Revolut Technologies Inc.
[redacted]

September 17, 2025

Office of the Comptroller of the Currency (OCC)
Chief Counsel's Office
Attn: Comment Processing
400 7th Street SW
Suite 3E-218
Washington, DC 20219

Federal Reserve Board of Governors
Attn: Ann E. Misback
Secretary of the Board
Mailstop M-4775
2001 C St. NW
Washington, DC 20551

Federal Deposit Insurance Corporation
Jennifer M. Jones, Deputy Executive Secretary
Attention: Comments — RIN 3064-ZA49
550 17th Street NW
Washington, DC 20429

RE: Request for Information on Potential Actions To Address Payments Fraud (Docket ID OCC-2025-0009; Docket No. OP-1866; RIN 3064-ZA49)

Revolut appreciates the opportunity to respond to the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), and the Federal Deposit Insurance Corporation (FDIC) (collectively, the Agencies) regarding the Agencies' Request for Information (RFI) on potential actions to address payments fraud.

As a global financial technology company serving more than 60 million customers across more than 38 markets, our perspective is shaped by our direct experience in a daily 'arms race' against fraudsters. At the forefront of our security measures is a proprietary fraud detection system using cutting-edge machine learning and artificial intelligence. This system, supported by a financial crime team of more than 4,000 specialists, analyzes hundreds of millions of transactions monthly to protect our customers. These advanced capabilities have enabled Revolut to prevent $1.5 billion in potential fraud since 2023.

Based on this experience, our recommendations are solution-oriented and focus on four key principles: establishing shared responsibility across the entire fraud value chain; creating common data standards to make intelligence actionable; implementing scalable, risk-based controls; and developing operator-level tools that benefit all institutions. Our proposals are designed to be rail-agnostic and strengthen the entire payments ecosystem.

We commend the Agencies for their leadership on this critical issue and stand ready to collaborate on approaches that measurably lower fraud, improve customer outcomes, and strengthen confidence in our financial system.

External Collaboration

1. What actions could increase collaboration among stakeholders to address payments fraud?

The most effective way to fight payments fraud is through broad, proactive collaboration across all stakeholders in the payments ecosystem. We recommend creating multidisciplinary working groups or task forces that include banks, payment companies, fintechs, telecommunications providers, and online platforms (social media, marketplaces), alongside law enforcement and regulators. For example, joint industry forums could be convened under agency sponsorship to regularly share fraud trend data, attack patterns, and best practices in real time. Such collaboration enables early warning of new fraud schemes and coordinated responses.

Additionally, public-private partnerships can be established to jointly disrupt fraud networks. The Australian National Anti-Scam Centre's "fusion cell" model is an instructive example: it brings together banks, telecom companies, and government agencies to share intelligence and take collective action, resulting in a 47% year-over-year decline in investment scam losses after targeted joint actions.[1]

Increasing collaboration also means ensuring all stakeholders have aligned incentives, for instance, considering shared responsibility frameworks so that those whose platforms may be used for fraudulent activities are invested in prevention efforts alongside banks. In summary, fraud is a cross-cutting threat that no single entity can tackle alone, so sustained collaboration and information exchange are essential.

2. What types of collaboration could be most effective in addressing payments fraud? What are some of the biggest obstacles to these types of collaboration?

Two forms of collaboration stand out as most effective: (i) Standard setting; and (ii) Real-time information-sharing networks. Standard setting can include developing common fraud classification taxonomies like the Federal Reserve's FraudClassifier℠ or establishing industry standards for account verification (such as "confirmation of payee" name-check services).

[1] National Anti-Scam Centre (Australian Competition & Consumer Commission), *Investment Scam Fusion Cell: Final Report (May 2024),* https://www.accc.gov.au/system/files/NASC-Investment-scam-fusion-cell-final-report-2024.pdf

Developing this shared language and baseline practices for all parties will improve consistency in fraud detection and reporting.

Real-time data-sharing networks, on the other hand, enable stakeholders to exchange fraud intelligence (e.g., known scam phone numbers, mule account identifiers, or emerging phishing scripts) to stop fraud as it unfolds. A collaborative, data-sharing approach is vital in prevention because fraudsters often exploit multiple institutions and channels. Connecting the dots quickly is key.

Obstacles exist, however. One major barrier is legal and privacy concerns that can make institutions hesitant to share customer or fraud data. Firms worry about violating privacy laws or tipping off criminals. To address this, regulators must provide clear safe harbor provisions or clarify permissive contexts (similar to the USA PATRIOT Act Section 314(b) framework for sharing Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) information) that allow sharing of fraud-related information without liability.

Another obstacle is a lack of trust or competitive concerns as organizations may be reluctant to share sensitive data with competitors. This can be mitigated by using neutral third-party utilities or industry consortia to aggregate and anonymize data. Additionally, technical challenges (differences in information technology systems and data formats) can hinder collaboration. Here, standard-setting bodies could promote interoperable data standards and Application Programming Interfaces (APIs) for fraud information exchange.

In sum, establishing clear legal frameworks and common standards will help overcome the biggest challenges to collaborative fraud-fighting efforts.

3. Which organizations outside of the payments or banking industry might provide additional insights related to payments fraud and be effective collaborators in detecting, preventing, and mitigating payments fraud?

Payments fraud often originates outside the traditional banking system, for example, through scammer outreach on phones or the internet. Collaboration must extend to non-bank sectors that can provide critical insights or mitigation. Telecommunications companies are essential partners: many fraud schemes (like one-time password interception, SIM swap, robocall scams) exploit telecom networks. Telecom providers can help detect and block scam communications, diverting calls from known scam numbers and playing a warning message. A three-month pilot program in Australia is estimated to have prevented millions in losses.[2]

Social media and technology platforms are another crucial group as a large share of modern scams begin through contact on social media or messaging apps. This includes encrypted messaging platforms like WhatsApp and Telegram, dating apps (a primary vector for romance scams), as well as community forums like Reddit and Discord where criminal tactics are shared and evolve faster than conventional security measures can adapt. The Federal Trade Commission (FTC) reports that one in four people who lost money to fraud since 2021 claim

[2] *Id. at 14.*

contact began on social media, with over $2.7 billion in reported losses originating on social platforms.[3] In the United Kingdom (UK), which is commonly seen as the most targeted country for fraud in Europe, the Payment Systems Regulator published data from the largest 14 banks that concluded that 54% of Authorized Push Payment (APP) scam cases were linked to a single social media platform.[4]

Holding all companies, not just banks and telecommunications firms, to account is vital, given their role within the fraud value chain. Involving these companies in fraud discussions (for example, through joint working groups or information sharing agreements) can yield better collaboration that could lead to improved fraud prevention. They can assist by shutting down fake profiles/ads, warning users, and verifying advertisers, all of which will help cut off fraud at the source.

Other valuable collaborators include email service providers, who are critical partners in addressing phishing; e-commerce marketplaces, which can monitor for fraudulent merchants and mule activity; and consumer advocacy or community organizations, who have essential on-the-ground insights into victim experiences.

Beyond these partners, it is critical to engage with industries that can be exploited as on-ramps to the financial system due to patchwork state-based regulatory frameworks. This includes sectors like online gaming and social casinos, and the network of prepaid card issuers and retailers. These entities possess unique insights into how unregulated payment methods are used to obscure fund sources before they enter the banking system. Finally, engaging with law enforcement agencies is essential to act on intelligence gathered from this entire coalition.

In sum, a broad coalition, spanning communications, technology, retail, consumer groups, and these less-obvious but critical sectors, will bring fresh perspectives and more points of intervention to detect, prevent, and mitigate payments fraud.

4. Could increased collaboration among Federal and State agencies help detect, prevent, and mitigate payments fraud? If so, how?

Yes. Increased collaboration among Federal and State agencies would materially improve detection, prevention, and recovery by closing jurisdictional gaps that fraudsters exploit. The Agencies, state banking departments, attorneys general, and law enforcement should issue joint advisories on prevalent fraud schemes to deliver a single, consistent message to financial institutions, telecommunications providers, social media platforms, and online marketplaces.

---

[3] Federal Trade Commission, *Social Media: A Golden Goose for Scammers* (October 2023), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers

[4] Payment Systems Regulator, *Unmasking How Fraudsters Target UK Consumers in the Digital Age* (December 2024), https://www.psr.org.uk/media/u0vnq1ra/unmasking-how-fraudsters-target-uk-consumers-in-the-digital-age-dec-2024.pdf

The Agencies could also establish a standing multiagency fraud coordination council that meets regularly to compare complaint and Suspicious Activity Report (SAR) trends, align policy responses, and launch coordinated crackdowns on emerging threats. Pooling authority, intelligence, and tools will enable faster interdiction and better outcomes for all Americans.

Consumer, Business, and Industry Education

5. In general, what types of payments fraud education are most effective, and why? Would different audiences (for example, industry and consumers) benefit from different types of payments fraud education?

Yes. The most effective education is timely, targeted, actionable, and measured. It works best when it is scenario-based and delivered at the point of risk (e.g., in-app warnings before a new or unusual payment, with a one-tap “learn more / cancel” option).

Different audiences indeed benefit from different approaches:

- **Consumers** need simple, relatable guidance on avoiding scams (avoid clicking on unknown links, verifying requests via known contacts, not sending money to strangers, etc.), often delivered through channels they trust (social media campaigns, financial institution email/SMS alerts, community seminars).
- **Businesses**, especially small businesses, may need education on topics like business email compromise, vendor invoice fraud, or payroll diversion schemes. Effective methods here include training webinars, industry association workshops, and checklists for internal controls (e.g., dual approvals for payments).
- **Industry professionals** (bank staff and employees of payment companies) benefit from more technical education, for example, detailed typology reports, red-flag indicators, and simulation exercises to test their fraud response processes.

6. Would additional education informing consumers and businesses about safe payment practices be helpful to reduce payments fraud and promote access to safe, secure payment options?

Yes, additional education would be highly beneficial, provided it moves beyond generic advice and addresses the behavioral and psychological tactics central to modern fraud. While promoting secure payment methods has its place, the most significant threats today, such as APP scams, succeed by manipulating the user, not by exploiting technical flaws in the payment system.

The most effective educational models focus on changing user behavior at the moment of risk. A premier example of this approach is the "Take Five to Stop Fraud"[5] campaign in the UK. We recommend the Agencies consider championing a similar national, public-private campaign in the United States.

[5] UK Finance, *Take Five to Stop Fraud*, https://www.takefive-stopfraud.org.uk/

The "Take Five" campaign's strength lies in its simple, memorable, and actionable message: "Stop, Challenge, Protect."

1. **Stop:** Urges the consumer to take a moment and pause before sending money or sharing information, especially when feeling rushed or pressured.
2. **Challenge:** Encourages the consumer to question the legitimacy of the request. It empowers them to reject, refuse, or ignore requests and to independently verify them using a trusted channel.
3. **Protect:** Instructs the consumer to contact their financial institution immediately if they suspect they have been scammed and to report the fraud to the proper authorities.

This behavioral-based approach is far more effective than simply recommending certain payment types because it equips consumers with tools to recognize red flags, regardless of the payment channel being used. It creates a critical moment of friction, allowing a potential victim to step back from a high-pressure situation and think critically. Such a campaign, consistently promoted by financial institutions, government agencies, and other stakeholders, would provide a powerful and unified defense against the primary tactics fraudsters use today.

7. Which approaches could make existing payments fraud education more effective? For example, would targeting outreach to particular audiences or conducting additional education in collaboration with other key stakeholders be effective?

There are several approaches to enhance current payments fraud education efforts. First, targeted outreach to vulnerable or high-risk groups can greatly increase effectiveness. Rather than one-size-fits-all messaging, educational campaigns should identify key demographics for particular fraud types (e.g., seniors for romance or tech support scams, young adults for social media purchase and crypto investment scams, small businesses for invoice fraud) and tailor content and delivery to those groups. This might mean partnering with community centers, colleges, or trade associations to reach the intended audience with relevant examples.

Second, collaboration in education amplifies impact. Financial institutions, government agencies, consumer protection groups, and tech platforms should coordinate their messaging so that it reinforces a common set of tips and warnings. Joint campaigns, such as the previously mentioned “Take Five to Stop Fraud” UK initiative, benefit from unified branding and broader dissemination.

Third, using more engaging formats and channels will improve effectiveness. Existing online resources can be supplemented with short explainer videos, infographics, interactive scam-spotting games, and social media content that catches the eye. For example, banks and regulators could produce shareable content (memes, short videos) that people might actually repost, turning consumers themselves into advocates of fraud awareness.

Finally, measuring and refreshing content regularly is key. If certain guidance becomes outdated due to new scam techniques, education materials should be updated and redistributed. By continuously improving relevance and delivery, targeting the right audience, working together

across sectors, and leveraging modern communication methods, we can significantly boost the impact of fraud education.

8. Are current online resources effective in providing education on payments fraud? If not, how could they be improved?

The existing online resources provided by regulators and industry (e.g., the Federal Reserve's consumer pages, FDIC's Consumer News, OCC's "Safe Money" fact sheets, etc.) are valuable repositories of information. However, they may not be reaching or resonating with as broad an audience as intended. One challenge is that many consumers and small businesses do not proactively seek out these websites until after they've been victimized.

To improve effectiveness, online resources should be made more visible, user-friendly, and interactive. For instance, the Agencies could consolidate disparate resources into a one-stop "Fraud Information Center" website that serves as a central hub, prominently linked from bank websites, social media, and search engines. Simplifying the language and using engaging visuals or short videos on such a site can help maintain visitors' attention. Another improvement is search engine optimization and online promotion, ensuring when people search common queries like "verify a check scam" or "payments fraud help," the official resource is the top result.

The content itself could be improved by incorporating real-time updates and alerts. Scammers constantly evolve tactics, so having a section for the latest scam alerts (in plain language) will keep the online guidance current. Interactive self-assessment tools could make the learning experience more engaging online. Additionally, translating key materials into other languages and making them accessible (for those with disabilities or limited internet access) will broaden their reach.

In summary, current resources are informative but can be improved by centralizing them, actively pushing them out through popular channels, updating them frequently with emerging scams, and making the content more interactive and user-centric. These steps would ensure online fraud education resources truly serve as effective tools in preventing payments fraud.

Regulation and Supervision

9. What potential changes to regulations (apart from the Board's Regulation CC, discussed separately below) could address payments fraud and mitigate the harms from payments fraud to consumers, businesses, and supervised institutions?

The most impactful regulatory change would be to create a framework that ensures all participants in the payments ecosystem have a clear incentive to prevent fraud. Fraud often starts on platforms outside of banking, such as social media, telecom networks, and online marketplaces, but financial institutions disproportionately bear the consequences. Regulations or interagency guidance should encourage shared responsibility so that every entity that facilitates a payment has a stake in its security.

Building on this principle, the Agencies could consider several targeted regulatory actions:

- **Prioritize Prevention Over Reimbursement:** The UK's approach to fraud prevention, creating a regime where the cost of reimbursement is split equally between the sending and receiving payment service provider, has not meaningfully reduced fraud rates. UK Finance reported that in 2024, total fraud losses fell by only around 2%, despite the regime being in force for the final quarter[6]. The UK Government is now establishing an updated fraud strategy that is focused on cross-sector data sharing. This policy pivot suggests that a regulatory regime focused on reimbursement is not as effective as a broader strategy centered on prevention.

- **Mandate Cross-Industry Data Sharing:** We believe that prevention is more effective than remediation and that mandatory, cross-sector data sharing is the single best tool to prevent fraud. The Agencies should establish a framework that requires real-time, reciprocal intelligence sharing between financial institutions, government, law enforcement, and the technology and telecommunications sectors. While operationally challenging, this approach is being pursued by international partners as an effective strategy. We would note the different approaches taken in the UK and Australia: the UK has thus far focused on a voluntary approach to data sharing from various sectors, while Australia has moved to mandate the involvement of key sectors, including banks, telcos, and tech firms, via legislation. A mandatory framework is essential to ensure universal participation and create a truly networked defense.

- **Establish an Ecosystem-Wide Liability Framework:** The Agencies should develop a framework that assigns accountability for scam losses to the entity in the payments ecosystem that was in the best position to prevent the fraud at its source. As our data shows, the vast majority of scams originate outside the banking system, meaning accountability must extend to the social media platforms, telecom providers, and online marketplaces where these crimes begin. For instance, if a platform fails to take action on a fraudulent account after being notified, or a telecom provider does not shut down a known scammer's phone number, they should bear the financial responsibility for resulting losses. This approach moves the burden away from the consumer and the financial institution, who are the final lines of defense, and creates a powerful incentive for all participants to invest in proactive fraud prevention

- **Create a Cross-Industry Safe Harbor for Information Sharing:** Section 314(b) permits information sharing among financial institutions to identify and report activity that may involve money laundering or terrorist financing, including suspected fraud as a predicate offense. It does not extend beyond financial institutions to non-financial counterparties. The Agencies should lead an interagency effort to establish a new or expanded, parallel safe harbor that explicitly permits the voluntary, real-time sharing of fraud-related information not only between financial institutions but also with other key

[6] UK Finance, *Annual Fraud Report 2025* (June 2025),

stakeholders like telecommunications companies, social media platforms, and online marketplaces. This would create a legally protected channel for a bank to, for example, alert a social media company to a fraudulent account or for a telecom provider to share a list of known scam phone numbers with banks. Breaking down these legal and liability barriers is essential for enabling the collective, real-time response needed to disrupt fraud networks.

- **Strengthen Baseline Security Standards:** The interagency guidelines under the Gramm-Leach-Bliley Act could be updated to explicitly require controls against payments fraud, not just data breaches. Mandating specific standards, such as robust multifactor authentication, anomaly detection, and client-side malware detection, would establish a consistent and resilient security floor across all institutions.

- **Disrupt Money Mule Activity:** Regulators could introduce rules aimed at disrupting the entire money mule ecosystem, addressing both the accounts themselves and the sources that fund them. This should include stronger requirements for ongoing account monitoring to detect mule activity, as well as a standardized process for financial institutions to report and share information about confirmed mule accounts. Equally important, this strategy must also harden the upstream entry points for illicit funds. The current patchwork of state-level licensing and supervision standards for Money Services Businesses creates a significant vulnerability, as illicit cash deposited in a jurisdiction with weaker controls and oversight can be moved instantly into the national financial system to fund these networks. Therefore, Federal regulators should work with state counterparts to establish consistent, baseline security and compliance standards for these critical cash entry points.

10. The Board, FDIC, and OCC have issued supervisory guidance on numerous topics that relate to payments fraud detection, prevention, and mitigation. Is existing supervisory guidance related to payments fraud sufficient and clear? If not, what new or revised supervisory guidance should the Board, FDIC, and OCC consider issuing on this topic within the respective authorities?

The existing supervisory guidance provides a solid foundation, but there is a significant opportunity to enhance and consolidate it to address the modern payments fraud environment. While individual guidance on topics like authentication or operational risk are helpful, they are fragmented and do not provide a single, comprehensive framework for managing today's sophisticated, cross-channel fraud threats.

We recommend the Agencies explore issuing new, joint supervisory guidance that consolidates expectations for an enterprise-wide payments fraud risk management program. This would provide greater clarity for the industry and examiners alike. This guidance should establish a clear benchmark for what an effective program looks like today, including:

- **Modern Fraud Controls:** Set expectations for the use of modern technologies like behavioral analytics and machine learning for real-time fraud detection, as well as the

need for robust, cross-channel monitoring to prevent fraudsters from exploiting siloed systems.

- **Clear Reporting Standards:** Formally endorse and encourage the use of the FraudClassifier model to ensure consistent and standardized fraud classification and reporting across the industry.
- **Clarification on Customer Communication**: Provide clear rules of the road for communicating with customers during a fraud investigation. Specifically, the guidance should clarify how to balance SAR confidentiality requirements with the need to keep customers informed, reducing legal uncertainty for institutions.
- **Scaled Expectations for Community Banks:** Include a dedicated section outlining how fraud management expectations can be scaled for smaller institutions. Providing concrete examples of how community banks can implement effective, risk-based controls would be immensely valuable.
- **Addressing Emerging Threats:** The guidance should be forward-looking, explicitly addressing newer fraud typologies involving instant payments, cryptocurrency, and scams originating on social media platforms.
- **A Commitment to Regular Updates:** The guidance should be established as a "living document." The Agencies should commit to a regular review cycle (e.g., every 24-36 months) to ensure the framework remains current with emerging fraud schemes, new technologies, and evolving industry best practices.

By consolidating these topics into a single piece of joint guidance, and keeping it current, the Agencies can build upon a strong foundation and provide a clear, modern, and holistic roadmap for mitigating payments fraud risk.

11. How might new or revised supervisory guidance assist small community banks in detecting, preventing, and mitigating payments fraud?

New or revised supervisory guidance would be a critical resource for small community banks, which face the same sophisticated fraud threats as larger institutions but with more limited resources. Guidance can serve as a practical roadmap by outlining clear, scalable, and risk-based expectations.

Specifically, guidance can assist community banks by:

- **Detailing Scalable Controls:** The guidance should provide examples of effective fraud controls that do not require massive investments. This includes foundational measures like robust employee training and dual controls, as well as leveraging built-in features of existing core banking systems.
- **Promoting Vendor and Third-Party Solutions:** Guidance can encourage core banking vendors and third-party service providers to offer affordable and effective fraud

monitoring tools tailored for smaller institutions. It could also provide a framework for how community banks can safely and effectively outsource certain fraud detection capabilities.

- **Highlighting Collaborative Models:** Regulators can encourage community banks to join industry information-sharing forums and data consortiums. These collaborative models give smaller institutions access to the broad fraud intelligence and analytical power of a much larger data pool, leveling the playing field.

- **Emphasizing "Right-Sized" Expectations:** The guidance should explicitly state that fraud risk management is not one-size-fits-all. It should reassure community banks that a less complex program is acceptable, provided it is effective and commensurate with the institution's specific risk profile. This helps alleviate pressure to purchase expensive systems that may be unnecessary.

By providing a clear framework that emphasizes practical, collaborative, and scalable solutions, the Agencies can empower community banks to strengthen their defenses effectively and efficiently.

12. What is the experience of consumers and businesses when supervised institutions place holds on depositors' funds because of suspected payments fraud?

For consumers and businesses, having funds frozen or a transaction held due to suspected fraud is a high-friction, anxiety-inducing experience. While these controls are essential, the process can feel opaque from the customer’s perspective and can erode trust.

Customers’ primary challenges are a lack of insight and a sense of powerlessness. They often do not know what activity triggered the review, and, without clear information, are left to speculate. This is compounded by the real-world impact of being unable to pay a bill, complete a time-sensitive purchase, or run a business. Limited, high-level updates can heighten concern.

12.a. How frequently are consumers and businesses affected by holds, delays, or account freezes, and how responsive are supervised institutions to inquiries from consumers and businesses regarding these issues?

For any individual consumer, an account hold may be a rare and alarming event. However, for the financial industry, these holds are now a high-volume, daily reality driven by the need to combat rising fraud. Impacted customers are often proactive in seeking answers, leading to a massive influx of inquiries.

This has created a significant operational strain on institutions, evidenced by the fact that many are now growing their fraud and customer experience teams faster than their traditional AML compliance teams just to manage the volume. However, even with more staff, an institution's responsiveness is ultimately limited by legal constraints like SAR confidentiality, which prevent them from providing the clear, specific updates customers demand.

12.b. Do current disclosure requirements effectively address consumer and business concerns when supervised institutions hold customer funds due to suspected payments fraud? For example, should changes be considered with respect to permissible customer communications under SAR confidentiality rules?

Disclosure is the central constraint. Current rules, particularly SAR confidentiality, often result in high-level notices. While proactive communication through robust Terms & Conditions and fraud-related Frequently Asked Questions can help set customer expectations, real-time communication during an incident is critical. We recommend the Agencies work with the Financial Crimes Enforcement Network (FinCEN) to issue guidance creating a safe harbor for pre-approved, SAR-safe communications, allowing institutions to provide: (i) a plain-language reason category (e.g., activity consistent with impersonation or Account Takeover (ATO) typologies), (ii) the steps in the review and likely next actions/documents, and (iii) a clear statement of what cannot be discussed. The Agencies could also publish model scripts/notices and a standardized hold-reason taxonomy to promote consistency across institutions.

By providing this clarity, regulators can empower financial institutions to meaningfully improve the customer experience during a necessary security procedure, turning a moment of friction into one of reassurance and partnership.

13-15. Questions around Reg CC and Check Fraud.

Revolut defers to those entities better placed to respond to and propose amendments to Reg CC.

Payments Fraud Data Collection and Information Sharing

16. Broadly, how could payments fraud data collection and information sharing be improved?

A more unified, complete picture of payments fraud is fundamental to fighting it. To improve data collection and sharing, we recommend a two-pronged approach: standardization of data and creation of centralized or federated sharing mechanisms**.** First, the industry, with leadership from the Agencies, should standardize what fraud data is collected and how it is defined. This could involve broad adoption of the FraudClassifier℠ and ScamClassifier℠ models developed by the Federal Reserve so that all institutions categorize incidents in a consistent way (for example, distinguishing clearly between authorized scams vs. unauthorized fraud, payment method involved, etc.). Standard data fields (like date, payment channel, amount, narrative of scheme, etc.) should be agreed upon for reporting purposes. Once data speaks the same language, wider collection becomes feasible and regulators could then require or strongly encourage financial institutions to report key fraud metrics regularly.

Second, to facilitate sharing, an industry-wide fraud data repository or network is needed. This doesn't have to mean a single monolithic database, but could be a secured platform where institutions contribute data on confirmed fraud cases and can query for emerging trends or to

check if an account/beneficiary has been flagged elsewhere. The goal is to break down the silos. Currently one bank only sees the fraud attempts on its own customers, but a scammer might be hitting dozens of banks in parallel. By pooling data, patterns can emerge that any one bank would not see. Additionally, better integration of fraud data from different sources should be pursued. For instance, combining data from consumer complaints (FTC, Consumer Financial Protection Bureau, SAR filings, network data (like wire/Automated Clearing House (ACH) return reason codes), and even tech platforms can provide a 360-degree view. To improve sharing, regulators might also consider modernizing privacy rules to explicitly permit sharing for fraud prevention. In short, improved data collection and sharing will come from having common standards (so data from Bank A and Bank B mean the same thing) and a collaborative infrastructure (so that insights from Bank A can help protect Bank B, and vice versa). This will enable earlier detection of systemic fraud threats and more effective industry-wide responses.

17. What barriers limit the collection and sharing of payments fraud data between industry stakeholders, and how could these barriers be alleviated? For example, have specific barriers limited development of solutions or participation in bilateral or multilateral payments fraud data collection and information sharing? What changes would address these barriers?

Several significant barriers currently hinder the collection and sharing of payments fraud data among stakeholders:

- **Legal and Privacy Ambiguity:** Financial institutions operate under strict privacy laws (like the Gramm-Leach-Bliley Act) and fear legal liability if they share customer-related fraud data that is later deemed improper. This legal uncertainty often chills the proactive sharing of information, even when it could prevent further harm.
    - **Solution:** To alleviate this, the Agencies should pursue a two-part solution.
        - They should immediately issue guidance that clarifies and encourages the appropriate use of the existing Section 314(b) safe harbor for fraud prevention. This guidance should explicitly affirm that sharing information on payments fraud is a permissible and encouraged use of the safe harbor when the activity is suspected of being a predicate offense to money laundering. This would provide immediate legal comfort for many common scenarios.
        - To cover all other instances of fraud where a money laundering nexus is not as clear, the Agencies should lead an interagency effort to establish a broader, explicit safe harbor for the good-faith sharing of specific, fraud-related data points among trusted parties. Together, these actions would remove legal ambiguity and provide the confidence institutions need to participate fully in collaborative defense.
- **Competitive and Reputational Concerns:** Some institutions may worry that sharing their fraud loss data could expose them to reputational risk or reveal weaknesses.

Similarly, tech platforms might fear admitting how much fraud originates on their services.

    - **Solution:** Have a neutral third party (or regulator) collect and aggregate the data, so individual contributions are not public. If a centralized database is run by a trusted party (e.g. a government agency or industry association bound by confidentiality), participants will be more willing to contribute. Emphasize the collective benefit, a shared fight against fraud improves trust in the whole system, which ultimately benefits all reputable players.

- **Technical and Standardization Issues:** Different institutions track fraud differently (one bank's "ACH fraud" might exclude certain scams that another bank includes). This inconsistency makes sharing like "apples vs. oranges." Also, the lack of a common platform means high implementation costs to participate in sharing programs.

    - **Solution:** As noted in Q16, drive standard definitions and invest in developing interoperable technology for data sharing. The Agencies could sponsor the development of an industry portal or API that makes it easy for banks (and possibly others like fintechs or telecom providers) to feed in data and retrieve aggregated intelligence. By lowering technical barriers and costs, more stakeholders will join in.

- **Underreporting by Victims and Institutions:** Many fraud incidents go unreported by victims (due to embarrassment or hopelessness), and some smaller institutions may not systematically collect internal fraud stats. This leads to incomplete data.

    - **Solution:** Increase public awareness on reporting fraud (e.g., promote channels like the FTC's ReportFraud.ftc.gov and the Federal Bureau of Investigation's Internet Crime Complaint Center) and create feedback loops where victims see value in reporting (like helping others, or maybe increasing chances of recovery). For institutions, regulators could incorporate fraud data collection into examination, asking, "Do you track and analyze fraud incidents?" to spur better internal data practices. Possibly mandate reporting of certain fraud losses above a threshold, akin to how cyber breaches must be reported.

- **Misaligned Incentives of Intermediaries:** A significant structural barrier exists with key intermediaries, such as major payment processors. While these firms aggregate immense volumes of transactional data that could identify fraud patterns, their business models are often not structured to incentivize prevention. Because they profit on transaction volume and can contractually push fraud liability to their business clients and acquiring banks, they have little financial stake in preventing it. This creates a critical gap where the entity with the most data has no economic incentive to act on it.

    - **Solution:** The most effective solution is to align incentives with security outcomes through new regulatory standards. The Agencies could establish frameworks that create clear financial accountability for intermediaries when their

platforms are exploited for fraud. This ensures that the entities who profit from payment processing also have a meaningful stake in the security of those payments. By creating this accountability, processors will be motivated to deploy their vast data and advanced technology to prevent fraud at the source.

18. What role should the FRS, FDIC, or OCC take in supporting further standardization of payments fraud data? For instance, can the FRS better leverage or improve the FraudClassifier and ScamClassifier models?

The Agencies should take a decisive leadership role in driving the standardization of payments fraud data. This action would directly support FinCEN's Anti-Money Laundering/Countering the Financing of Terrorism National Priorities, which explicitly identify fraud as a key threat to the U.S. financial system. We recommend a three-part strategy:

- **Champion Existing Models:** The Agencies should jointly issue guidance that formally endorses and strongly encourages all supervised institutions to adopt the Federal Reserve's FraudClassifier and ScamClassifier models. This would accelerate the move toward a common industry language for defining and categorizing fraud. Over time, these classifications could be integrated into regulatory reporting to ensure uniform data collection.

- **Convene an Industry Working Group:** The Federal Reserve, in its role as a payments catalyst, is perfectly positioned to convene an industry working group to establish a standard fraud data template. This group, with OCC and FDIC participation, would define the key data elements to be collected for every fraud incident (e.g., payment channel, scam typology, point of compromise) to ensure richness and consistency.

- **Leverage Existing Infrastructure:** The Agencies can use their existing operational and supervisory roles to promote these standards. For example, the Federal Reserve could enhance the fraud reporting requirements for its payment services (like FedNow and FedACH) to align with the standardized data template. Similarly, the Agencies could incorporate these standards into their examination procedures for both fraud risk management and BSA/AML programs. This would help bridge the current gap where fraud is often reviewed in isolation, despite its direct role as a predicate offense to money laundering.

19. What types of payments fraud data, if available, would have the largest impact on addressing payments fraud? If these data are not currently being collected or shared, what entities are best positioned to collect and share such data?

To have the largest impact, data collection should focus on creating a real-time, comprehensive view of fraud networks and tactics. The following three data types would be most valuable:

- **Shared Negative Lists:** A real-time, industry-wide repository of identifiers confirmed to be associated with fraud. This would include mule account numbers, scammer-controlled crypto wallet addresses, fraudulent phone numbers, device IDs, and IP addresses.

- **Detailed Fraud Typology Data:** Granular, standardized data on the *modus operandi* of fraud schemes, including the initial point of compromise (e.g., social media platform), the method of victim contact, the specific scam narrative used, and the payment channel exploited.

- **Recovery and Resolution Outcomes:** Data on the outcomes of fraud cases is needed to establish best practices. This should include not only the percentage of funds recovered but also, critically, feedback from FinCEN and law enforcement on which data points in fraud-related SAR filings proved most valuable for investigations. Currently, institutions have little to no insight into whether their SARs are helpful, creating a missed opportunity to improve the quality of actionable intelligence.

No single entity can collect all this data alone; a public-private partnership is essential. However, to anchor this partnership, a central government utility is needed to act as a trusted intermediary. FinCEN is the logical entity to operate this central repository. It already possesses the legal authority, security infrastructure, and trusted relationships with financial institutions to handle sensitive financial crime data, as it does today with Bank Secrecy Act reporting.

Expanding FinCEN's mandate to ingest and disseminate real-time, standardized fraud data would be a natural evolution of its mission. This would create a powerful feedback loop: financial institutions would contribute data to prevent fraud proactively, and in return, FinCEN and law enforcement would gain a much richer, more structured dataset than SARs alone currently provide, enhancing their ability to disrupt criminal networks.

Furthermore, for this FinCEN-led repository to be truly effective, its mandate must include the contribution of data from non-financial entities. The initial point of compromise often occurs on social media, through telecommunications networks, or on e-commerce marketplaces. Therefore, a mechanism to require or strongly incentivize these platforms to contribute relevant fraud data, such as confirmed scammer profiles, fraudulent advertisements, or malicious phone numbers, is essential. Integrating this data would provide a true end-to-end view of fraud schemes, enabling interventions at the source, not just at the point of payment.

20. Is there a need for centralized databases or repositories for the sharing of payments fraud data across entities? What legal, privacy, or practical risks and challenges could such a centralized database or repository pose? Which entities are best positioned to develop and participate in a centralized database or repository?

Yes, there is an urgent need for a centralized repository for sharing payments fraud data. Such a system is a foundational requirement for moving from a reactive, siloed approach to a proactive, collective defense against increasingly sophisticated and organized fraud networks.

As detailed in our responses, the primary challenges to establishing such a repository are legal, competitive, technical, and critically, governance related. In addition to legal ambiguity and the lack of common data standards, a practical challenge is the risk of improperly de-risking consumers and businesses. Without strong governance, inconsistent fraud thresholds among

participants could lead to legitimate actors being blacklisted across the system based on poor data from a single institution.

These barriers can be overcome with a proper framework. This includes a clear legal safe harbor, the use of a trusted intermediary, and the adoption of standardized fraud classifications. To address the de-risking challenge, the framework must also include robust governance and consumer protection rules, such as:

- Clear, standardized criteria for what constitutes a "confirmed" fraudulent identifier.
- A formal and transparent dispute resolution process for consumers and businesses to challenge and correct inaccurate information.
- Regular audits of the data to ensure its accuracy and integrity.

The most effective model would be a public-private partnership anchored by FinCEN. Leveraging its existing authority, FinCEN is the logical entity to operate a central utility that ingests real-time data under these strict governance rules. For this to be successful, participation must be ecosystem-wide, with contributions from financial institutions, telecommunications providers, and technology platforms.

Reserve Banks' Operator Tools and Services

21 - 22. Reserve Banks' Operator Tools and Services Questions

As we are not currently a direct participant in the Reserve Banks' payment systems, we will defer to participating institutions on specific operational enhancements. However, from our perspective as a global financial technology company, we believe the most impactful enhancements the Reserve Banks could make would be those that foster real-time, networked, and data-driven fraud prevention.

We strongly support the specific proposals mentioned in the RFI and believe the Reserve Banks are uniquely positioned to offer them as a centralized utility for all participants:

1. **Confirmation of Payee:** We strongly endorse the introduction of a centralized "Confirmation of Payee" service. This is a foundational anti-fraud control that has proven effective in other markets at stopping APP fraud before it happens. The Reserve Banks could operate this as a network-level utility, allowing an originating institution to verify that a recipient's name and account number match before initiating a payment.
2. **Network-Level Fraud Monitoring:** The Reserve Banks should expand their network-level monitoring beyond simple anomaly detection. They could offer advanced, API-driven tools that allow participating institutions to screen payments against network-wide fraud data in real time. This would help identify, for example, a mule account that is receiving fraudulent payments from multiple institutions simultaneously, a pattern no single institution could see on its own.

3. **Mandatory Fraud Reporting:** Yes, the fraud reporting requirements currently in place for the FedNow Service should be expanded to cover all payment rails operated by the Reserve Banks. Using a standardized reporting format, as discussed in our previous answers, would create an invaluable repository of fraud data that can be used to protect the entire network.

By providing these critical services at the network level, the Reserve Banks can uplift the fraud prevention capabilities of the entire U.S. payments ecosystem, especially for smaller institutions that lack the resources to develop these tools on their own.

General Questions

23. What types of payments fraud have most impacted your organization and its stakeholders? What tactics have criminals employed when perpetrating these types of payments fraud?

The most common and impactful types of fraud we face are APP and ATO scams targeting legitimate customers, and the use of accounts created with fraudulent identities.

For APP and ATO scams, fraud increasingly originates on encrypted messengers and social platforms. Tactics are dominated by social engineering and “coaching” (including instructions to misrepresent the purpose of a payment), impersonation scams, and the use of remote-access tools to defeat security controls.

In parallel, we see criminals creating new fraudulent accounts at scale using Artificial Intelligence (AI) generated identity documents combined with legitimately stolen personal data. These synthetic or stolen identities can bypass initial automated screening. Once established, these accounts are used to exploit e-commerce platforms as points of entry for illicit funds, while cryptocurrency exchanges and other digital wallets are often used as exit points. The funds are then moved through the financial system using various layering methods that make it extremely difficult for any single institution to ascertain their legitimacy.

24. What measures, including technological solutions or services, have been most effective in identifying, preventing, and mitigating payments fraud at your institution? Are there actions that consumers can take that help institutions? For example, do financial institutions find it helpful when consumers alert the institution in advance when making large purchases, transferring large amounts of money, and traveling abroad?

- **Advanced Analytics and AI:** We utilize real-time fraud detection algorithms that analyze transaction patterns and customer behavior. Machine learning models flag unusual payments, for example, a sudden high-value transfer by a typically low-activity account, or logins from atypical locations. These systems have been highly effective at catching both unauthorized transactions and potential scam-induced transactions (like a customer suddenly trying to wire their entire savings to an unfamiliar recipient). By

examining hundreds of data points (device, time, geolocation, history, etc.), our system can often stop fraud before funds go out, or at least prompt additional verification.

- **In-App Customer Warnings and Confirmation Steps:** A relatively low-tech but effective control is deploying dynamic warnings that introduce a short cool-off period in the payment workflow. When a user initiates a large or atypical transfer, the app displays a brief risk warning and asks the customer to confirm the payment is legitimate (e.g., that they recognize the recipient and purpose). This pause has prevented scam-induced payments and effectively embeds education at the moment of risk.
- **Customer-Initiated Actions:** While the examples of customers alerting their institution in advance were helpful in a legacy environment, our approach is to make such manual notifications largely unnecessary. A financial product designed for global travel should not require a customer to report their location, just as a modern fraud detection system should be able to assess the risk of a large purchase in real time without prior warning. Our systems are built to analyze user behavior, device, and location data automatically to approve legitimate transactions seamlessly while flagging genuinely anomalous activity. This automated approach provides a more secure and frictionless customer experience, as manual notifications are inefficient and provide little value compared to real-time, data-driven analysis.

25. To the extent not already addressed here, are there other actions that would support stakeholders in identifying, preventing, and mitigating payments fraud?

A critical area for additional action is empowering frontline financial institution staff to intervene in cases of elder financial exploitation. Bank tellers and branch staff are often in a unique position to witness these tragic scams in real time, but they frequently feel helpless to act. They may fear legal or professional repercussions for delaying a transaction or questioning a vulnerable customer who is being coerced.

The Agencies can provide direct support by issuing clear guidance and a specific safe harbor for frontline employees. This would empower them to pause suspicious transactions involving elderly or vulnerable adults and escalate the situation to a trained specialist or report it to Adult Protective Services and law enforcement without fear of liability. Providing clear protocols and legal protection for these good faith interventions would turn a moment of helplessness into an opportunity for prevention and would be a significant step in protecting our most vulnerable citizens.

26. Are there specific actions that commenters believe could encourage the use of payment methods with strong security features?

The most effective way to encourage the use of secure payment methods is to ensure the market is structured to reward security. Rather than promoting specific payment methods, the Agencies should focus on creating an environment where payment providers compete on the strength of their security and fraud prevention capabilities.

This can be achieved by establishing clear rules that align liability with the ability to prevent fraud. When payment processors and other intermediaries have a clear financial stake in preventing fraudulent transactions, they are strongly incentivized to develop and offer more secure products.

We are already seeing an emerging market for this, where e-commerce businesses are willing to pay a premium for payment services that guarantee payments and absorb the risk of fraud. This market-based approach drives innovation and naturally encourages the adoption of stronger security features. By clarifying the liability landscape and ensuring that risk is borne by the party best positioned to mitigate it, the Agencies can accelerate this trend, making the entire payments ecosystem safer as a result.

Conclusion

In conclusion, Revolut again thanks the Agencies for this opportunity to comment and respectfully submits that the most effective path forward requires a fundamental shift from a siloed, reactive posture to a real-time, collaborative, and ecosystem-wide model of defense.

The most impactful solutions will involve establishing clear lines of shared responsibility among all participants, creating the legal and technical infrastructure for real-time intelligence sharing, and modernizing rules to reflect the sophistication of today's threats.

We welcome the Agencies' leadership and stand ready to serve as a resource, offering our global expertise in financial technology and fraud prevention as you develop next steps. We look forward to continued collaboration in building a safer financial future for all.