# VISA INC., KY TRAN-TRONG

## Proposal and Comment Information

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

**Comment ID:** FR-2025-0036-01-C72

## Subject

Docket No. OP-1866; RIN 3064-ZA49 - Visa comment on Fraud RFI

## Submitter Information

**Organization Name:** Visa Inc.

**Organization Type:** Company

**Name:** Ky Tran-Trong

**Submitted Date:** 09/18/2025

Thank you for the opportunity to comment.

Ky Tran-Trong (he/him)
Associate General Counsel
Visa, Global Regulatory Affairs
[redacted]
Washington DC

[cid:image001.png@01DC28C2.447BC200]

By Electronic Submission to www.regulations.gov

September 15, 2025

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 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 [Docket ID OCC–2025–0009]**

All,

Visa Inc. ("Visa") appreciates the opportunity to provide input on how the Office of the Comptroller of the Currency (OCC), the Federal Reserve System (FRS), and the Federal Deposit Insurance Corporation (FDIC) can both collectively and independently within their respective roles, help consumers, businesses, and financial institutions mitigate payments fraud.

## ABOUT VISA

**Visa facilitates approximately $16 trillion in transactions annually between consumers, merchants, technology providers, financial institutions, and government entities across more than 200 countries and territories. Our core processing network, VisaNet, processes over 300 billion transactions annually[1].**

Our broad portfolio of products and capabilities addresses a wide spectrum of use cases through a combination of Visa-specific solutions and network- or payment-rail agnostic solutions. This flexibility enables us to meet partners and clients where they are, providing appropriate solutions for their existing payments and technology infrastructure. Our network of networks strategy means we are continuously working towards providing value-added services and solutions that help our partners and clients address fraud on all transactions, no matter which network.

[1] Visa Fact Sheet.

As a global leader in payments, maintaining the integrity and security of the payments ecosystem is essential to our success. Visa dedicates significant resources to advanced fraud-prevention technologies and has invested more than $12 billion over the past five years in intelligence and technology infrastructure. These efforts have helped block $40 billion+ in attempted fraud[2]. Since 2024 Visa Scam Disruption has detected $650 million in scams[3]. For more than 30 years, Visa has been at the center of using Artificial Intelligence (AI) in payments, investing $3.3 billion[4] in our AI and data infrastructure over the last decade. In 2024, we introduced new AI-powered risk and fraud prevention solutions that are designed to reduce fraud across A2A and card-not-present (CNP) payments, as well as transactions on and off Visa's network.

The quality of Visa's infrastructure and the breadth of our solution set provide a strong foundation for tailoring our existing capabilities to help reduce fraud and improper payments in government programs. Solutions we deliver to government clients inherently benefit from the security features and advanced technologies already embedded in millions of Visa credentials and money movement rails — such as tokenization and contactless technology — to accelerate fraud prevention efforts.

**Visa values its longstanding collaboration with the United States Government and remains committed to supporting federal priorities through dependable, efficient payment solutions.** Since 1998, Visa has partnered with the General Services Administration to operate GSA SmartPay, a program that supports charge cards for work-related travel, procurement, and fleet maintenance, while providing government officials access to centralized, discounted rates. This program serves more than 300 federal agencies and supports over $20 billion in purchase, travel, and fleet card payments annually[5].

Our IntelliLink Compliance Management solution, currently used by multiple agencies including the Department of Defense (DoD), Department of Homeland Security (DHS), Social Security Administration (SSA) and the Department of Health and Human Services (HHS), enables agencies to implement transaction guardrails such as restricted merchant categories (e.g., no payments to casinos or nightclubs). A recent DoD audit report[6] specifically noted that proper usage of IntelliLink Compliance could decrease fraud in government payments.

As part of its COVID-19 response, the Treasury Department used the U.S Debit Card (USDC) program to distribute more than $25 billion in Economic Impact Payments on Visa prepaid cards. Visa's real-time payments solution — Visa Direct — is also enabled for the USDC program and provides federal agencies the ability to quickly and securely send payments to bank accounts, digital wallets and neobanks[7].

Visa is proud to continue our partnership with the U.S. government and is committed to applying our expertise, innovative solutions, and global perspective to support the OCC, FRS and FDIC in their shared goal of mitigating payments fraud for the benefit of all participants in the U.S. government payment ecosystem.

---

[2] Visa Unveils its Scram Disruption Practice; $40B+ blocked annually in FY23 and FY24.

[3] Visa Payments Vault 2025 | Visa.

[4] From AI to RTP: Top trends shaping 2025 payments.

[5] Represents agency payment volume in FY23 (October 2022 – September 2023) on VisaNet.

[6] Audit of the DoD Government Travel Charge Card Program: The Visa IntelliLink Compliance Management System

[7] Funds are sent to bank accounts using debit card information linked to the bank account. Actual fund availability for all Visa Direct transactions may depend on receiving financial institution, account type, region, compliance processes, along with other factors, as applicable.

## RESPONSES TO REQUEST FOR INFORMATION

### SECTION A: EXTERNAL COLLABORATION

**Visa is committed to reducing payments fraud across the U.S. payment ecosystem through a multi-layered, collaborative approach.** Achieving meaningful progress requires close coordination among financial institutions, merchants, consumers, technology providers, and government agencies. Visa's leadership in combating fraud includes active participation in forums, task forces, and partnerships that set industry standards, share intelligence, address emerging threats, and develop actionable solutions, including:

*Payment Card Industry Data Security Standard (PCI DSS)*

Visa has a long history of leading the development of security standards that protect the integrity of the payments ecosystem. For example, we helped create PCI DSS, a globally adopted framework for securing cardholder data. PCI DSS minimizes vulnerabilities and ensures that all entities handling payment information maintain robust and consistent security practices.

*EMVCo*

Visa continues to shape the future of payments security through our active role in EMVCo, where we help define and evolve global standards for secure, interoperable card-based payments. For example, EMVCo Secure Remote Commerce (SRC) specifications — known as "Click to Pay" — standardize online checkout by defining precise data fields to ensure consistent, secure, and convenient payment experiences across websites and devices. These fields include tokenized payment credentials, billing and shipping addresses, consumer identity information, and transaction details such as amount and currency.

Click to Pay leverages our tokenization technology to ensure that sensitive payment data is protected and cannot be reused if compromised, which enables more effective fraud prevention. As digital commerce expands and omnichannel payments grow, these standards are playing an increasingly critical role in ensuring security and consumer trust.

*Fast Identity Online (FIDO) Alliance*

FIDO Alliance is a global consortium driving open standards for password-less authentication. Visa is a key contributor, serving as a board member and co-chair of the FIDO Payments Working Group. Through initiatives like Visa Payment Passkey[8], Visa is actively shaping the future of secure digital commerce by replacing passwords with biometrics and device-based authentication to improve both security and user experience across the payments ecosystem.

*National Task Force on Fraud and Scam Prevention*

Visa serves as an active member of this task force, convened by the Aspen Institute's Financial Security Program (FSP), alongside financial services firms, technology companies, consumer advocacy groups, and federal agencies. The task force develops a comprehensive national strategy to combat fraud and scams. In July 2025, Visa partnered with the FSP to host a panel at the Visa Payments Vault in Washington, D.C., showcasing how Visa and key

[8] Visa Payment Passkey (VPP) delivers a modern authentication solution.

partners deploy advanced AI tools and technologies to detect and counter rapidly evolving threats, and highlighting preventive education and resources available to fraud victims.

*Merchant Risk Council (MRC) Partnership*

Visa works closely with the MRC, a global trade association focused on payments and fraud prevention, participating year-round in its committees, providing support, and presenting at its annual regional summits in the US, Europe, and Asia Pacific. Together, we developed Compelling Evidence 3.0, a framework that enables merchants to provide richer transactional data in response to dispute requests to address first-party misuse and reduce chargebacks.

Each year, Visa and MRC co-author the Global Payments and Fraud Report to share timely insights into fraud trends and risk management. MRC also collaborates with Visa to enhance programs such as the Visa Acquirer Monitoring Program, which targets high e-commerce fraud rates at the acquirer level.

## ***Driving Consistent Fraud Intelligence and Consumer Protections Across the Payments Ecosystem***

The U.S. government, through the Federal Reserve, has taken important steps to address interoperability challenges with the introduction of FraudClassifier and ScamClassifier. These models provide a standardized language for categorizing fraud and scams. While adoption is currently voluntary, requiring their use specifically for data shared with government agencies could help eliminate inconsistencies in definitions and data formats when sharing fraud and scam intelligence.

In addition, inconsistencies in dispute resolution processes across payment rails create exploitable gaps. For example, a consumer paying with a card can dispute a transaction if the goods or services purchased were never received. Those using ACH payments (or check) often have no equivalent recourse. Visa's decades of experience designing and operating efficient, transparent, and consumer-focused dispute frameworks for the card ecosystem position us to help evaluate, design, and inform potential protections for other payment rails, where dispute rights are often inconsistent or limited.

For example, we launched our Pay by Bank solution in the UK in June 2025[9], which gives consumers more choice, control, and protection over bank transfer payments. With this solution, we extended our best-in-class consumer protections — long associated with card payments — to bank transfers. These protections include clear, standardized guidelines for consumers, businesses, and banks that define rights and responsibilities when something goes wrong. They also give consumers the ability to recover their money in the event of an error. Together, these measures create a card-like safety net for covered bank transfers, closing a long-standing protection gap and building greater trust in these transactions.

---

[9] Visa brings Smarter Pay by Bank with Built-In Consumer Protections to the UK Market.

## SECTION B: CONSUMER, BUSINESS & INDUSTRY EDUCATION

**For more than 25 years, Visa has been a leader in financial literacy, creating free, high-quality education programs for learners of every age around the globe.** Our award-winning Practical Money Skills platform — available in 19 languages and 46 countries — offers articles, lesson plans, mobile apps, and games that have helped millions of consumers, educators, parents, and students build stronger financial futures.

We amplify this impact through high-profile partnerships that make learning engaging and accessible. Our FIFA World Cup-themed Financial Soccer game is localized in 18 languages and active in 45 countries, bringing financial education to classrooms and communities worldwide. In the U.S., our NFL-themed Financial Football curriculum — distributed with state officials in 49 states — reaches nearly 30,000 middle and high schools. By co-branding financial literacy sites with more than 570 banks and credit unions, we leverage the trusted relationships those institutions have with their customers, extending our resources to millions more through channels they know and trust.

Below are ways Visa can support the government in delivering consumer, business, and industry education on fraud, leveraging our proven models, broad partnerships, and practical tools to promote ongoing awareness and proactive fraud prevention.

### *Applying Proven Engagement Models to Raising Fraud Awareness*

**Visa can apply this same proven formula — engaging content, strategic partnerships, broad language coverage, and co-branded delivery channels — to build consumer awareness of payments fraud.**

Industry dialogue is essential but not sufficient by itself to eliminate fraud, as bad actors continue to take advantage of consumer trust. Effective fraud prevention requires increasing public awareness through accurate and accessible media coverage and providing practical, repeatable steps consumers can take to protect themselves.

Visa has launched extensive consumer educational campaigns[10] specifically targeting consumers to help them recognize and avoid payment fraud and scams. Through ongoing media relations and strategic partnerships, we distribute educational materials about common scam tactics, including romance scams[11], back to school scams[12], holiday shopping scams[13] and more.

These resources are tailored to address scams that exploit high-impact cultural events, holidays, and shopping patterns. Visa also uses its sponsorships to educate consumers around scams, especially during cultural moments such as the Super Bowl[14]. Additionally, Visa releases a Biannual Threats Report[15] both to consumers and clients to keep the public up to date with common scams and fraud schemes that affect consumers, as well as regular ad hoc updates on particularly notable scams.

---

[10] Visa sets up new team to take down all scammers.

[11] Swipe left on romance scams.

[12] Experts sound alarm over back-to-school shopping scams.

[13] How Scammers Are Using AI This Holiday Season to Steal Your Money.

[14] Super Bowl scams: What to know if you're buying tickets for the 49ers vs. Chiefs in Las Vegas.

[15] Biannual Threats Report (Spring 2025).

Effective fraud prevention also depends on encouraging victims to report incidents without fear of stigma. With that in mind, Featurespace, a Visa company, sponsors "Scam Detectors," a podcast that pairs firsthand victim stories with insights from fraud-prevention experts to reveal how romance scams, phishing, impersonation, deepfakes, and other schemes operate. By amplifying victims' voices and demystifying criminals' tactics, the podcast raises public awareness and equips listeners with practical tools to recognize and avoid fraud in an increasingly digital world.

***Providing Digital Fraud Education for Consumers At Scale***

**Visa builds industry-level expertise through Visa University, our global learning organization offering in-person, virtual, and on-demand courses to strengthen technical, business, and leadership skills in today's payments environment**. Our Fraud Risk I course provides a practical, end-to-end view of detecting, preventing, and responding to fraud across the payment lifecycle, covering fraud foundations, dispute reporting, acceptance risk, and issuer fraud management. Participants examine current trends, review Visa's risk standards, work through real world cases, and earn a Visa-issued digital badge certifying their achievement.

**Visa is ready to partner with the OCC, FRS, and FDIC to extend on-demand fraud education courses to U.S. consumers through agency-supported financial literacy and protection programs**. We can repackage existing modules into endorsed learning paths and deliver them through banks, neobanks, and community initiatives targeting underbanked, low-income, and senior populations at key moments such as onboarding, senior-outreach events, and first-time homebuyer workshops.

To maximize reach, Visa's Marketing Services team can provide turnkey toolkits with tested messaging, creative assets, and deployment guides for financial institutions to adapt across channels, including email campaigns, webinars, and Visa Access, our online platform for issuers and acquirers. By combining practical educational content with ready to use marketing support, Visa and the OCC, FRS, and FDIC can equip millions of Americans to recognize and avoid scams, strengthening public confidence in the financial system.

***Equipping Financial Institutions as First Responders***

While awareness efforts often center on consumers, empowering financial institutions with effective customer-engagement strategies is equally critical. Banks and credit unions interact with customers at the very moment a risky transaction is about to occur — making them the first line of defense.

Visa can help institutions turn their digital banking platforms into active fraud-prevention tools with communication playbooks that deliver real-time, point-of-prevention alerts. For instance, the platform might ask a customer to verify a suspicious transfer and explain why it appears fraudulent — stopping the transaction and building the customer's ability to spot similar scams in the future.

By turning high-risk transactions into teachable moments, financial institutions can both stop fraud and build lasting awareness — helping the government meet its goal of expanding access to safe, secure payment options.

## SECTION C: REGULATION & SUPERVISION

Regulatory frameworks that support the responsible use of AI and other new technologies used in fighting fraud would enable sustained investment in advanced fraud prevention tools. As Governor Waller noted in his "Technological Advancements in Payments" speech at the Wyoming Blockchain Symposium 2025, payment companies have used machine learning to detect fraud since the early 1990s. More recently, as large language models and generative AI have matured, payment companies including Visa have used them to further enhance fraud detection.

To enable innovative technologies like AI, we encourage regulators to adopt regulations that focus on the outcomes of AI models — rather than taking a prescriptive, process-based approach to the technical specifics of developing, modelling, and implementing AI. Technology-neutral and outcomes-based regulation which seeks to complement, rather than to displace, existing laws is likely to be the most effective means of mitigating the potential risks of AI technologies while facilitating sustainable and scalable innovation.

Moreover, the use of AI and other innovative technologies to combat fraud requires continuous investment from financial institutions, payment networks, and technology providers. Accordingly, policymakers and regulators must ensure that they continue to encourage such investment by providing financial institutions with adequate cost recovery and an appropriate rate of return. For example, under the Federal Reserve's Regulation II, covered issuers today may recover for certain fraud prevention costs in the debit interchange fee standard which helps to ensure that issuers are able to continue to invest in fraud fighting technologies.

Regulators should also consider safe harbor provisions or pilot programs to allow controlled testing of innovative AI-driven fraud prevention tools without undue enforcement risk, provided safeguards are in place. Such frameworks could set parameters for scope, data handling, oversight, and duration, and require results reporting. This would reduce fear of penalties for good-faith experimentation and promote collaborative learning between regulators and industry.

## SECTION D: PAYMENTS FRAUD DATA COLLECTION & INFORMATION SHARING

As noted in our response to the "External Collaboration" section, the Federal Reserve's FraudClassifier and ScamClassifier models provide a strong foundation for standardizing how payments fraud is categorized specifically for data shared with government agencies. It is also essential for stakeholders to reach alignment on what specific fraud data has the greatest impact on fraud prevention efforts when shared.

Valuable fraud detection data includes transaction-level identifiers, such as transaction IDs and authorization codes, which uniquely identify a payment, and technical and behavioral indicators, such as email addresses, IP addresses, device fingerprints, and usage patterns, which reveal how and from where a payment was made. Used together, these data points make it easier to spot synthetic identities, detect account takeovers, and uncover coordinated fraud schemes.

Achieving broad industry agreement on which specific data elements to prioritize — and ensuring they are consistently factored into participants' fraud monitoring and risk assessments — would make these tools far more effective. When these data elements are

consistently collected by all participants and shared securely — for example, through standardized APIs — they give the entire payments ecosystem a clearer, faster, and more actionable view of emerging threats.

## SECTION E: RESERVE BANKS' OPERATOR TOOLS & SERVICES

We have identified key opportunities for the Federal Reserve Banks to enhance their risk-management tools and frameworks.

### *Enhance Treasury's Existing Do Not Pay System with Visa Capabilities to Flag High-Risk Recipients*

The Do Not Pay (DNP) system, managed by the Treasury's Bureau of the Fiscal Service, plays a critical role in safeguarding federal payments by verifying payee eligibility — confirming that recipients meet all legal and program requirements to receive federal funds. This includes ensuring the payee is a living individual or active entity, has no outstanding delinquent debts subject to collection, and is not suspended, debarred, or otherwise excluded from participation in federal programs.

Building on this strong foundation, there is an opportunity to increase DNP's use and expand its utility by incorporating data that identifies accounts or entities exhibiting patterns of suspicious or potentially fraudulent activity. This enhancement would enable agencies to prevent not only ineligible payments but also those with elevated fraud risk.

Furthermore, there could be value in enabling controlled sharing of DNP data with regulated banks and financial institutions under clear legal and privacy safeguards. This could augment AML/KYC data used in account onboarding and transaction monitoring and enhance early fraud detection.

### *Utilize Visa's Account Name Inquiry as a Confirmation of Payee Solution to Prevent Authorized Push Payment Fraud*

We encourage the Federal Reserve to consider implementing a confirmation of payee solution to help mitigate rising authorized push payment (APP) fraud as account-to-account (A2A) payments grow. This prepayment name matching tool compares the payee name entered by the payer with the name on the destination account (held by the payee's financial institution). If there is a mismatch, the payer can be immediately alerted. This enables the payer to make an informed decision on how to proceed and can help prevent misdirected payments and authorized push payment fraud.

*Visa's Account Name Inquiry* (ANI)[16] delivers the same core function by providing real-time account name verification for A2A payments. By adding this layer of protection, ANI can prevent fraud before payment occurs. ANI is available across VisaNet transactions, including *Visa Direct*, our network-agnostic money-movement platform that reaches 99% of U.S. bank accounts, including neobanks and digital wallets. Together, ANI and Visa Direct can enable payer agencies to verify payee information in real time before sending secure, fast digital disbursements backed by the security and trust of the Visa network.

[16] Account Name Inquiry functionality is currently limited to VisaNet.

***Collaborate with Featurespace to Use Privacy-Enhancing Technologies (PETs) for Secure, Cross-Institution Fraud Intelligence Sharing***

To amplify existing data-standardization efforts, the Federal Reserve Banks could promote adoption of privacy-enhancing technologies (PETs) — such as tokenization, hashing, federated learning, and secure multi-party computation — that enable institutions to share and analyze high-value fraud indicators without exposing underlying customer data.

By reducing the risk of personally identifiable information (PII) exposure, PETs address security concerns that often limit participation in data-sharing initiatives. This would encourage more institutions to contribute richer, fraud-related data and complement future fraud-reporting standards — making them easier to implement while maintaining privacy compliance.

Featurespace has demonstrated experience designing and deploying PETs, having been selected to participate in the U.S. & U.K.'s joint PETs challenge. During the challenge, Featurespace built privacy-preserving solutions that enable AI models to be trained on sensitive data without organizations needing to share or combine their raw data. Featurespace achieved the highest accuracy score and was awarded special recognition for its usability and production readiness.

## SECTION F: GENERAL QUESTIONS

Fraud threats are evolving rapidly, with criminals exploiting both legacy and modern payment rails and leveraging speed, automation, and deception to bypass traditional controls. **Visa offers a comprehensive suite of risk solutions designed to secure digital payments and prevent fraud across the global payments ecosystem.**

At the core of our risk intelligence is *Visa Advanced Authorization*, a real-time, AI-driven risk scoring system that analyzes over 500 transaction attributes in milliseconds, helping to prevent an estimated $30 billion[17] in fraud annually across transactions processed through VisaNet.

With our recent acquisition of Featurespace, a global leader in adaptive behavioral analytics, we have enhanced our network-agnostic, real-time, AI-powered fraud detection solutions across all payment types — including card, check, ACH, and account-to-account (A2A) transactions.

In this section, we will highlight the fraud types we see affecting the payments ecosystem and the tactics criminals use to perpetrate them. We then connect our capabilities to these threats to show how our solutions effectively identify, mitigate, and prevent them.

*Check Fraud*

Check fraud continues to pose a significant risk for all payments, including government disbursement programs. Criminals exploit this legacy payment rail with forged or altered checks and counterfeit instruments, change payee details, and move funds quickly through ACH or other channels to evade detection.

Featurespace's check fraud solution combines real-time behavioral analytics with image-forensic technology to more accurately detect stolen, altered, and counterfeit checks. By

[17] Per VisaNet data for July 2023 – June 2024.

leveraging behavioral profiling and forensic image analysis, our platform flags duplicate deposits, device anomalies, and visual alterations to signatures or check stock during the deposit and clearing process. One credit union using our solution significantly reduced check fraud, catching more than 90% of fraudulent activity while keeping false positives low[18].

*Authorized Push Payment (APP) Scams*

APP scams are an emerging threat where fraudsters impersonate trusted organizations, including government agencies, and use phishing and social engineering to trick victims into sending irreversible transfers to fraudulent accounts

Visa and Featurespace's combined A2A capabilities use advanced AI and behavioral analytics to analyze transaction histories and identify patterns consistent with APP scams. In a recent pilot with Pay.UK[19], we applied these capabilities to analyze billions of historic transactions from banks across the United Kingdom. Utilizing Featurespace's Generative AI solution, Tallier, we increased fraud detection rates to 56% versus a pilot average of 40% and identified fraudulent transactions that had already passed through the sophisticated fraud detection systems of the participating banks and payment service providers (PSPs).

*Provisioning Fraud & Token Relay Attacks*

Provisioning fraud occurs when criminals use compromised credentials to enroll unauthorized digital wallets, bypass identity verification, and initiate fraudulent transactions. Token relay attacks extend this threat by transferring valid payment tokens across devices to circumvent issuer controls.

*Visa Provisioning Intelligence (VPI)* is an AI-driven fraud detection tool that evaluates token provisioning requests in real time, assigning a risk score to help issuers identify and block fraudulent attempts. Its value lies in significantly improving fraud detection accuracy. When compared to risk scores provided by token requestors, VPI detected up to six times more fraud and produced 83% fewer false positives[20].

Additionally, *Visa Push Provisioning* enables cardholders to instantly and securely load their payment credentials — typically tokenized card data — into digital wallets or merchant platforms directly from their issuer's app or website. Together, these solutions provide real-time defenses that can help reduce provisioning and token-relay fraud and support scalable, secure digital onboarding across the payments ecosystem.

*Enumeration Attacks*

Enumeration attacks involve largescale, automated testing of stolen or guessed payment credentials, often targeting ecommerce or government fee collection portals.

*Visa Account Attack Intelligence* provides networkwide monitoring to identify and disrupt automated credential testing activities in real time. Upon detection, issuers and agencies can be alerted to block suspicious attempts before they result in unauthorized transactions. This capability can help clients reduce fraud and operational losses due to enumeration, and ensure clients are safeguarded.

---

[18] Featurespace's ARIC for Check Fraud; Measured from June 2023 – August 2024.

[19] Featurespace's pilot with Pay.UK again demonstrates the potential for national payments systems to help combat fraud! - Featurespace.

[20] Harness AI power to detect token provisioning fraud | Visa; VisaNet, issuer reported fraud rates for mobile devices using secure element or host cloud emulation in December 2023 occurring within 7 days of token provisioning. Results are based on comparing the VPI score to other wallet risk scores provided by token requestors in a random sample of token requests that is statistically meaningful while also maintaining Visa's confidentiality obligations to other parties. The fraud prevention rate and false positive ratios comparison is determined by comparing the highest risk-rated token requestor scores versus the highest risk-rated VPI scores.

*Social Engineering & OTP Bypass*

Social engineering remains one of the most challenging fraud vectors, with attackers impersonating trusted parties, conducting phishing campaigns, executing SIM swaps, and even deploying deepfake technologies to obtain or intercept one-time passwords (OTPs). Such methods can enable large-scale account takeovers and compromise payment credentials and accounts.

*Visa Payment Passkey* addresses OTP intercept by replacing vulnerable SMS-based authentication with secure, device-bound credentials. Instead of transmitting a one-time passcode that could be intercepted via phishing or SIM swapping, Passkeys use FIDO®-based cryptography and biometric authentication stored locally on the consumer's device. This is important as biometric authentication via Passkeys can reduce fraud rates by up to 50%[21] compared to SMS OTPs. This mode of authentication happens entirely on the consumer's device and sends no additional data sent over the network, which closes off points where OTPs can be intercepted by attackers.

**Below, we have highlighted two additional opportunities where our capabilities can help the government identify, prevent, and mitigate fraud in government payments.**

***Visa and Featurespace: AI-Powered Risk Scoring to Prevent Fraud in Federal Payments***

Visa (including our Featurespace offering) can help Treasury and other federal payer agencies strengthen fraud prevention and improper payment controls in government payments through proven, real-time, rail-agnostic risk scoring capabilities.

Our AI-powered adaptive behavioral analytics tool can evaluate hundreds of data points in milliseconds to assign a fraud likelihood score to every transaction. These capabilities can integrate seamlessly with Treasury/FRS-operated payment systems and risk feeds to assess payments before funds are disbursed — enabling payer agencies to make informed decisions on whether to proceed, flag for review, or block transactions that present elevated risk.

Depending on the capacity and operational resources of each payer agency, the tool can be configured to automatically adjust the volume of transactions sent for manual review or to make real-time decisions based on agency defined rules and thresholds. By applying these advanced analytics, Treasury, FRS and partner agencies can better protect taxpayer dollars, reduce improper payments, and strengthen public trust in government programs.

***Visa Tap Technology to Improve Recipient Authentication Pre-Payment***

Visa could adapt its widespread Tap to Phone technology — also known as contactless — to address specific government use cases. This capability could help prevent fraud by authenticating recipients pre-payment, ensuring payments are delivered securely to the correct recipient. A solution of this nature could leverage the millions of Visa cards and credentials already in circulation and would be backed by the strength and resiliency of the Visa network, which is safeguarded by advanced security technologies such as tokenization.

---

[21] Visa Payment Passkey—a modern authentication solution | Visa.

**SUMMARY OF ACTIONABLE OPPORTUNITIES IDENTIFIED BY VISA TO STRENGTHEN GOVERNMENT PAYMENT SECURITY**

While we recognize that the OCC, FRS, and FDIC are primarily regulatory bodies, we understand that this document will be read broadly by other federal agencies and stakeholders committed to reducing fraud in government payments. As such, we have identified actionable opportunities below where we can leverage our decades of global payments security experience and the proven quality and scale of our infrastructure to support the OCC, FRS, FDIC and other federal agencies in their payment fraud-reduction objectives.

1. Collaborate on integrating Featurespace's real-time AI risk-scoring capabilities into Treasury and FRS payments to detect & stop potential fraud pre-payment
2. Work with Treasury (and respective FRS banks) to enhance the Do Not Pay (DNP) system to dynamically identify and add known fraudulent recipients to DNP lists
3. Conduct a proof-of-concept leveraging our Tap technology to authenticate recipients pre-payment to reduce fraud and improper payments
4. Join ongoing agency and FRS payment pilots to accelerate innovation and strengthen fraud detection with Visa's technology and expertise
5. Partner with government agencies (including the OCC, FDIC and the FRS) to expand fraud-prevention education using Visa University's digital platform and Visa Marketing Services to deliver agency-endorsed courses and turnkey communications for financial institutions to engage customers at key touchpoints

Visa appreciates the opportunity to respond to this important matter and is looking forward to working closely with the government to achieve their fraud reduction goals. If you have any questions, please do not hesitate to contact me at [redacted] or [redacted]

Sincerely,

[redacted]

Ky Tran–Trong
Associate General Counsel, Global Risk and Regulatory Affairs
Visa Inc.