Written Testimony before the House Financial Services Committee
Subcommittee on Financial Institutions

Joseph J. Schuster
Partner
Ballard Spahr LLP

Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions

March 5, 2026

Table of Contents

Page

I. Introduction

Chairman Hill, Ranking Member Waters, and Members of the Committee:
Thank you for the opportunity to testify at today's hearing, *Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions*.

I am a partner in Ballard Spahr LLP's Consumer Financial Services Group, where I advise banks, credit unions, payments companies, and technology providers that support financial institutions on federal and state consumer financial laws. A substantial portion of my practice is devoted to fraud-related matters, including payments fraud, identity-based fraud, account takeover, check and wire fraud, scam typologies, loss allocation, and the operational and legal frameworks governing fraud detection and response. I previously served as a Managing Director and Senior Counsel at Goldman Sachs Bank USA, which provided me with direct, in-house experience navigating the practical and operational realities financial institutions face in complying with the legal frameworks discussed today.

I regularly work not only with financial institutions themselves, but also with the technology companies that design and deploy fraud detection systems, identity verification tools, behavioral analytics, and information-sharing utilities. Fraud prevention today is a coordinated effort that depends on financial institutions, their service providers, and inter-institution collaboration.

These efforts take place within a layered legal and supervisory framework. Fraud prevention is shaped not only by statutory regimes, such as the Electronic Fund Transfer Act, Truth in Lending Act, Fair Credit Reporting Act, Expedited Funds Availability Act, Gramm-Leach-Bliley Act, and the Bank Secrecy Act, but also by regulatory guidance, supervisory expectations, and the practical realities of examinations and investigative oversight. Financial institutions must navigate compliance reviews, model risk expectations, fair lending considerations, UDAAP standards, vendor oversight, and cybersecurity requirements while simultaneously responding to increasingly sophisticated and fast-moving fraud threats.

In addition, financial institutions must navigate state consumer protection statutes, state privacy, data usage, and artificial intelligence laws, and state-level enforcement authorities, which may impose additional or overlapping requirements. The interaction between federal and state law can create uncertainty in areas such as information sharing, funds availability practices, fraud-related holds, consumer dispute handling, and use of advanced analytics. Institutions operating nationally must reconcile these overlapping regimes while responding to fraud schemes that do not respect jurisdictional boundaries.

My testimony today reflects a legal practitioner's perspective across institutions of varying sizes and business models. Fraud has evolved rapidly in recent years. At the same time, many elements of the legal and supervisory framework were developed in an era when

fraud was slower, more siloed, and less technologically coordinated. The result is a growing tension between the speed and scale of emerging fraud trends and the structure of the regulatory architecture governing prevention efforts.

I appreciate the Committee's attention to these issues and look forward to discussing how policymakers can support effective fraud mitigation while preserving consumer protections, privacy, and fair access to financial services.

II. Emerging Fraud Trends Affecting Financial Institutions

Fraud is not a new phenomenon. Many of today's schemes are variations on themes that have existed for decades (*e.g.*, impersonation, forged instruments, confidence scams, and theft. What is new is how fraud is executed). Fraud is increasingly *industrialized, technology-enabled, cross-channel, and scalable*, with sophisticated coordination among actors and rapid adaptation to controls. In practice, that means financial institutions are confronting fraud that moves faster, spreads more quickly, and exploits seams between legal frameworks, payment rails, and institutional boundaries.

a. Check Fraud

Although checks are a longstanding payment instrument, check fraud has re-emerged as an "emerging trend" because the threat model has changed. Historically, check fraud often involved localized forgery or counterfeit checks presented in person. Today, the combination of organized theft, digital alteration tools, remote deposit channels, and predictable funds-availability timelines has created a materially different risk environment.

Key modern check-fraud typologies include:

1. **Mail Theft and Check Interception at Scale.**
   Organized criminal groups increasingly steal checks from mailboxes and postal facilities, exploiting the continued reliance of many consumers, small businesses, and government agencies on checks. Once obtained, checks can be altered, counterfeited, or used as templates to create additional fraudulent items.

2. **Check Washing and Alteration Using Modern Tools.**
   "Check washing" is not new, but it has become more scalable and precise. Fraudsters use readily available chemical and digital techniques to remove or modify payee names and amounts. In parallel, higher-quality imaging and printing technology makes counterfeit checks and altered items more convincing and more difficult to detect through traditional visual review.

3. **Remote Deposit Capture and Mobile Deposit Exploitation.**
   Remote deposit channels reduce friction for legitimate customers, but they also enable fraudsters to deposit altered or counterfeit items without the traditional

controls present in branch environments. A fraudulent item can be deposited quickly, sometimes across multiple institutions, before the receiving institution can validate authenticity.

4. **Funds Availability Timing and "Float" Exploitation.**
   Fraudsters are highly attuned to the gap between (i) when deposited funds become available and (ii) when final settlement and return processes confirm an item is fraudulent or uncollectible. That timing gap can be exploited to withdraw or transfer funds before the loss is identified. This dynamic is particularly challenging because institutions must balance the need to make funds available promptly for legitimate customers against the risk of subsidizing fraud.

5. **Account Opening and Mule Accounts Supporting Check Fraud.**
   Check fraud is often paired with "mule" accounts, which are accounts opened or controlled by fraud networks to receive proceeds and rapidly move funds. The growth of synthetic identity tools and compromised credentials has made mule-account creation easier, which in turn supports the scale of check fraud.

These modern conditions mean check fraud is not simply a "return to an old risk." It is an example of how longstanding schemes become "emerging" again when new channels, new tooling, and new operational constraints change the economics of fraud.

b. Social Engineering: Fraudulent Inducement at Scale

A defining feature of current fraud is the rise of scams in which consumers are manipulated into authorizing payments or disclosing credentials. This category of fraud is particularly difficult because the customer's action may appear "authorized" (and sometimes *are* "authorized") from a technical standpoint, even though it is the product of deception or coercion.

Common scam typologies include:

1. **Impersonation Scams.**
   Fraudsters impersonate banks, government agencies, law enforcement, employers, utilities, or well-known brands. They use phone spoofing, fake emails, cloned websites, and sometimes deepfake audio or video to appear credible. These scams often pressure consumers into urgently moving funds to "safe accounts" or providing one-time passcodes.

2. **Account Takeover Combined with Consumer Manipulation.**
   Fraudsters compromise credentials through phishing, malware, credential stuffing, SIM swaps, or social engineering. They then use the account access to initiate transfers, update contact information, or add payees. Sometimes they interact

directly with the consumer while simultaneously acting within the account, which can reduce the likelihood of timely intervention.

3. **Investment and Cryptocurrency Scams.**
   These scams leverage social media, messaging apps, and online advertising to lure consumers into fraudulent investment opportunities. The use of crypto exchanges and off-platform communications can complicate recovery and investigative pathways. Often, the initial "returns" shown to consumers are fabricated to induce larger transfers.

4. **Romance, Employment, and "Task" Scams.**
   Romance scams exploit personal trust. Employment and task scams offer "jobs" that require consumers to send funds, purchase gift cards, or move money through their accounts. These scams can generate multiple transfers over time, increasing total losses.

5. **Invoice and Business Email Compromise (BEC).**
   BEC schemes target businesses and individuals through spoofed or compromised email accounts, manipulating recipients into sending wires or ACH payments to fraudulent accounts. These schemes often rely on careful timing, knowledge of business relationships, and plausible documentation.

Modern scams are not isolated events. They are often multi-step playbooks. Fraudsters test a consumer's susceptibility, escalate pressure, and then route funds through mule networks. These scams create acute consumer harm, and they also impose operational and reputational costs on institutions even where the institution is not the ultimate bearer of the loss.

c. Fraud in Faster Payments and Cross-Rail Exploitation

As payment rails accelerate, fraud has adapted to exploit the reduced time available to detect and interrupt transactions. Faster payments improve efficiency and customer experience, but they also compress decision windows. In many cases, once funds are transmitted and received, recovery rates decline sharply. Even when a fraud scheme begins with a check deposit, card transaction, or account takeover, proceeds are often quickly transferred into faster rails (*e.g.*, ACH, real-time payments (RTP), wire transfers, or peer-to-peer platforms) and then dispersed across multiple accounts.

Key emerging typologies in faster-payment fraud include:

1. **Immediate Funds Availability and Settlement Compression.**
   Faster rails reduce float and settlement delays that historically provided time for review, verification, and potential intervention. Fraudsters exploit immediate funds availability by structuring transfers to minimize review triggers and rapidly

withdrawing or transferring funds once credited. Once funds are withdrawn in cash, converted to digital assets, or moved offshore, recovery rates decline significantly.

2. **Authorized Push Payment (APP) Fraud and Fraudulently Induced Transfers.** In APP fraud patterns, a consumer initiates the payment, often in real time, after being deceived through impersonation, investment, emergency, or account-security scams. From a technical standpoint, authentication protocols may be satisfied. However, the authorization is obtained through manipulation or coercion. The speed of faster-payment rails means that funds may be credited and made available almost immediately, leaving only a narrow opportunity to detect anomalies or interrupt the transfer before onward movement.

3. **Rapid Cross-Rail Movement to Defeat Recovery Mechanisms.** Fraud schemes frequently involve layering transactions across multiple rails. For example, proceeds from a compromised account may move from ACH to real-time payment, then to wire transfer, and ultimately to cash-out or conversion. Each rail has its own dispute, recall, and return processes, and rapid cross-rail movement is designed to outpace these mechanisms. This fragmentation complicates recovery and reduces the likelihood that any single institution can halt the full scheme. The result is a fragmentation of visibility, where no single institution sees the entire lifecycle of the fraud event.

4. **Multi-Institution Mule Networks and Asymmetric Information.** Fraud actors leverage networks of mule accounts across multiple financial institutions. The sending institution may have limited visibility into whether the receiving account is newly opened, previously associated with fraud, or linked to suspicious device identifiers. Similarly, the receiving institution may lack context about the originating transaction. This asymmetric information combined with limited cross-institution sharing of device, network, or behavioral indicators creates exploitable gaps.

5. **Exploitation of Confirmation and Identity Gaps.** Inconsistent implementation of payee verification, beneficiary confirmation, and account-validation tools can create confirmation gaps. Fraudsters direct victims to send funds to accounts that appear legitimate but are controlled by criminal networks. Where confirmation-of-payee mechanisms are not interoperable or universally deployed, consumers may receive limited warning before initiating irrevocable transfers.

6. **Compression of Detection and Escalation Windows.** The operational reality of faster payments requires institutions to rely heavily on automated detection systems operating in real time. Manual review processes that were viable in slower settlement environments are increasingly impractical. Institutions must calibrate fraud controls to minimize false positives and consumer

friction while identifying high-risk transactions within seconds. This compressed timeline increases the importance of high-quality, timely risk signals and coordinated action across institutions.

The combination of speed, cross-rail layering, and multi-institution coordination makes faster-payment fraud particularly challenging. While faster rails are an important innovation, they alter the fraud calculus: prevention must occur earlier in the transaction lifecycle, and recovery options become more limited once funds are transmitted.

d. Identity-Centric Fraud: Synthetic Identity and Credential Abuse

Fraud increasingly hinges on weaknesses in identity proofing and authentication:

1. **Synthetic Identity Fraud.**
   Fraudsters combine real and fabricated identifiers to build "synthetic" personas that can pass certain checks. These identities may be aged over time, used to open accounts, obtain credit, and support mule networks.

2. **Credential Compromise and Account Takeover (ATO).**
   Credential theft is scaled through phishing kits, malware, and credential stuffing attacks using breached credentials. Account takeover is often paired with social engineering to defeat multi-factor authentication or to induce the consumer to disclose codes. Once access is obtained, funds are often moved quickly through multiple channels (*e.g.*, ACH, wire, instant payments, or card-based rails) frequently through networks of mule accounts.

3. **Document Fraud and Digital Identity Manipulation.**
   Fraudsters use manipulated IDs, synthetic documents, and increasingly sophisticated digital forgeries to pass onboarding checks and exploit remote channels.

III. The Challenges Financial Institutions are Facing with Emerging Fraud Trends

The fraud trends described above create operational, legal, supervisory, and economic challenges for financial institutions. These challenges are not limited to detecting individual fraudulent transactions; they implicate how institutions structure customer experience, deploy technology, allocate losses, coordinate across the financial system, and navigate overlapping regulatory regimes.

a. Balancing Fraud Prevention with Customer Experience and Access

Financial institutions must strike a difficult balance between preventing fraud and maintaining efficient, accessible services for legitimate customers. That balance is not

theoretical. It plays out in daily operational decisions across onboarding, funds availability, payment execution, and account servicing.

To combat emerging fraud trends, institutions are implementing increasingly sophisticated controls, including:

- Risk-based multi-factor authentication and step-up verification;
- Behavioral analytics evaluating device, geolocation, and transaction patterns;
- Real-time transaction monitoring systems designed to identify anomalies within seconds;
- Targeted transaction holds or outbound call-back verification for high-risk transfers;
- Enhanced identity verification and document authentication at onboarding;
- Participation in consortium-based fraud data or typology feeds where available.

At the same time, institutions are actively working to reduce unnecessary friction for legitimate customers. For example:

- Adaptive authentication limits additional verification steps to high-risk transactions rather than applying blanket requirements;
- Real-time customer alerts allow immediate confirmation or denial of suspicious activity;
- Streamlined digital onboarding processes rely on automated identity tools rather than manual documentation;
- Targeted holds are applied to specific transactions rather than entire accounts;
- Predictive analytics are continuously refined to reduce false positives.

These efforts reflect a fundamental economic reality: in a competitive marketplace, such as banking, customer experience is a key differentiator. Market economics strongly incentivize institutions to reduce fraud while minimizing friction. Consumers have choices, and institutions that impose excessive delays, unnecessary account restrictions, or repetitive authentication hurdles risk losing customers to competitors.

Fraud losses and fraud-prevention expenditures also carry broader economic consequences. Even when institutions absorb fraud losses directly, those losses affect capital allocation, operational costs, and investment decisions. Over time, fraud operates as a distributed cost across the customer base, impacting pricing, product availability, credit access, and innovation investment. Effective fraud prevention therefore serves not only institutional interests but systemic efficiency.

Accordingly, legal and regulatory frameworks should be structured to enable (rather than inhibit) good-faith fraud mitigation efforts. Institutions already possess strong commercial incentives to calibrate fraud controls responsibly. Policymaker and supervisory intent should focus on equipping institutions with the flexibility and clarity needed to deploy

proportionate, risk-based interventions without inadvertently creating new avenues for fraud or shielding fraudulent actors at the expense of legitimate customers.

b. Operating in Real Time with Compressed Decision Windows

Emerging fraud trends are unfolding in payment environments where the time available for intervention has materially compressed. Financial institutions increasingly must make high-stakes determinations about whether to allow, delay, flag, or block transactions.

This operational reality requires heavy reliance on automated systems, including machine learning models, behavioral analytics, and risk scoring. Traditional models that relied on extended manual review are often incompatible with real-time payment expectations.

The calibration challenge is significant. Systems that are overly sensitive can generate excessive false positives, increase customer friction, and elevate complaint volume. Systems that are overly permissive may allow rapid loss accumulation before controls adapt. Institutions must continuously refine detection models in response to evolving fraud typologies while documenting governance, validation, and performance.

The central dynamic confronting institutions is that fraud innovation is accelerating faster than the legal and supervisory structures designed to address it. Fraud actors increasingly leverage advanced technologies, including artificial intelligence and emerging AI agents capable of automating social engineering, credential harvesting, synthetic identity creation, and real-time transaction manipulation at scale. These tools significantly amplify the reach, speed, and sophistication of fraudulent activity. Fraud networks iterate rapidly, test vulnerabilities in real time, and operate without regulatory constraint. Financial institutions, by contrast, must respond within established statutory frameworks and supervisory expectations that were often developed for a slower and more contained threat environment. Bridging this speed and capability differential is one of the defining operational challenges in modern fraud prevention. Regulatory and oversight structures must therefore evolve in a manner that enables institutions to deploy comprehensive, technology-driven countermeasures commensurate with the commensurate technological capabilities necessary for modern fraud prevention.

c. Information Silos and Fragmented Visibility

Fraud is network-based and increasingly coordinated across institutions and platforms, yet detection often remains institution-specific.

No single institution typically sees:

- The full mule account network;
- The complete cross-rail movement of funds;
- Behavioral indicators flagged elsewhere;

- Parallel activity occurring across multiple institutions.

While limited information-sharing mechanisms exist, there is no comprehensive, real-time, legally streamlined framework for broad fraud-signal exchange across the ecosystem. As a result, institutions frequently operate with partial visibility, while fraud networks operate with coordinated intelligence.

Modern fraud networks are multi-actor, cross-institutional, and often cross-border. Tactics and scripts are shared rapidly across digital channels. Attack methods are tested, refined, and redeployed. What appears to be an isolated anomaly at one institution may be part of a broader coordinated scheme visible only when activity is viewed across the system. This asymmetry, coordinated fraud networks versus fragmented institutional visibility, remains a core structural challenge.

d. Legal and Supervisory Uncertainty

Institutions must deploy fraud controls within a layered legal and supervisory environment that was not constructed for today's real-time, cross-channel fraud ecosystem.

They must evaluate, often simultaneously:

- When fraud-related transaction holds are permissible and for how long;
- Whether funds must be made available under Regulation CC notwithstanding emerging fraud indicators, and when exception holds are appropriately invoked in light of modern check fraud dynamics;
- How Regulation E applies to fraudulent transfers;
- Whether certain fraud-signal sharing practices implicate FCRA obligations;
- How fraud detection models intersect with notice requirements and fair lending standards;
- Whether transaction denials or delays create UDAAP exposure.

Supervisory expectations introduce additional cross-pressures. Institutions may be criticized for elevated fraud losses, yet may also face scrutiny when aggressive controls increase friction or delay funds. In the context of check fraud, for example, institutions must reconcile prompt funds-availability requirements with the operational reality that altered or counterfeit items may not be identified until after provisional availability has been provided.

Navigating these competing expectations requires substantial legal analysis, documentation, governance, and resource allocation.

Even where statutory authority exists, uncertainty about supervisory interpretation can create hesitation in deploying more assertive fraud interventions. The result can be predictability that sophisticated fraud actors exploit.

e. Technology Deployment and Governance Complexity

The sophistication of modern fraud requires equally sophisticated detection tools. Artificial intelligence, behavioral biometrics, predictive analytics, and cross-channel risk scoring are increasingly essential components of effective fraud programs.

However, deploying these tools entails significant governance obligations. Institutions must address:

- Model validation and ongoing performance monitoring;
- Explainability and documentation standards;
- Vendor oversight and third-party risk management;
- Cybersecurity protections;
- Ongoing monitoring for perceived disparate impact.

Governance is critical to responsible innovation. However, legal standards should be structured to enable responsible deployment of fraud controls. They should not impose incremental costs, delays, or procedural burdens that fail to enhance consumer protection and, in practice, advantage fraud actors over legitimate financial institutions and their customers.

f. Resource Constraints for Community Institutions

Community banks and credit unions play an essential role in financial inclusion, small-business lending, and local economic stability. However, they often operate with smaller fraud teams, more limited in-house analytics capabilities, and less access to real-time typology intelligence than larger institutions. Many rely heavily on third-party vendors for fraud detection and monitoring.

Fraud actors routinely probe for the weakest point in the financial ecosystem. When smaller institutions lack access to robust information-sharing networks, cross-institution fraud signals, and scalable detection tools, they can become disproportionate targets for mule accounts, check fraud, and scam-driven payment flows.

Strengthening information-sharing frameworks and providing clear statutory safe harbors would benefit the entire financial system, but the impact would be particularly meaningful for community banks and credit unions. Broader access to shared fraud intelligence, standardized risk indicators, and legally certain collaboration mechanisms would allow smaller institutions to participate more effectively in coordinated defense efforts without bearing unsustainable compliance costs.

System-wide resilience depends on ensuring that fraud prevention capabilities are not concentrated solely in the largest institutions. When fraud losses concentrate in under-

resourced segments of the market, the consequences extend beyond individual institutions. Losses and remediation costs reverberate across the broader financial system, affecting pricing, access, and consumer trust. A framework that enables scalable collaboration and technological adoption across institutions of all sizes strengthens financial stability as a whole.

IV. Legal and Regulatory Framework Governing Fraud Prevention

a. Statutes

Several federal statutes directly or indirectly govern fraud prevention and loss allocation.

Expedited Funds Availability Act (EFAA) and Regulation CC.
Regulation CC governs funds availability schedules and check return processes. While designed to ensure timely access to funds, funds-availability requirements interact directly with modern check fraud dynamics, particularly in environments involving remote deposit capture and organized mail theft.

Fair Credit Reporting Act (FCRA).
FCRA governs the furnishing, use, and sharing of consumer report information. Fraud detection tools that rely on consortium data, negative file information, device identifiers, or certain identity-verification processes may implicate FCRA definitions of "consumer report," "furnisher," or "consumer reporting agency." Institutions must evaluate whether particular data-sharing arrangements fall within FCRA's scope and whether fraud-related decisions (*e.g.*, account closures, onboarding denials, or transaction restrictions) trigger adverse action notice requirements.

As a result of FCRA's definitions are broad and fact-specific, institutions must carefully structure fraud-information sharing and consortium participation to ensure compliance with permissible purpose, accuracy, and dispute-resolution obligations.

Equal Credit Opportunity Act (ECOA).
ECOA prohibits discrimination in credit transactions and requires creditors to provide adverse action notices when credit is denied or other adverse credit decisions are made. When fraud detection tools influence onboarding decisions, credit approvals, account access, or transaction authorizations tied to credit products, institutions must evaluate whether those decisions constitute adverse action under ECOA and its implementing Regulation B.

If an adverse action occurs, institutions are generally required to provide a statement of reasons that is specific and accurate. In fraud-related contexts, this can present operational complexity. Fraud detection models often rely on dynamic, multi-factor risk scoring, behavioral indicators, device analytics, or cross-channel typology signals.

Translating these risk determinations into clear, legally sufficient reasons for decline requires careful documentation and model governance.

Institutions must also evaluate potential fair lending implications, including whether fraud detection models could produce perceived disparate impact across protected classes. Even when a model is designed solely for fraud prevention and not credit risk assessment, its outputs may affect access to credit or account functionality, thereby implicating ECOA compliance considerations.

Gramm-Leach-Bliley Act (GLBA).
GLBA imposes privacy and safeguarding obligations, shaping how institutions collect, use, and share consumer financial information. Fraud prevention often depends on data sharing across entities and platforms, which must be evaluated against GLBA's privacy restrictions and exceptions.

Bank Secrecy Act (BSA), Anti-Money Laundering (AML), and Section 314(b).
Under the BSA, financial institutions are required to maintain anti-money laundering programs, monitor for suspicious activity, and file Suspicious Activity Reports (SARs) where appropriate. These obligations often capture fraud-related conduct, particularly when fraud proceeds are moved through networks designed to obscure origin and ownership.

Section 314(b) of the USA PATRIOT Act permits financial institutions to share information with one another, under specified conditions, for purposes of identifying and reporting activities that may involve money laundering or terrorist financing. In practice, some institutions utilize Section 314(b) frameworks to facilitate limited information sharing related to fraud schemes that may also implicate financial crime concerns.

However, Section 314(b) is structured around AML objectives and includes procedural and definitional limitations. As fraud schemes increasingly overlap with money movement typologies traditionally associated with AML risk, institutions must evaluate carefully how and when fraud-related information sharing fits within the 314(b) safe harbor framework.

Electronic Fund Transfer Act (EFTA) and Regulation E.
EFTA establishes consumer protections for electronic fund transfers, including error resolution procedures and liability limitations for unauthorized transactions. In practice, Regulation E plays a central role in how institutions allocate losses arising from account takeover and certain types of fraudulently induced transfers. Institutions must evaluate whether a transaction qualifies as "unauthorized," the timeliness of consumer notice, and the scope of required investigation and credit.

Truth in Lending Act (TILA) and Regulation Z.
For credit card transactions, TILA provides liability limitations for unauthorized use and establishes billing error procedures. As fraud increasingly spans debit, credit, and hybrid

products, institutions must apply different statutory frameworks depending on product structure (even when fraud typologies are operationally similar leading to differing outcomes depending on the product involved in the fraud).

b. Regulatory Guidance

Beyond statutory text, regulators have issued guidance addressing fraud risk management, cybersecurity, third-party oversight, and model governance.

Federal banking agencies have articulated expectations regarding:

- Risk-based authentication and layered security programs;
- Information security standards and safeguarding obligations;
- Third-party vendor management and oversight;
- Model risk management frameworks for advanced analytics;
- Consumer compliance management systems.

Agencies have also issued statements, interpretive guidance, and frequently asked questions addressing payments fraud, faster-payment systems, scam typologies, and consumer dispute obligations. While these materials provide important supervisory context, they are often issued outside of formal notice-and-comment rulemaking processes.

In some instances during the prior administration, interpretive guidance and FAQs were viewed by institutions as expanding statutory frameworks beyond their original scope. For example, FAQs interpreting EFTA and Regulation E addressed fraudulently induced transfers in ways that some institutions believed extended liability expectations beyond the statutory text, without formal rulemaking. Similarly, interpretive positions under Regulation Z were perceived as potentially extending coverage to products or operational practices not clearly contemplated by the statute or implementing regulation.

These developments contribute to interpretive uncertainty. Institutions must navigate evolving guidance while ensuring compliance with statutory text, and must assess whether informal supervisory materials effectively alter operational expectations without the clarity and procedural safeguards associated with rulemaking. That uncertainty is particularly consequential in fraud contexts, where decisions must often be made in real time and under compressed timelines.

c. Supervisory Expectations

In practice, supervisory expectations play a central role in shaping fraud-prevention programs. While statutes and regulations should set legal requirements, standards are often defined through examination processes, supervisory communications, and enforcement posture.

Institutions are examined not only for technical compliance with statutory requirements, but also for the effectiveness of their risk management, governance, and control environments. Examiners may evaluate:

- Fraud loss metrics and trend data;
- Customer complaint volumes and narratives;
- Model performance, validation, and documentation;
- Fair lending implications of fraud detection models;
- UDAAP risk associated with transaction denials, account restrictions, or delays;
- Vendor oversight and third-party fraud detection arrangements;
- Error resolution determinations under EFTA and Regulation E;
- Adverse action notices and stated reasons under ECOA and Regulation B.

Supervisory scrutiny can arise both when fraud losses increase and when institutions implement assertive fraud controls that create customer friction. Institutions may be required to explain why particular fraud events were not prevented, while simultaneously being asked to justify transaction holds, onboarding denials, or account closures implemented to mitigate risk. In some instances, institutions face pressure to provide highly specific reasons for fraud-related decisions, which raises concerns that detailed disclosures could inadvertently reveal sensitive fraud-detection methodologies or provide information that sophisticated actors could exploit.

Examination findings can carry significant operational and reputational consequences, which leads institutions to calibrate fraud programs not only to statutory requirements but also to perceived supervisory posture.

d. State Laws

Institutions operating nationally must implement fraud controls in a manner that fully complies with federal statutes, regulatory guidance, supervisory expectations, and state consumer protection and privacy regimes. These frameworks serve important and legitimate purposes, including safeguarding consumer rights and protecting sensitive financial information. At the same time, differences in scope, interpretation, and enforcement priorities across jurisdictions can create operational complexity for institutions attempting to deploy consistent, real-time fraud prevention programs.

This complexity affects:

- Information sharing practices;
- Fraud-related account restrictions;
- Data retention policies;
- Consumer notification requirements;
- Use of analytics and risk modeling.

Fraud schemes operate without regard to jurisdictional boundaries. Financial institutions, by contrast, must ensure that controls comply with overlapping federal and state requirements. This legal fragmentation can introduce delay or hesitation in implementing collaborative fraud solutions.

V. Areas Where Current Law Constrains Fraud Prevention Efforts

The legal framework governing fraud prevention reflects important consumer protection, privacy, and fairness objectives. However, as fraud has become faster, more coordinated, and more technology-enabled, certain features of current law (and, in some instances, its interpretation and supervisory application) can constrain timely fraud intervention. These constraints arise most acutely in (1) information sharing, (2) liability and dispute frameworks, (3) funds availability rules, (4) supervisory and UDAAP risk, and (5) the ability to deploy technology consistently across jurisdictions.

a. Constraints on Information Sharing and Collaborative Fraud Mitigation

Modern fraud is network-based, and effective prevention increasingly depends on the ability to identify mule accounts, device patterns, typologies, and risk signals across institutions. Current law provides pathways for sharing in limited circumstances, but those pathways are often fragmented, uncertain, or not designed for real-time fraud mitigation.

FCRA definitional and recharacterization risk.
Institutions may hesitate to share certain fraud indicators such as signals tied to identity attributes, device identifiers, or behavior patterns due to concern that sharing could be characterized as furnishing a "consumer report" or creating consumer reporting obligations. This uncertainty can discourage the very kind of consortium-based sharing that is most effective against coordinated fraud networks.

Section 314(b) Limitations in Modern Fraud Contexts.
Section 314(b) of the USA PATRIOT Act permits voluntary institution-to-institution information sharing under specified conditions for purposes related to identifying and reporting money laundering or terrorist financing. While this framework can support certain fraud-related coordination, it was designed primarily around AML objectives and contains definitional and procedural requirements that do not always align with modern, high-velocity fraud typologies, particularly scam-driven authorized payments and other non-AML fraud patterns.

As fraud schemes increasingly overlap with AML-related behaviors such as mule accounts and layered transactions, institutions must carefully evaluate whether fraud-related information sharing falls within the scope of Section 314(b). In time-sensitive scenarios, institutions may also assess whether the framework is operationally suited for real-time fraud mitigation. This can result in uncertainty

about the extent to which 314(b) provides a comprehensive solution for coordinated fraud defense.

GLBA privacy and safeguarding considerations.
Institutions must evaluate whether and how nonpublic personal information can be shared for fraud prevention purposes, including whether the sharing fits within available exceptions and how notice and opt-out requirements may apply in particular contexts. These requirements can slow or narrow the sharing of fraud signals that are most useful when transmitted quickly and at scale.

The practical result is that fraud networks operate across institutions with high coordination, while institutions often face legal uncertainty about whether they can share the risk signals needed to identify those networks quickly.

b. Funds Availability and the Operational Reality of Modern Check Fraud

Check fraud illustrates a core friction point: fraud prevention often requires time, while funds availability rules and customer expectations demand speed.

Institutions must balance prompt funds availability with the reality that counterfeit, altered, or otherwise uncollectible items may not be identified until return and adjustment processes occur. In a world of remote deposit capture, mail theft, and sophisticated alteration, the time gap between deposit and final collectability is frequently the window fraudsters exploit.

Even where Regulation CC provides exceptions and hold authorities, operational and supervisory uncertainty about when those exceptions are appropriate, and how they will be evaluated after the fact, can make institutions reluctant to apply holds as aggressively as fraud trends might otherwise warrant.

c. Supervisory and UDAAP Risk That Can Discourage Proactive Intervention

Institutions seeking to implement robust fraud controls must simultaneously manage UDAAP, and complaint-related risk. Managing these risks can create a challenging dynamic in which institutions face scrutiny both when fraud losses occur and when preventive controls result in customer friction, transaction delays, or account restrictions affecting users.

UDAAP risk in fraud controls. Fraud controls can trigger allegations of unfairness when they delay funds, restrict account access, or create inconveniences for consumers. Institutions must therefore design controls that are risk-based, targeted, and well-governed. At the same time, fraud prevention requires fast action and relies on imperfect information.

Inconsistent Supervisory Interpretation. In practice, the application of statutory and regulatory text can be influenced by supervisory posture. At times, institutions report that supervisory staff apply interpretations that extend beyond the requirements of the governing statute or implementing regulation. When expectations are perceived as broader than the underlying legal framework, institutions may experience uncertainty in determining the appropriate scope of fraud controls. This can create hesitation around reasonable, good-faith intervention measures, particularly where institutions are concerned that a risk-based hold, transaction denial, or account restriction may later be second-guessed despite being supported by documented fraud indicators.

This is not an argument for weakening consumer protection. It is an argument for ensuring that supervision and interpretive approaches align with statutory text and with the legitimate interests of preventing fraud so that the law does not inadvertently become a tool that fraud actors can exploit.

d. Liability Allocation Challenges in Multi-Platform Fraud Environments

Fraud today frequently involves fraudulently induced payments, credential compromise, and multi-platform transaction flows that do not fit neatly within older authorized versus unauthorized liability categories.

Modern fraud schemes frequently span multiple institutions, non-bank payment providers, digital wallets, fintech platforms, and intermediaries. A single scam event may involve credential compromise at one institution, initiation through a peer-to-peer platform, rapid movement across payment rails, and ultimate withdrawal at a separate institution. In these multi-party scenarios, determining which entity bears which investigative, reimbursement, or notice obligations can be legally and operationally complex.

Institutions must assess at what point an “error” arises under applicable statutes, which entity is responsible for conducting the investigation, and how liability should be allocated when funds move quickly across platforms. In practice, institutions often have limited visibility into the full lifecycle of the transaction, particularly where non-bank providers or intermediaries control portions of the customer interface or transaction flow.

CFPB guidance has emphasized that consumer protections may apply even when a non-bank peer-to-peer provider or wallet is involved. While protecting consumers in multi-party environments is important, this interpretive approach can place primary investigative and reimbursement pressure on depository institutions that may not control the originating interface, authentication environment, or transaction design. Banks and credit unions are therefore required to resolve disputes and make liability determinations based on incomplete information while coordinating across entities with differing legal obligations and operational timelines.

The constraint is not the existence of consumer protections, which are fundamental. Rather, the challenge is that statutory frameworks built around bilateral transactions are increasingly applied to multi-platform ecosystems. When liability expectations are expanded without corresponding clarity regarding inter-institution responsibility and information sharing, institutions' ability to interrupt suspicious transactions promptly can be diminished by heightened and asymmetric liability risk.

e. State Privacy and Emerging State AI Laws Create Additional Friction for Modern Fraud Technology

As institutions increasingly rely on advanced analytics, behavioral biometrics, and machine learning to detect fraud in real time, state-level legal fragmentation creates practical obstacles.

State data-use constraints. State data laws may limit collection, processing, and sharing of data elements that are important for fraud prevention, including, consumer specific information, behavioral signals, and cross-platform typology analytics. Institutions must navigate varying definitions, exemptions, and consumer rights requirements across jurisdictions.

Emerging state AI laws and algorithmic governance mandates. State AI laws and proposals increasingly impose requirements relating to automated decision systems (which are sometimes defined extremely broadly). Fraud prevention tools frequently depend on rapid iteration and continuous tuning in response to new typologies. Divergent state-level AI requirements can frustrate the ability of institutions to deploy and update fraud models quickly and consistently.

Recent federal policy developments also reflect a recognition of this tension. For example, President Trump's executive actions regarding AI policy emphasize a national approach designed to reduce barriers to AI adoption and address state-level regulatory obstruction, reflecting an effort to promote innovation and deployment across sectors. The executive order underscores a policy direction that lawmakers should further advance through durable statutory clarity.

The practical risk is that fraud evolves in days or weeks, while institutions face a patchwork of governance and compliance obligations that may slow adoption of new tools, deter experimentation, or force one-size-fits-none model constraints that ultimately favor fraudulent actors rather than legitimate customers. This dynamic is particularly acute for community banks and credit unions, which often lack the resources to engage in prolonged supervisory disputes or to challenge expansive interpretations that exceed statutory text. In practice, smaller institutions may feel compelled to acquiesce to aggressive (many times incorrect) supervisory positions because the cost of resistance can exceed their available compliance capacity. The result is not only regulatory

uncertainty, but a disproportionate burden on community institutions that are critical to local economies and financial inclusion.

VI. Opportunities for Policymakers to Support Fraud Prevention

The fraud environment described above requires more than incremental guidance. It requires targeted statutory clarity, carefully structured safe harbors, and explicit direction to regulators to align supervisory posture with technological reality.

Congress has the opportunity to modernize existing frameworks in ways that preserve core consumer protections while enabling institutions to prevent fraud effectively and in real time. The following measures provide a legislative roadmap.

a. Establish a Fraud-Prevention Safe Harbor Under the FCRA

Congress should provide an explicit safe harbor allowing financial institutions and regulated entities to share fraud-risk indicators for prevention purposes.

Such a provision could:

- Clarify that sharing limited fraud signals (*e.g.*, mule account identifiers, device fingerprints, behavioral risk scores, or typology flags) solely for fraud prevention does not constitute furnishing a consumer report;
- Provide immunity from civil liability for good-faith fraud-signal sharing within defined parameters;
- Authorize standardized fraud consortium frameworks;
- Encourage development of interoperable fraud signal exchange systems.

This clarification would directly address fragmented visibility challenges and would complement, but not replace, AML-focused mechanisms under Section 314(b).

b. Clarify and Expand Section 314(b) for Fraud Coordination

Congress should modernize Section 314(b) to explicitly encompass coordinated fraud prevention, including scam networks and mule-account activity.

Legislative improvements could:

- Clarify that sharing information related to organized fraud schemes qualifies as permissible activity;
- Streamline registration and certification procedures to facilitate real-time sharing;
- Provide liability protection for good-faith sharing related to fraud detection and mitigation;

- Encourage cross-rail fraud coordination between banks, credit unions, and regulated payment providers.

Modern fraud networks use layered transactions and mule accounts that overlap with AML typologies. Clarifying 314(b) would reflect that operational reality.

c. Provide Safe Harbors for Risk-Based Fraud Controls Under ECOA and TILA

Fraud detection programs increasingly intersect with account access, onboarding, and transaction approvals involving credit products. While ECOA and TILA provide critical consumer protections, modern fraud typologies create ambiguity about how those frameworks apply to risk-based fraud interventions.

Congress could consider the following clarifications:

1. **Clarify that fraud-based interventions are distinct from creditworthiness determinations.**
   Statutory language could confirm that actions taken based on documented fraud-risk indicators do not constitute adverse action under ECOA where the decision is not based on creditworthiness.

2. **Protect sensitive fraud detection methodologies.**
   Congress could provide that where an adverse action notice is required, institutions are not obligated to disclose specific fraud-detection algorithms, typologies, or security controls in a manner that would compromise system integrity or facilitate evasion.

3. **Provide a safe harbor for commercially reasonable fraud controls.**
   A statutory safe harbor could protect institutions that deploy validated, risk-based fraud detection models designed to prevent identity theft, account takeover, or scam-related losses, provided such models are implemented in a manner consistent with fair lending laws.

4. **Reinforce statutory scope boundaries under TILA and Regulation Z.**
   Congress could clarify, through express statutory language where necessary, the categories of products that fall within or outside TILA's scope. For example, providing explicit statutory confirmation regarding products such as certain earned wage access arrangements or defined pay-in-four structures would reduce uncertainty and avoid expansion through informal interpretation rather than rulemaking.

These measures would preserve core fair lending and disclosure protections while reducing ambiguity around fraud-prevention tools and product scope. Clarifying the

distinction between fraud mitigation and credit underwriting would enhance regulatory certainty and allow institutions to act decisively against fraudulent activity without undermining consumer rights.

d. Establish a Dynamic Commercially Reasonable Security Safe Harbor

Many existing statutes rely, either explicitly or implicitly, on concepts such as "reasonable" or "commercially reasonable" security. However, what constitutes commercially reasonable fraud prevention evolves rapidly as technology, threat vectors, and detection capabilities advance.

Congress could direct the relevant federal regulators to conduct periodic, technology-focused studies examining current fraud typologies, authentication methods, behavioral analytics, artificial intelligence applications, and inter-institution information-sharing tools. Based on those studies, regulators could be required to articulate and regularly update a commercially reasonable security standard for fraud prevention.

Congress could further codify a cross-statute safe harbor providing that:
An institution that implements and maintains a documented, risk-based fraud prevention program consistent with regulator-defined commercially reasonable security standards shall not be subject to liability *solely* because a fraud event occurred, provided the institution acts in good faith and in accordance with those standards.

Such a framework could incorporate:

- Adoption of industry-standard authentication and identity verification protocols;
- Use of adaptive and AI-driven fraud detection systems;
- Participation in authorized information-sharing frameworks;
- Periodic independent validation and performance testing of fraud controls;
- Ongoing model governance and bias monitoring consistent with fair lending principles.

Requiring regulators to study and understand emerging technological capabilities before criticizing institutional practices would promote informed regulation and supervision. A regularly updated safe harbor would reduce hindsight-based litigation and supervisory second-guessing, while encouraging continued investment in advanced fraud prevention tools.

This approach would not weaken consumer protections. Rather, it would align liability expectations with evolving security standards and create regulatory certainty for institutions acting in good faith to protect consumers and the financial system.

e. Direction to Regulators

Legislative modernization alone will not resolve the structural challenges described above. Effective fraud prevention also depends on regulatory alignment, procedural discipline, and informed supervision. Congress can provide clear direction to ensure that regulatory implementation supports, rather than constrains, good-faith fraud mitigation.

1. **Reinforce Statutory Boundaries and Procedural Discipline.**
   Congress should reaffirm that material expansions of statutory liability or coverage must occur through legislation or formal notice-and-comment rulemaking.

   In recent years, institutions have experienced significant operational shifts through FAQs, supervisory statements, and interpretive materials (particularly in the context of Regulation E and fraudulent transfers). While agencies appropriately issue interpretive guidance, substantive changes to statutory liability standards should not occur through informal mechanisms that lack procedural safeguards, economic analysis, and public input.

   Congress could:

   - Require that significant changes to liability allocation or product coverage under EFTA, TILA, and other statutes proceed through formal rulemaking;
   - Clarify that FAQs and supervisory guidance do not independently alter statutory scope;
   - Direct agencies to review prior informal interpretations that materially expand statutory obligations absent rulemaking.

   This would restore transparency, ensure accountability, and provide institutions with predictable legal standards in fast-moving fraud environments.

2. **Provide Guardrails for Supervisory Use of UDAAP and ECOA**

   Congress should clarify that core consumer protection authorities are not intended to deter documented, risk-based fraud controls.

   Statutory direction could provide that:

   - Temporary holds, transaction delays, enhanced authentication, or account restrictions implemented pursuant to commercially reasonable fraud prevention programs do not constitute unfair or abusive practices absent bad faith, discriminatory intent, or systemic misconduct;
   - Adverse action requirements under ECOA apply to creditworthiness determinations and should not be interpreted to require disclosure of sensitive fraud-detection methodologies;

- Institutions shall not be deemed to engage in unfair practices solely because fraud controls introduce incidental friction when implemented in good faith.

Such clarification would preserve robust consumer protections while reducing hesitation around reasonable intervention measures. UDAAP should remain a tool to prevent genuine consumer harm, not a source of uncertainty that discourages proactive fraud mitigation.

3. Require Technology-Informed Supervision and Establish a Dynamic Commercially Reasonable Safe Harbor

Fraud prevention is increasingly dependent on advanced authentication, behavioral analytics, artificial intelligence, and cross-institution coordination. Regulatory expectations must evolve in parallel with technological capabilities.

Congress should require federal regulators to conduct periodic, technology-focused studies addressing:

- Emerging fraud typologies and scam evolution;
- The effectiveness and limitations of AI-driven fraud detection systems;
- Cross-rail and multi-platform coordination challenges;
- The interaction between fraud prevention tools and statutory liability frameworks.

Based on these studies, regulators should be directed to articulate and regularly update a commercially reasonable security standard for fraud prevention. Congress could further provide that institutions implementing documented, risk-based fraud programs consistent with regulator-defined commercially reasonable standards receive a liability safe harbor against claims based solely on the occurrence of fraud.

Regulatory expectations should be grounded in an informed understanding of technological tools, operational constraints, and evolving threat environments. A dynamic safe harbor framework would reduce hindsight-based enforcement and litigation while encouraging continued investment in advanced fraud mitigation systems.

4. Promote National Consistency in AI Governance for Fraud Detection

Fraud detection increasingly relies on artificial intelligence, adaptive modeling, and real-time analytics. Emerging state-level AI regulatory regimes risk creating fragmentation that slows deployment, increases compliance cost, and complicates model iteration across jurisdictions.

Recent executive action has emphasized the importance of coordinated national AI policy. Congress has an opportunity to build on that direction by:

- Establishing harmonized federal governance standards for AI systems used in fraud detection;
- Providing preemption or safe harbor protections where institutions comply with federal AI oversight requirements;
- Requiring transparency, documentation, and bias mitigation safeguards that preserve fair lending protections without imposing conflicting state mandates.

A coherent national framework would allow institutions of all sizes to deploy rapidly improving fraud technologies responsibly, while maintaining appropriate oversight and consumer safeguards.

Regulators play an essential role in protecting consumers and maintaining financial stability. Clear congressional direction that reinforces statutory boundaries, encourages procedural discipline, and aligns supervision with technological reality would strengthen that role. A regulatory environment grounded in clarity and informed oversight will better equip financial institutions to combat increasingly sophisticated fraud without undermining core consumer protections.

Taken together, these reforms would:

- Clarify fraud-signal sharing under FCRA and 314(b);
- Protect risk-based fraud controls under ECOA, TILA, and UDAAP;
- Codify commercially reasonable fraud-prevention safe harbors;
- Align regulatory guidance and supervision with statutory text;
- Promote nationally consistent AI governance.

The objective is not deregulation. The objective is to ensure that the law does not inadvertently create new avenues for fraud or favor fraudulent actors over legitimate consumers and financial institutions.

Fraud prevention requires speed, coordination, and technological adaptation. The legal framework should enable those attributes while preserving the core consumer protections that Congress has rightly established.

VII. Conclusion

Fraud today is not episodic, localized, or unsophisticated. It is coordinated, technology-enabled, cross-channel, and adaptive. Fraud networks iterate rapidly, share tactics in real time, and exploit structural seams between institutions, payment rails, and regulatory frameworks. They operate without regard to jurisdictional boundaries or statutory silos.

Financial institutions, by contrast, must operate within layered federal and state statutes, regulatory guidance, supervisory expectations, privacy constraints, and evolving governance standards. They must navigate FCRA data-sharing constraints, Regulation CC funds-availability requirements, Section 314(b) information-sharing parameters, TILA and Regulation Z obligations, EFTA and Regulation E liability frameworks, and UDAAP standards simultaneously and under compressed decision timelines. They are expected to reduce fraud losses, protect consumers, deploy advanced technology responsibly, avoid disparate impact, maintain seamless customer experiences, and absorb losses when fraud succeeds while operating within statutory frameworks developed in a different fraud era.

Despite these constraints, institutions have strong independent incentives to prevent fraud. Customer trust is foundational. In a competitive marketplace, customer experience is a key differentiator. Institutions that fail to prevent fraud or that impose excessive friction lose customers. Fraud losses, investigation costs, and compliance expenditures do not disappear; they ultimately influence pricing, access, and innovation across the financial system. Fraud functions as a systemic cost that affects every legitimate participant in the financial ecosystem.

The question before policymakers is not whether to protect consumers. It is how to ensure that the legal and supervisory framework enables institutions to protect consumers effectively in a modern threat environment.

The recommendations outlined in this testimony reflect several core principles:

1. **Safe harbors for good-faith fraud prevention.**
   Institutions that implement commercially reasonable, risk-based fraud controls should have legal certainty that those efforts will not be second-guessed solely because fraud occurred or because customer friction was unavoidable.

2. **Modernized information sharing.**
   Coordinated fraud requires coordinated defense. Clarifying and strengthening Section 314(b) to explicitly encompass organized fraud activity and providing explicit safe harbors for fraud-signal sharing, would materially improve system-wide resilience.

3. **Alignment of funds-availability rules with modern fraud dynamics.**
   Regulation CC was designed to promote timely access to funds, but modern check fraud exploits predictable timing gaps. Policymakers should ensure that institutions retain appropriate authority to apply risk-based holds when warranted by evolving fraud typologies.

4. **Clarity over ambiguity.**
   Statutory standards—particularly under EFTA, Regulation CC, FCRA, ECOA, and TILA—should be applied consistent with their text and expanded only through transparent legislative or rulemaking processes.

5. **Supervisory alignment with technological reality.**
   Regulators should evaluate fraud prevention efforts based on informed understanding of evolving technology and the operational constraints of real-time payment systems. Criticism untethered from technological context discourages innovation rather than promoting consumer protection.

6. **National coherence in AI governance.**
   Fraud detection increasingly depends on advanced analytics and machine learning. A fragmented regulatory environment that slows adoption or imposes inconsistent mandates across jurisdictions will disadvantage legitimate institutions while fraud networks continue to evolve.

Effective fraud prevention and strong consumer protection are complementary objectives. A legal framework that enables timely, collaborative, technology-driven intervention will reduce losses, improve trust, and strengthen financial system integrity.

Fraud will continue to evolve. The legal framework must evolve with it.