adyen

September 18, 2025

Via Electronic Submission

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

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

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

Re: Request for Information on Potential Actions to Address Payments Fraud
(*OCC: Docket ID OCC-2025-0009; Federal Reserve System: Docket No. OP-1866; FDIC: RIN 3064-ZA49*)

Adyen N.V. (Adyen) appreciates the opportunity to submit comments to the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Federal Reserve), and the Federal Deposit Insurance Corporation (FDIC) in response to the request for information and comment on potential actions to address payments fraud.

We applaud the federal banking agencies for their proactive leadership in engaging stakeholders on the critical issue of payments fraud. This request for information comes at a pivotal moment, presenting an opportunity to strengthen the resilience of the U.S. payment system through deeper public-private collaboration, continued innovation, and forward-looking policy.

At Adyen, we have long been focused on strengthening fraud prevention, hand-in-hand with reducing payment costs and improving seamless retail payments. We recognized early that as consumer expectations rise and fraud tactics become more sophisticated, businesses need more than reactive tools; they require adaptive solutions that can anticipate and evolve with shifting behaviors and emerging threats. Whereas legacy systems often treat fraud, conversion, and cost as separate challenges, Adyen takes a

holistic approach that integrates these issues to deliver efficiency and meaningful protection, especially to emerging threats.

Modern payments fraud is constantly evolving and no longer confined to a single payment type or scheme. It spans scams, money laundering, identity theft, and other financial crimes, and its expansion across payment rails has had especially harmful effects on small businesses and vulnerable consumers.

One notable trend is the rise of "authorized push payment fraud," where consumers are deceived into authorizing transfers under false pretenses. Other growing risks include synthetic identities, chargeback fraud, policy abuse, and increasingly, AI-driven social engineering. Generative AI represents a fundamental shift, enabling voice and identity impersonation as well as sophisticated automated fraud attacks that can bypass traditional diligence and investigation tools at scale.

Merchant-originated threats also remain a concern, including money laundering, illicit sales, and collusion schemes. The rapid "platform-ification" of digital commerce has massively expanded opportunities for legitimate small businesses ("sub-merchants" in Adyen's ecosystem), but also illegitimate sub-merchants, as small businesses and individual sellers now reach far larger audiences through online platforms than on their own. While this scale and reach benefit consumers and merchants alike, we need modernized risk management solutions to prevent fraud and mitigate bad actor attempts to exploit streamlined onboarding and trust mechanisms.

To combat modern fraud and protect the payment system from emerging threats, it is essential that regulatory and policy frameworks not only safeguard the system but also enable innovation in fraud prevention, detection, and mitigation. By fostering an environment where data-driven solutions can develop and scale, the federal banking agencies can help ensure that businesses and consumers alike benefit from a modern, efficient, and resilient payments ecosystem.

Background

Adyen is the financial technology platform of choice for leading companies. By providing end-to-end payments capabilities, data-driven insights, and financial products in a single global solution, Adyen helps businesses achieve their ambitions faster.

Adyen maintains a compliance-forward, globally supervised posture, including as an OCC-supervised U.S. federal branch of a foreign bank in the United States, as well as holding banking licenses in Europe and the United Kingdom. We provide payments, business accounts, card issuing, and working capital directly to merchants, meaning merchants know exactly who is responsible for their service and have a single, accountable partner for all their financial needs.

Traditional banks often depend on legacy core systems and multiple outside vendors. In contrast, Adyen's platform is built and managed entirely in-house using modern, cloud-based technology. We capture payment processing steps in real time, without gaps, delays, or data inconsistencies associated with passing information between third parties. Our in-house and modern infrastructure gives us a single, unified view of all transactions, allowing us to spot fraud quickly, adapt to new threats, and offer merchants tailored, real-time recommendations that balance security, customer experience, and cost.

Compared to non-bank providers, our direct connections to payment networks and owned banking solutions mean we capture cleaner, timelier, and more consistent data on every transaction, without the lags or reconciliation issues that come from relying on fragmented or legacy infrastructure. This includes settlement details, account flows, and risk signals that others may only see in part or with a delay. This comprehensive data set powers our AI-driven tools and allows us to see emerging risks across the entire ecosystem.

Fraud is not confined to any single payment type or scheme, and it broadly encompasses money laundering, scams, identity theft, and a spectrum of other financial crimes that pose risks to the integrity of the payments system. To mitigate the risk of payments fraud, we believe the federal banking agencies should focus on three key objectives. First, we recommend the formation of an industry working group to establish a Payments Fraud Standard that sets baseline best practices across payment types, remains payment-agnostic and privacy-preserving, and allows financial institutions and businesses to strengthen defenses across all payment rails and platforms. Second, regulatory frameworks should emphasize outcomes rather than inputs, measuring the effectiveness of fraud controls and allowing innovation while maintaining accountability and adaptability. Third, dynamic fraud detection requires dynamic use of data: as fraud tactics rapidly evolve, regulators should encourage and further foster the responsible use of expanded data elements (such as device identifiers, behavioral analytics, and transaction history) in ways that support effective fraud safeguards while respecting privacy.

Although this request for information does not directly address anti-money laundering regulations issued by the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), we believe efforts to mitigate payments fraud should be integrated with measures to identify, prevent, and report illicit financial activity, reinforcing a comprehensive approach to financial system integrity. Below, we elaborate on specific recommendations to advance these objectives.

Recommendations for External Collaboration (Questions 1-4)

We commend the federal banking agencies for their leadership in fostering cross-industry collaboration, including initiatives such as FraudClassifier℠, ScamClassifier℠, and guidance on elder exploitation. The evolving threat landscape, accelerated by AI and amplified by fragmented fraud defenses, underscores the urgency of coordinated action. A collaborative approach is essential to effectively combat fraud and related financial crimes across the payments ecosystem.

To further foster collaboration and ensure that no single payment method becomes a vector for fraud, we recommend that the federal banking agencies convene an industry working group to develop a Payments Fraud Standard to support a safer and more secure payments system. The standard should specify minimum controls based on transaction risk that financial institutions and other parties in the payments ecosystem may utilize to detect, prevent, and respond to fraud, such as:

- Use of tokenization to enable secure, seamless credential sharing. Payment credentials should be protected by provider-agnostic, end-to-end tokenization – enabling secure, seamless commerce across providers and channels while minimizing the risk of credential compromise.
- Intelligent authentication controls that reduce fraud risk while ensuring legitimate transactions do not experience unnecessary frictions or delays. Baseline requirements could require multi-factor and biometric authentication for high-risk transactions for example, with a roadmap to incorporate newer technologies, such as passkeys.
- Dynamic risk management at the point-of-sale using data-driven insights to continuously strengthen fraud detection. Best practices deploy behavioral analytics and device intelligence at the point of sale, leveraging ecosystem-level data to detect and block fraud in real time, rather than relying solely on static rules or post-transaction reviews.

Some payment types today benefit from more mature and robust technological solutions to combat fraud (e.g., card networks with tokenization and authentication standards), while other payment methods (e.g., electronic check, ACH, account-to-account payments, and digital wallets) have varying levels of protection – fraudsters will inevitably exploit the weakest links. A baseline standard across all rails would help close those gaps, create consistent expectations, and ensure that no payment method is perceived as inherently "less safe." It would also extend enterprise-grade protections to small and mid-sized merchants that may lack the resources to build their own defenses. Together, these measures form the foundation of a robust, payment-agnostic framework that adapts to evolving threats and safeguards consumers and merchants.

These safeguards are critical not only to address current fraud risks but also to ensure the safe and scalable adoption of agentic commerce (in which AI agents initiate and manage transactions on behalf of consumers and businesses). Agentic commerce

raises new policy and technology considerations (e.g. authenticating non-human actors and maintaining end-to-end trusted digital identities) that require baseline protections. Embedding universal tokenization, adaptive authentication, and risk management into agent transactions can help facilitate trust and mitigate fraud as these models evolve.

Adyen's experience shows that this approach not only reduces fraud losses and false positives but also enhances customer experience and operational efficiency. We are well positioned to contribute to this effort, drawing on our dual role as a supervised bank and a global payments infrastructure provider. With a strong record of building both internal compliance capabilities and merchant-facing safeguards, such as behavioral analytics, refund abuse detection, biometric and network tokens, and advanced authentication tools, we deliver proven protections across the ecosystem. Our scale across merchants, payment types, and geographies allows us to detect sophisticated fraud schemes that no single participant could identify alone. At the same time, our supervision as a financial institution ensures accountability and alignment with regulatory objectives. This combination enables us to identify emerging risks early, extend enterprise-grade protections to small and mid-sized merchants, and maintain consistent defenses across all payment rails, closing fraud "hot spots" that arise when protections vary by payment type.

Safeguards must dynamically adapt to the sophistication of fraud tactics. We recommend that the federal banking agencies promote industry collaboration in the development of a Payments Fraud Standard, under which financial institutions and merchants can deploy baseline data-driven best practices to collectively strengthen fraud defenses, with the goal of moving beyond traditional, static controls. Any new standards must be adaptive and forward-looking from the outset, ensuring they remain effective as threats evolve. The cost of inaction is clear: without dynamic protections, the payments ecosystem risks falling behind those who exploit its vulnerabilities.

Recommendations for Regulation and Supervision (Questions 5-8)

A static system of regulation and supervision, rooted in rigid rules and checklists, is not equipped to combat sophisticated, rapidly evolving fraud tactics. For financial institutions operating under these regimes, this often means defenses are calibrated to yesterday's threats, leaving gaps against today's more dynamic schemes.

We urge the federal banking agencies to advance outcome-based fraud and compliance frameworks in place of prescriptive, checklist-driven rulemaking. Such an approach would incentivize real-time, adaptive fraud detection, prevention, and mitigation across all payment types, while giving financial institutions flexibility to deploy the tools, data, and models best suited to the risk profile of the transactions they process, so long as they can demonstrate measurable results.

For example, Adyen has a proven track record of successfully mitigating merchant-originated fraud threats through dynamic fraud controls, in addition to using more "traditional" controls that are known and more easily tested by regulators. As noted above, we serve as the infrastructure layer between merchants and the broader payments ecosystem. This vantage point allows us to leverage our broad market and geographic reach, actionable data, and advanced risk models to dynamically detect and respond to fraudulent merchant activity (such as money laundering, illicit sales, and collusion schemes). When a new merchant begins processing, the customers transacting with the merchant are often already known within our network, allowing us to identify patterns and anomalies to validate the legitimacy of the new merchant. Whereas traditional document-based identity verification can be vulnerable to increasingly sophisticated forgeries, including through the use of generative AI, Adyen's dynamic, data-driven controls provide a more robust safeguard. Our role is critical in light of the "platform-ification" of digital commerce described above. By embedding dynamic compliance into its infrastructure, Adyen helps platforms ensure that fraudulent SMBs are identified and blocked before they can access the broader payments ecosystem. In doing so, we enable platforms to offer their SMB customers enterprise-grade protections from day one, while also giving regulators confidence that embedded finance can scale safely and securely.

By prioritizing performance metrics (such as fraud loss rates, detection speed, false-positive ratios, and remediation times), supervisors can assess financial institutions on measurable outcomes rather than against static rules, which too often create the illusion that risks are fully addressed when in fact sophisticated actors have outpaced existing defenses. Such an approach would also give financial institutions greater flexibility to deploy dynamic, data-driven approaches while still meeting supervisory objectives, enabling stronger fraud protections across the system, including for small and mid-sized businesses and consumers.

Financial crime is evolving faster than rigid safeguards, and we cannot afford to fall behind. Fraud today is fast-moving, cross-platform, and increasingly coordinated, amplified by generative AI, synthetic identities, and the speed of instant payment rails. Prescriptive rules cannot keep pace with these dynamics. Modernized, outcome-based frameworks, by contrast, direct resources toward measurable reduction in fraud risk.

Recommendations for Payments Fraud Data Collection and Information Sharing (Questions 16-20)

Effective fraud prevention depends not only on robust internal controls but also on timely, meaningful information sharing with financial institutions, including from regulators. We commend FinCEN's recent guidance, issued in consultation with the OCC, FDIC, and National Credit Union Administration, and its recognition that "robust and appropriate sharing of financial information (such as transaction records, customer

and account information, and investigative materials) that would otherwise be siloed at individual financial institutions amplifies financial institutions' collective ability to detect, prevent, and mitigate illicit finance activity."

In that spirit, we recommend that the federal banking agencies expand the sharing of clear, outcomes-focused guidance to help financial institutions address emerging threats and align with supervisory priorities. Such an approach would move beyond one-way obligations like suspicious activity report filings, and toward dynamic, feedback-driven engagement in which regulators share anonymized typology updates and cross-institutional patterns, which can help financial institutions improve their fraud defense models. By sharing examples of fraud schemes, guidance on effective controls, and upfront communication on examination expectations with financial institutions, regulators can strengthen the overall resilience of the payments ecosystem against fraud and drive faster adaptation to new and evolving fraud schemes.

More generally, timely intelligence shared from regulators and law enforcement back to financial institutions would provide a more comprehensive understanding of fraud losses and emerging typologies. This, in turn, helps financial institutions detect fraud more effectively and implement stronger protections, particularly against AI-enabled schemes and new instant payment methods. Feedback loops and case studies further support fraud prevention and enhance resource efficiency, as well as mitigate the risk of fraudsters removed by one financial institution continuing to operate elsewhere due to otherwise fragmented communication or delayed reporting.

In addition, increased information-sharing by parties in the payments ecosystem with certain financial institutions can further enhance collective defenses. As an infrastructure provider, Adyen has a system-wide vantage point and advanced analytics capabilities. We currently use dynamic, real-time intelligence to detect cross-platform fraud typologies that other institutions that lack our scale are generally unable to identify in isolation, in line with regulatory objectives given our status as an OCC-supervised institution. Regulators should foster the sharing of pertinent, timely inputs by merchants and other parties in the payments ecosystem with prudentially supervised infrastructure providers in privacy-conscious ways, which can support identifying fraud via methods analyzing device risk patterns, anonymized behavioral trends, and transaction anomaly typologies. At the same time, this approach should respect commercial realities and competitive differentiation. Prudentially supervised infrastructure providers can, in turn, contribute anonymized, outcome-level risk insights — without sharing proprietary models or analytics — to other parties in the payments ecosystem, preserving incentives to invest in fraud detection capabilities. This collective approach strengthens fraud defenses, reduces false positives, and safeguards businesses of all sizes, while encouraging market-driven innovation to combat fraud across the payments ecosystem.

General Recommendations (Question 24)

In response to the question of which measures have been most effective in identifying, preventing, and mitigating payments fraud, as noted above Adyen leverages its system-wide vantage point and advanced analytics capabilities as an OCC-supervised infrastructure provider. We employ dynamic, real-time intelligence to detect cross-platform fraud typologies that individual institutions that lack our scale are generally unable to identify in isolation. Behavioral insights derived in privacy-preserving ways from cross-merchant and cross-channel data power our next-generation fraud analytics, allowing us to analyze transaction patterns, account histories, and other contextual signals in real time.

Moreover, detection must keep pace with real-time settlement, particularly for sophisticated threats such as authorized push payment fraud or fraudulent merchant activity. By analyzing transaction patterns and contextual data, Adyen distinguishes suspicious activity from normal or low-risk behavior, blocking bad actors early while minimizing friction for legitimate customers. We leverage dynamic, real-time behavioral analysis and the aggregation of contextual signals to deliver stronger fraud prevention and mitigation across the payments ecosystem. This approach enhances system-wide security and resilience without compromising trust, convenience, or efficiency for consumers and businesses.

As payments fraud becomes more sophisticated and complex, combating it requires advanced, data-driven solutions. We encourage the federal banking agencies to foster the responsible adoption of pragmatic, dynamic, and intelligent solutions to mitigate the risk of fraud.

* * *

Adyen appreciates the agencies' consideration of our comments. If you have any questions or would like to discuss our comments further, please contact Katie Suskind by email at [redacted].

Respectfully submitted,

Mariëtte Swart
Chief Risk & Compliance Officer
Adyen

Katie Suskind
Policy Lead
Adyen