STRIPE, JONAH CRANE

Proposal and Comment Information

Title: Request for Information on Potential Actions to Address Payments Fraud, OP-1866

Comment ID: FR-2025-0036-01-C75

Subject

Stripe Response to Docket No. OP-1866 / RIN 3064-ZA49

Submitter Information

Organization Name: Stripe

Organization Type: Company

Name: Jonah Crane

Submitted Date: 09/18/2025

Please see Stripe's attached response to Docket No. OP-1866 / RIN 3064-ZA49.

stripe

September 18, 2025

Via eRulemaking Portal; publiccomments@frb.gov; comments@fdic.gov

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

Ms. Ann Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

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

Subject: Re: Request for Information on Potential Actions to Address Payments Fraud (Docket ID OCC-2025-0009, Docket No. OP-1866, RIN 3064-ZA49)

Introduction

Stripe appreciates the opportunity to respond to the interagency Request for Information on potential actions to address payments fraud. As a payments service provider with deep experience combating fraud online, Stripe supports efforts to reduce payments fraud while preserving the speed, innovation, and accessibility of today's payment systems.

Stripe's mission is to grow the GDP of the internet. We do that by providing programmable financial services and a range of related products and services to businesses operating on the internet. Our users include for-profit and not-for-profit businesses of every size, from small start-ups to large public companies, and from local sole proprietors to global Fortune 100 companies. In 2024, Stripe processed $1.4 trillion in payment volume, equivalent to around 1.3% of the global GDP. In addition to operating under our own licenses, we often partner with banks to serve our users.

Fraud is a societal challenge and Stripe proposes a comprehensive principles-based approach to countering it. Stripe recommends that the federal banking agencies, working with their counterparts across government and the private sector, as appropriate: (1) adopt outcomes-based policies designed to foster innovation to combat fraud; (2) encourage cooperation across financial and non-financial sectors to address information gaps; (3) foster the conditions to establish a real-time, safe-harbored information-sharing framework; and (4) preserve critical data access while enhancing security measures. These principles, which align to the Administration's recent public remarks at ACAMS,[1] aim to leverage technological innovation and collaborative efforts to effectively mitigate fraud risks while enabling

[1] *Remarks by Under Secretary for Terrorism and Financial Intelligence John K. Hurley at the Association of Certified Anti-Money Laundering Specialists Assembly Conference*, https://home.treasury.gov/news/press-releases/sb0251

economic growth.

Enabling commerce and fighting fraud

Stripe supports millions of active users and onboards thousands of new businesses every day. To manage risk at this scale, Stripe invests significant resources to develop, deploy, and continuously improve a wide range of preventive and detective fraud controls that are deployed throughout the merchant lifecycle. For example, we built machine learning algorithms that analyze vast amounts of transaction data in real-time to detect suspicious patterns and flag potentially fraudulent activities that are escalated for review by specialists. By analyzing a diverse range of signals, including transaction patterns, user behavior, and historical data across sectors, Stripe can detect fraudulent activities swiftly and accurately. This approach enables Stripe to differentiate between legitimate transactions and fraudulent ones with high accuracy. As a result, we have increased conversion for our merchants and reduced fraud. Stripe's models are continuously evolving, adapting to emerging data to effectively address new threats in the fraud landscape. We also productize our innovations and make them available to Stripe users. By leveraging our scale, we help protect the payments ecosystem as a whole - 92% of card users have been seen by Stripe before, giving our merchants benefits for both fraud detection and confidence in authorization.

Policy Principles and Recommendations

Fraudsters are constantly evolving their tactics, creating an ever-changing and increasingly sophisticated threat landscape. Combatting fraud is therefore conceptually a technology "arms race." Fraudsters use generative AI to evade onboarding controls and create plausible-looking fake websites and social media scams, then use automated tools to manage and weaponise vast sets of stolen credit card credentials. The industry is similarly innovative. For example, Stripe recently developed a payments foundation model built on tens of billions of transactions that captures intricate relationships and patterns within payments data, enabling significantly improved detection. The attackers, however, have some inherent advantages–they can fail infinitely, and succeed once, while industry must defend everywhere.

Principle 1: Adopt outcomes-based policies to encourage innovation in fraud prevention and detection

We urge the federal banking agencies to work with the Administration to build on recent statements encouraging outcomes-based innovation. Effective regulation should be driven by a flexible, outcomes-focused approach that encourages innovation while maintaining appropriate oversight.

Specifically, we recommend the following actions:

- Anchor supervisory examinations in the performance of fraud controls, and adaptability to new fraud vectors, rather than prescriptive checklists;
- Establish tiered and outcome-driven model risk management regulatory frameworks, including actively encouraging iterative managed testing. Fraud and financial crime models are not the same as, and do not present the same risks as, prudential and credit models. They require far more rapid iteration to keep pace with criminals; and
- Create safe spaces for experimentation that enable the development of advanced solutions while maintaining regulatory oversight. For example, the banking agencies could issue guidance similar to the interagency Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing[2] issued during the first Trump Administration, with a focus on encouraging innovation in fraud prevention.

[2] *Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing*, https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20181203a1.pdf

By adopting this approach regulators can help fraud prevention measures keep pace with technological advancements and evolving criminal tactics, thus bolstering the integrity and security of the financial system.

Principle 2: Fraud is a societal problem that requires broad engagement across financial and non-financial sectors.

Decades of effort in public-private information sharing between law enforcement and primarily banks have shown that the most effective way to combat financial crime is to engage collaboratively and broadly across a variety of institutions. We would strongly urge law enforcement to expand and prioritize efforts to share fraud-related information across financial and non-financial sectors to help track fraudulent actors' activity more comprehensively.

Some fraudulent transactions originate within the system itself, such as an account takeover or stolen payment information. However, in more sophisticated frauds, such as romance scams, the payment is often just the final step in a complex series of actions that take place outside of payment rails. The first steps in the fraud lifecycle frequently take place through fraudulent or spam communications. Visibility of these activities is typically limited to social media companies, telecom providers, and NGOs. Incorporating these other sectors into information-sharing forums will add critical data that today are missing from the equation, enabling the broader ecosystem to craft a more comprehensive approach to fraud mitigation.

We believe law enforcement would benefit from creating fraud-focused forums which include fintech and payments companies, similar to many of the public-private bank-centric information sharing. Fintech and payments companies often partner with banks, and in the case of Stripe we are also a regulated payments company with our own responsibilities for fraud risk management. In addition, we work with a broad array of users and partners outside the regulated perimeter who nevertheless have their own fraud risks. This positions us well to see some of the connections between financial and non-financial activity. A broader information-sharing mechanism including both regulated and unregulated firms would allow a broader array of innovative fraud detection and prevention solutions developed by fintechs to directly aid law enforcement and inform the development of regulatory policy and contribute directly to the overall security and resilience of the US payment ecosystem.

Principle 3: Build a cohesive, real-time information-sharing framework with safe harbor for participants.

Stripe’s experience demonstrates that real-time data sharing from across the payments ecosystem is an effective way to counter emerging fraud incidents. Stripe supports data sharing with broad participation of stakeholders across the current and, ideally, expanded ecosystem.

Currently, the information sharing channels maintained by regulators operate as a patchwork of partnerships and agreements, which do not adequately prioritize fraud mitigation. Existing data sharing regimes, such as those governed by FinCEN, have proven insufficient and lack the scalability necessary to support the real-time decision-making processes essential for tackling payments fraud. The increasing threat of AI-enabled fraud makes this an even greater challenge, and the manual nature of 314(b) frameworks as currently implemented are not conducive to countering modern fraud tactics. Regulatory guidance should explicitly encourage the creation of larger-scale and more automated information-sharing to keep pace with the nature and scale of fraud.

An effective information sharing framework needs to disseminate real-time fraud signals to enable the rapid propagation of knowledge about emerging fraud patterns throughout the payments ecosystem.

The framework should be built on open standards that define fraud, operational burdens, expectations, data quality, and access control. Manual portals, batch-only or after-the-fact sharing will not successfully support the split-second automated decisioning that underlies modern fraud systems. To underpin this sharing, regulatory guidance should clarify an explicit safe harbor within existing 314(b) authorities to facilitate automated private-to-private information sharing initiatives.

Principle 4: Preserve data access for effective fraud prevention while enhancing security measures.

The evolution of payment technologies demonstrates that significant security enhancements can be achieved without overhauling existing infrastructure. The transition from magstripe to chip-and-PIN dramatically reduced card-present fraud while largely maintaining underlying payment systems. This approach shows how targeted upgrades can yield substantial security benefits without disrupting core operations. As the industry advances identity and authentication technologies, it is crucial to leverage these innovations to address evolving fraud challenges. This strategy enables continuous improvement in fraud prevention without compromising the speed, efficiency, and accessibility that define modern payment systems.

Stripe urges the banking agencies to carefully scrutinize proposed solutions that may inadvertently impede fraud prevention efforts or inhibit economic growth. For example, any regulatory proposal requiring tokenized account numbers, while potentially reducing data compromises, also risks walling off critical information needed for cross-institution analytics. Such measures could limit our ability to implement comprehensive anti-fraud measures, including advanced behavioral analytics and real-time transaction monitoring.

Instead, we advocate for a balanced approach that strengthens security without compromising fraud detection capabilities. Regulators should:

- Advance interoperable identity and authentication standards;
- Preserve access to essential data fields (like account and routing numbers) to enable fraud analytics across accounts and transactions;
- Encourage innovation in fraud detection that leverages, rather than restricts, data access; and
- Promote broadly accepted identity and authorization standards developed collaboratively by ecosystem participants.

This approach fosters a resilient ecosystem that protects consumers and businesses while enabling ongoing innovation to counter evolving fraud threats.

Conclusion

Stripe appreciates the opportunity to comment. We are committed to protecting our users and the integrity of the financial system, and stand ready to provide further technical expertise or operational insights, and to participate in working groups to support the development and implementation of effective fraud prevention strategies that benefit the entire payments ecosystem.

Respectfully Submitted,

/s/

Jonah Crane
Head of Global Regulatory and Policy Development