Testimony of Jodie Kelley, CEO of ETA
Before the House Financial Services Committee
Subcommittee on Digital Assets, Financial Technology and Artificial Intelligence
Hearing: "Delivering for American Consumers: A Review of FinTech Innovations and Regulations."

January 13, 2026

Chairman Steil, Ranking Member Lynch, and members of the Subcommittee on Digital Assets, Financial Technology and Artificial Intelligence, my name is Jodie Kelley, and it is my privilege as Chief Executive Officer of the Electronic Transactions Association (ETA) to submit this written statement on how the digital payments industry is driving innovation by providing consumers and businesses with safe, competitive, convenient, innovative, and cost-effective financial services. On behalf of ETA and its members, thank you for the opportunity to participate in this important discussion.

ETA is the world's leading advocacy and trade association for the payments industry. Our members span the breadth of significant payments companies, from the largest incumbent players to fintech innovators in the U.S. and in more than a dozen countries. ETA members facilitate commerce by processing approximately $57 trillion annually in purchases and peer-to-peer (P2P) payments worldwide by developing and deploying payments innovations to merchants and consumers alike.

The digital payments industry is one of the most innovative, dynamic, and competitive industries, leveraging a sophisticated, interconnected infrastructure to deliver financial products and services that benefit consumers, businesses, and the American economy. Access to payments technology enhances affordability by increasing consumers' effective spending power and by enabling entrepreneurship -- driving tens of billions of dollars in incremental sales to new businesses and providing efficiency gains of hundreds of millions of labor hours. These benefits provided by the payments industry translate directly into small business success.

I. The Evolution of the Payments Industry: Innovation, Security, and Collaboration

Over the past several decades, the payments ecosystem has undergone a profound transformation, driven by advances in technology, changing consumer expectations, and increased economic interconnectedness. What was once a largely invisible function of the banking system has become critical national infrastructure - supporting household financial stability, small business growth, job creation, and economic resilience.

At the same time, the industry has taken on expanded responsibilities, particularly in combating fraud, protecting consumers, and safeguarding the integrity of the financial system. Today's payments industry reflects a collaborative model in which banks, fintech companies, payment

networks, and technology providers work together to deliver secure, efficient, and inclusive financial services.

A. From Cash and Checks to Electronic Payments

For much of the twentieth century, payments in the United States were dominated by cash and paper checks. While effective for local commerce, these methods were slow, costly, and vulnerable to theft and fraud. As the economy grew and commerce became more national and global, the limitations of paper-based payments became increasingly clear.

Indeed, the modern payments era arguably began with a forgotten wallet. In 1949, dining out in Manhattan, financier Frank McNamara realized he had no cash and therefore no way to pay. The embarrassment led him to found Diners Club in 1950. It was the first "general purpose" charge card, acting as a third-party guarantor between diners and restaurants. Debit cards followed just over a decade later.

The introduction of credit and debit cards in the 1950s and 1960s marked a major shift. Card-based systems allowed consumers to access funds and credit at the point of sale while providing merchants with faster settlement and reduced risk. Banks and the payment networks that emerged invested heavily in authorization, clearing, and settlement infrastructure, laying the groundwork for the modern payments system.

Even in these early stages, fraud prevention was embedded into the payments system. Transaction monitoring, account verification, and spending controls became standard features, reflecting an understanding that trust is foundational to any payment system.

B. The Internet and E-Commerce

The rise of the internet and e-commerce in the late 1990s and early 2000s accelerated the evolution of payments. Credit and debit cards were (and remain) the primary form of payments as consumers moved online.

This same era also saw the rise of new entrants. For example, fintech companies facilitating payments online – including Adyen and Stripe – emerged that reduced checkout friction and provided easier access to more payment systems.

However, remote transactions introduced new vulnerabilities. Card-not-present fraud increased as physical verification disappeared, requiring the industry to adapt quickly. In response, payments providers deployed encryption, secure authentication protocols, and centralized monitoring systems. Digital wallets and online payment platforms reduced the need for consumers to repeatedly share sensitive financial information, while tokenization replaced actual account numbers with secure digital substitutes.

These innovations helped ensure that the growth of online commerce did not come at the expense of customer trust. They also demonstrated how industry-wide coordination could reduce systemic risk by identifying fraud patterns across millions of transactions.

C. Mobile Payments and the Emergence of Peer-to-Peer

The widespread adoption of smartphones further transformed payments. Mobile wallets, contactless payments, and peer-to-peer transfer services have integrated payments into everyday digital activity.

In 2009, Jack Dorsey and Jim McKelvey launched Square. Major mobile wallets including Google Wallet/Google Pay and Apple Pay launched in 2011 and 2014, respectively. Square enabled small and casual merchants to accept credit and debit cards from mobile phones instead of dedicated point-of-sale terminals, and streamlined direct merchant onboarding, and branded acceptance. This enormously expanded the number and kinds of small merchants that could accept electronic payments. For their part, Apple Pay and Google Wallet/Google Pay enabled payment credentials to be securely managed and used from mobile phones in lieu of swiping or inserting a piece of plastic.

Peer-to-peer payment platforms also expanded rapidly in this timeframe, particularly for small-dollar transactions and informal commerce, reshaping how people move money outside traditional banking channels. Venmo, founded in 2009 and later acquired by PayPal in 2013, helped proliferate mobile P2P transfers, especially for splitting bills and social payments; by the early 2020s it was handling hundreds of billions in annual transaction volume and serving tens of millions of users with integrated social features. Cash App, launched by Block (then Square, Inc.) in 2013 as "Square Cash," expanded beyond money transfers to include banking features, debit cards, stock and bitcoin investing. Zelle, built by Early Warning Services and launched nationally in 2017, integrate directly into the apps of over 2,000 financial institutions; in 2024 it processed 3.6 billion transactions totaling over $1 trillion.[1]

At its core, mobile provided consumers with the ability to make and receive payments anywhere anytime. Consumers could now pay bills, send money to friends, shop online, and make in-store purchases using a single device. Today any American with a smart phone and an internet connection has access to digital payments.

With new innovation came new security elements. Mobile payments commonly rely on biometric authentication, such as fingerprint or facial recognition, combined with device-level encryption and dynamic transaction credentials. These layers make mobile transactions among the most secure forms of payment available today. In the peer-to peer arena, to address risks

[1] Zelle, *Zelle® Shatters Records with $1 Trillion Sent in a Single Year* (Feb. 12, 2025), https://www.zelle.com/press-releases/zelle-shatters-records-1-trillion-sent-single-year

such as account takeovers and social engineering scams, providers implemented behavioral analytics, transaction limits, real-time alerts, and consumer education initiatives.

D. Embedded Payments

Around this same time, another shift emerged with the rise of application programming interfaces (APIs). These tools allow software companies to integrate payments directly into their platforms. Large platforms began embedding payments not merely as a convenience, but as a core business line. Ride-hailing apps processed driver payouts internally. Software companies bundled payments with subscriptions.

The result was the emergence of what we now call embedded payments: payment systems that are technically operated by regulated financial institutions, but functionally controlled by non-financial platforms.

Most platforms offering embedded payments do not hold banking licenses. Instead, they partner with regulated banks and payment processors that handle compliance obligations such as anti-money-laundering checks, sanctions screening, and settlement.

Typically, the platform controls the user experience, pricing and fees, and transaction rules, while the regulated partner controls licenses, formal compliance processes, and movement and custody of funds.

This model is now widespread across the economy. It is common in online marketplaces, business-to-business payments, and payroll services. One of the most important, and least visible, drivers of embedded payments today is the rise of vertical software-as-a-service platforms, often referred to as vertical SaaS.

These are software companies that serve a single industry or profession, such as restaurants, medical practices, property managers, contractors, or fitness studios. Unlike general-purpose software, these SaaS platforms combine scheduling, billing, payroll, inventory, compliance workflows, and payments into a single system tailored to the day-to-day operations of a specific business.

The adoption of embedded payments is expected to continue. Eighty-one percent of small businesses surveyed by U.S. Bank in 2025 reported that they would prefer a single source of banking, payments, and operational digital tools and 90% of small businesses view embedded payments as essential for growth.

E. Artificial Intelligence

Artificial Intelligence has the potential to positively impact the payments industry, consumers, businesses, and banks.

a. AI as a Core Capability

Artificial intelligence and machine learning are now central to how the payments industry fights fraud and manages risk. Unlike static rules-based systems, AI models continuously learn from new data, allowing them to adapt as fraud tactics evolve.

AI enables the detection of sophisticated threats, including coordinated fraud rings, synthetic identities, and previously unseen attack patterns. It also improves accuracy, reducing false declines that can frustrate consumers and harm legitimate commerce. AI-powered systems analyze transaction patterns to block fraudulent purchases and identify money laundering schemes that may evade traditional rule-based detection.

Beyond fraud prevention, AI is increasingly used to personalize security alerts and authentication, optimize payment routing and settlement, and enhance customer service and dispute resolution. AI-based customer service systems can provide 24/7 support, helping consumers navigate dispute processes and account inquiries without waiting for human representatives during business hours. These capabilities allow the industry to deliver both greater security and better consumer experiences.

Small businesses benefit from AI-enhanced payment acceptance and working capital products. AI systems analyze real-time sales data to identify cash flow patterns, helping businesses optimize their operations. These capabilities are particularly valuable for smaller businesses operating with fewer resources.

b. Agentic Commerce

Agentic commerce is a new type of digital commerce in which software agents – powered by artificial intelligence – act on behalf of individuals and businesses to make purchasing decisions and execute transactions autonomously.

In traditional e-commerce, a human decides what to buy, selects a merchant, and completes a checkout process. In agentic commerce, that process changes fundamentally. A consumer or business sets goals and constraints – such as budget limits, delivery requirements, or compliance rules – and an AI agent continuously monitors markets, compares options, negotiates terms, and completes purchases when conditions are met.

Agentic commerce promises efficiency gains, cost savings, and broader access to services. Many existing principles – authorization, consent, liability, auditability – apply in the agentic context. Ensuring clarity on the application of these principles in the agentic context will be critical to ensuring the promise of this technology is realized.

II. The Payments Industry Delivers Enormous Value to Consumers and is Critical to Entrepreneurship and Small Business Success

The innovation that is the hallmark of the payments industry is a key economic driver. As a recent PwC[2] study found, the industry generates more than $350 billion annually for the U.S. economy, supporting more than two million high-paying jobs, and acting as a catalyst that unlocks massive downstream economic activity that spurs entrepreneurship and allows small businesses to compete.

A. Digital Payments and Credit Enhance Consumer Affordability

Digital payments companies play an increasingly central role in making everyday life more affordable for consumers in the United States. Through expanded access to spending power, flexible financing options, and rewards such as cash back, these companies help households manage expenses, respond to financial shocks, and stretch limited budgets.

One of the most significant ways digital payments enhance affordability is by increasing consumers' effective spending power. Modern payment tools – particularly credit – cards provide consumers access to capital when they need it, rather than restricting purchases to available cash on hand. This access is critical for managing unexpected expenses, such as emergency car repairs or medical bills, as well as during planned but financially demanding periods like back-to-school shopping or the holiday season. By allowing consumers to smooth spending over time, credit cards help households avoid more disruptive financial tradeoffs, including delaying essential purchases.

In addition to traditional credit cards, newer payment options such as Buy Now, Pay Later services have expanded consumer choice and affordability. BNPL allows consumers to divide purchases into smaller, predictable payments, often with little or no interest. This structure can make necessary purchases—such as household goods, electronics for work or school, or essential services—more manageable while offering an alternative to revolving credit balances.

Rewards programs are another important component of consumer affordability. Cash-back rewards provide immediate, tangible value by returning a portion of spending directly to consumers. These rewards effectively lower the net cost of purchases and help households

[2] Contribution of the Payments Industry to the US Economy in 2024, PwC (January 2026)

manage rising costs. In 2024 alone, U.S. consumers received an estimated $43.5 billion[3] in value from cash-back programs, underscoring the role of rewards as a meaningful source of household savings rather than a discretionary perk.

The benefits of expanded consumer spending power extend beyond individual households. Enhanced consumer spending enabled by digital payments and credit supports approximately 1.7 million jobs and contributes an estimated $199 billion to U.S. GDP[4], driving demand across retail, services, manufacturing, and logistics while reinforcing overall economic resilience.

B. Digital Payments Enable Entrepreneurship and Small Business Growth, and are Transforming the Efficiency of Small Business Operations

Digital payments play a vital role in enabling entrepreneurship and supporting small businesses – the backbone of the American economy. Acceptance of electronic payments is now table stakes for any new business. Consumers expect to pay digitally, and businesses that cannot meet that expectation are immediately disadvantaged.

Today, entrepreneurs can begin accepting digital payments quickly and affordably, often using nothing more than a smartphone. This accessibility lowers startup costs, accelerates time to market, and expands opportunity across income levels, regions, and communities. Digital payments also allow small businesses to compete with large corporate retailers by expanding their reach. A local store, restaurant, or sole proprietor can sell online to customers nationwide or globally. Embedded payments integrated into software platforms have leveled the playing field, enabling growth without costly infrastructure investments.

The impact on sales is direct and measurable. Small businesses that accept digital payments experience sales increases of approximately 8 to 10 percent, driven by higher conversion rates, increased average transaction size, and reduced friction at checkout.[5]

That translates directly into small business success. Expanded access to electronic payment acceptance has generated an estimated $33.9 billion in incremental sales for new merchants, supporting approximately 301,200 jobs, $16.4 billion in labor income, and $28.2 billion in GDP.[6]

Digital payments also help small businesses operate efficiently and compete with larger enterprises. Small businesses do not have teams devoted to operations, accounting, or compliance. Owners and employees often perform multiple roles, making time one of their

[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Ibid.

most constrained resources. Payments technology embedded directly into business software automates transaction processing, reporting, and reconciliation, reducing administrative burdens and minimizing errors.

Faster digital checkout improves customer experience while reducing staffing pressure at the point of sale. Back-office automation enables real-time visibility into cash flow and simplifies recordkeeping. These efficiency gains are extraordinary: faster digital checkout and back-office automation saved an estimated 806 million labor hours in 2024 alone, equivalent to roughly 365,000 full-time employee equivalents.[7] For small businesses, these savings translate into lower operating costs and more time devoted to growth, innovation, and customer service.

In addition to enhanced customer experience and reduced costs, embedded payments allow for increased efficiencies, better cash flow management, ease of tax and accounting processes, regulatory and tax compliance, access to enhanced data, and enhanced security.

C. Digital Payments Support the Broader Economy

The economic impact of digital payments extends far beyond individual consumers and small businesses. The payments ecosystem functions as foundational economic infrastructure, enabling commerce at scale, increasing productivity, supporting high-quality employment, and strengthening economic resilience across all regions of the country.

At the national level, digital payments support approximately 2.0 million jobs across all 50 states.[8] These jobs span a wide range of sectors, including retail, technology, logistics, cybersecurity, customer support, data analytics, and professional services. This broad employment footprint reflects how deeply payments are integrated into nearly every industry that participates in modern commerce.

These are high-quality, high-paying jobs, with average compensation more than twice the national average. The income generated by these jobs supports local economies, increases tax revenues, and drives demand for housing and services, ensuring that the benefits of payments innovation are widely distributed across communities.

Digital payments also play a central role in driving economic output. The payments ecosystem directly contributes an estimated $354 billion to U.S. gross domestic product and contributes $210 billion to labor income.[9]

[7] Ibid.
[8] Ibid.
[9] Ibid.

Digital payments also enhance economic resilience. During periods of disruption – whether driven by public health emergencies, natural disasters, or economic shocks – businesses and consumers with access to digital payments are better positioned to adapt. Electronic payments support remote commerce, contactless transactions, rapid disbursement of funds, and continuity of economic activity.

Never was this more obvious than during the pandemic. As public health restrictions limited in-person commerce, small businesses moved to e-commerce with over 70% of small businesses either adopting new digital payment tools or expanding existing ones.[10] This kept business going; U.S. e-commerce sales grew by approximately 32% in 2020, representing over $240 billion in additional online spending in a single year.[11]

The payments industry also helped address the liquidity constraints that were among the most immediate threats to business survival. At the height of the pandemic, over 40% of small businesses reported having less than three weeks of cash reserves.[12] Payments providers responded, expanding same-day and instant settlement, and offering short-term working capital.

Finally, digital payments promote competition, innovation, and transparency. Lower barriers to entry encourage innovation in pricing, security, and consumer protection. Electronic records improve accountability, reduce fraud, and support compliance – benefiting consumers, businesses, and governments alike.

Taken together, these effects demonstrate that digital payments are not merely transactional tools, but a core driver of economic performance and resilience.

III. Payments Are Highly Regulated

All of this innovation and the benefits it brings take place in the context of a highly robust and multi-faceted regulatory framework. Indeed, the payments industry is one of the most highly regulated sectors in the global economy. The industry is subject to a comprehensive legal and regulatory framework at both the state and federal levels, in addition to significant industry-led requirements.

A. Public Laws and Regulations

[10] Craig Parker, Scott Bingley, & Stephen Burgess, *The nature of small business digital responses during crises*, 33 *Information and Organization* 100487 (Dec. 2023), https://doi.org/10.1016/j.infoandorg.2023.100487

[11] Pattern, *Ecommerce Trends for 2021*, Pattern (2021), https://www.pattern.com/blog/ecommerce-trends-for-2021

[12] JPMorgan Chase Institute, Small Business Cash Liquidity in 25 Metro Areas (Apr. 2020), https://www.jpmorganchase.com/institute/all-topics/business-growth-and-entrepreneurship/small-business-cash-liquidity-in-25-metro-areas

In the United States, payments companies are subject to the following laws and regulations:

1. Consumer Protection: Electronic Funds Transfer Act, as implemented by Regulation e; Truth in Lending Act; the Credit Card Accountability and Disclosure (CARD) Act; the Unfair, Deceptive, or Abusive Acts or Practices standard.

2. Anti-Fraud: Anti-Money Laundering Act of 2020; the Bank Secrecy Act (BSA), enforced by FinCEN requires registration as Money Services Businesses (MSBs) mandatory AML/KYC controls, suspicious activity reporting; Office of Foreign Assets Control Sanctions Regulations (OFAC).

3. Privacy, Information Security & Data Protection: Graham-Leach-Bliley Act (GLBA), Federal Trade Commission Act; California Consumer Protection Act/ California Privacy Rights Act; other states' privacy statutes.

4. Operational Resilience & Risk Management: GLBA Safeguards Rule; Interagency Guidelines on Information Security; state cybersecurity regulations

5. Cross-Border Payments: Bank Secrecy Act, FinCEN Cross-Border Guidance, and OFAC Regulations, Interagency Guidance on Cross-Border Funds Transfers.

6. Licensing and Market Entry: Nearly every state requires businesses that transmit money – whether through digital wallets, exchanges, peer-to-peer apps or bill payment services – to obtain a state-specific money transmitter license via the Nationwide Multistate Licensing System (NMLS) or direct application, with requirements including surety bonds, minimum net worth, AML/KYC compliance, and ongoing reporting.

Taken together, these laws impose comprehensive requirements on the activity of the payments industry.

B. Industry Self-Regulation

In addition to the policy framework, the payments industry and its members have led in self-regulatory efforts, including the development of technology and self-regulatory programs designed to protect the integrity of the payments ecosystem and the consumers and businesses that rely on it with every transaction.

The major card networks all have rules designed to promote efficiency, ensure security, protect consumers, and foster trust. Among other things, these rules cover chargeback thresholds, fraud monitoring programs, data security mandates, and merchant underwriting standards.

The industry also participates in the Payment Card Industry Security Standards Council which, has created the PCI Data Security Standard (PCI-DSS). The PCI-DSS is focused on the security of

cardholder data and sets forth requirements designed to ensure that companies that process, store, or transmit credit card information maintain a secure environment for such data. In addition, the PCI-DSS establishes a framework for implementation of the data security standards, such as assessment and scanning qualifications for covered entities, self-assessment questionnaires, training and education, and product certification programs.

Similarly, the industry created and participates in EMVCo. EMVCo engages and collaborates with hundreds of industry stakeholders, technical bodies and regulators to develop specifications that support innovation and address marketplace needs. The work results in specifications used across the payments industry to create products and services that deliver trusted and convenient payments for merchants and consumers around the world.

In addition, ETA members have developed due diligence programs to prevent fraudulent actors from accessing payment systems, to monitor the use of those systems, and to terminate access for network participants that engage in fraud. Working with its members and industry and government stakeholders, for example, ETA has published and subsequently updated various guidelines that provide underwriting and diligence best practices for merchant and risk underwriting, including the "Guidelines on Merchant and ISO Underwriting and Risk Monitoring" and "Payment Facilitator Guidelines."

IV. Regulating for the Present and the Future

As the payments industry rapidly evolves, the regulatory framework that exists continues to be highly relevant. The comprehensive system in place, covering market entry, consumer protection, fraud, privacy, and operations applies in full force to the industry as it exists today as it did to the payments industry of the past.

Although technology evolves – and will continue to evolve at a rapid pace – regulation that focuses on activity (as opposed to the technology itself) will continue to be relevant and timely. Maintaining that focus – applying the existing legal framework to activity – will ensure that consumers remain protected, institutions remain sound, and innovation continues to deliver on its promise.

Although new legislation is largely unnecessary, there are two areas in which Congress could act to strengthen the existing framework. The first is in the area of frauds and scams – an intense area of focus for the payments industry and an area in which federal partnership could strengthen existing efforts. The second is by creating a uniform national standard in the area of artificial intelligence - where inconsistent legal frameworks in the states threaten to derail the promise of the technology before it fully takes off.

A. Fighting Fraud and Scams

Willie Sutton said he robbed banks because that's where the money was. Throughout the history of the movement of money, bad actors have tried to intervene, although frauds and scams in payments have changed and evolved as technology evolved. Each major shift in how we pay has created new attack surfaces, pushing fraudsters to adapt faster, become more organized, and increasingly exploit human behavior rather than technical flaws alone. Fighting payments fraud and scams has always been an integral part of the digital payments ecosystem - as the threats become more sophisticated and increase at an alarming pace, education must be combined with technology to effectively fight back.

1. The Evolving Threat Landscape

Payments fraud and scams are rising not just in volume but in sophistication – posing an increasing threat to consumers and the payments industry. Leveraging sophisticated tech like AI and deepfakes, synthetic IDs, texts that mimic trusted sources, and sophisticated phishing and traditional social engineering, fraudsters are searching for technological vulnerabilities and exploiting human vulnerabilities. Authorized Push Payment (APP) fraud, Realtime payment scams, First-party fraud, and synthetic identity fraud are increasingly outpacing traditional card-based fraud.

a. Fraud

While fraud has always existed in payments, today it is increasingly driven by identity and account compromise rather than traditional card misuse. According to Euromonitor, during 2025 in the U.S. the payments industry saw an estimated $24.2 billion in fraud; globally payment card fraud topped $35 billion.[13]

In the U.S. last year, over 20% of consumers faced fraud threats. Most of those came through digital commerce. Approximately 92 percent of card fraud occurs in online or remote transactions, and card-not-present fraud accounts for roughly 81 percent of all card fraud cases worldwide, according to Euromonitor. At the same time, account-based fraud is growing faster than card fraud, particularly across real-time payments and peer-to-peer platforms.

Synthetic identity fraud, which combines real and fabricated personal data to create new identities, represents a significant share of unsecured credit losses and often remains undetected for years. First-party or "friendly" fraud and new account fraud further contribute to rising losses across e-commerce and digital banking.

[13] *2025 Global eCommerce Payments & Fraud Report,* Visa

The financial impact is substantial. In the United States, consumers reported more than $12.5 billion in fraud losses in 2024, a 25 percent increase year over year[14], and U.S. merchants are estimated to have lost approximately $7.5 billion to credit card fraud in 2025, driven largely by e-commerce transactions.[15]

Fraud attempts are even more widespread. Seventy-nine percent of U.S. organizations experienced attempted or actual payments fraud in 2024[16], with business email compromise cited by 63 percent as the most common fraud vector. On the consumer side, approximately 41 percent of U.S. adults report having lost money to fraud, and globally, a fraudulent card transaction now occurs roughly every fourteen seconds.[17]

b. Scams

We are also seeing a dramatic rise in scams, as bad actors exploit human vulnerability. In a typical scam, the thief pretends to be someone trusted – such as the IRS or Social Security, your bank, a tech-support agent, or a loved one – to pressure consumers into sending money or giving personal information. In 2025, Americans collectively lost $64 billion to scams with over 70% of adults reporting exposure and affected individuals losing an average of $1,000 per scam event.[18] Worldwide, scams cost an estimated $400 billion.[19]

The most common scams are a) imposter scams, b) identity theft & account takeover where scammers steal personal information (SSNs, credit card, or banking info) via phishing, mail theft, or breaches, then assume your identity to open accounts or make transactions and c) Phishing (email) and smishing (text) where scammers use fake emails or texts that mimic banks, retailers, employers, or government agencies, prompting you to click malicious links or share credentials and d) high-return investment scams, especially utilizing digital assets.

Financial scams succeed largely because they exploit fundamental aspects of human psychology and behavior, focusing on fear, greed, and empathy. The actual payment is typically the last step in the scam. At this point, the victim is committed to sending money to the scammer, convinced by the deception perpetrated on them.

---

[14] Federal Trade Commission, New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024 (Mar. 10, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

[15] Navarrete, J., $15 Billion in Chargeback Fraud Looms Over Businesses in 2025, GetVMS (Oct. 13, 2025), https://www.getvms.com/15-billion-in-chargeback-fraud-looms-over-businesses-in-2025/

[16] AFP Payments Fraud and Control Survey Report, April 15, 2025

[17] Ianzito, C., *4 in 10 Americans Have Lost Money to Fraud, AARP Survey Finds*, AARP (Apr. 21, 2025), https://www.aarp.org/money/scams-fraud/fraud-awareness-survey-2025/

[18] Feedzai & Global Anti-Scam Alliance, *Global State of Scams Report 2025* (2025), https://www.feedzai.com/resource/global-state-of-scams-report-2025/

[19] Ibid.

2. Industry's Continuous Vigilance

The payments industry recognizes the severity of the threat posed by fraud and scams and has responded with massive investments in prevention. In 2025 alone, the payments industry spent billions on fighting fraud and scams through a multi-layered, holistic approach. This includes heavily leveraging tokenization, encryption, biometrics, artificial intelligence, real-time analytics for advanced detection, boosting industry-wide collaboration and data sharing, enhancing employee and consumer awareness training, and strengthening controls across all channels.

Across the industry, merchants and financial services organizations collectively spend an estimated $9.3 billion annually[20] on fraud detection and prevention tools. Global expenditures on emerging AI technologies for fraud and risk management are projected to reach $50 billion by 2026[21], reflecting the imperative for more sophisticated defenses. One system alone blocked over 20.9 million fraudulent transactions during Black Friday and Cyber Monday in 2024, with an estimated value of $917 million prevented in fraudulent charges.[22]

These investments demonstrate the industry's recognition that addressing fraud and scams is core to consumer trust and the integrity of payment systems. However, it is clear that a holistic set of solutions is needed to adequately address this challenge.

3. The Need for Coordinated Collaboration

Combating increasingly sophisticated, well-resourced criminals, including state-sponsored actors, requires a collective effort beyond just financial institutions, involving telecom companies, social media platforms, policymakers, and law enforcement to disrupt fraud and scams at their source. Consumers share in the responsibility and must also be educated on red flags, suspicious links, and the importance of securing personal information, recognizing that knowledge and vigilance are key defenses against the common threat of fraud and scams.

The payments industry already works regularly with federal and state governments, including FinCEN, and OFAC, as well as law enforcement to fight fraud and scams. Through these efforts, payments industry participants share millions of data points, emerging technologies, and best practices. The collaboration allows industry participants to deploy risk-based frameworks and transaction-level monitoring, enabling early detection and deterrence of fraud and scams.

---

[20] Juniper Research, *Online payment fraud detection spend to reach $9.3 billion by 2022, driven by IoT and 3-D Secure* (July 25, 2017), https://www.juniperresearch.com/press/online-payment-fraud-detection-spend-to-reach-93-billion-by-2022-driven-by-iot-and-3-d-secure/

[21] Sydorenko, I., *Agentic AI in Financial Services: A Research Roundup for 2026*, Neurons Lab (Dec. 30, 2025), https://neurons-lab.com/article/agentic-ai-in-financial-services-2026/

[22] Stripe, *Businesses Processed More Than $31 Billion on Stripe from Black Friday Through Cyber Monday* (Dec. 3, 2024), https://stripe.com/newsroom/news/bfcm2024

Even with these efforts, more can be done. Although collaboration exists, it is frequently siloed. ETA supports strengthening coordinated collaboration between policymakers and industry to combat fraud and scams. Any effort must be guided by principles of shared, cross-sector responsibility; the need for technology-neutral standards that can adapt as threats evolve; and collaboration between domestic and international law enforcement.

To operationalize this approach, ETA supports targeted legislation, like the bipartisan, bicameral *Task Force for Recognizing and Averting Payment Scams Act* ("TRAPS") that formalizes cross-sector collaboration, strengthens information sharing, and enhances national coordination to prevent and disrupt payment scams. It is clear that a holistic, collaborative approach to fighting fraud and scams is needed to continue to strengthen resilience against scams and fraud across all payment networks, while preserving agility for innovation.

B. A Uniform National Standard for Artificial Intelligence in Payments

1. Artificial Intelligence in Payments

The use of artificial intelligence in payments is subject to an extensive and well-established federal regulatory framework. Payments providers must comply with federal consumer protection statutes, including the Electronic Funds Transfer Act, Truth in Lending Act, Equal Credit Opportunity Act, and Fair Credit Reporting Act, as well as the prohibition on unfair, deceptive, or abusive acts or practices.

Supervised financial institutions are also required to manage model risk through documented development, validation, and ongoing monitoring, regardless of whether decision-making systems rely on traditional models or advanced AI techniques. [23] When payments companies rely on third-party AI vendors, existing guidance requires robust oversight across the full vendor lifecycle.[24] In addition, payments providers remain subject to federal rules governing data security and privacy under GLBA and to anti-money laundering and sanctions requirements under the Bank Secrecy Act. As a result, AI-supported payments activities are already meaningfully regulated at the federal level.

2. State-Level AI Legislation Is Creating Regulatory Fragmentation for National Payments Providers

[23] Federal Reserve SR11-7, Guidance on Model Risk Management (Apr. 4, 2011); OCC Bulletin 2011-12, Sound Practices for Model Risk Management (Apr. 4, 2011); FDIC FIL-22-2017, Adoption of Supervisory Guidance on Model Risk Management (June 7, 2017).
[24] Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed. Reg. 37916 (June 9, 2023); CFPB Bulletin 2016-02, Service Providers (Oct. 31, 2016).

Nonetheless, states have begun to enact AI legislation outside of existing federal financial regulatory frameworks. In 2025 alone, all 50 states introduced AI-related bills, reflecting a decentralized approach to regulating AI technology that varies widely in scope, terminology, and compliance obligations. Some enacted laws are relevant to payments. For example, Colorado adopted legislation imposing obligations on the use of certain "high-risk" AI systems in consequential decision-making, while California enacted requirements applicable to large AI model developers related to safety planning, critical incident reporting, and whistleblower protections.[25]

As additional states pursue similar but non-uniform approaches, nationally operating payments companies face a growing patchwork of definitions, reporting standards, risk assessments, and enforcement regimes. This fragmentation increases compliance costs, complicates operations across state lines, and creates uncertainty for consumers and merchants, without clear evidence of improved consumer protection or risk mitigation.

3. ETA Policy Recommendation: Federal Leadership for a Uniform National AI Framework

For these reasons, ETA supports the establishment of a uniform national framework for artificial intelligence that applies consistently across jurisdictions and provides clarity for consumers, merchants, and payments providers. Payment systems operate on a national scale, and effective oversight depends on consistent rules rather than a state-by-state approach.

A federal framework should be risk-based, technology-neutral, and focused on real-world outcomes. It should build on existing federal consumer protection, safety and soundness, and financial integrity regimes, rather than layering new, duplicative compliance requirements on top of them. By establishing a clear national standard, Congress can protect consumers, preserve competition, and enable the responsible deployment of AI in payments. Absent federal action, continued regulatory fragmentation will impede innovation, raise costs, and weaken confidence in the payments system without delivering corresponding public benefits.

Conclusion

The digital payments industry is innovative, dynamic, competitive, highly regulated, and focused on delivering cutting-edge, convenient, safe, and affordable payments and fraud prevention products and services. The payments ecosystem is critical to our nation's economy, providing the infrastructure that supports financial stability, small business growth, job creation, and economic resilience. The benefits the digital payments industry delivers are

[25] Consumer Protections for Artificial Intelligence (Colorado AI Act), SB 24-205, CO Rev Stat §§ 6-1-1701–1707 (2024); Transparency in Frontier Artificial Intelligence Act, Cal. Sen. Bill 53 (2025–2026 Reg. Sess.) (enacted Sept. 29, 2025).

enormous, promoting entrepreneurship, helping small businesses compete, and providing high-paying jobs and access to products and services that help Americans make ends meet when they need it most.