

## **The Electronic Transactions Association**

### **2026 Federal Legislative and Regulatory Policy Priorities**

The digital payments industry is one of the most innovative, dynamic, and competitive sectors in the American economy—and also one of the most highly regulated. Built on sophisticated, interconnected infrastructure, it delivers secure, reliable financial products and services that drive economic growth, empower small businesses, and expand opportunities for consumers. These services are not only safe and highly secure; they are essential to advancing financial inclusion by ensuring that all consumers—including those historically underserved or excluded—can access and participate in everyday financial activity.

ETA supports a policy environment that protects consumers while enabling innovation, competition, and continued investment in modern payments technology. Smart, forward-looking policy is critical to preserving consumer choice, strengthening economic participation, and making true financial inclusion a reality for millions of Americans.

ETA's policy priorities for 2026 include:

**Interchange and the Credit Card Competition Act** – ETA broadly opposes interchange legislation, including the Credit Card Competition Act (CCCA), that mandate routing requirements and/or regulating interchange rates. These policies would undermine the security, reliability, and consumer-protection features that card networks and issuers currently fund through interchange revenue. They would shift costs rather than reduce them, placing downward pressure on the industry to for fraud prevention, credit availability, rewards programs, and cybersecurity investments that help protect both merchants and consumers. These policies would reduce consumer choice and weaken the economic model that supports the fast, secure, reliable, open, and widely-accepted payments infrastructure.

ETA opposes legislation that seeks to negatively affect the current interchange framework and process.

ETA supports policy efforts that:

- **Preserve Market Competition:** Allow competitive forces to drive pricing, innovation, and value creation
- **Protect Consumer Choice:** Ensure consumers retain access to diverse payment options and the benefits they provide
- **Encourage Innovation:** Maintain an environment where investment in new payment technologies and security measures can flourish

**Interchange and the Credit Card Competition Act** – ETA broadly opposes interchange legislation, including the Credit Card Competition Act (CCCA), that mandate routing requirements and/or regulating interchange rates. These policies would undermine the security, reliability, and

consumer-protection features that card networks and issuers currently fund through interchange revenue. They would shift costs rather than reduce them, placing downward pressure on the industry for fraud prevention, credit availability, rewards programs, and cybersecurity investments that help protect both merchants and consumers. These policies would reduce consumer choice and weaken the economic model that supports the fast, secure, reliable, open, and widely-accepted payments infrastructure.

ETA opposes legislation that seeks to negatively affect the current interchange framework and process.

ETA supports policy efforts that:

- Preserve Market Competition: Allow competitive forces to drive pricing, innovation, and value creation
- Protect Consumer Choice: Ensure consumers retain access to diverse payment options and the benefits they provide
- Encourage Innovation: Maintain an environment where investment in new payment technologies and security measures can flourish

**Artificial Intelligence in Payments** – AI, including generative AI and agentic AI, is rapidly becoming operational infrastructure across the U.S. payments system, powering fraud detection, dispute resolution, onboarding, customer service, and risk management. Policymakers should ensure that AI governance aligns with the existing federal financial regulatory framework rather than creating duplicative or conflicting requirements that hinder innovation or reduce consumer protection.

ETA supports policy efforts that:

- Maintain a consistent national framework by avoiding state AI mandates that conflict with federal requirements.
- Recognize and rely upon the existing body of federal laws and standards that already govern AI, including consumer protection, data privacy, transparency, and explainability.
- Apply risk-based, technology-neutral oversight that focuses on outcomes and accountability rather than specific AI techniques.
- Support responsible deployment of AI and agentic workflows through clear guardrails, human oversight, and safeguards against model or agent drift and bias.
- Promote a balanced liability framework for developers and deployers of AI systems.

**Bank Charters and Payments Innovation** – The federal banking agencies are reassessing aspects of the US chartering framework, including the treatment of novel bank applicants and the eligibility criteria for access to Fed master account services. These deliberations occur against the backdrop of increasing industry interest in de novo charters. ETA supports innovation but recognizes that changes to eligibility for Fed services and the expansion of novel charter types could have material and systemic effects across the payments industry. Therefore, ETA believes that any contemplated changes to charter policy or master account access must proceed through transparent, inclusive,

and procedurally sound processes, including full public notice-and-comment. Only through open rulemaking can the agencies produce durable, equitable outcomes that maintain confidence in the regulatory framework and support long-term industry innovation.

ETA supports policy efforts that:

- Promote competition, financial stability, and safe and sound financial institutions.
- Ensure transparency, timeliness, and procedural fairness in the chartering process, including clear criteria for evaluating novel applications.
- Clarify access to essential Fed services for eligible depository institutions, including clear standards governing master account applications, appeals, and supervisory expectations.
- Apply the principle of “same activity, same risk, same rules” to any new charter types or novel institutions seeking access to Fed services, ensuring competitive neutrality and a level regulatory playing field.

**Payment Stablecoins and Tokenized Deposits Rules** – Payment stablecoins and tokenized deposits offer new opportunities for the payments industry. To ensure these innovations develop responsibly, policymakers need to adopt clear and consistent frameworks and definitions that integrate them into the regulated financial system without inhibiting technological progress.

ETA supports policy efforts that:

- Establish comprehensive, risk-proportionate regulatory frameworks for payment stablecoins and tokenized deposits that ensure safety, soundness, operational resilience, and consumer protection.
- Provide clear standards for reserve assets, issuance and redemption practices, governance, and transparency.
- Encourage regulatory coordination across agencies and jurisdictions to reduce fragmentation and promote a coherent national approach.
- Ensure consistent treatment across entities and products through a “same activity, same risk, same regulation” approach.

**Payments Fraud & Scams** – The payments industry invests billions each year in advanced security tools that make digital payments among the safest ways to transact. As fraud and scams evolve, policymakers should strengthen national coordination, support public-private information sharing, and preserve the flexibility needed for providers to deploy emerging fraud-prevention technologies. That is why ETA strongly supports the Taskforce for Recognizing and Averting Payment Scams Act (TRAPS Act), which would improve information sharing between industry and law enforcement, and represents an important step towards a more unified anti-fraud/scam strategy.

To further advance these goals, policymakers should:

- Support consumer education and ensure awareness efforts are a national priority, helping individuals recognize and avoid scams before harm occurs.

- Improve information sharing between industry and government, including law enforcement, so emerging scam typologies and cyber threats can be identified and mitigated quickly.
- Encourage robust industry standards and best practices, such as the *ETA Underwriting and Risk Monitoring Guidelines*, which evolve to address new fraud trends and support consistent risk management across the ecosystem.
- Preserve the ability of payments providers to innovate in fraud detection, avoiding prescriptive mandates that limit the deployment of new tools or slow responses to fast-moving threats.
- Promote adoption of advanced security technologies, including tokenization, encryption, biometrics, and continuous monitoring, to prevent fraud before it occurs.
- Support strong authentication and identity-verification practices that help prevent account takeovers, synthetic identities, and other forms of digital fraud.
- Support for increased coordination and funding for US and international law enforcement.
- Coordinating with PSP, mobile carriers and others to prevent fraud.

**Re-Authorization of CISA 2015** – ETA supports the timely reauthorization of the Cybersecurity Information Sharing Act of 2015, which remains a foundational tool for strengthening the nation’s cyber defense posture and protecting the integrity of the electronic payments ecosystem. CISA 2015 has enabled trusted, bidirectional information-sharing between the public and private sectors, allowing payments companies to receive actionable threat intelligence, rapidly identify emerging vulnerabilities, and coordinate incident responses across interconnected financial networks. Reauthorization should preserve the law’s liability protections, confidentiality safeguards, and voluntary participation framework, all of which are essential for fostering open, real-time collaboration between industry and government. ETA also supports targeted enhancements that promote more timely dissemination of indicators of compromise, modernize reporting channels, and reduce duplicative requirements across agencies. Maintaining and improving this statutory framework is critical to ensuring that payments providers can continue to protect consumers, secure financial infrastructure, and respond effectively to increasingly sophisticated cyber threats.

ETA supports policy efforts that:

- Modernize the framework in ways that enhance real-time cyber defense across the payments ecosystem.
- Preserve and strengthen liability protections for companies that voluntarily share cyber threat indicators and defensive measures, recognizing these protections as essential to transparent and timely information exchange.
- Expand and streamline channels for operational intelligence sharing, including automated, machine-readable feeds and sector-specific updates tailored to financial and payments infrastructure.
- Harmonize incident-reporting obligations across federal agencies, reducing duplicative or conflicting timelines that burden payments providers without improving security outcomes.
- Ensure agencies share indicators of compromise and mitigation guidance as close to real time as possible, including during active events.

- Enable more robust public-private collaboration exercises, updated joint playbooks for ransomware and payment-fraud-related threats, and continued protections for shared proprietary or sensitive operational data.

**Regulation E** – Regulation E establishes liability and error-resolution requirements for electronic fund transfers, including many modern payment methods. As policymakers consider changes related to fraud trends and evolving consumer expectations, it is important to maintain a framework that protects consumers while supporting innovation and the integrity of the payments system.

ETA supports policy efforts that:

- Maintain the existing Regulation E rules for unauthorized transactions and avoid expanding it to include authorized transactions where the consumer has initiated the payment.
- Address the root causes of fraud through improved consumer education, industry collaboration, law-enforcement partnerships, and tools that prevent fraud before it occurs.
- Encourage coordinated efforts across the ecosystem to reduce fraud while preserving fast, convenient, and low-cost payment options for consumers.

**Personal Financial Data Rights Rule** – Open banking has the potential to improve payments, expand consumer choice, and enhance financial transparency. To succeed, the CFPB’s financial data rights rule must prioritize clarity and security and be workable across the diverse payments ecosystem. ETA supports open banking policies that reflect the market realities associated with the Personal Financial Data Rights rulemaking and that promote durable, consumer-centric implementation.

ETA supports policy efforts that:

- Provide a principles-based framework with regulatory clarity on key issues such as the scope of “representative,” fees, and data access rights.
- Rely on private-sector innovation and secure, standardized APIs – phasing out screen scraping in favor of interoperable, tokenized data sharing.
- Center consumer control through strong authorization, revocation, security, and privacy protections.
- Align obligations with entities that hold or control consumer financial data, avoiding unnecessary or duplicative requirements on intermediaries.
- Ensure consistent national standards and realistic, phased compliance timelines that reduce litigation risk and support stable industry implementation.

**Privacy and Identity Standards** - Protecting consumer privacy is a crucial element of maintaining trust in the payments industry, which has a long history of privacy protection consumer privacy. The industry is focused on fighting fraud and identity crime and is continuously developing and deploying new technologies to detect and deter fraud. ETA supports a uniform national privacy law that is principles based and harmonized to ensure predictability and consistency for consumers. Privacy laws must also ensure that the industry can continue to use data in order to fight fraud and protect consumers.

ETA supports data privacy standards that:

- Provision for permissible uses of data to prevent fraud and protect consumers
- Establish reasonable consumer rights to access and request correction or deletion of personally identifiable information
- Maintain the appropriate enforcement regime, which strikes a balance between consumer protection and fostering innovation.
- Promote harmonized and reasonable data breach notification schemes.

**Continuation of USMCA** – In 2018, the United States, Mexico, and Canada ratified the USMCA trade agreement. USMCA is scheduled for the first joint review in 2026 of the USMCA, ETA encourages all three countries to continue the agreement. USMCA address key areas affecting the payments industry, including digital trade, data flows, privacy, and financial services - areas that directly affect the operational environment for payments and fintech companies.

ETA supports continuation of USMCA and policy efforts that:

- Preserve seamless data movement, encourage innovation in digital payments, avoid fragmented regulatory requirements, and protect the ability of payments providers to operate efficiently across North America.

**Patent Reform** – ETA believes strong patent reform is essential to safeguarding innovation, competition, and domestic economic security. Accordingly, ETA supports policies that:

- Preserve robust, science and law driven patent-validity review procedures - including inter partes review and other PTAB processes - to ensure that companies can challenge weak or invalid patents before expert patent judges rather than being forced into costly, inefficient jury litigation.

**Cannabis Banking** – ETA supports the passage of legislation that resolves the conflict between state and federal laws to allow payment companies to serve cannabis businesses and the ancillary businesses that are relied upon to operate in states where those businesses are legal under state law.