims Fund under the Victims of Crime Act of 1984, financed by fines and penalties from convictions of federal cases – as opposed to tax dollars. According to the Department of Justice, "[f]or the first 15 years of the Fund's existence, the total deposits for each fiscal year were distributed the following year to support services to crime victims."[9] As of May 2024, however, the Fund balance is over $1.5 billion.[10] Similarly, in January 2023, the CBA wrote Consumer Financial Protection Bureau (CFPB) Director Chopra, urging the CFPB to "direct unallocated funds in the CFPB's Civil Penalty Fund toward consumer education initiatives focused on financial scam identification and prevention in accordance with Section 1075.107(a) of the Consumer Civil Penalty Rule."[11] The following year, eighteen members of the House of Representatives similarly wrote CFPB Director Rohit Chopra, asking that the CFPB direct unallocated funds in the CFPB's Civil Penalty Fund towards consumer education initiatives

[9] Department of Justice Office for Victims of Crime, Crime Victims Fund (last visited July 21, 2024), https://ovc.ojp.gov/about/crime-victims-fund.
[10] Id.
[11] CBA, Letter to CFPB Director Rohit Chopra re: "A Coordinated Approach to Protecting Consumers From Scams: How the CFPB, Government Agencies Can Bolster Ongoing Industry Efforts" (Jan. 10, 2023), https://consumerbankers.com/wp-content/uploads/2024/03/CFPB-Consumer-Education-Letter-Final-.pdf ("These education initiatives will help bolster efforts already underway to teach consumers how to spot scams on P2P payment networks and internet transactions, further preventing consumer harm before it occurs.").

focused on scam identification.[12] As the members of Congress noted, according to the Civil Penalty Fund's FY 2023 annual report, the total unallocated fund balance was $1,990,888,747.[13]

***A national fraud and scam strategy requires coordination across a range of relevant industries.***

The Paper underscores the importance for robust cross-industry collaboration among financial institutions, technology companies (particularly social media and dating companies), and the telecommunications sector in engaging with public sector policymakers in a national strategy. Participants discussed and did not identify other industries that are necessary for initial progress to be made towards a national strategy.

***Government participation will be necessary to enable knowledge sharing across industries and the public-private divide.***

The Paper identified the need for government agencies to enable firms to share knowledge and signals for private sector actors to effectively detect and prevent fraud. Participants identified several obstacles that would benefit from government clarity or action. A few Participants spoke about the obstacle of information- and data-sharing across industry silos. Another Participant mentioned that a lack of clarity about regulatory requirements that would otherwise restrict data sharing could benefit from Congressional intervention.

Participants noted the critical importance of policymakers appropriately creating liability protection for better information sharing. In that regard, Participants discussed the potential opportunities for regulators to clarify, and possibly expand, the applicability of the USA Patriot Act 314(b) safe harbor to cover information-sharing for financial institutions relating to fraud and scams, not just money laundering.[14] However, Participants noted that even if expanded in scope, Patriot Act 314(b) contains inherent limitations about the types of entities that can share

---

[12] Letter from Representatives William Timmons; Blaine Luetkemeyer; Bill Posey; Bill Huizenga; Ann Wagner; French Hill; Tom Emmer; Barry Loudermilk; Alex X. Mooney; John Rose; Dan Meuser; Scott Fitzgerald; Andrew R. Garbarino; Young Kim; Byron Donalds; Mike Flood; Mike V. Lawler; and Erin Houchin to CFPB Director Rohit Chopra (Jan. 16, 2024), https://consumerbankers.com/wp-content/uploads/2024/03/CFPB20Civil20Penalty20Fund20Ltr-1.pdf ("As the consumer demand to perform real-time payments across P2P networks grows, and the number of Americans affected by scammers increases, the federal government must be a willing partner with the financial services industry in order to protect consumers. By partnering with industry stakeholders, the CFPB can significantly enhance the impact of scam prevention efforts by equipping consumers with knowledge to recognize and avoid scams.").

[13] See Consumer Financial Protection Bureau, Financial report of the Consumer Financial Protection Bureau - Fiscal Year 2023, (Nov. 15, 2023) at 22, https://files.consumerfinance.gov/f/documents/cfpb_final-financial-report-fy_2023-11.pdf; https://www.consumerfinance.gov/data-research/researchreports/financial-report-cfpb-fiscal-year-2023/ ("Under the Act, funds in the Civil Penalty Fund may be used for payments to the victims of activities for which civil penalties have been imposed under the Federal consumer financial laws. To the extent that such victims cannot be located, or such payments are otherwise not practicable, the CFPB may use funds in the Civil Penalty Fund for the purpose of consumer education and financial literacy programs.").

[14] See, e.g., Financial Crimes Enforcement Network, Section 314(b) Fact Sheet (Dec. 2020) https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf ("Section 314(b) of the USA PATRIOT Act provides financial institutions with the ability to share information with one another, under a safe harbor that offers protections from liability, in order to better identify and report activities that may involve money laundering or terrorist activities. Participation in information sharing pursuant to Section 314(b) is voluntary, and FinCEN strongly encourages financial institutions to participate.").

information and, importantly, the types of claims included in the safe harbor (e.g., civil, but not criminal, claims).

Outside of the need for government intervention, Participants emphasized the need for finding relevant and actionable overlaps across industries. For instance, one Participant noted that what is useful information to one industry may not be useful to another industry. Participants noted that building shared standards and definitions could be useful in combatting this issue. However, other Participants cautioned that, given the potential for bureaucratic sprawl, the creation of shared standards and definitions should not halt or significantly slow down other work related to combatting fraud and scams. Instead, the Participant urged that any work relating to standards and definitions should be tailored to doing just enough work to help government policymakers appropriately prioritize fraud and scams and join in the work.

***Incentives for information sharing and data exchange may be reevaluated.***

The Paper suggests there needs to be stronger incentives and guidance for participating in data exchange. Liability concerns and disincentives related to information sharing thwart efforts to allocate internal resources at firms. During the discussion, Participants shared different perspectives on the best approach the government can use to incentivize industries to share information and exchange data to prevent fraud.

One Participant suggested the creation of a nonprofit data exchange, but other Participants questioned the feasibility of such a creation, given that many such companies in the United States are publicly traded. One Participant noted that a government agency could act as a "network of networks," sharing signals across fraud-and-scam-detection networks within various industries or, more importantly, across international lines.

Another Participant suggested a framework similar to the call-blocking framework used by the FCC for the telecommunications sectors, under which companies set up systems to block fraudulent text messages and calls within certain parameters.[15] Due to limitations in the telecommunication sector from sharing information with the government, Participants referenced the Information Sharing Analysis Center (ISAC) structure, which enables the telecommunication sector to focus on cybersecurity and legal challenges related to sharing information.[16] Participants discussed an ISAC in the financial services industry, but concerns were expressed regarding overbroad sharing, legal issues, and the credibility and validity of the process. One Participant suggested that perhaps the government could fund a research and development center, or a national laboratory/research program.

---

[15] Federal Communications Commission, Call Blocking Tools and Resources, https://www.fcc.gov/call-blocking (last visited July 21, 2024) (providing hyperlinks to over two-dozen resources relating to call blocking and labeling, including CTIA resources for stopping robocalls and US Telecom consumer information regarding illegal robocalls); see also CTIA, Consumer Resources: How to Stop Robocalls (last visited July 21, 2024), https://www.ctia.org/consumer-resources/how-to-stop-robocalls; US Telecom, Illegal Robocalls (last visited July 21, 2024) ("Stopping the plague of illegal robocalls is a serious issue for consumers, and our USTelecom member companies, industry partners, and folks at the FCC, FTC, DOJ and state Attorneys General offices are investing time and resources to fight back.").

[16] See, e.g., National Council of Isacs (last visited July 21, 2024), https://www.nationalisacs.org/ ("ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness.").

Participants highlighted the importance of balancing privacy risks, firms' commercial interests, and data sharing for fraud prevention. They noted that developments not expressly related to fraud and scams could significantly impact the ability of private-sector parties to balance these interests and successfully share data to prevent fraud. For example, the proposed secondary use of data restrictions under the CFPB's proposed rulemaking to implementation Section 1033 of the Dodd-Frank Act could limit the use of data for fraud prevention.[17] Participants debated the balancing of privacy and commercial interests, with some Participants suggesting that privacy concerns should not hold back ongoing efforts to establish a national strategy to prevent scams against consumers and businesses. Participants also questioned whether tighter restrictions on consumer social media and machine learning could be used to stop fraudulent activity, though other Participants noted that these uses would stop fraudulent activity but not necessarily the bad actor.

Overall, the discussion of information sharing and data exchange underscored the need for government leadership of a coordinated approach to enhance fraud and scam detection and prevention while navigating legal, privacy, and commercial challenges.

***Law enforcement must be actively invested in, and adequately resourced for, the fight against fraud and scams.***

Participants discussed the apparent challenges law enforcement faces in having sufficient resources for addressing fraud and scams and in making fraud and scam prevention a national law enforcement priority. Some Participants lamented that current prosecution efforts and punishments are seen as insufficient to deter repeat fraudsters and scammers. Other Participants emphasized the need for U.S. government leadership with respect to international strategy and cooperation, including in prosecution. Participants expressed that the increasing law enforcement prioritization of fraud and scams should be seen as essential, particularly because many frauds and scams are perpetuated by highly sophisticated criminal organizations engaged in other criminal activity.

Participants noted that when fraud and scams are prosecuted, the potential criminal charges are not comparable to the severe penalties typically associated with "traditional" gang activity, such as drug- and gun-crimes. Participants raised concerns that there is a greater sense of national urgency to fight certain (violent) crimes rather than other (financial) crimes. And, indeed, Participants noted anecdotal evidence that organized crime has shifted *away* from drugs and violence and *toward* financial crime, specifically because of the difference in the likelihood and severity of law enforcement investigation and prosecution. Participants noted that such criminals may also perceive financial crimes to be easier, cheaper, and more profitable ways to fund other criminal endeavors.

One Participant noted that the first 72 hours are critical for recovering consumers' funds, suggesting that already-existing rapid response programs could be utilized for halting fraudulent and scam transactions. A Participant referenced FinCEN's Rapid Response Program,

---

[17] Federal Register, Consumer Financial Protection Bureau "Required rulemaking on Personal Financial Data Rights," Docket No. CFPB-2023-0052 (Oct. 19, 2023), https://files.consumerfinance.gov/f/documents/cfpb-1033-nprm-fr-notice_2023-10.pdf. See, e.g., CBA, Letter to CFPB re: Docket No. CFPB-2023-0052 – Required Rulemaking on Personal Financial Data Rights (Dec. 29, 2023), https://consumerbankers.com/wp-content/uploads/2024/03/CBA20Comment20on20Docket20No.20CFPBE280932023E280930052-1.pdf ("As drafted, third parties will face significant uncertainty as to whether each specific use that is not required by law or to prevent fraud constitutes permissible 'servicing or processing.'").

a partnership between FinCEN, US law enforcement, and foreign partner agencies to share financial intelligence rapidly and recover stolen funds.[18] A Participant also referenced the Financial Fraud Kill Chain, which is a process that may be utilized for recovering large international wire transfers stolen from victim US bank accounts. As described by a Federal Bureau of Investigation memorandum made available by private industry, "The Financial Fraud Kill Chain utilizes FinCEN's relationship with the Egmont Group of Financial Intelligence Units, as well as law enforcement globally, to try to prevent the successful withdrawal of funds by criminal actors."[19] The Financial Fraud Kill Chain does have certain criteria that may not be always applicable for addressing all relevant types of fraud and scams.

Another Participant acknowledged the law enforcement resource concern, and further noted the Federal Trade Commission's lack of grant-making authority and the underutilization of the Department of Justice's Office of Victims of Crime as a source of funding.

[18] See, e.g., FinCEN, FinCEN Fact Sheet on the Rapid Response Program (RPP), FIN-2022-FCT1 (Feb. 11, 2022), https://www.fincen.gov/sites/default/files/shared/RRP%20Fact%20Sheet%20Notice%20FINAL%20508.pdf ("The RRP has been used to confront cyber threats involving approximately 70 foreign jurisdictions to date, and has the capacity to reach more than 160 foreign jurisdictions through FIU-to-FIU channels. Through these collaborative efforts, FinCEN has successfully assisted in the recovery of over $1.1 billion.").

[19] Federal Bureau of Investigation, Financial Fraud Kill Chain (Jan. 11, 2016), https://pbigroupsolutions.com/wp-content/uploads/2021/05/FFKC.pdf.

**THE CONSUMER BANKERS ASSOCIATION RECOMMENDS A GOVERNMENT-PRIVATE, CROSS-INDUSTRY NATIONAL STRATEGY FOR ADDRESSING FRAUD AND SCAMS.**

Based on Participant feedback on the Bourke Paper at the Roundtable, CBA recommends the following next steps and deliverables:[20]

1. Near-Term Efforts

    a. ***Inventory and promote*** pre-existing tools that are already in market and can help consumers, such as:

        i. The Telecom Industry Traceback Group, a tool created by the telecommunications industry but endorsed by relevant government agencies for identifying the source of automated "robocalls," as discussed further in the Paper;

        ii. The Identity Theft Resource Center reporting and victim support tools, which can be integrated with public and private organizations that already work with victims of frauds and scams.

    b. Commit to a broad-based ***consumer education*** strategy that, among other goals, ***destigmatizes reporting*** by victims of frauds and scams and provides encouragement to consumers that such reporting will both help prevent other consumers from falling prey to similar tactics as well as lead to a higher likelihood that law enforcement will be better positioned to recover illicit funds and bring enforcement actions against bad actors.

2. Medium-Term Efforts[21]

    a. Advocate for ***safe harbor frameworks***, such as Patriot Act Section 314(b), to be ***clarified and broadened*** to encourage information-sharing regarding fraud and scams;

    b. Advocate for the expansion of the use of the Rapid Response Program and Financial Fraud Kill Chain to be used to ***trace and assist with recovery*** of the proceeds of fraud and scams from bad actors, as well as to encourage with potential law enforcement activity;

    c. Advocate for the Department of Justice to ***extend grant funding*** from the Office of Victims of Crimes for work relating to fraud and scams;

[20] These positions reflect the CBA's recommendations that emerged from the July 17 roundtable discussion. This is a nonexclusive list, in that CBA's broader advocacy regarding scams, fraud, and the need for a national strategy will be both broader than the contours of the July 17 discussion and also developing over time. We do believe, however, that the positions stated here should form the core of a strong start to such work.

[21] These medium-term efforts should be primarily focused on repurposing frameworks "adjacent" to fraud and scams issues, such as tools and networks currently used to combat money laundering and other illicit fund transactions.

d. Continue to advocate for the CFPB to ***use its Civil Penalty Fund*** for consumer education and other efforts relating to fraud and scams.

3. Long-Term Efforts

    a. Identify and, where necessary, ***create metrics and definitions*** to help educate policymakers on the need to prioritize work relating to fraud and scams.

        i. Such efforts should be tailored so that resources are spent on metric and definition creation only to the extent ***necessary to mobilize*** policymakers.

    b. Explore alignment on ***data standards for sharing information*** across industries and between the private and public sectors.

        i. Encourage the government to act as a ***"network of networks"*** to help disseminate appropriate data across for- and non-profit consortia that may be more limited by industry sectors.

    c. Support National Institute of Standards and Technology efforts regarding ***digital identity standards***, as applicable for use in retail consumer financial services.

    d. Emphasize urgency for law enforcement officials to ***prioritize*** fraud- and scam-related ***prosecutions***.

    e. Call for greater ***international coordination*** on fraud and scam enforcement, highlighting the proximity to money laundering issues and bad actors.

As the Roundtable concluded, CBA (and many participants) underscored the importance of joining larger, ongoing conversations about a national fraud and scam strategy. CBA will champion the recommendations in this document in these forums and in its future action.

CBA will:

- Continue to work with its members to explore fraud and scam mitigation measures (e.g., best practices) that can be pursued within the retail banking industry alone;

- Explore working with other industries to identify information that can be useful in identifying and mitigating fraud and scams;

- Explore facilitating fraud and scam expertise sharing, across industries;

- Explore studying best practices from other jurisdictions (e.g., comparing the different approaches in the U.K. and Australia) for potential applicability to the U.S. market, recognizing differences in market composition and payment infrastructure; and

- Explore research and publication to draw attention to the need for greater law enforcement relating to fraud and scams.
    - Such work may explore (i) the societal impact of fraud and scams; (ii) the allocation of law enforcement resources relating to fraud and scams; and (iii) surveying remedies and penalties relating to fraud and scams vis-à-vis similar crimes.