EVER-EVOLVING COMPLIANCE ECOSYSTEM

THE INTERSECTION OF LAW, COMPLIANCE AND POLITICAL WHIPLASH

Patti D. Joyner, CRCM
September 2026

1

REGULATORY COMPLIANCE WITH THE LAW

- **Definition:** The process of proving that a bank meets specific external laws, regulations, and internal policies.
- **Core Focus:** Adherence to statutes, regulations and guidance. We must be able to positively answer the question, "*Did we follow the rules?*"
- **Scope:** Tactical and prescriptive. It deals with fixed mandates like Truth in Lending Act, Servicemember Civil Relief Act and other consumer protection laws.
- **Main Goal:** Avoid legal penalties, fines, and regulatory sanctions.

https://resources.fenergo.com/blogs/risk-and-compliance-in-banking

2

RISK MANAGEMENT

- **Definition:** The broader process of identifying, measuring, and managing any event that could harm the bank.
- **Core Focus:** Strategy and survival. It answers the question, "*What events could hurt our business, and how big would the impact be?*"
- **Scope:** Strategic and predictive. It covers financial threats like credit risk, market risk, and liquidity risk, alongside operational and strategic risks.
- **Main Goal:** Protect the bank's capital, ensure long-term stability, and decide how much risk the bank can safely take guided by the board's risk tolerance

https://www.metricstream.com/risk-management-in-banking.html

3

3

Key Differences at a Glance

Feature	Banking Compliance	Banking Risk Management
Primary Driver	External laws and regulatory mandates	Internal strategy and overall business safety
Nature	Rules-based and tactical	Analytical and predictive
Overlap	Includes **compliance risk** (the specific risk of breaking a law)	Encompasses compliance as one part of a larger enterprise framework

4

4

POLITICAL WHIPLASH

- Everyday reality for years now when political leaders try to "throw out everything" to put their stamp on things by pushing the limits of interpretations of the laws and regulations.
- In a banking context, **political whiplash** (often called regulatory whiplash) refers to the severe operational and strategic disruption financial institutions face when shifting political regimes abruptly reverse, implement, or gut major banking laws and enforcement priorities.
- Banks are highly sensitive to federal oversight. With the installment of a new political regime, we have recently seen huge swing from strict regulatory stances to an aggressive deregulatory environment—or vice versa—forces compliance teams to continuously tear down and rebuild their internal risk structures, costing millions in wasted capital.

5

5

THE DEMISE OF THE COMPLIANCE SILO

- Risks have evolved into an interconnected, complex, and dynamic set of processes spanning financial, operational, technological, and geopolitical domains.
- The role of the Chief Risk Officer has evolved into a strategic, technology-driven leadership position that directly influences corporate decision-making at the highest governance levels.
- The CRO has become a central architect of enterprise resilience. Digital transformation, data analytics, artificial intelligence, hybrid risks, and cyber risks have redefined the threat landscape, requiring the CRO to integrate technological foresight into risk governance, and to interpret technical signals in strategic terms for the board and executive management.
- This evolution positions the CRO as a key participant in shaping corporate strategy and resource allocation. The CRO's authority must be sufficient to challenge senior management decisions, escalate concerns to the board, and veto actions that would place the organization outside of lawful or strategic limits.

6

6

THE EVOLVING REGULATORY ENVIRONMENT

- The most significant challenge to our compliance culture is the sheer volume and complexity of changes, further complicated by the fact changes are originating from so many sources such as the executive order nuances, regulators, the courts and many states with complex changes of their own!
- Banks are naturally very conservative and work hard to mitigate risk of regulatory constraints, fines, legal action and reputation risk.
- Banks tend to take a rigid, sequential approach to implementing changed or new requirements rather than an agile, fluid approach.
- ***Compliance remains the infrastructure for successful banks!***

7

7

KEY CHALLENGES OF COMPLIANCE RISK MANAGEMENT

- Cost of compliance continues to increase
- Temporary state of compliance subject to political whiplash with every administration change
- Critical methods for data management and security are significantly evolving, changing rapidly as cybercrimes and traditional crimes escalates
- "Big Picture" thinking is absolutely mandatory!
- Operationalizing compliance requires comprehensive understanding of how all the pieces work together

8 8

8

COMPLIANCE AND RISK MANAGEMENT

Compliance is inseparable from risk management. A CCO's job includes:

- Conducting risk assessments to identify areas of vulnerability.
- Prioritizing compliance risks based on potential impact.
- Implementing controls and training to mitigate risks before they escalate.
- For example, if a bank identifies weaknesses in its anti-money laundering program, the CCO must act immediately to tighten controls, update systems, and report progress to the Board of Directors.

9

9

WHAT MAKES A GREAT STRATEGIC LEADER?

- A great strategic leader possesses a combination of visionary, strategic, and people-focused skills, including the ability to anticipate the future, strategically think and make decisions, communicate clearly, empower and motivate teams, and adapt to changing circumstances.
- Strong leaders are proactive, focus on creating long-term value, foster a learning mindset and culture, and lead with integrity to guide their organization through complexity and disruption.
- Six skills that, when mastered and used in concert, allow strategic leaders to think strategically and navigate the unknown effectively: the abilities to **anticipate, challenge, interpret, decide, align, and learn**.
  - Harvard Business Review - Strategic Leadership: Six Essential Skills

10

10

STRATEGIC COMPLIANCE LEADERSHIP

- CCOs are increasingly focused on driving cultural change, rather than simply managing their institutions' compliance policies and procedures. Historically, the compliance function was where the least strategically focused people served, the ones who knew process but did not have direct access to business leaders or regulators. CCOs were not always given a seat at the strategic table.
- Evolution in bank risk management has increased 3 crucial needs
  - the need for strategic risk management leadership,
  - the need for an advanced understanding of technological ecosystem within which banks operate, and
  - the need to manage rapid regulatory and technological changes on a daily basis.
- These and other factors have necessitated a more well rounded, strategically minded compliance and risk management officer.

11

11

COMPLIANCE OFFICER AS AN INFLUENCER

The CCO must never be considered the "Committee of No." Instead, they are charged to collaborate with key leaders to balance business strategies with compliance and risk management requirements.

- Advising on implications of market expansion or products and services changes
- Ensuring compliance considerations are embedded in strategic planning.
- Collaborating with IT, HR, and Operations to integrate compliance into business decisions and daily business processes.
- A well-respected CCO should be proficient in both regulatory expertise and business management sensitivity, helping the organization take advantage of strategic opportunities while managing associated risks.

12

12

AN EFFECTIVE COMPLIANCE LEADER

The CCO are often the direct intermediators of the organization in dealings with examiners and regulatory counsel.

- Proactively managing and resolving issues before they escalate.
- Managing audits and responding to findings.
- Strengthening the bank's commitment to compliance through development of effective solutions and transparent reporting woven into all businesses. Listen to your business people!!
- An honest and professional relationship with regulators and auditors can mean the difference between a manageable remediation process and costly, high-profile enforcement action.

13

13

CFPB SEMIANNUAL REGULATORY AGENDA

- CFPB (July 13, 2026) issued Semiannual Regulatory Agenda covering period January – November 2026
  - Lists anticipated regulatory activity during the remainder of 2026
  - This is actually the Fall 2025 agenda (publication was delayed); preamble to the agenda states that it reflects developments only through January 13, 2026
    - 3 of the 9 final rule actions listed on the agenda address rulemaking actions issued after January 13, 2026: Financial Data Transparency Act, 1071, and amendments to Reg. B
- Lists 21 rulemaking actions that CFPB expects to pursue in addition to 5 long-term actions
  - CFPB plans to retain 125 staff members in the Research, Monitoring and Regulations Division (second only to planned 133 staff members in the Operations Division)
- CFPB is reviewing all rules implemented during the previous administration
  - They are reconsidering, rescinding, refining, or streamlining existing regulations, rather than implementing any new consumer protection rules
- Also examining how it governs its own operations
  - Evidenced through new rules concerning guidance documents, periodic review of regulations, supervisory designation proceedings, and state official notification procedures

14

CFPB SEMIANNUAL REGULATORY AGENDA

- 3 pre-rule activities:
  - Amendments to Dodd-Frank Act Sections 1031 and 1036 (UDAAP)
  - Possible adjustments to ATR/QM rules
  - Prepaid Accounts Under Regulations E and Z
- 9 proposed rulemakings:
  - Reconsideration of the Payday Lending Rule
  - Reconsideration of the Personal Financial Data Rights or open banking (1033) Rule
  - Procedures for Guidance Documents
  - Procedures for Periodic Review of Bureau Regulations
  - Larger Participant Rules covering the automobile finance, debt collection, consumer reporting, and international money transfer markets
  - Contingency Calculations for Determining the Average Prime Offer Rate

15

CFPB SEMIANNUAL REGULATORY AGENDA

- 9 final rules:
  - Streamlining Mortgage Servicing for Borrowers Experiencing Payment Difficulties (RESPA)
  - Remittance Transfers Under Regulation E
  - Rescission of the COVID-19 mortgage servicing protections adopted during the pandemic
  - Rescission of the State Official Notification Rules
  - Legal Standard Applicable to Supervisory Designation Proceedings
  - Amendments to the Consumer Financial Civil Penalty Fund Rule
  - Financial Data Transparency Act (already done)
  - Reconsideration of 1071 Small Business Lending Data Collection Rule (already done)
  - Amendments to Regulation B under the Equal Credit Opportunity Act (already done)

16

CFPB SEMIANNUAL REGULATORY AGENDA

- No change to list of inactive rulemakings:
  - Alternative Mortgage Transaction Parity (Regulation D)
  - Supervision of Larger Participants in Markets for Personal Loans
  - Expedited Funds Availability Act (Regulation CC)
  - Consumer Financial Civil Penalty Fund
  - Defining Larger Participants in Certain Consumer Financial Product and Service Markets
  - Student Loan Servicing
  - Review of Inherited Regulations: Credit Cards
  - Regulation E Modernization
  - Loan Originator Compensation
  - E-Sign Act Requirements
- CFPB (July 6, 2026) notified Office of Information and Regulatory Affairs (OIRA) that it intends to publish a Request for Information about credit card late fees
  - Not known what information CFPB intends to solicit or what regulatory path it ultimately may pursue – could be updating the record or exploring any narrower regulatory approach
- Acting Director Vought has in the past indicated that CFPB will be looking for evidence of debanking, but there is no item on the agenda related to debanking

17

CFPB ENFORCEMENT LOOKBACK AND PRIORITIES

- CFPB (May 28, 2026) issued pages on Supervision and Enforcement Priorities, Enforcement Principles, Life cycle of an enforcement action, and 2025 Enforcement lookback
- Observations:
  - Enforcement Actions: around 40% of pending investigations were closed; 19 public enforcement actions were dismissed or withdrawn; 22 pending orders terminated or modified; 7 actions were resolved; and 8 actions were pending at end of year 2025
  - Supervisory Activity: 76% (1,477 of 1,946) of outstanding Supervisory Actions were closed; 66 of 80 open exams were closed; exams were reduced by more than 50%
    - "Humility Pledge" introduced for all exams going forward
  - Enforcement and Supervision Priorities: servicemembers, veterans, and their families; mortgages, FCRA/data furnishing violations; FDCPA F violations; fraudulent overcharges and fees; and inadequate controls resulting in actual consumer loss
  - Enforcement Principles: updated focus on actual, measurable consumer harm with identifiable victims; no novel legal theories or expansive interpretations; consumer redress prioritized over civil money penalties; collaboration and self reporting encouraged; and reduced duplication with states and other federal regulators
  - Complaint Trends: credit or consumer reporting accounted for 87% of all complaints in FY2025 (over 5 million), up from ~145,000 in FY2019
    - Surge attributed in part to credit repair scammers, social media "finfluencers," and AI driven automation of the complaint process
  - Regulatory Actions: FCRA preemption interpretive rule issued (October 2025); Medical Debt Rule (Reg V) vacated; data broker proposed rule (Reg V) withdrawn, multiple guidance documents withdrawn, including circulars and bulletins

18

CFPB ACTING DIRECTOR VOUGHT COMMENTS

- CFPB Acting Director Russell Vought testimony to House Financial Services Committee (July 15, 2026)
  - Congress should enact legislation to better define UDAAP to avoid abuses by future regulators
    - Current administration has concerns about the definition of abusiveness, and lawmakers should codify a better definition
  - Most positive change would be to subject CFPB to congressional appropriation to make it more responsive to elected officials
    - CFPB is unique among federal agencies in that its funding comes from the Federal Reserve
    - He would prefer the agency be abolished
  - CFPB is "very close" to having a proposed rule to replace previous 1033 rule
    - Noted that President has nominated former CFPB Deputy Director Brian Johnson to serve as full-time director, and CFPB is timing release of the proposal with possible Senate confirmation of Johnson
  - CFPB has also paused efforts to reduce workforce by more than half until the new director is in place (according to a court filing)

19

21ST CENTURY ROAD TO HOUSING ACT

- 21st Century ROAD to Housing Act (Section-by-Section) became law on July 11, 2026, after President failed to sign or veto it
  - Combined elements of housing and banking proposals put forward by the House Financial Services Committee and Senate Banking Committee
  - Rewards communities that build more housing supply, ease environmental review of new construction, rethink regulations that hamper additional lending for small-dollar mortgages and expand tenant assistance and protections
- Market disruption restrictions:
  - Prohibits large institutional investors (defined as for-profit entities controlling 350 or more single-family homes) from purchasing single-family residential properties
    - Mortgage servicers and lenders are exempted from this ban when acquiring properties during foreclosure, loss mitigation, or compliance-driven REO dispositions
    - Servicers must utilize "first-look" programs giving owner-occupants and qualified non-profits initial access to REO properties, but final bill limits time frame and scope of these requirements to prevent excessive carrying costs
- Central Bank Digital Currency:
  - Ban on Fed Retail Digital Currency (Sec. 1101)
    - Explicitly prohibits Fed from issuing or creating a retail Central Bank Digital Currency (CBDC) or utilizing financial intermediaries to establish a widely available digital dollar; this effectively freezes retail CBDC development through December 31, 2030, giving banks clear runway to construct long-term payment and deposit roadmaps

20

21ST CENTURY ROAD TO HOUSING ACT

- Banking-related provisions:
  - Modernizing Manufactured Housing (Sec. 301 & 302)
    - Expands statutory definition of manufactured homes to include structures built without a permanent chassis and directs FHA to eliminate financing barriers for modular construction
  - Appraisal Industry Expansion (Sec. 403)
    - Appraisal Industry Improvement Act permits state-licensed appraisers to conduct appraisals for FHA-insured mortgages, alleviating widespread appraiser shortages
  - Reconsideration of Value (Sec. 704)
    - Directs FHFA, FHA, USDA and VA to require that participating lenders implement and maintain formal procedures in consumer-initiated reconsiderations of value and second appraisal requests, and requires Comptroller General to advance with feasibility studies for creating a publicly available appraisal database
  - Custodial Deposit Reclassification (Sec. 901)
    - Incorporating the Community Bank Deposits Access Act, this section exempts custodial deposits at well capitalized institutions with less than $10 billion in total assets from the being classified as brokered deposits, provided they do not exceed 20% of the institution's total liabilities
  - Extended Exam Cycles (Sec. 903)
    - Under the TRUST Act, asset threshold qualifying well-capitalized insured depository institutions for an extended 18-month exam cycle is raised from $3 billion to $6 billion

21

21ST CENTURY ROAD TO HOUSING ACT

- Banking-related provisions:
  - Credit Union Board Modernization (Sec. 904)
    - Reduces mandatory meeting frequency for well-run federal credit unions from monthly to 6 times annually, aligning administrative burdens more closely with risk profiles
  - Mentor-Protégé Program (Sec. 906)
    - Codifies Treasury program pairing small, rural, and minority depository institutions (MDIs) with large banks to stream capital, technical expertise, and correspondent relationships to smaller institutions
  - Reviving De Novo Bank Formation (Sec. 907 & 908)
    - American Access to Banking Act and Promoting New Bank Formation Act direct agencies to streamline application process, and establishes a 2-year phase-in period for federal capital requirements, drastically lowering upfront capital drag
  - Rural Depositories Study (Sec. 909)
    - Mandates joint agency study to identify federal barriers preventing growth, capital adequacy, and profitability in rural community banks

22

HOW TECHNOLOGY IS RESHAPING COMPLIANCE

- In today's environment of tight margins and erroneous perception that compliance isn't important anymore, it is more important than ever to maintain a strong compliance culture.
- Most institutions use some form of Artificial Intelligence in core decision-making processes, according to the Bank for International Settlements. While AI expansion drives scalable and optimized performance, deploying AI within a control infrastructure built for a non-AI world introduces fundamental vulnerabilities.
- This can easily translate into increased reputation risk, earnings volatility, and heightened regulatory exposure. Together, these dynamics give rise to three critical exposures that reveal underlying weaknesses and point to the controls needed to address them.
- For financial analysts, the maturity of a bank's AI control environment, revealed through disclosures, regulatory interactions, and operational outcomes, is becoming as telling as capital discipline or risk culture.

23

23

THREE FACTORS TRANSFORMING BANKING RISK

- AI introduces unique complexities across traditional banking risk categories, including credit, market, operational, and compliance risk.
- Three factors define the transformed risk landscape:
  1. Systemic Model Risk: When Accuracy Masks Fragility
  2. Data Risk at Scale: Bias, Drift, and Compliance Exposure
  3. Automation Risk: When Small Errors Scale Systemically

rpc.cfainstitute.org/blogs/enterprising-investor/2026/ai-is-reshaping-bank-risk

24

24

SYSTEMIC MODEL RISK: WHEN ACCURACY MASKS FRAGILITY

- Unlike conventional models, AI systems often rely on highly complex, nonlinear architectures. While they can generate highly accurate predictions, their internal logic is frequently opaque, creating "black box" risks in which decision-making cannot easily be explained or validated. A model may perform well statistically yet fail in specific scenarios, such as unusual economic conditions, extreme market volatility, or rare credit events.
  - For example, an AI-based credit scoring model might approve a high volume of loans during stable market conditions but fail to detect subtle indicators of default during an economic downturn. This lack of transparency can undermine regulatory compliance, erode customer trust, and expose institutions to financial losses. As a result, regulators increasingly expect banks to maintain clear accountability for AI-driven decisions, including the ability to explain outcomes to auditors and supervisory authorities.



25

25

DATA RISK AT SCALE: BIAS, DRIFT, AND COMPLIANCE EXPOSURE

- AI's performance is intrinsically tied to the quality of the data it consumes.
- Biased, incomplete, or outdated datasets can result in discriminatory lending, inaccurate fraud detection, or misleading risk assessments. These data quality issues are particularly acute in areas such as anti-money laundering (AML) monitoring, where false positives or false negatives can carry significant legal, reputational, and financial consequences.
  - For example, consider a fraud detection AI tool that flags transactions for review. If the model is trained on historical datasets with embedded biases, it may disproportionately target certain demographics or geographic regions, creating compliance risks under fair lending laws.
  - Similarly, credit scoring models trained on incomplete or outdated data can misclassify high-risk borrowers as low risk, leading to loan losses that cascade across the balance sheet. Robust data governance, including rigorous validation, continuous monitoring, and clear ownership of data sources, is therefore critical.



26

26

AUTOMATION RISK: WHEN SMALL ERRORS SCALE SYSTEMICALLY

- As AI embeds deeper into operations, small errors can rapidly scale across millions of transactions. In traditional systems, localized errors might affect a handful of cases; in AI-driven operations, minor flaws can propagate systemically. A coding error, misconfiguration, or unanticipated model drift can escalate into regulatory scrutiny, financial loss, or reputational damage.
  - For instance, an algorithmic trading AI might inadvertently take excessive positions in markets if safeguards are not in place. The consequences could include significant losses, liquidity stress, or systemic impact.
  - Automation magnifies the speed and scale of risk exposure, making real-time monitoring and scenario-based stress testing essential components of governance.
    - How great is the scope of generative AI decision-making? Who reviews it? When?

27

27

WHY LEGACY CONTROLS BREAK DOWN IN THE AI ENVIRONMENT

- Most banks still rely on deterministic control frameworks designed for rule-based systems. AI, by contrast, is probabilistic, adaptive, and often self-learning. This creates three critical governance gaps:
  1. **Explainability Gap:** Senior management and regulators must be able to explain why decisions are made, not just whether outcomes appear correct.
  2. **Accountability Gap:** Automation can blur responsibility among business owners, data scientists, technology teams, and compliance functions.
  3. **Lifecycle Gap:** AI risk does not end at model deployment, it evolves with new data, environmental changes, and shifts in customer behavior.
- Bridging these gaps requires a fundamentally different approach to AI governance, combining technical sophistication with practical, human-centered oversight.

rpc.cfainstitute.org/blogs/enterprising-investor/2026/ai-is-reshaping-bank-risk

28

28

WHAT EFFECTIVE AI GOVERNANCE LOOKS LIKE IN PRACTICE

- Financial leaders are adopting holistic AI risk and control approaches that treat AI as an enterprise-wide risk rather than a technical tool. Effective frameworks embed accountability, transparency, and resilience across the AI lifecycle and are typically built around five core pillars.
  1. Board-Level Oversight of AI Risk
  2. Model Transparency and Validation
  3. Data Governance as a Strategic Control
  4. Human-in-the-Loop Decision Making
  5. Continuous Monitoring, Scenario Testing, and Stress Simulations

rpc.cfainstitute.org/blogs/enterprising-investor/2026/ai-is-reshaping-bank-risk

29

29

INTEGRATING FINANCIAL TECHNOLOGY INNOVATION INTO REGULATORY FRAMEWORKS (EXECUTIVE ORDER, MAY 19, 2026)

- EO appears designed to accelerate the integration of fintech firms, digital asset providers, and other non-bank innovators into the traditional banking and payments system. It is noteworthy not only because of its broad deregulatory tone, but also because it expressly directs federal banking regulators, including the Federal Reserve, to reconsider longstanding barriers limiting fintech and crypto firms' access to the US payment infrastructure.
- The Order reflects the continuation and expansion of the Administration's broader digital financial technology agenda.
  - Ballard Spahr, Consumer Finance Monitor

30

30

INTEGRATING FINANCIAL TECHNOLOGY INNOVATION INTO REGULATORY FRAMEWORKS (EXECUTIVE ORDER, MAY 19, 2026)

Among the most consequential aspects of the Order are directives aimed at:

- Expanding consideration of fintech and digital asset firms' access to Federal Reserve payment services and "master accounts";
- Encouraging collaboration between banks and fintech companies;
- Reducing regulatory fragmentation;
- Modernizing payments infrastructure;
- Reviewing supervisory policies that may inhibit innovation;
- Integrating emerging technologies into mainstream financial services.

Many banks are likely to be concerned about:

- Expanded competitive pressure from non-bank firms;
- Potential erosion of the traditional banking charter advantage;
- Uneven regulatory obligations between banks and fintech firms;
- Operational and compliance risks associated with expanded digital asset integration.

31

31

INTEGRATING FINANCIAL TECHNOLOGY INNOVATION INTO REGULATORY FRAMEWORKS (EXECUTIVE ORDER, MAY 19, 2026)

- **Break Barriers For Financial Technology Innovation And Competition**: President Trump intends to streamline regulations and promote financial innovation and collaboration between financial technology (fintech) firms, federally regulated financial institutions, and Federal financial regulators.
  - Directs Federal financial regulators to review existing regulations, guidance, supervisory practices, and application processes to identify those that could be updated to facilitate innovation and greater competition in the provision of financial services, while maintaining safety and soundness.

32

32

INTEGRATING FINANCIAL TECHNOLOGY INNOVATION INTO REGULATORY FRAMEWORKS (EXECUTIVE ORDER, MAY 19, 2026)

- **Promote Financial Innovation and Cutting Out Regulatory Protections for Incumbents**: Ensure that the United States is the global leader in financial innovation by removing outdated regulatory burdens that do not fit the digital age.
  - Foster Americans' ability to benefit from FinTech, mandating Federal government update of outdated regulations to allow integration of digital assets and other novel financial technology into traditional financial services and payment systems.
- **Lead the World in Financial Innovation:** Establish the United States as a leader in financial and other cutting-edge technologies by cutting red tape and prioritizing innovation and global competitiveness – common sense measures that will lower costs and increase economic opportunities for all Americans.

33

33

FTC PROPOSED POLICY STATEMENT ON AI ACCURACY

- FTC (July 1, 2026) issued a "Proposed Policy Statement Concerning the Suppression of Accuracy in Artificial Intelligence Systems"
  - Addresses whether AI companies that steer their' outputs toward undisclosed ideological objectives, rather than toward objectives that customers request or reasonably expect, may be engaging in deceptive acts or practices (UDAP)
  - Issued pursuant to Executive Order 14365 (Dec. 11, 2025), which directed FTC to clarify how FTC Act §5 applies to AI models and, in particular, to address how state laws requiring alterations to accurate outputs of AI models can conflict with federal law
- AI companies have made both explicit and implicit representations that their systems are designed to produce the best, most accurate, and most faithful output possible within their technological and resource constraints
  - Because customers rely on those representations and accept AI outputs without independent fact-checking more than 90% of the time, customers have a reasonable expectation that AI systems are not secretly designed to pursue undisclosed objectives that distort those outputs
  - Deception under UDAP: conduct is deceptive if there is a representation, omission, or practice that is likely to mislead a reasonable consumer in a material way
    - Therefore, an AI company that trains or configures its model to pursue undisclosed ideological objectives, whether of its own volition or in response to a state law requirement, may be deceiving consumers regardless of motivation for doing so
  - Draws distinction between intentional ideological steering and hallucinations – hallucinations arise from technological and resource limitations rather than design decision

34

FTC PROPOSED POLICY STATEMENT ON AI ACCURACY

- Preemption of state laws
  - State laws that may pressure AI companies to suppress output accuracy in order to avoid disparate impact liability, such as Colorado's Artificial Intelligence Act, is an example of a state law that is impliedly preempted to the extent it conflicts with the federal regulatory scheme established by §5 of the FTC Act
    - State laws that effectively require AI companies to deceive consumers conflicts with §5's express purpose of protecting consumers from deceptive conduct
- AI companies can avoid §5 liability by making clear, conspicuous, and adequate disclosures that its system is designed to prioritize certain objectives over what users request or would otherwise expect
  - Disclosure must be sufficiently prominent and persistent to shift the reasonable consumer expectations created by the company's broader marketing and inherent nature of AI as a problem-solving tool
- Implications:
  - Determine if companies that market AI systems as accurate, neutral, or objective problem-solving tools are actually consistent with those representations, and whether any intentional constraints on output are adequately and prominently disclosed
    - Check whether the company that does configure its system to prioritize objectives beyond those users would otherwise expect sufficiently and prominently discloses that fact, by examining terms of service, product descriptions, and onboarding flows

35

FINANCIAL STABILITY BOARD: SOUND AI PRACTICES

- Financial Stability Board (FSB, June 10, 2026) published a consultation report on "sound practices" for responsible adoption of AI by financial institutions
- Identifies 12 sound practices covering:
  - Organization-wide AI governance, including strategic direction and board oversight, governance and accountability frameworks, incorporation of AI risks into risk management, and organizational adaptability
  - AI lifecycle management, including materiality and risk assessment, model selection, data governance, explainability and transparency, performance management, and human oversight
  - Management of AI-related cyber and information and communication technology risks, and third-party AI risk management addressing performance, transparency, data quality, supply chain concentration, and business continuity
- Builds on existing and ongoing work by the FSB and other standard-setting bodies and seek to foster coordination, cooperation, and information-sharing among financial institutions and supervisors within and across jurisdictions
- Not intended to establish an international standard or impose a prescriptive approach for AI adoption, nor developed to address risks related to frontier AI models, although some practices would help institutions respond to such risks
- Strongly encourages boards and senior management of financial institutions to reference the practices as they consider business strategy, technology adoption, and risk management

36

FSB FINANCIAL STABILITY BOARD

Sound Practices for Responsible Adoption of Artificial Intelligence (AI)

Consultation report



10 June 2026

Table of Contents

Questions for consultation iii
Executive summary 1
Introduction 3
1. An overview of the use of AI in the financial system 5
1.1. AI adoption in the financial sector 5
1.2. Use cases and benefits of AI in the financial system 6
1.3. Risks and implementation challenges of AI adoption for financial institutions 12
2. Organisation-wide AI governance 18
2.1. Strategic direction and oversight 18
2.2. Governance and accountability 20
2.3. AI risk management framework and effective documentation 21
2.4. Organisational adaptability 23
3. AI lifecycle management 26
3.1. Stages of AI development and deployment 26
3.2. Materiality and risk assessment 27
3.3. Selection 29
3.4. Data governance 30
3.5. Explainability and transparency 33
3.6. Performance management 37
3.7. Human oversight 41
3.8. Cyber and ICT risk management 44
3.9. Third-party risk management 48
Annex 1: List of Sound Practices for financial institutions' responsible AI adoption 52
Annex 2: Examples of explainability for different AI approaches 53
Annex 3: Examples of AI performance testing 55
Glossary 56
References 59

37

37

FSB'S SOUND PRACTICES FOR RESPONSIBLE ADOPTION OF ARTIFICIAL INTELLIGENCE (AI)

- Artificial Intelligence Transformation Office (AITO) focuses on its mission to bolster the strength and resilience of the US Financial system amid rapid technological advancements.
- AI is poised to profoundly transform financial services and bank business models, from automating repetitive tasks to augmenting complex decision making and execution.
- Financial institutions are rapidly adopting, using and innovating with AI adoption to
  - Reap efficiency gains,
  - Transform their business models,
  - Improve the services offered to customers, and
  - Enhance risk management capabilities.
- Significant benefits can arise from AI adoption and effective risk management is required to promote sustained value creation and financial stability.

FINANCIAL SOLUTIONS FOR GROWING COMPANIES, INC.

38

38

AI ADOPTION IN THE FINANCIAL SECTOR CREDIT SCORING

AI is increasingly transforming financial services through a wide range of use cases

- AI use has improved accuracy through advanced analytics on large volumes of financial and behavioral data to better assess credit risk where traditional methods are slower and less effective.
- AI is enhancing credit underwriting, particularly for small and medium sized enterprises. Automating data extraction from financial documents including cash flow statements and market information provides better predictive monitoring.
- Many banks are using AI credit decision models to improve risk profiling by adding nontraditional sources of credit data, contributing significantly to lower default rates and expanded credit access, particularly for borrowers who may not qualify under traditional credit assessment methods.

39

39

AI ADOPTION IN THE FINANCIAL SECTOR REGULATORY COMPLIANCE, AML/CFT AND FRAUD DETECTION

- Banks are using AI to improve fraud detection and financial crime monitoring by analyzing large volumes of transactions and unstructured data.
- Traditional AI enhances anomaly detection and uncovering hidden relationships between transactions, strengthening monitoring capabilities to identify marketing surveillance and abuse detection. Additional alerts for human-in-the-loop oversight is extremely beneficial!
- AI enhances AML/KYC by automating document verification, identity checks and fraud detection.
- Biometric verification and contextual analysis can strengthen security, reduce manual work, and enhance the overall customer experience.
- Increasingly used to detect identify fraud, synthetic identities, and deepfake-based cyber-attacks often in real-time. AI is very effective in supporting compliance reviews of marketing materials and disclosure documentation.

40

40

AI ADOPTION IN THE FINANCIAL SECTOR CUSTOMER-FOCUSED APPLICATIONS

- AI is increasingly used across banks to enhance customer engagement in areas of portfolio engagement, marketing and customer service.
- Large Language Models (LLM) are great tool enhancements for internal knowledge retrieval and analysis, automating customer complaint triage and document classification, significantly enhancing operational efficiency!
- In customer service, AI-driven chatbots and virtual assistants can handle routine queries, payments and loan requests, improving response times, service availability and customer satisfaction (within some constraints!!), reducing reliance on call centers.
- AI is widely used in marketing activities, optimizing new product campaigns, generating customer leads and creating marketing content.

41

41

AI ADOPTION IN THE FINANCIAL SECTOR PRODUCTIVITY ENHANCING APPLICATIONS

- Financial institutions are finding efficiency and productivity gains from AI as it enables automation of labor-intensive activities, faster execution, more consistent processes and outcomes, lower operational costs, and allowing staff to focus on higher-value tasks.
- Lots of gains are realized in modernizing internal operations, including back office automation, risk analytics, content and code generation and risk management.
- Large scale analysis of unstructured data is greatly beneficial in strengthening internal controls through automated documentation, monitoring and anomaly detection in increasingly complex transaction patterns. Information retrieval across business functions has contributed greatly to overall efficiency.

42

42

AI ADOPTION IN THE FINANCIAL SECTOR OPERATIONAL RESILIENCE

- Financial institutions and their vendors and partners are using AI to enhance operational and cyber resilience by improved threat detection and response.
- AI can analyze large volumes of data in real time to identify anomalies and detect potential attacks faster than human analysts, while also reducing false positives, allowing for effective containment of threats.
- AI strengthens organizational resilience by identifying vulnerabilities and promoting business continuity through swift recovery from incidents like ransomware attacks. AI is used to monitor anomalous network behavior across employee access, data transfers, unusual API calls, and phishing attempts, using a combination of internal and third-party tools.

43

43

SOUND PRACTICES FOR RESPONSIBLE AI ADOPTION

- **Sound Practice 1 (Strategic direction and oversight):** The board and senior management align AI adoption and governance with the financial institution's business model, risk appetite, and strategy.
- **Sound Practice 2 (Governance and accountability):** Financial institutions define clear roles and responsibilities, and maintain an appropriate governance framework to enable responsible AI adoption.
- **Sound Practice 3 (Incorporation of AI risks into risk management framework):** Financial institutions adopt risk management frameworks that effectively address AI risks, and include processes for AI identification, documentation, as well as materiality and risk assessment.
- **Sound Practice 4 (Organizational adaptability):** Financial institutions learn, adapt and adjust their oversight, governance, risk management practices, and capabilities as AI evolves.

44

44

SOUND PRACTICES FOR RESPONSIBLE AI ADOPTION

- **Sound Practice 5 (Materiality and risk assessment)**: Financial institutions implement an effective and systematic approach to assess the materiality and risk of AI use cases at the inception stage and thereafter.
- **Sound Practice 6 (Selection):** When selecting AI models or systems, financial institutions consider business objectives, operational and technical needs, as well as the materiality and risks of AI use cases.
- **Sound Practice 7 (Data governance):** Financial institutions establish appropriate data governance to maintain data that is fit-for-purpose for training, testing, and using AI (i.e. accurate, complete, consistent, reliable, secure).
- **Sound Practice 8 (Explainability and transparency):** Financial institutions understand differences in the explainability of various types of AI. If appropriate and feasible, financial institutions adopt more explainable AI, or consider compensating controls. Financial institutions also provide appropriate transparency tailored to different stakeholders.

45

45

SOUND PRACTICES FOR RESPONSIBLE AI ADOPTION

- **Sound Practice 9 (Performance management):** Financial institutions evaluate the performance of AI use cases proportionately to their materiality and risk, including through performance assessments, testing, and ongoing monitoring**.**
- **Sound Practice 10 (Human oversight):** Financial institutions implement appropriate and effective human oversight relevant to the materiality, risk, autonomy, complexity, and explainability of different AI use cases.
- **Sound Practice 11 (Cyber and ICT risk management**): Financial institutions manage AI-related cyber and ICT risks, including, where appropriate, by incorporating AI cyber and ICT risk scenarios into tests and exercises, sharing relevant information, and using AI tools in cyber and ICT risk management.
- **Sound Practice 12 (Third-party AI risk management):** Financial institutions appropriately manage risks from AI third-party use with a focus on performance, transparency, data quality, supply chain and concentration risks, and business continuity.

46

46

FDIC POTENTIAL STANDARDS SETTING ORGANIZATION (AUG 2026)

- According to an exclusive Bloomberg Law report, the Federal Deposit Insurance Corporation is considering plans to work with banking and financial technology industry groups to establish a new standard-setting organization.
- The report is based on a term sheet that would establish a Banking Industry Standards Development Organization (BISDO) to develop standards and issue standard certifications to third-party service providers that partner with banks.
- The initiative could represent one of the most significant developments in the federal regulatory approach to bank-fintech partnerships, and service provider relationships more broadly, in recent years. This effort is conceptually similar to a previous FDIC initiative, when it issued a Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services.

https://www.consumerfinancemonitor.com/2026/08/17/fdic-considers-industry-standard-setting-organization-for-third-party-service-providers/

47

47

FDIC POTENTIAL STANDARDS SETTING ORGANIZATION (AUG 2026)

- The new organization would set baseline standards that would make it easier for banks to evaluate whether fintechs and other third-party service providers meet risk management standards and to onboard those firms to internal bank systems, according to a July 21 draft term sheet obtained exclusively by Bloomberg Law.
- The standard-development organization would also certify that third-party firms meet those standards, though independent assessors would conduct their own reviews to determine compliance, the draft term sheet said.
- The goal is to help banks, particularly community banks, avoid duplicative reviews of the same service providers while providing regulators and examiners with some baseline assurances about the safety of those vendors' offerings, according to the FDIC's outline.

48

48

https://www.consumerfinancemonitor.com/wp-content/uploads/sites/14/2026/08/BANKING-INNOVATION-STANDARDS-DEVELOPMENT-ORGANIZATION-1.pdf

DRAFT TERM SHEET (7/21/2026)

BANKING INNOVATION STANDARDS DEVELOPMENT ORGANIZATION

This term sheet outlines a framework for establishing a voluntary public-private standards development organization (SDO), along with a conformity assessment (i.e., attestation and certification) program, to support third-party risk management and technology integration at banks. The term sheet contains certain key provisions related to the formation and operation of the SDO, is not a detailed concept of operations, and is subject to review and modification.

Overview	
Strategic Rationale	Banks increasingly rely on third-party service providers for technology, operations, payments, compliance support, customer-facing services, cloud infrastructure, cybersecurity, data processing, and other critical or important functions. Many banks conduct duplicative reviews of the same providers, control environments, due diligence materials, monitoring information, and evidence packages. This duplication can be particularly burdensome for community banks, which may have limited personnel, technical expertise, negotiating leverage, and resources to evaluate complex or novel third-party arrangements. Third-party service providers also face repeated, inconsistent, and costly information requests from multiple institutions, even when those institutions are seeking similar information about the same provider-level controls, solution-level risks, or evidence packages. A voluntary public-private standards development organization and conformity assessment program would address these inefficiencies by standardizing and certifying common third-party risk management (TPRM) information that can be assessed once, refreshed over time, and reused by multiple banks, while preserving each bank's responsibility for institution-specific risk assessment, contract decisions, integration, monitoring, and oversight.

49

49

Artificial Intelligence Executive Oversight Group AI Lexicon February 2026

The Shared Artificial Intelligence (AI) Lexicon was created by the AI Lexicon workstream of the Artificial Intelligence Executive Oversight Group (AIEOG). The AIEOG is a public-private partnership formed by the U.S. Department of the Treasury (Treasury), in collaboration with the Financial and Banking Information Infrastructure Committee (FBIIC) and the Financial Services Sector Coordinating Council (FSSCC).

The Lexicon was developed to promote a shared vocabulary for communication and collaboration on AI-related matters in the financial sector. It compiles commonly used risk management and technical terms that have specific meanings in the context of AI use in financial services. Definitions are drawn from a range of standards, academic publications, and government resources, and were informed by input from financial institutions, AI service providers, and public-sector participants. As AI technology and practice evolve, the Lexicon may be updated.

The Lexicon is an optional tool and is not intended for use either in the legal interpretation of any regulations or regulatory oversight reports or supervisory statements of US financial regulators, international arrangements or agreements, or private contracts. The inclusion of any source, term, or definition is for transparency and does not imply endorsement of any product, service provider, or organization. The Lexicon reflects the practical experience and collaborative work of participants and does not represent the official views of Treasury or any participating organization.

50

50

TREASURY CONCLUDES AI INNOVATION SERIES

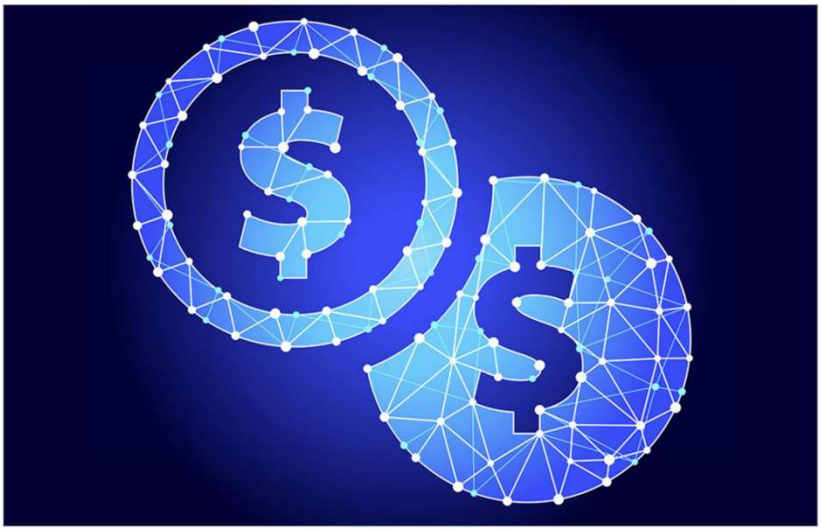
- Treasury (June 24, 2026) announced the Office of the Financial Stability Oversight Council (FSOC) and the Artificial Intelligence (AI) Transformation Office (AITO) held the fourth and final roundtable of the AI Innovation Series on May 19, 2026
  - Public-private initiative supports the continued strength and resilience of the U.S. financial system in an era of accelerating technological change
  - Supports Treasury's implementation of Executive Order 14179, "Removing Barriers to American Leadership in Artificial Intelligence," and Administration's AI Action Plan
- AI Innovation Series convened a variety of financial institutions, technology firms, and regulators for cross-sector dialogue on high-value AI use cases, practical approaches to scaling innovation, and regulatory impediments to adoption
  - Participants highlighted AI's potential to support financial stability and drive economic growth; enhance productivity; and combat increasingly sophisticated cyber-attacks, fraud, and financial crimes
  - Emphasized need for governance and regulatory frameworks to evolve alongside the rapid technological change
  - Requested greater regulatory clarity and harmonization as well as continued public-private engagement to support responsible innovation
- Readouts from each of the 4 sessions

51

Stablecoins and the GENIUS Act: An Overview

By Tony Murray

Supervision News Flash
November 2025



FEDERAL RESERVE BANK OF RICHMOND
Richmond • Baltimore • Charlotte

52

THE GENIUS ACT: GUIDING AND ESTABLISHING NATIONAL INNOVATION FOR U.S. STABLECOINS

- The regulatory landscape for digital assets reached a significant milestone with the passage of the GENIUS Act in July 2025. This landmark legislation establishes a comprehensive framework for payment stablecoins in the United States, addressing a critical gap in financial regulation.
- Payment stablecoins—privately issued digital assets designed to maintain a 1:1 backing with reserves assets like the U.S. dollar—now have clear regulatory parameters, consumer protections and oversight mechanisms.
- The GENIUS Act carefully distinguishes between payment stablecoins and other digital assets, requiring 100% reserves and implementing disclosure requirements similar to those in traditional banking.
- As financial institutions prepare for this new era of digital payment infrastructure, understanding the nuances between payment stablecoins and tokenized deposits becomes essential for compliance and strategic planning in the evolving financial ecosystem.

53

THE GENIUS ACT

- Worth noting is that institutions interested in establishing their own payment stablecoins must be federally or state chartered. The GENIUS Act differentiates charter options based on size and complexity of the issuer. Banks need to create a subsidiary that would serve as the payment stablecoin issuer, and it would be supervised by the bank's primary federal regulator. Non-bank entities approved to issue payment stablecoins would be supervised through the Office of the Comptroller of the Currency (OCC) or its appropriate state regulatory agency based on certain conditions outlined in the law.
- The GENIUS Act explicitly excludes payment stablecoins from securities or commodities designation and issuers of payment stablecoins cannot pay interest or yield to customers who hold them. Any issuer of payment stablecoins must hold high-quality, liquid reserve assets that are backed at least at a 1:1 basis (i.e. 100% reserve). The GENIUS Act also defines the disclosure requirements of any payment stablecoin issuer. These include its redemption policy, monthly attestations of the composition of the reserves and monthly CEO and CFO certifications of the reports.

54

TOKENIZED DEPOSITS

- "Tokenized deposits" are a digital representation of a customer's bank deposits. The GENIUS Act preserves the ability of financial institutions to issue tokenized deposits that would be able to pay yield or interest.
- Tokenized deposits are not considered payment stablecoins and the GENIUS Act preserves existing banking authority of financial institutions to engage in activities permissible under applicable state and federal law.
- Deposit insurance is another critical difference between tokenized deposits and payment stablecoins. As digital representations of bank deposits, tokenized deposits inherit the deposit insurance while payment stablecoins do not. This will be an area that we at the Richmond Fed will continue to monitor going forward.

55

REGULATORY FRAMEWORKS

- Finally, the GENIUS Act requires any payment stablecoin issuer to adhere to a regulatory framework that financial institutions are quite familiar with. Federal and state regulators must impose capital, liquidity and risk management requirements that are tailored to the business model and risk profile of the payment stablecoin issuer. All payment stablecoin issuers also are treated as financial institutions under the Bank Secrecy Act and must comply with the associated requirements.
- Innovation within the banking sector continues at a breakneck speed, and the GENIUS Act is one step towards establishing a formal framework to safely implement newer digital assets in the regulated financial system.
- While the GENIUS Act has received a significant amount of news coverage, the implementation will take time as federal and state regulators conduct rulemaking to implement the law.

56

FRB NEW YORK: STABLECOINS VS. TOKENIZED DEPOSITS

- Tokenized deposits and stablecoins are both digital forms of fiat currency that operate on blockchain networks.
  - **Tokenized deposits** are direct claims on regulated banks and are backed by the traditional banking system.
  - **Stablecoins** are privately issued tokens backed by off-chain reserve assets like U.S. Treasuries.
    - **Off-chain reserve assets** are traditional financial assets—like fiat currency, U.S. Treasury bills, or physical gold—held by an issuer to back a digital token on a blockchain. Because these physical or traditional assets cannot be natively stored on a blockchain, they must be held in the legacy financial system by a custodian.
- As blockchain-based economic activity has developed in recent years, demand has grown for a blockchain-native or "tokenized" form of money denominated in a traditional unit of account, especially the U.S. dollar. A number of so-called stablecoins have emerged to play this role, and the market capitalization of these stablecoins exceeded $300 billion in November 2025.

57

WHY OFF-CHAIN RESERVES MATTER

- They are the foundation of collateralized stablecoins (e.g., Tether or USD Coin). The issuer holds one U.S. dollar in a traditional bank account for every stablecoin minted, aiming to keep the token's value pegged to $1.
- **Real-World Connection:** They allow real-world assets (RWAs), such as real estate or securities, to be represented and traded as digital tokens without altering their underlying legal or physical status.
- **Risk Factor:** Because the reserves are not stored on the blockchain, users must trust a centralized custodian or rely on regular audits (like a Chainlink Proof of Reserve) to verify assets actually exist and tokens are fully backed
  - Proof of Reserves verifies digital asset collateralization held by crypto businesses, helping bring greater transparency to depositors via public reserves reporting or independent audits.

58

GENIUS ACT RESTRICTS STABLECOIN YIELDS

- In July 2025, Congress passed the GENIUS Act establishing a regulatory framework for *payment stablecoins*.
- Among the requirements established in GENIUS is a restriction on stablecoin issuers paying interest or yield or rewards (hereinafter, yield) to stablecoin holders.
- Crypto exchanges' and banks' opposing views on the yield restrictions has reportedly stalled crypto market structure legislation in the Senate.

www.congress.gov/crs-product/IF13174

59

THE GENIUS ACT YIELD RESTRICTION

- While this appears to create a blanket prohibition on interest, the restriction may not apply to the current market practice for issuing and holding stablecoins involving exchanges (the "three-party model" shown in **Figure 1**).
- Most stablecoin issuers—those companies that create stablecoins, and to whom most of GENIUS applies—only sell stablecoins to exchanges and larger market participants. Much retail use of stablecoins currently occurs through an intermediary—usually a cryptocurrency exchange.
- The exchange holds the stablecoin in custody—on the blockchain—on behalf of retail investor; the issuer passes interest on reserves to the exchange, which it uses to pay the investor yield. GENIUS does not explicitly prevent exchanges from paying rewards on stablecoins held on their exchange (which can be structured to be effectively equivalent to yield)—and many do.
- According to a regulatory filing, Circle, the issuer of the USDC stablecoin (the second largest stablecoin), pays a portion of the interest it earns on its reserves to Coinbase, the largest U.S.-based crypto exchange, proportionate to the stablecoins held on that platform.
- Also, some issuers reportedly pay exchanges a marketing budget to use at their discretion, which can presumably be passed on to holders of specific stablecoins. Therefore, while the issuer may not be paying the holder directly, they are supplying the funding that is simply passed through the exchange.

60

STABLECOINS AND DEPOSITS

- Payment stablecoins are intended to facilitate retail payments, but they can also potentially be held as relatively liquid and nonvolatile assets to store wealth. That makes them a potential substitute for bank deposits that could reduce banks' deposit base as the stablecoin market grows. According to one model, demand for stablecoins would rise significantly with yield, increasing their appeal as a store of value. Prevailing interest rates will affect the relevance of yield and the growth of the stablecoin market.
- The banking industry claims the ability to pay interest on stablecoins could result in a significant drain of bank deposits. Research from a Department of the Treasury advisory council identified U.S. transactional deposits (a $6.6 trillion market) as "at risk" from stablecoins (with around $281 billion outstanding in March 2026).
- Citigroup research estimates stablecoins outstanding will grow to $0.5-$3.7 trillion by 2030, displacing bank deposits equal to $182-$908 billion.
- Banks favor the strict prohibition on paying interest on stablecoins and have argued to close the "loophole" in GENIUS. The crypto industry views bank opposition to yield as anticompetitive behavior by an entrenched incumbent—bank deposits may pay interest—to thwart entry by a potential competitor.
- Banks argue that stablecoins could benefit from regulatory arbitrage, since issuers are subject to less complex, costly, and far-reaching regulatory requirements than banks. However, issuers are permitted to engage in far more limited activities than banks and play a more limited role in the financial system.

61

THE CLARITY ACT HAS NOT PASSED. STALLED FOR THIS SESSION.

- **House of Representatives:** Passed the Digital Asset Market Clarity Act (H.R. 3633) in July 2025.
- **Senate:** Advanced through committee consideration, but stalled due to debates over ethics rules and oversight.
- A key procedural cloture vote in the Senate was scheduled for September 15, 2026. The Senate failed, to advance the bill, falling short of the 60-vote threshold.
- Without congressional action the CFTC cannot create a registration and licensing regime. The SEC proposed a two-tier fundraising exemption of up to $75 million for Tier 2 in a 12-month period, but on a much less durable legal foundation.
- CLARITY's bankruptcy and BSA provisions cannot be replicated through agency action and does require an act of Congress.

62

62

PATTI D. JOYNER, CRCM

PATTI.JOYNER@FINSOLINC.COM

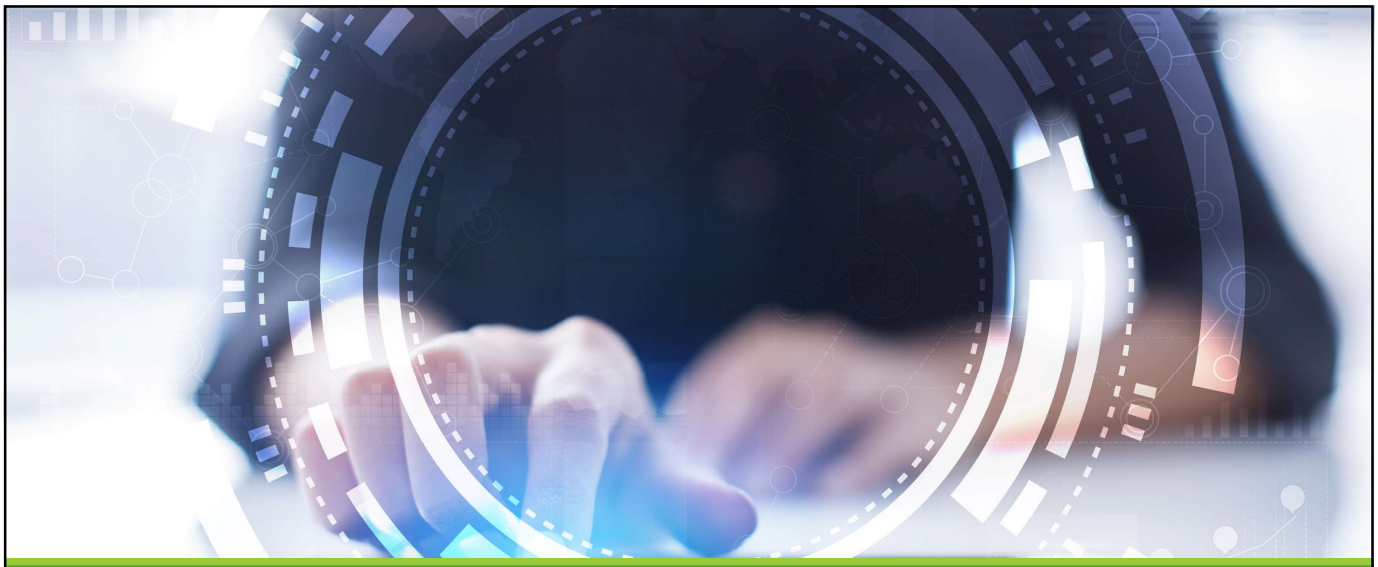
WWW.FINSOLINC.COM



FINANCIAL SOLUTIONS FOR GROWING COMPANIES, INC.

63

63

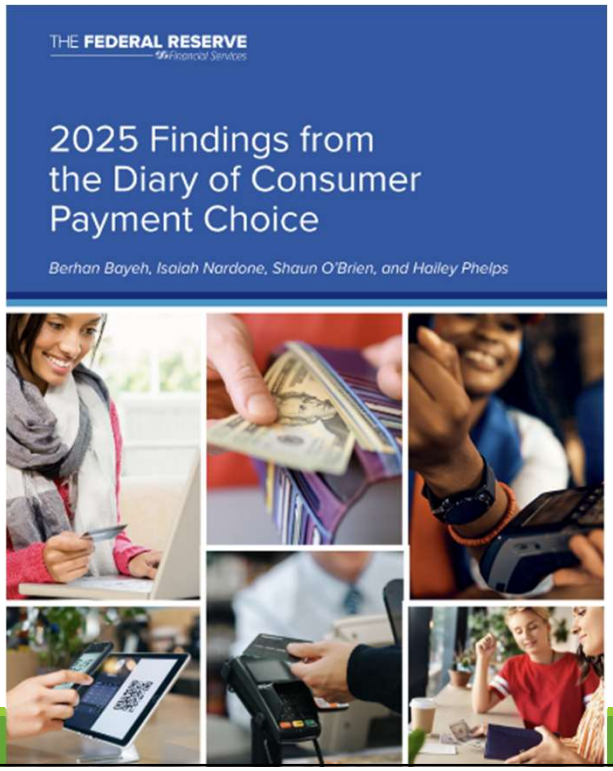


Reg E Refresh, Disputes and Effective Investigations

Thomas J. Healy, CRCM and Patti D. Joyner, CRCM

September 2026

1



The Survey and Diary of Consumer Payment Choice is a collaboration of the Federal Reserve Banks of Atlanta and Boston and Federal Reserve Financial Services FedCash® Services.

This research project aims to bring the voices of consumers into policy making and innovation as the payment system evolves.

FedCash Services works to understand when, how and why people use cash to fulfill its mission of ensuring depository institutions have a sufficient supply of currency and coin to meet public demand.

2024 statistics, report released in June 2025

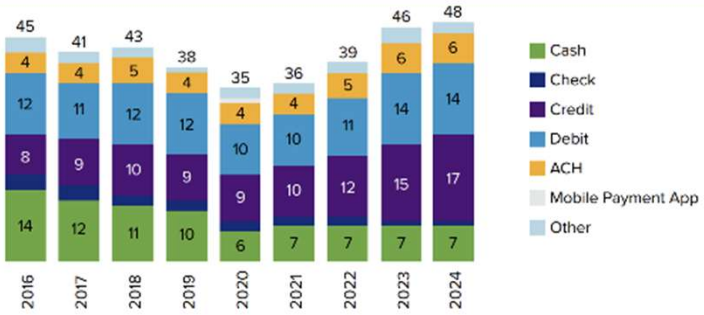
2

2

Number of Consumer Payments Increased

The average number of consumer payments per month has increased since 2021 (Figure 1).[9,10] October 2024 saw the highest reported number of payments in the Diary's history, at an average of 48 payments per month, an increase of two payments over the previous high reported in October 2023. This payment growth is reflected in consumers' use of credit cards both in person and remotely. Consumers' cash payments have remained consistent at seven payments per month since 2021, suggesting consumer cash use may be at the "floor." Consumers' steady use of cash since 2020 may be attributed to its unique characteristics — anonymity, ubiquity, accessibility, reliability, absence of marginal transaction costs — as well as its use as a secondary payment option and store of value.

Figure 1: Average number of total payments



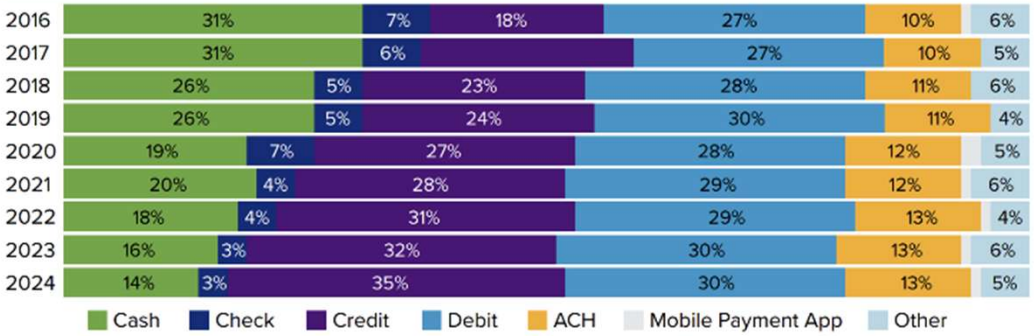
Note: All payments, including bills, purchases and person-to-person (P2P) payments.
Source: Survey and Diary of Consumer Payment Choice.

3

3

While the number of cash payments has remained unchanged since 2021, cash has decreased as a share of total payments (Figure 2). The share of ACH and debit card payments have increased by three percentage points since 2016, in conjunction with the increase in total payments. In contrast, the number of credit card payments grew more rapidly than payments overall and made up 35% of all payments in 2024, a 17 percentage-point increase from 2016.

Figure 2: Share of payment instrument use for all payments



Note: All payments, including bills, purchases and person-to-person (P2P) payments.
Source: Survey and Diary of Consumer Payment Choice.

4

4



Capgemini RESEARCH INSTITUTE

World Report Series 2026
World Payments Report

5

5

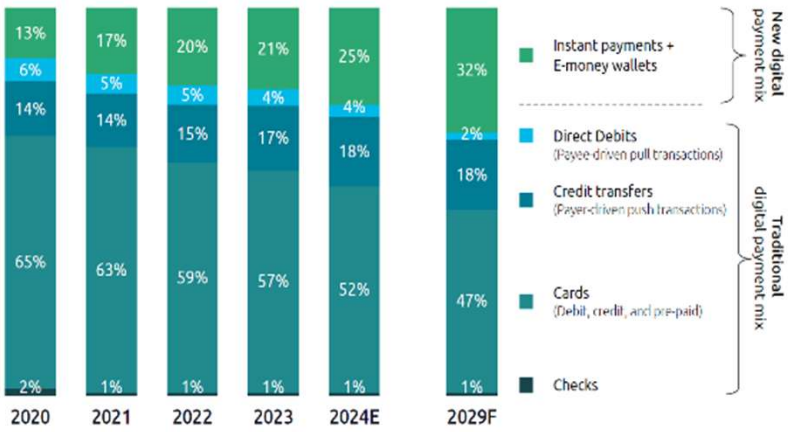
As figure 2 shows, this shift in transaction value is reflected in an equally significant change in transaction volume. The emergence of new digital tools, especially instant payments and e-money wallets, has fundamentally altered the landscape of non-cash payments:

- In 2020, cards made up 65% of the total non-cash payment volume.
- Instant payments and e-money wallets accounted for just 13%. But by 2024, that share increased to 25%, and it's projected to reach 32% by 2029.
- Share of cards, in contrast, are expected to decline to 47% during the same period even though its total transaction volume is on rise.
- Checks are becoming nearly obsolete, with a predicted decrease to just 1% of total non-cash payment volume.

Share of cards in non-cash transaction volume

65% (2020) vs **47%** (2029F)

Figure 2.
The new payments mix is taking up a bigger global share



Sources: Capgemini Research Institute for Financial Services Analysis, 2025; GlobalData Payments Analytics 2025.
Note: E = estimate and F = forecast.

6

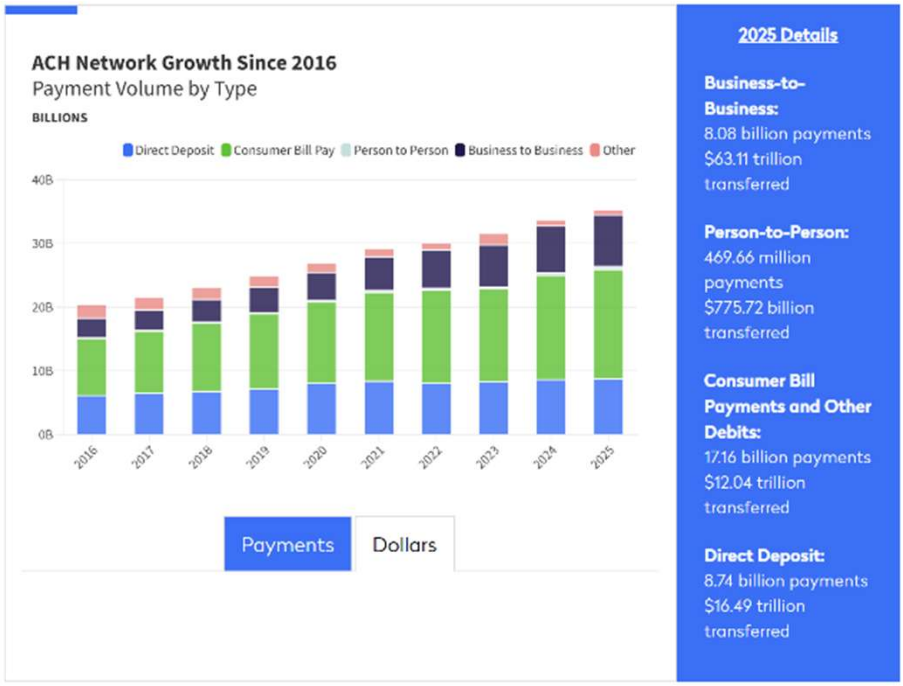
6



https://www.nacha.org/content/ach-network-volume-and-value-statistics

7

7



https://www.nacha.org/content/ach-network-volume-and-value-statistics

8

8

Nacha Statistics

https://www.nacha.org/content/ach-network-volume-and-value-statistics

In 2025, Same Day ACH payment volume reached 1.4 billion payments for the year, valued at $3.9 trillion.

From 2024 to 2025, Same Day ACH volume grew 16.7%, while the value of those payments increased 21.4%.

Overall, ACH Network payment volume rose nearly 4.9% from 2024 to 35.2 billion payments in 2025, climbing to an average 141 million daily transactions.

The value of those payments reached $93 trillion, a 7.9% increase over 2024.

The fourth quarter saw significant milestones for the ACH Network.

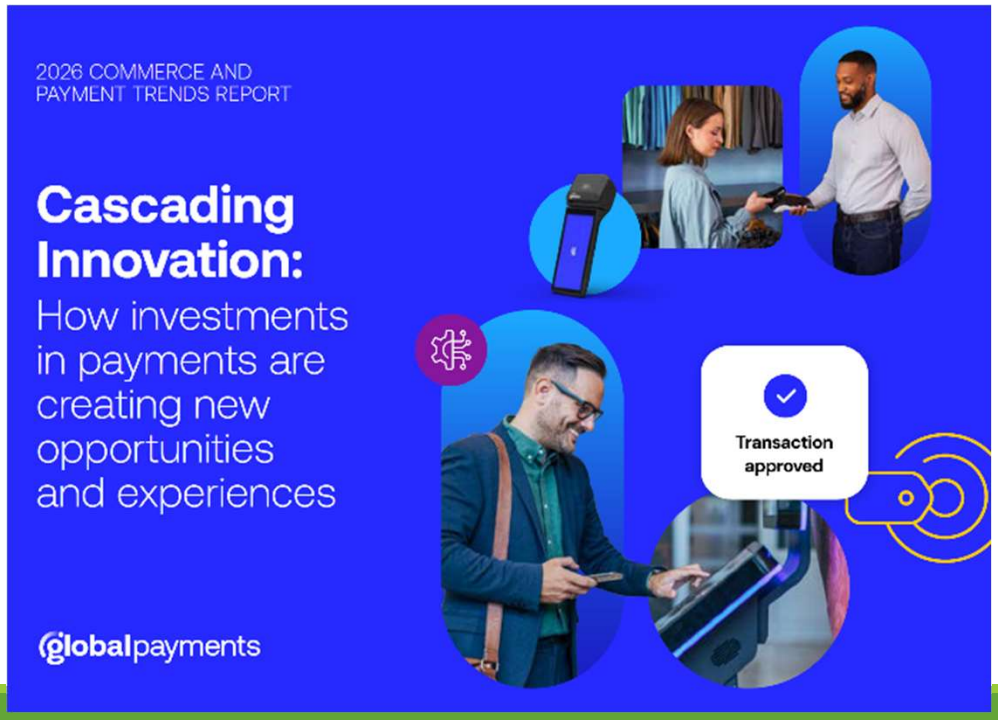
December 2025 saw the ACH Network's highest-ever monthly volume of 3.22 billion payments, and the highest monthly volume of Same Day ACH payments of 172.1 million.

Total fourth-quarter ACH Network volume was 9.1 billion payments valued at $24.4 trillion, respective increases of 5.1% and 8.9% over 2024 fourth quarter.

https://www.nacha.org/content/ach-network-volume-and-value-statistics

9

9



10

10

Global Payments: 2026 Cascading Innovation
Six Key Trends Reshaping the Future Of Commerce

1. AI is your shopping agent with Agentic Commerce
2. POS revolution has gone far beyond static terminals with more personal customer engagement
3. Embedded finance is helping businesses expand their relationships with consumers
4. Instant payments have become an urgent need
5. Stablecoins broke onto the scene in 2025 and have quickly captured the attention of businesses throughout the payment ecosystem
6. Evidenced by the self-service revolution, both consumers and businesses expect to fly through transactions without friction, using intuitive, self-directed tools including payment prompts. Self-service now means low-touch, no-waiting commerce!

11

11

Future of Federal Reserve Check Processing

Fed (Dec. 9, 2025) published a Request for Information to get public input on the future of the Federal Reserve's check services

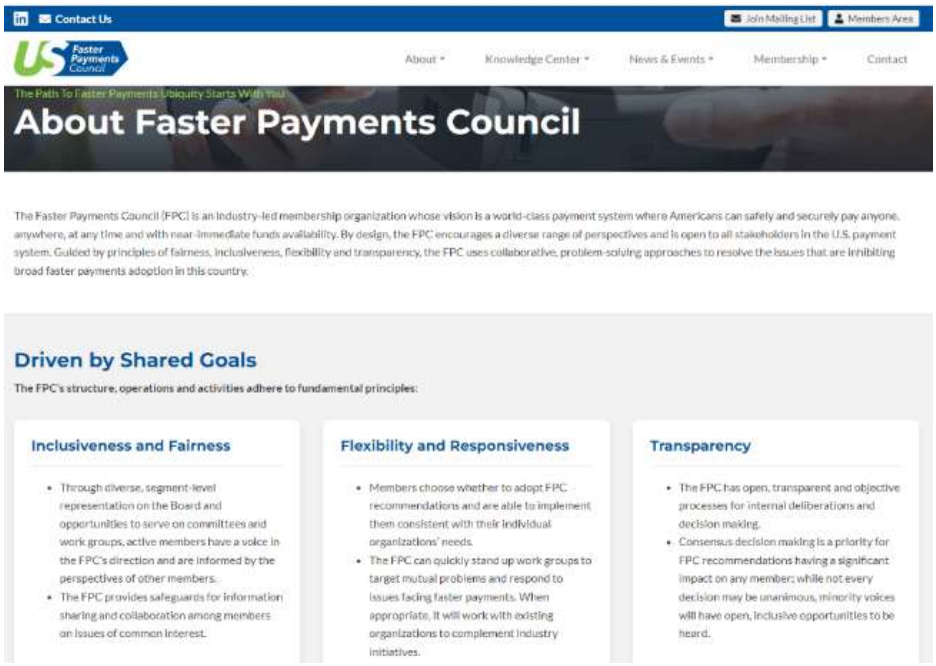
- Fed will assess possible strategies for the future of checks, acknowledging that check usage in the U.S. has steadily declined over recent decades even as noncash payments increased
- Strategies proposed range from maintaining current operations without new investments and resulting in degraded services, to simplifying and winding down check services to reduce costs, to investing heavily to upgrade aging infrastructure and improve reliability
- Any investment would have to be recovered through higher bank check processing fees

Fed is seeking input by March 9, 2026, on 10 items it will consider regarding check services, emphasizing continued use of checks as opposed to check fraud

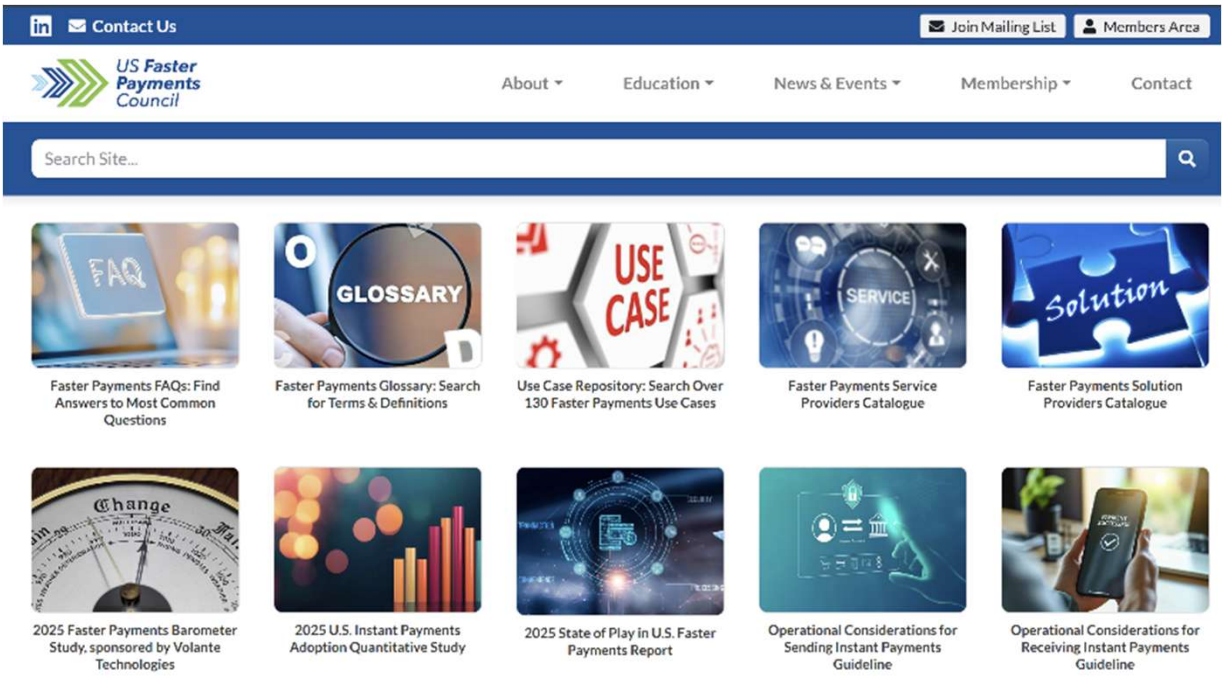
- Encouraged to weigh in on the importance of Fed's check services, impact of potential changes, willingness to incur additional costs, and challenges of transitioning to alternative payment methods
- How important are checks to your organization?

12

12


Contact Us
Join Mailing List
Members Area
About
Knowledge Center
News & Events
Membership
Contact
The Path To Faster Payments Ubiquity Starts With You
About Faster Payments Council
The Faster Payments Council (FPC) is an industry-led membership organization whose vision is a world-class payment system where Americans can safely and securely pay anyone, anywhere, at any time and with near-immediate funds availability. By design, the FPC encourages a diverse range of perspectives and is open to all stakeholders in the U.S. payment system. Guided by principles of fairness, inclusiveness, flexibility and transparency, the FPC uses collaborative, problem-solving approaches to resolve the issues that are inhibiting broad faster payments adoption in this country.
Driven by Shared Goals
The FPC's structure, operations and activities adhere to fundamental principles:
Inclusiveness and Fairness
Through diverse, segment-level representation on the Board and opportunities to serve on committees and work groups, active members have a voice in the FPC's direction and are informed by the perspectives of other members.
The FPC provides safeguards for information sharing and collaboration among members on issues of common interest.
Flexibility and Responsiveness
Members choose whether to adopt FPC recommendations and are able to implement them consistent with their individual organizations' needs.
The FPC can quickly stand up work groups to target mutual problems and respond to issues facing faster payments. When appropriate, it will work with existing organizations to complement industry initiatives.
Transparency
The FPC has open, transparent and objective processes for internal deliberations and decision making.
Consensus decision making is a priority for FPC recommendations having a significant impact on any member; while not every decision may be unanimous, minority voices will have open, inclusive opportunities to be heard.
13

13

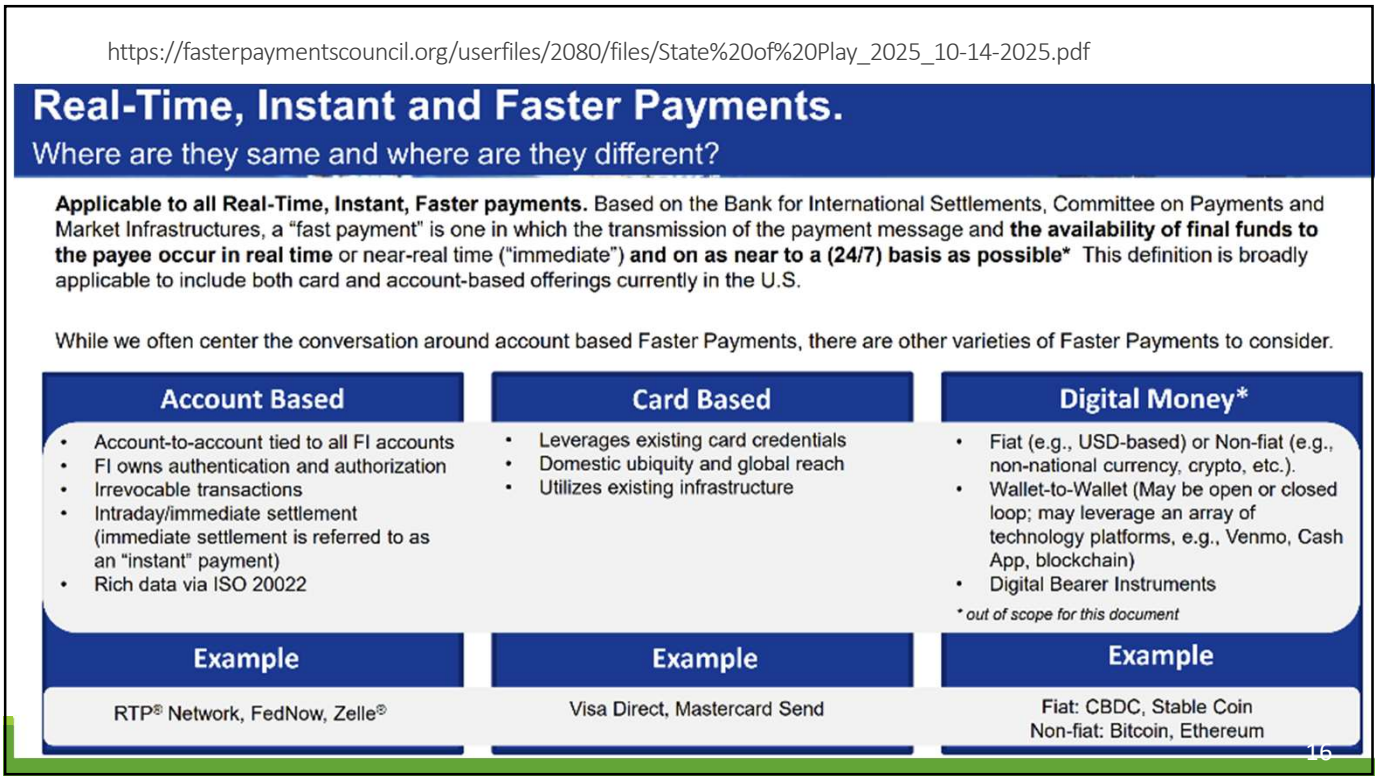

Contact Us
Join Mailing List
Members Area
US Faster Payments Council
About
Education
News & Events
Membership
Contact
Search Site...
FAQ
Faster Payments FAQs: Find Answers to Most Common Questions
GLOSSARY
Faster Payments Glossary: Search for Terms & Definitions
USE CASE
Use Case Repository: Search Over 130 Faster Payments Use Cases
SERVICE
Faster Payments Service Providers Catalogue
Solution
Faster Payments Solution Providers Catalogue
Change
2025 Faster Payments Barometer Study, sponsored by Volante Technologies
2025 U.S. Instant Payments Adoption Quantitative Study
2025 State of Play in U.S. Faster Payments Report
Operational Considerations for Sending Instant Payments Guideline
Operational Considerations for Receiving Instant Payments Guideline
14

14

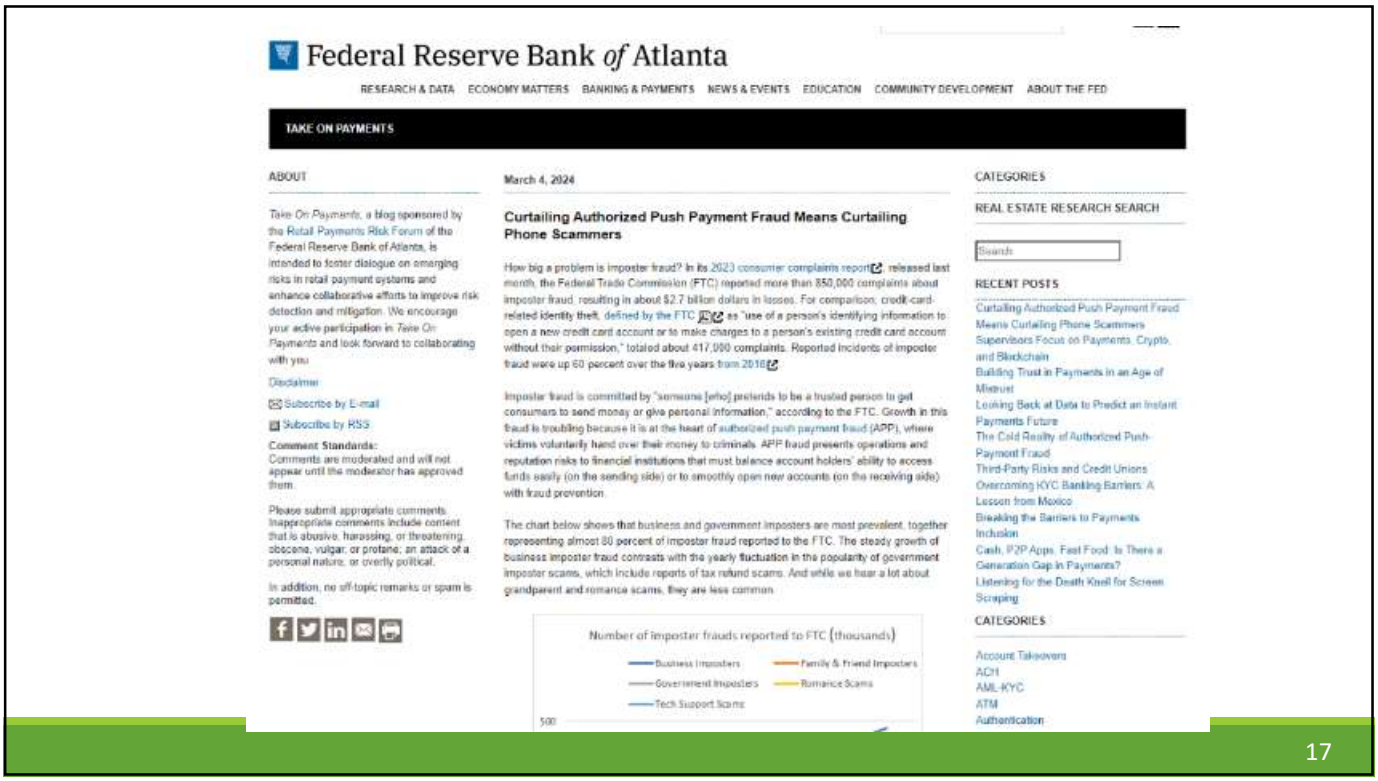


15

https://fasterpaymentscouncil.org/userfiles/2080/files/State%20of%20Play_2025_10-14-2025.pdf



16



17

17



EFTA and Its Implementing Regulation E

18

18

Legacy Reg E Covered Transactions (§ 1005.3)

- ATM and debit card transactions
- Payments under a bill payment system unless specifically noted otherwise
- ACH debits & credits
- Preauthorized transfers
- Transfer where merchant scans check's MICR line and generates an ECK ACH transaction

19

19

Legacy Reg E What's Not Covered? (§ 1005.3 (c))

- Transfers to/from in-bank accounts owned by same family that were not executed using an electronic means
- Paper transfers such as a check, draft or other paper instrument (Covered by UCC)
- Electronic benefit transfers (Covered by Agency's rules)
- Check guarantees or authorizations not resulting in debit or credit to a consumer's account
- Credit (loan) transactions (Covered by TILA & Reg Z)
- Wire transfers (Only covered by Foreign Remittance Rules)
- Business transfers (Covered by NACHA, VISA & MC Rules)
- Merchant disputes (Covered by VISA & MC Rules)

20

20

Reg E Coverage & Terms

Protects consumers engaging in electronic transfers and require disclosures

Establish the rights, liabilities and responsibilities of all parties involved in an electronic funds transfer

- Access Device: card, code or other means of access to initiate customer transfers
- Account: a DDA, savings or other consumer account used primarily for personal, family or household uses, including "payroll card account" established for EFTs of wages, salary or other employee compensation
- Consumer: any natural person
- Electronic Funds Transfer: any transfer of funds initiated via electronic terminal, telephone, computer or magnetic tape to debit or credit an account
- ACH Payment: includes check purchases converted into electronic transactions by the merchant
- ATM or Debit Card Transaction: ATM withdrawal or point of sale type transaction requiring PIN verification by customer
- Non-PIN POS Transaction: includes debit card transactions not requiring customer input of a PIN and authorized through Visa or MC ➔ must also follow network rules in addition to Reg E

21

21

§1005.2(i) Financial Institution

(i) "Financial institution" means

- A bank, savings association, credit union, or any other person that directly or indirectly holds an account belonging to a consumer, **or**
- That issues an access device and agrees with a consumer to provide electronic fund transfer services,
- Other than a person excluded from coverage of this part by section 1029 of the Consumer Financial Protection Act of 2010, title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act, Public Law 111-203, 124 Stat. 1376.

22

22

CFPB FAQ 2 "Financial Institutions"

Any P2P payment provider that meets the definition of a financial institution, as discussed in Electronic Fund Transfers Coverage: Financial Institutions Question 1, is a financial institution under Regulation E.

Thus, if a P2P payment provider directly or indirectly holds an account belonging to a consumer, they are considered a financial institution under Regulation E. 12 CFR 1005.2(i).

An example of an account that a non-bank P2P payment provider may directly or indirectly hold is a prepaid or mobile account whose primary function is to conduct P2P transfers. 12 CFR 1005.2(b)(3); Comment 2(b)(3)(i)-10.

Additionally, as discussed in Electronic Fund Transfers Coverage: Financial Institutions Question 1, non-account-holding providers of P2P payment or bill payment services are considered covered financial institutions under Regulation E if the provider issues an access device and agrees with a consumer to provide EFT services. 12 CFR 1005.2(i).

For example, a P2P provider may enter into an agreement with a consumer for a mobile wallet that the consumer can use to initiate debit card transactions from their external bank account to another person's external bank account.

23

23

Service Provider

§1005.14(a) Electronic Fund Transfer Service Provider Not Holding Consumer's Account

(a) Provider of electronic fund transfer service.

A person that provides an electronic fund transfer service to a consumer but that does not hold the consumer's account is subject to all requirements of this part if the person:

(1) Issues a debit card (or other access device) that the consumer can use to access the consumer's account held by a financial institution; **and**

(2) Has no agreement with the account-holding institution regarding such access.

24

24

§1005.14(b)(1) Electronic Fund Transfer Service Provider Not Holding Consumer's Account

(b) Compliance by service provider. In addition to the requirements generally applicable under this part, the service provider shall comply with the following special rules:

(1) Disclosures and documentation. The service provider shall give the disclosures and documentation required by §§ 1005.7, 1005.8, and 1005.9 of this part that are within the purview of its relationship with the consumer. The service provider need not furnish the periodic statement required by § 1005.9(b) if the following conditions are met:

(i) The debit card (or other access device) issued to the consumer bears the service provider's name and an address or telephone number for making inquiries or giving notice of error;

(ii) The consumer receives a notice concerning use of the debit card that is substantially similar to the notice contained in appendix A of this part;

(iii) The consumer receives, on or with the receipts required by § 1005.9(a), the address and telephone number to be used for an inquiry, to give notice of an error, or to report the loss or theft of the debit card;

(iv) The service provider transmits to the account-holding institution the information specified in § 1005.9(b)(1), in the format prescribed by the automated clearinghouse (ACH) system used to clear the fund transfers;

(v) The service provider extends the time period for notice of loss or theft of a debit card, set forth in § 1005.6(b)(1) and (2), from two business days to four business days after the consumer learns of the loss or theft; and extends the time periods for reporting unauthorized transfers or errors, set forth in §§ 1005.6(b)(3) and 1005.11(b)(1)(i), from 60 days to 90 days following the transmittal of a periodic statement by the account-holding institution.

25

25

§1005.14(b)(2) Electronic Fund Transfer Service Provider Not Holding Consumer's Account

(2) Error resolution.

(i) The service provider shall extend by a reasonable time the period in which notice of an error must be received, specified in § 1005.11(b)(1)(i), if a delay resulted from an initial attempt by the consumer to notify the account-holding institution.

(ii) The service provider shall disclose to the consumer the date on which it initiates a transfer to effect a provisional credit in accordance with § 1005.11(c)(2)(ii).

(iii) If the service provider determines an error occurred, it shall transfer funds to or from the consumer's account, in the appropriate amount and within the applicable time period, in accordance with § 1005.11(c)(2)(i).

(iv) If funds were provisionally credited and the service provider determines no error occurred, it may reverse the credit. The service provider shall notify the account-holding institution of the period during which the account-holding institution must honor debits to the account in accordance with § 1005.11(d)(2)(ii). If an overdraft results, the service provider shall promptly reimburse the account-holding institution in the amount of the overdraft.

26

26

§1005.14(c) Electronic Fund Transfer Service Provider Not Holding Consumer's Account

(c) Compliance by account-holding institution. The account-holding institution need not comply with the requirements of the Act and this part with respect to electronic fund transfers initiated through the service provider except as follows:

(1) Documentation. The account-holding institution shall provide a periodic statement that describes each electronic fund transfer initiated by the consumer with the access device issued by the service provider. The account-holding institution has no liability for the failure to comply with this requirement if the service provider did not provide the necessary information; and

(2) Error resolution. Upon request, the account-holding institution shall provide information or copies of documents needed by the service provider to investigate errors or to furnish copies of documents to the consumer. The account-holding institution shall also honor debits to the account in accordance with § 1005.11(d)(2)(ii).

27

27

REG E FINANCIAL INSTITUTION	REG E EFT SERVICE PROVIDER
Directly holds the consumer's account **OR** Issues an access device (like a debit card) to the consumer Has an agreement with the consumer to provide EFT services **Note:** Non-bank P2P payment providers can also be considered financial institutions if they hold consumer accounts or issue access devices and agree to provide EFT services. This results in both the non-bank P2P payment provider and the depository institution holding the consumer's account having error resolution obligations under Regulation E.	Does not hold the consumer's account. Does not hold the consumer's account but is still involved in providing EFT services They provide a service to facilitate the EFT **Example:** Company is a service provider under Regulation E if they issue an access device and there is **no specific agreement** between them and the account-holding financial institution for the EFT service. A payment processor would be considered a service provider in this context.

28

28

Reg E Basic Disclosures

- Initial disclosure
- Terminal receipts
- Preauthorized transfers
- Periodic statements
- Change in terms notice
- Error resolution notice



29

29

Initial Disclosure (§ 1005.7)

Define bank's business days

Consumer's right to EFT documentation

Consumer's liability for unauthorized trans

Telephone number and address to contact in event of unauthorized transaction

Error resolution notice & procedures

- Stop payment procedures and liabilities

Circumstances when bank will disclose consumer information to third parties

Notice of possible ATM surcharges as required under GLBA and Reg E

30

30

Terminal Receipts (§ 1005.9 (a))

- Transfer amount and charge, if any
- Date of transfer
- Type of transfer and account type
- Identifying code or #
- Terminal location
- Name of any third party to or from whom funds are transferred, if applicable

31

31

EFT Stop Payments (§ 1005.10(c))

- Notice may be oral or written
- Given any time up to 3 business days preceding the scheduled transfer date
- Bank may require written confirmation within 14 days of oral notification if bank notifies consumer of written requirement & address
- Oral stop payment becomes invalid if written confirmation not received from the consumer within 14 days
- Preauthorized Transfer Stop Pays:
  - If debit amount varies, payee must forward written notice of amount and date of transfer 10 days in advance
  - If credit from same payor every 60 days, payor or bank must notify customer within 2 days

32

32

Preauthorized Transfer Stop Pays

- If debit amount varies, payee must forward written notice of amount and date of transfer 10 days in advance
- If credit from same payor every 60 days, payor or bank must notify customer within 2 days

33

33

Periodic Statements (§ 205.9 (b))

- Must mail for each monthly cycle if EFT occurs but at least quarterly when no EFT has occurred.
  - Date and amount of transfer
  - Type of transfer and account type
  - Third party name, if applicable
  - If ATM transaction, location of terminal
- Account numbers involved and related EFT fees
- Statement opening and closing account balances
- Contact address & telephone # for confirmation of EFTs and in event of unauthorized transactions

34 34

34

Change in Terms Notice (§ 205.8)

Mail or deliver written notice 21 days before effective date if :

- It increases fees
- Change increases consumer liability
- Restricts types of available eft's
- Restricts frequency or dollar amount of eft's

35

35

Delivery of Change-in-Terms Notice (§ 205.8)

- May send revised initial disclosure statement if you highlight the changed terms or conditions
- Could provide a change in terms notice on the institution's periodic statement
- Provide electronically with consumer consent and follow electronic disclosure rules
- Post on Internet and notify consumers of its availability at least 21 days in advance of change.

36

36

Error Resolution Notice (§ 1005.8)

- Long form at least once per year -OR- short form with each periodic statement
  - **Best Practice: I highly recommend that you include "Consumer Account" in your error resolution notice to clearly identify this protection is CONSUMER ONLY!**
- Defines customer and bank process to resolve actual or suspected EFT errors
- Must be substantially the same as sample in Appendix A

Electronic Delivery (§ 1005.17)

- All disclosures may be delivered in electronic form:
- If the consumer agrees to such delivery and
- If delivery method allows visual text to be displayed (personal computer terminal)

37

37

EFT Error (§ 1005.11)

1. Unauthorized EFT
2. Incorrect EFT to or from consumer account
3. Omission of an EFT from statement
4. Computational or bookkeeping error
5. Receipt of incorrect amount of money at an ATM or other cash dispensing terminal
6. EFT not properly identified
7. Consumer request for clarification or info to determine whether an error was made

Not all Chargebacks are EFT Errors subject to Reg E Resolution Requirements!!!

38

38

15 USC § 1693a(12) Unauthorized Electronic Fund Transfer

(12) the term "unauthorized electronic fund transfer" means an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate such transfer **and** from which the consumer receives no benefit, but the term does **not** include any electronic fund transfer

A. initiated by a person other than the consumer who was furnished with the card, code, or other means of access to such consumer's account by such consumer, unless the consumer has notified the financial institution involved that transfers by such other person are no longer authorized,
B. initiated with fraudulent intent by the consumer or any person acting in concert with the consumer, or
C. which constitutes an error committed by a financial institution.

39

39

Reg E §1005.2(m) Unauthorized Transaction

(m) "Unauthorized electronic fund transfer" means an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit. The term does not include an electronic fund transfer initiated:

1) By a person who was furnished the access device to the consumer's account by the consumer, unless the consumer has notified the financial institution that transfers by that person are no longer authorized;
2) With fraudulent intent by the consumer or any person acting in concert with the consumer; or
3) By the financial institution or its employee.

40

40

Reg E §1005.2(m) Unauthorized Transaction Commentary

1. **Transfer by institution's employee.** A consumer has no liability for erroneous or fraudulent transfers initiated by an employee of a financial institution.

2. **Authority.** If a consumer furnishes an access device and grants authority to make transfers to a person (such as a family member or co-worker) who exceeds the authority given, the consumer is fully liable for the transfers unless the consumer has notified the financial institution that transfers by that person are no longer authorized.

3. **Access device obtained through robbery or fraud.** An unauthorized EFT includes a transfer initiated by a person who obtained the access device from the consumer through fraud or robbery.

4. **Forced initiation.** An EFT at an ATM is an unauthorized transfer if the consumer has been induced by force to initiate the transfer.

5. **Reversal of direct deposits.** The reversal of a direct deposit made in error is not an unauthorized EFT when it involves:

i. A credit made to the wrong consumer's account;
ii. A duplicate credit made to a consumer's account; or
iii. A credit in the wrong amount (for example, when the amount credited to the consumer's account differs from the amount in the transmittal instructions).

41

41

CFPB FAQ 4: Does an EFT initiated by a fraudster using stolen credentials meet the definition of unauthorized EFT?

Yes. Regulation E defines an unauthorized EFT as a transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit. 12 CFR 1005.2(m). When a consumer's account access information is obtained from a third party through fraudulent means such as computer hacking, and a hacker uses that information to make an EFT from the consumer's account, the transfer is an unauthorized EFT under Regulation E.

For example, the Bureau is aware of the following situations involving unauthorized EFTs:

- A consumer shares their account access information in order to enter into a transaction with a third party, such as a merchant, lender, or employer offering direct deposit, and a fraudster obtains the consumer's account access information by hacking into the computer system of the third party. The fraudster then uses a bank-provided P2P payment application to initiate a credit push payment out of the consumer's deposit account.
- A consumer shares their debit card information with a P2P payment provider in order to use a mobile wallet. A fraudster then hacks into the consumer's phone and uses the mobile wallet to initiate a debit card transfer out of the consumer's deposit or prepaid account.
- A thief steals a consumer's physical wallet and initiates a payment using the consumer's stolen debit card.

42

42

CFPB FAQ 5: A third party fraudulently induces a consumer into sharing account access information that is used to initiate an EFT from a consumer's account. Is this a Reg E unauthorized transaction?

Yes. Regulation E defines an unauthorized EFT as an EFT from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit. 12 CFR 1005.2(m). Comment 1005.2(m)-3 explains further that an unauthorized EFT includes a transfer initiated by a person who **obtained the access device from the consumer through fraud or robbery**. Similarly, when a consumer is fraudulently induced into sharing account access information with a third party, and a third party uses that information to make an EFT from the consumer's account, the transfer is an unauthorized EFT under Regulation E.

For example, the Bureau is aware of the following situations where a third party has fraudulently obtained a consumer's account access information, and thus, are considered unauthorized EFTs under Regulation E:

(1) a third-party calling the consumer and pretending to be a representative from the consumer's financial institution and then tricking the consumer into providing their account login information, texted account confirmation code, debit card number, or other information that could be used to initiate an EFT out of the consumer's account, and

(2) a third party using phishing or other methods to gain access to a consumer's computer and observe the consumer entering account login information. EFTs stemming from these situations meet the Regulation E definition of unauthorized EFTs. *Updated June 4, 2021*

43

43

Error Resolution Responsibilities

- Customer must notify financial institution as soon as error is known or suspected
- Financial institution must investigate the potential error and quickly resolve appropriately
- Consumer negligence cannot be held against them
- You cannot require a consumer to submit a police report or any written documents

Customer Responsibilities:

- Oral or written notice
  - Within 2 business days following learning of the loss or theft

    -OR-
  - Within 60 calendar days of transmittal of statement containing first error
- Bank's option to require written notice within 10 Bdays to receive provisional credit
  - Name, account number and description of error

(§ 1005.11)

44

44

Third Party Vendor Arrangements for Chargebacks & Disputes

Have you carefully examined your contract with your third party vendor?

- Are they processing **chargebacks** only or Reg E EFT Errors and Reg Z Billing Disputes for you?
- Are you complying with the contractual responsibilities imposed on the bank?
- Are you ensuring the vendor is providing the level and timeliness of service contracted for?
- Do you receive regular reports from the vendor on service level compliance?
- What notifications is the vendor to provide you for rejects, customer complaints, system changes, significant business interruptions or cybersecurity breaches, and other important incidents?

45

45

Bank's Responsibilities

- Investigate and notify customer of results within time period specified by regulation
- If error can't be resolved within period can take extra time if following actions are taken within 10 business days (20 business days if a new account) :
  - Re-credit disputed funds on provisional basis IF written customer notice received as requested
  - Advise consumer within 2 business days of provisional credit
  - Give consumer full use of provisional funds (§ 1005.11)

46

46

Investigations – Reg E 1005.11(c)(4)

(4) Investigation. With the exception of transfers covered by § 1005.14 of this part, a financial institution's review of its own records regarding an alleged error satisfies the requirements of this section if:

(i) The alleged error concerns a transfer to or from a third party; and

(ii) There is no agreement between the institution and the third party for the type of electronic fund transfer involved.

§ 1005.14 Electronic fund transfer service provider not holding consumer's account.

47

47

Investigations – Reg E 1005.11(c)(4) Commentary

1. ***Third parties.*** When information or documentation requested by the consumer is in the possession of a third party with whom the financial institution does not have an agreement, the institution satisfies the error resolution requirement by so advising the consumer within the specified time period.

2. ***Scope of investigation.*** When an alleged error involves a payment to a third party under the financial institution's telephone bill-payment plan, a review of the institution's own records is sufficient, assuming no agreement exists between the institution and the third party concerning the bill-payment service.

3. ***POS transfers.*** When a consumer alleges an error involving a transfer to a merchant via a POS terminal, the institution must verify the information previously transmitted when executing the transfer. For example, the financial institution may request a copy of the sales receipt to verify that the amount of the transfer correctly corresponds to the amount of the consumer's purchase.

4. ***Agreement.*** An agreement that a third party will honor an access device is an agreement for purposes of this paragraph. A financial institution does not have an agreement for purposes of § 1005.11(c)(4)(ii) solely because it participates in transactions that occur under the Federal recurring payments programs, or that are cleared through an ACH or similar arrangement for the clearing and settlement of fund transfers generally, or because the institution agrees to be bound by the rules of such an arrangement.

48

48

Investigations – Reg E 1005.11(c)(4)

5. ***No EFT agreement.*** When there is no agreement between the institution and the third party for the type of EFT involved, **the financial institution must review any relevant information within the institution's own records for the particular account to resolve the consumer's claim**. The extent of the investigation required may vary depending on the facts and circumstances. However, a financial institution may not limit its investigation solely to the payment instructions where additional information **within its own records** pertaining to the particular account in question could help to resolve a consumer's claim. Information that may be reviewed as part of an investigation might include:

i. The ACH transaction records for the transfer;

ii. The transaction history of the particular account for a reasonable period of time immediately preceding the allegation of error;

iii. Whether the check number of the transaction in question is notably out-of-sequence;

iv. The location of either the transaction or the payee in question relative to the consumer's place of residence and habitual transaction area;

v. Information relative to the account in question within the control of the institution's third-party service providers if the financial institution reasonably believes that it may have records or other information that could be dispositive; or

vi. Any other information appropriate to resolve the claim.

49

49

Failure to Promptly Initiate an Investigation

www.consumercomplianceoutlook.org/2021/second-issue/error-resolution-and-liability-limitations-under-regulations-e-and-z/

Institutions must investigate alleged errors promptly after receiving an error notice containing the information set forth in Regulation E,[7] whether written or oral.[8] While financial institutions may request a written confirmation after receiving an oral notice of error, they still must promptly begin investigating after receiving the oral notice.[9] Additionally, while institutions may require that notice be provided only to the telephone number or address disclosed by the institution, if the consumer attempts to provide notice in a different manner, the institution must maintain reasonable procedures to refer the consumer to the specific telephone number or address required.[10]

An institution does not comply with the prompt investigation requirement if it requires, as a condition for starting the investigation, that consumers provide information not specified in the regulation. **Common examples of requests the regulation does not require in a consumer's error notice and therefore may not be used as a condition to begin the investigation, include**

- **asking a consumer to visit a branch to complete an error notice,**
- **requesting that the consumer first try to resolve the dispute with the merchant, or**
- **requiring a notarized affidavit or the filing of a police report.**[11]

50

50

Failure to Promptly Initiate an Investigation

www.consumercomplianceoutlook.org/2021/second-issue/error-resolution-and-liability-limitations-under-regulations-e-and-z/

A 2019 Bureau consent order against USAA Federal Savings Bank (USAA) provides additional examples of conduct inconsistent with the regulatory obligation to promptly initiate an investigation. For consumers who notified USAA of a suspected error concerning a payday loan, the bank's procedures directed representatives to warn consumers about potential financial and legal consequences of proceeding with the investigation.

- Staff informed consumers that if USAA determined that the ACH debit was authorized, consumers would put their USAA membership at risk, they may be ineligible to purchase additional USAA products, and their existing USAA accounts could be closed.
- The script also stated that it is a federal crime to make a false statement to a bank and doing so is punishable by a fine of up to $1 million or imprisonment for up to 30 years, or both.
- If the customer still wanted to proceed with the error resolution procedure, the bank required the customer to complete and notarize a written dispute form.

The consent order noted that these practices violated Regulation E's requirement to promptly initiate and conduct error resolution investigations.[12]

To help manage this risk, compliance officers can review error resolution procedures for any steps that may delay an investigation and confirm they are consistent with the regulatory requirement for a prompt investigation. Additionally, compliance officers can review the procedures for receiving consumer disputes from different channels to ensure disputes are routed to the correct point of contact. This could include tellers, receptionists receiving incoming calls, and email inboxes for consumer feedback.

51

51

Not Conducting a Reasonable Investigation

www.consumercomplianceoutlook.org/2021/second-issue/error-resolution-and-liability-limitations-under-regulations-e-and-z/

A financial institution cannot deny a consumer's claim of an error without conducting a reasonable investigation, unless it corrects the error as alleged by the consumer. A reasonable investigation includes reviewing relevant information within the institution's records. If this review confirms the error, the claim cannot be denied.

When the alleged error is an unauthorized EFT, the EFTA places the burden of proof on the financial institution to establish the transaction was authorized. Therefore, if the institution cannot establish the disputed EFT transaction was authorized, the institution must credit the consumer's account.[15]

- For example, in the *USAA* enforcement action, the Bureau found that when consumers had previously authorized transactions with a merchant that predated a disputed transaction with the merchant**, the bank summarily determined an error had not occurred without considering other evidence in its records,** including the consumer's error notice.

In numerous instances when USAA found no error, the Bureau determined a reasonable review of all relevant information within USAA's records would have validated the error. The consent order noted that an institution's "reviews must include 'any relevant information within the institution's own records,' … and the investigation 'must be reasonable.'"[16]

To mitigate this risk, compliance departments can conduct transaction testing on previously denied error notices. For each previously denied allegation within the selected sample, the institution can confirm that employees reviewed all relevant information within the institution's records and that the findings of the investigation met the institution's burden of proof to establish that an error did not occur. If the transaction testing revealed it was not adhering to regulatory requirements, the staff handling the investigations can receive additional training on this issue.

52

52

What Constitutes A Reasonable Investigation?

Reviewing the institution's own records:

This is a foundational requirement and includes checking the transaction details, account statements, and any written communications related to the transaction.

Checking for common patterns:

Examining historical information and the consumer's location at the time of the alleged unauthorized transfer can help identify patterns or anomalies.

Verifying information transmitted for POS transactions:

For point-of-sale transfers, the institution needs to verify the information that was sent to the merchant.

Involving third parties:

If a transaction involves a third party and the institution has an agreement with that party, the investigation may extend to the third party's records.

Collecting other relevant information:

The investigation can include reviewing security camera footage, signature information on POS transactions, or police reports or other official complaints filed, if any.

53

53

CFPB Orders Operator of Cash App to Pay $175 Million and Fix Its Failures on Fraud (Jan 16, 2025)

Block allowed fraud to proliferate, **closed cases of reported fraud without even opening a legally required investigation.**

The CFPB ordered Block, the operator of the peer-to-peer payments app Cash App, to refund and pay other redress to consumers up to $120 million and pay a penalty of $55 million into the CFPB's victims relief fund.

Block employed weak security protocols for Cash App and put its users at risk. While Block is required by law to investigate and resolve disputes about unauthorized transactions, the company's investigations were woefully incomplete. Block directed users — who had suffered financial losses as a result of fraud — to ask their bank to attempt to reverse transactions, which Block would subsequently deny. Block also deployed a range of tactics to suppress Cash App users from seeking help, reducing its own costs.

"Cash App created the conditions for fraud to proliferate on its popular payment platform," said CFPB Director Rohit Chopra. "When things went wrong, Cash App flouted its responsibilities and even burdened local banks with problems that the company caused."

54

54

CFPB Orders Operator of Cash App to Pay $175 Million and Fix Its Failures on Fraud (Jan 16, 2025)

Cash App attempted to avoid many of its investigative obligations through tricking consumers with its Terms of Service.

- For example, many Cash App users link their bank account to the app. When a transaction occurs, the money is pulled from the user's bank account and sent to the transaction recipient. In Cash App's Terms of Service, consumers are led to believe that disputes are the responsibility of their linked bank.
- The Electronic Fund Transfer Act generally requires that peer-to-peer platforms, including Cash App, investigate disputes of unauthorized transactions, and a company cannot simply use fine print to escape these legal requirements.
- When it did conduct investigations, Block used intentionally shoddy investigation practices to close reports of unauthorized transactions in the company's favor.

Block also deprived Cash App users of meaningful and effective customer service and left the network vulnerable to criminals defrauding users.

- While Block included a telephone number on the back of its Cash Card and in its Cash App Terms of Service, for many years this telephone number did not connect consumers to customer support of any type. Instead, it led to a pre-recorded message directing consumers to contact customer support through the app. Consumers could only contact Block through the app or through U.S. mail and were often met with delayed, inadequate, confusing, or inaccurate responses.
- Consumers looking for an alternate route to Cash App customer service through web searches were targeted by fraudsters posing as Cash App representatives, who tricked them into giving up their passwords and other personal information.

Block knew that its customers were being targeted by fraudsters in this way but failed to take timely action to address the issue.

55

55

Acceptable Error Investigation

(Examples per OCC AL 2001-9)

There's a LOT of focus on Investigations in Supervisory Highlights!!!!

- Review customer statements and transaction documentation
- Historical information regarding customer activity (time, frequency, location, amounts and transaction types)
- Transaction location relative to customer's home, business or shopping locale
- Customer's location at the time of error
- Pertinent problems reported by other customers
- Signature information or other verification tools for transactions
- Police reports or security camera photographs
- Communications between customer and merchant
- AVS, CVV, and delivery verification

  - Burden of Proof is on the BANK!!!
  - Without evidence to prove otherwise, you must assume the customer is correct.

56

56

Investigation Resolution

(§ 1005.11)

If error did occur:

- Correct error within 1 business day of determination, refund must include interest and charges
- Provide written or oral notice to customer
- Provisional credit cannot be taken back once it has been made final – regardless of information you find out later
  - If merchant credits customer after you have already given customer's money back, bank may keep the merchant's credit. Based on the principle that customer is not entitled to double payment, "unjust enrichment"

57

57

Provisional Funds

(§ 1005.11)

- NOT required if customer did NOT submit the written complaint per your instructions
- If provisional funds reversed, give notice of date and amount of reversing transaction
- Honor without charge any **third party** debits for 5 business days after notice is sent
- Honor third party items **totaling amount less than or equal to amount provisionally credited** and then reversed
- Not required If customer reports dispute later than 60 calendar days following transmittal of statement where error first appeared
  - Must still investigate, but provisional credit does not apply!

58

58

Two Categories of Customer Liability

(§ 1005.11)

1. Access Device Missing or Stolen
2. Customer Statement Includes Unauthorized Transactions

Each category has its own liability calculation!

59

59

Two Business Day Notice Rule

Does NOT include the day the consumer learns of the loss or theft or any day that is not a business day

Calculated based on two 24-hour business days without regard to bank's business hours or time of day the consumer learns of loss or theft

- Business day ends at midnight!

Consumer learns of loss at 6:00 PM on Friday. Assuming Saturday is a business day and Sunday is not*, the 2-business-day period begins on Saturday and expires **at 11:59 PM on Monday** – NOT at the close of business Monday.

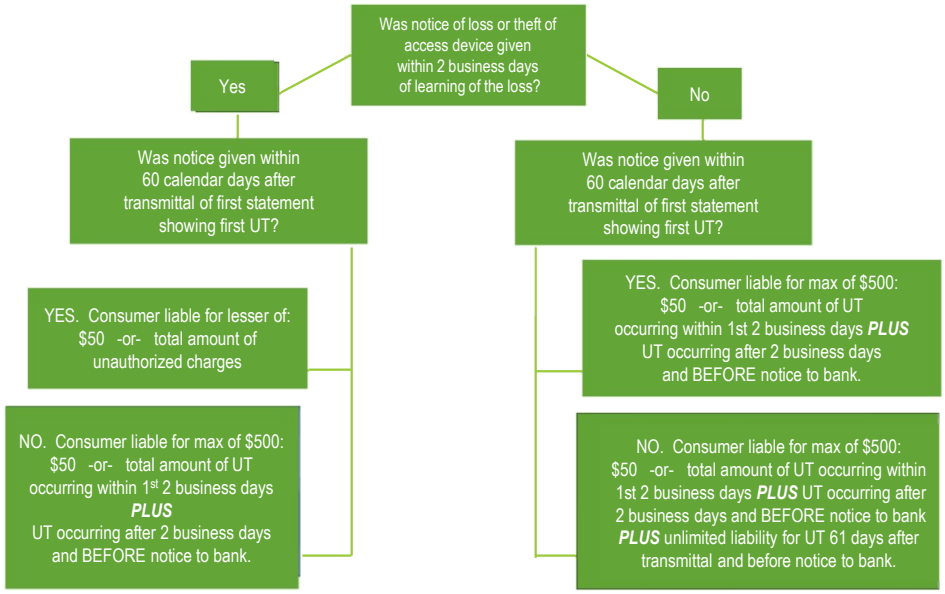
(§ 1005.11)

60

60

Loss or Theft of Access Device

UT = Unauthorized Transaction

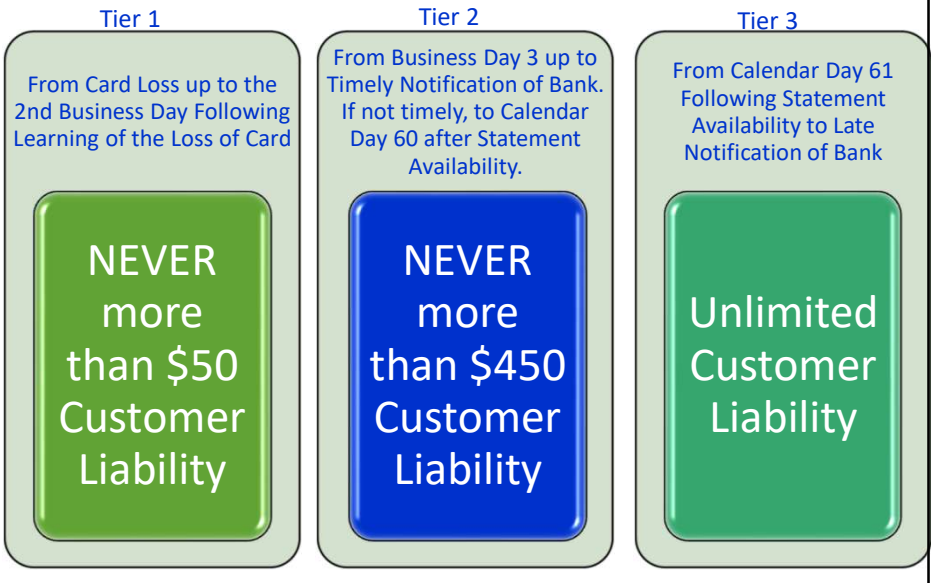


61

61

Customer Liability: Lost or Stolen Card

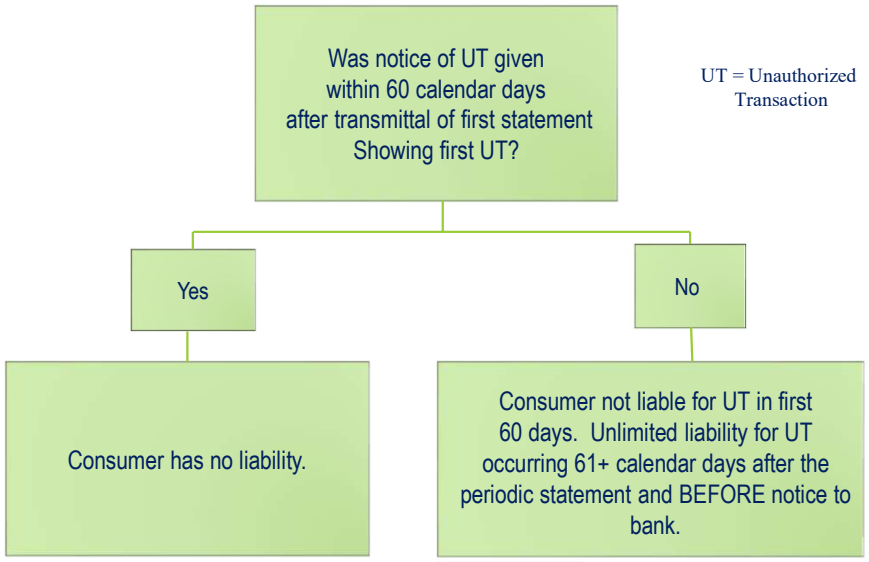
Tier 1 + Tier 2 may never exceed $500 combined customer liability! If no $50 in Tier 1, full $500 may be assessed in Tier 2.



62

62

Unauthorized Transfers on Periodic Statement



63

63

Late Reports of Disputed Transactions

If consumer customer reports dispute later than 60 calendar days following transmittal of statement where error first appeared:

- a) You must still investigate and determine whether or not an error occurred;
- b) No Reg E deadlines for timely completion of investigation apply;
- c) No Reg E provisional credit is required, regardless of customer's written or verbal dispute; and
- d) Same liability calculations apply to determine customer liability as for a timely reported dispute. Final resolution cannot be reversed, even if more information later proves the error did not occur.

NOTE: The consumer can even dispute transactions after the deposit account has been closed.

64

64

CFPB Supervisory Highlights #24, Summer 2021, June 2021 2.4.3 Failure to Timely Investigate errors

If a financial institution is unable to complete its investigation within 10 business days, 12 C.F.R. §1005.11(c)(2) provides that an institution may take up to 45 days from receipt of the notice of error to investigate and determine whether an error occurred provided it, among other things, provisionally credits the consumer's account as discussed above.

If the alleged error involves an EFT that was not initiated within a state, resulted from a point-of-sale debit card transaction, or occurred within 30 days after the first deposit to the account was made, the institution may take up to 90 days to investigate and determine whether an error occurred, provided it otherwise complied with the requirements of 12 C.F.R. §1005.11(c)(2).

Examiners found that financial institutions violated Reg E by failing to complete investigations and make a determination within 45 days from receipt of the notice of error and within 90 days from receipt of the notice of error for point-of-sale debit transactions, respectively, after providing provisional credit within 10 business days of the error notice.

In each instance, the financial institutions exceeded the applicable timelines.

65

65

CFPB Supervisory Highlights #24, Summer 2021, June 2021 2.4.4 Failure to Conduct Reasonable Investigations

All error investigations "must be reasonable." When it applies, Reg E, 12 C.F.R. §1005.11(c)(4), requires that a financial institution in investigating an error must conduct, at a minimum, a "review of its own records regarding [the] alleged error." This review must include at least "any relevant information within the institution's own records."

Examiners found that some financial institutions violated Reg E by failing to conduct a reasonable investigation and instead denied claims solely because the consumers had previously conducted business with a merchant.

- One institution, upon seeing that a consumer was challenging a charge from a merchant with whom the consumer had prior transactions, closed error investigations without completing them, and instead instructed consumers to first direct the claim to the merchant that made the charge.

In response to examiners' findings, the financial institutions updated their training to ensure that employees were properly trained on the applicable Reg E investigation requirements and enhanced certain policies and procedures and monitoring to ensure investigations are completed properly. In addition, the financial institutions identified and remediated all consumers whose Reg E error claims were wrongly denied based upon pre-existing relationships with the merchant and whose error resolution claims were not investigated as required.

66 66

66

Recommendations for Reasonable Investigations

These actions should be taken collectively as a whole, not individually as any one may not be enough alone to support an authorized/unauthorized decision:

- Interviewing consumer (most important!)
- Contacting Merchant for proof of purchase (e.g., copy of sales receipt to verify amount)
- Pictures of physical delivery or delivery to an IP address
  - Note: Could demonstrate receipt but doesn't mean the cardholder authorized or received the item!
  - Use caution when using this since receipt doesn't necessarily mean authorized
    - Teenage child steals mom's card and orders stuff, has it delivered to the house but hides/uses the stuff without mom's knowledge
    - IP address shows the PC that received the new gaming "assets" ordered and received by minor not authorized to use the card
- Obtaining video evidence from store or ATM
- For bill pay transactions, review of bank's records assuming no agreement exists between bank and third-party involved in the payment transaction
- Location of customer when transaction occurred – useful if fraudulent transaction was conducted in-person
- Other information in bank's records
  - Primary obligation is to always fully examine all records in our possession
- Just because a customer used this merchant before does not automatically justify denying claim this transaction was actually unauthorized

67

67



Critical Reg E Points for Compliant Investigations

Be cautious on what your financial institution requires from consumers:

Reg E prohibits including burdensome requirements as part of EFT Consumer Error investigations

- Cannot require consumer sign your form before starting your investigation
- Prohibited from including in consumer deposit terms and conditions agreement consumer waives Reg E protections included by statute and regulation
  - Waiving liability protection if consumer has shared account
  - Increasing the regulatory thresholds for consumer liability
  - Shortening time for consumer notifications to bank of suspected unauthorized transactions
- May NOT require consumer to contact merchant or third-party service provider before bank accepts the dispute
- Prohibited from requiring consumer file a police report or network reports of unauthorized or unknown transactions

Customer need only indicate which transaction(s) is suspected of being unauthorized, such that the bank knows which transaction(s) and why customer does not believe it to be valid

Bank must investigate promptly upon receipt of a verbal or written notice of error and may NOT delay initiating or completing investigation pending receipt of information from consumer!

68

68

Investigation Resolution

(§ 1005.11)

If error did occur:

- Correct error within 1 business day of determination, refund must include interest and charges
- Provide written or oral notice to customer
- Provisional credit cannot be taken back once it has been made final – regardless of information you find out later
  - If merchant credits customer after you have already given customer's money back, bank may keep the merchant's credit. Based on the principle that customer is not entitled to double payment, "unjust enrichment"

69

69

Provisional Funds

(§ 1005.11)

- NOT required if customer did NOT submit the written complaint per your instructions
- If provisional funds reversed, give notice of date and amount of reversing transaction
- Honor without charge any **third party** debits for 5 business days after notice is sent
- Honor third party items **totaling amount less than or equal to amount provisionally credited** and then reversed
- Not required If customer reports dispute later than 60 calendar days following transmittal of statement where error first appeared
  - Must still investigate, but provisional credit does not apply!

70

70

Two Business Day Notice Rule

Does NOT include the day the consumer learns of the loss or theft or any day that is not a business day

Calculated based on two 24-hour business days without regard to bank's business hours or time of day the consumer learns of loss or theft

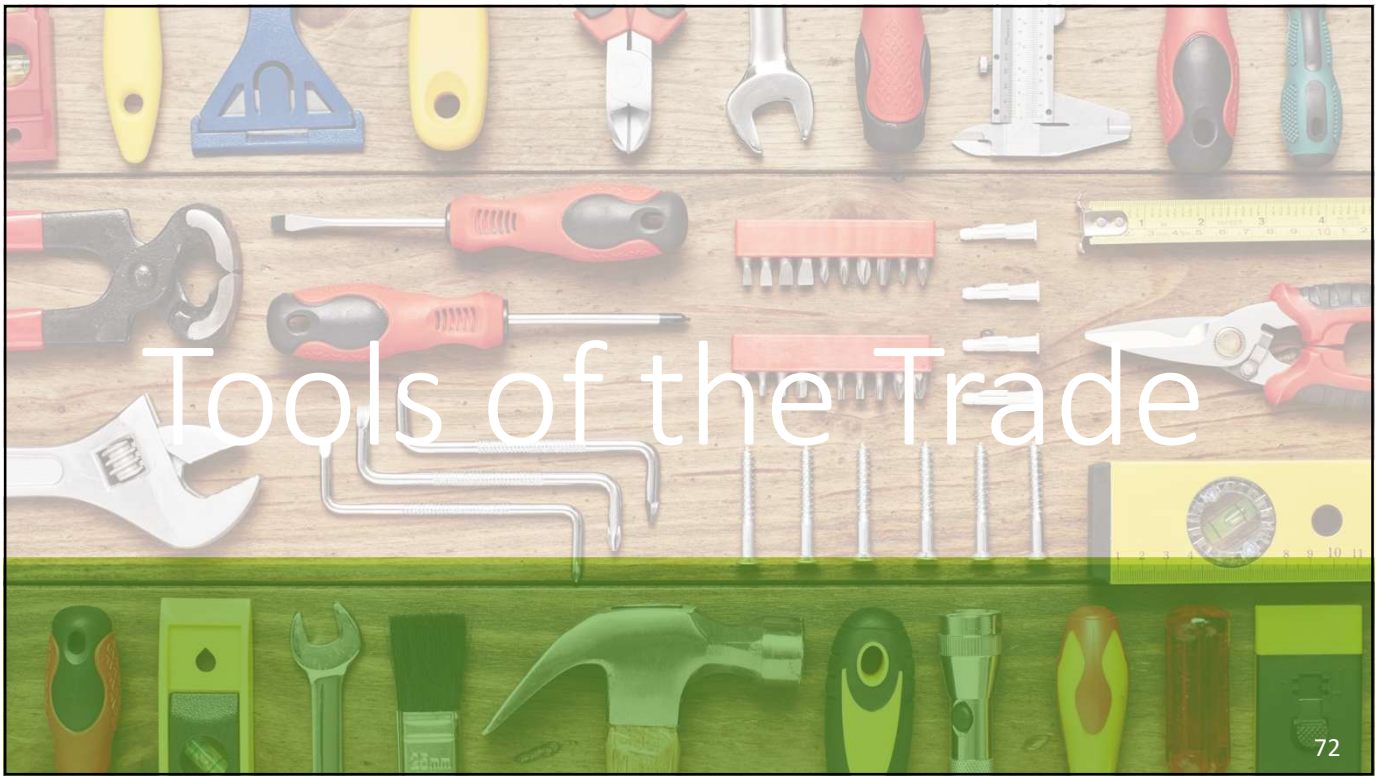
- Business day ends at midnight!

Consumer learns of loss at 6:00 PM on Friday. Assuming Saturday is a business day and Sunday is not*, the 2-business-day period begins on Saturday and expires **at 11:59 PM on Monday** – NOT at the close of business Monday.

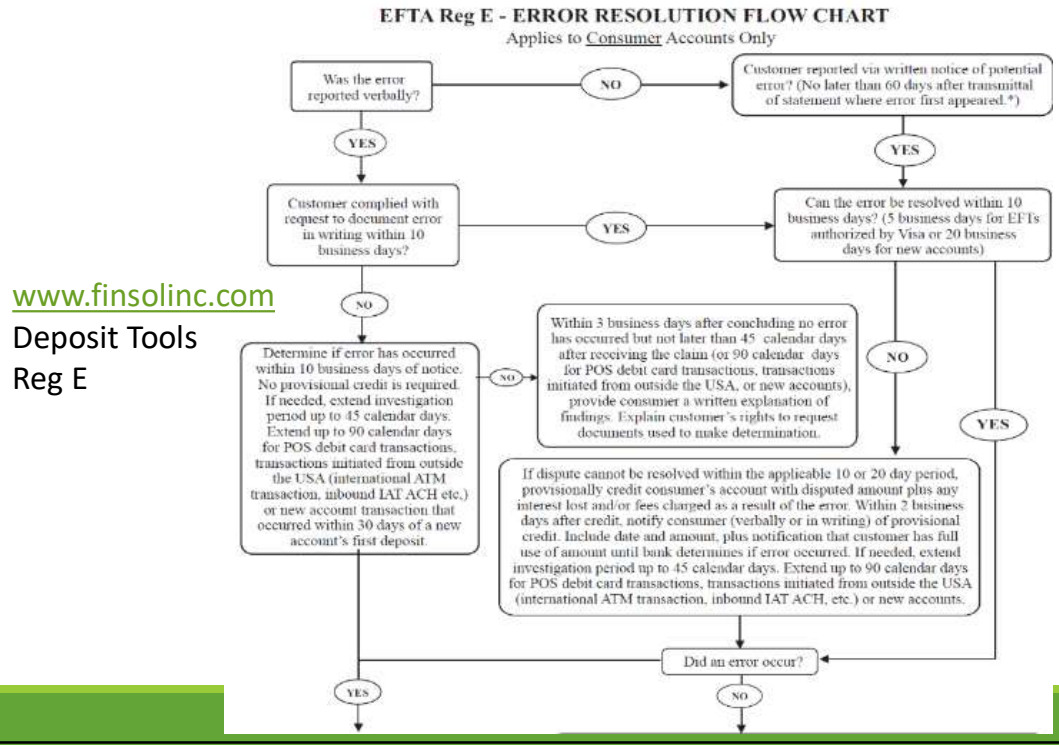
(§ 1005.11)

71

71



72



www.finsolinc.com
Deposit Tools
Reg E

73

73

BETTER FRAUD DATA. BETTER DEFENSE.

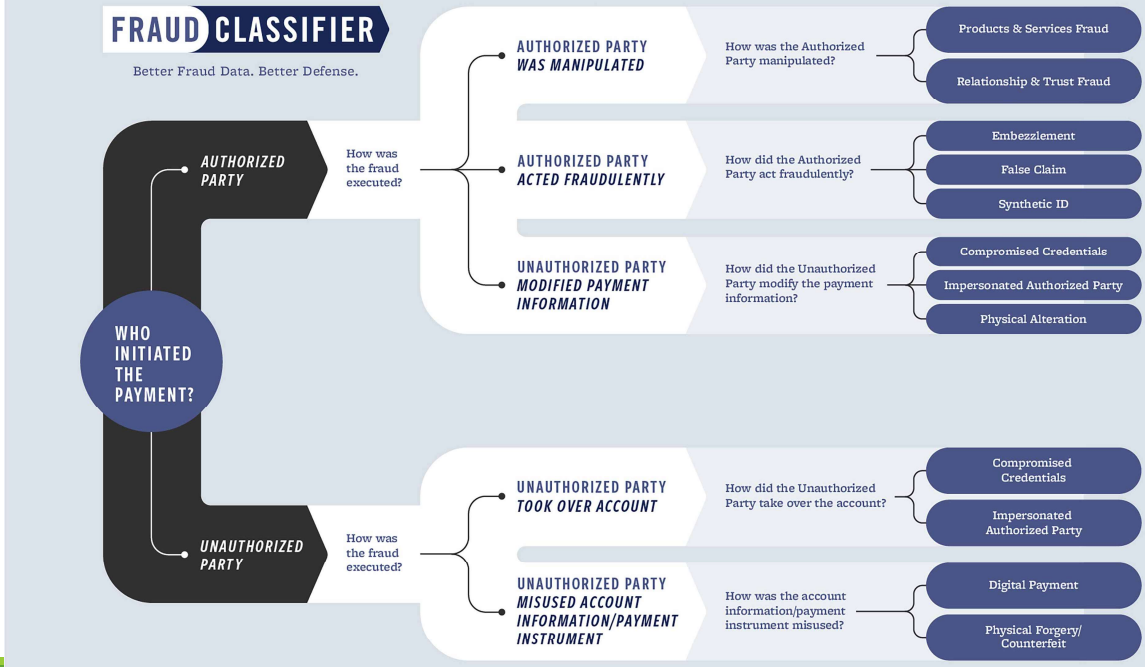
HTTPS://FEDPAYMENTSIMPROVEMENT.ORG/FRAUDCLASSIFIER/INDEX.HTML

The FraudClassifier℠ model provides an intuitive approach to classifying fraud involving payments. It enables payments stakeholders to classify fraud independently of payment type, payment channel or other payment characteristics. The model includes supporting definitions to facilitate consistent application across the industry.

This interactive experience provides the ability to navigate through different fraud classification paths within the model and view a fraud scenario that relates to that particular classification path. Once you've navigated through one path, there is an option to start over and try a new path!

74

74



75

Who Initiated the Payment?

Payment Initiation

Payment Initiation is the creation of an instruction to transfer funds. Examples of instructions include a signed check, ACH individual payment or file, or wire instructions; this also includes the instructions for a future-dated or recurring payment.

Authorized Party

An individual or entity with the right to initiate the payment.

Unauthorized Party

An individual or entity without the right to initiate the payment.

76

76

How Was the Fraud Executed? By an Authorized Party

Authorized Party Was Manipulated

Authorized Party is deceived or coerced to initiate a payment.

Authorized Party Acted Fraudulently

Authorized Party initiated the payment with intent to defraud.

Unauthorized Party Modified Payment Information

Unauthorized Party modified the payment information and/or payment instructions (including forged endorsement) after initiation without the knowledge of the payment initiator/Authorized Party.

77

77

How Was the Fraud Executed? By an Unauthorized Party

Unauthorized Party Took Over Account

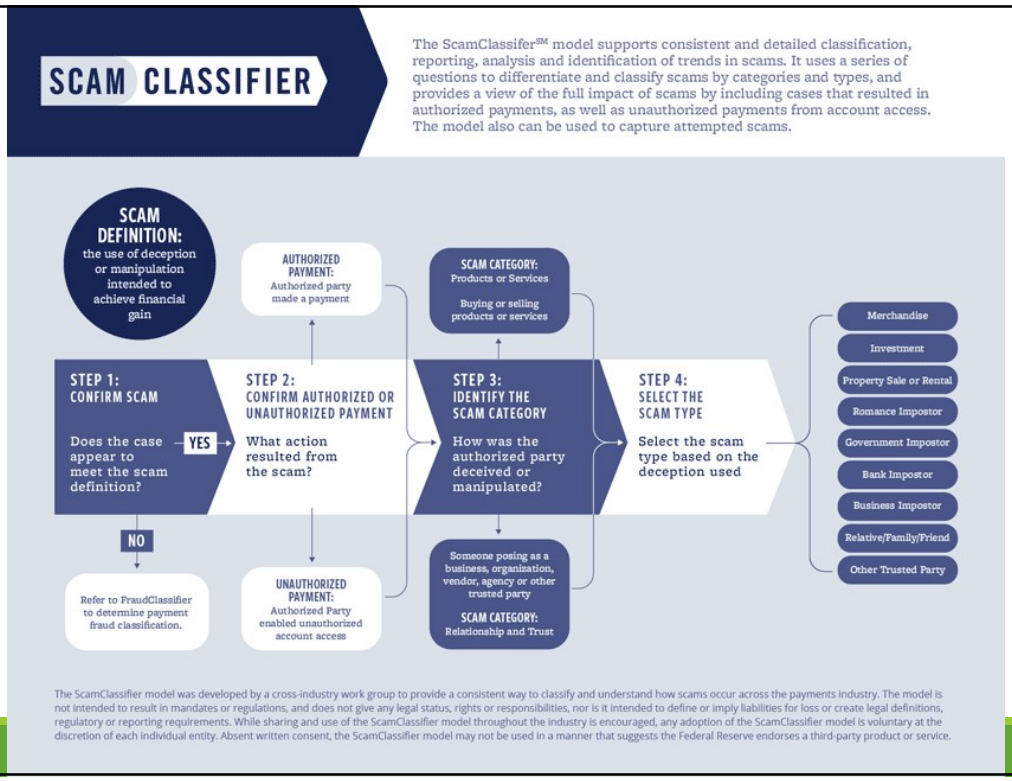
Unauthorized Party took over the account via compromised credentials or impersonated an authorized party.

Unauthorized Party Misused Account Information or Payment Instrument

Unauthorized Party misused the account or payment instrument by using digital payments or physical forgery or creation of counterfeit documents.

78

78



79

79

How to Use the ScamClassifier Model

https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/scams/scamclassifier-model/

Step 1: Does the incident meet the definition of a scam: the use of deception or manipulation intended to achieve financial gain?

Step 2: What action resulted from the scam?

- Either an authorized party was tricked into making the payment, OR the authorized party was tricked into enabling the fraudster to access the account.

Step 3: How was the authorized party deceived or manipulated?

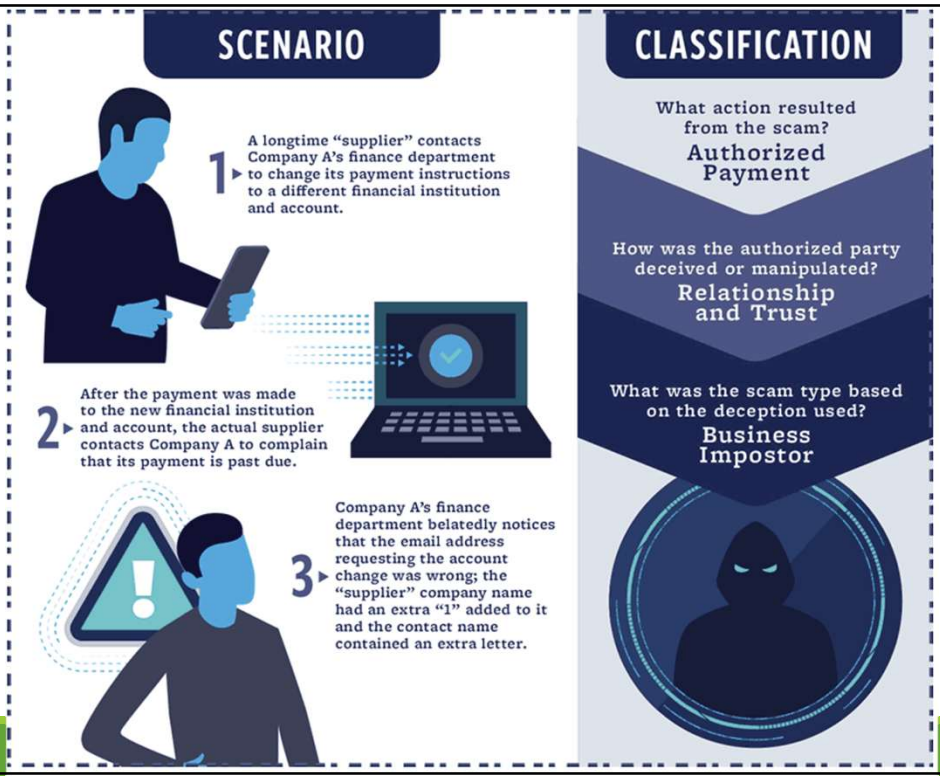
- Answers to this question are used to categorize the incident as either a *products or services scam* (e.g., to buy or sell something), OR as a *relationship and trust scam* (e.g., someone posing as a business, organization, vendor, agency or other trusted party). Incidents that are suspected of being fraudulent but not classified as scams can be further investigated using the FraudClassifier model.

Step 4: Classify the scam type based on the type of deception.

- The nine scam types in the ScamClassifier model focus on characteristics of the impostor and desired outcome: *merchandise scam, investment scam, property sale or rental scam, romance impostor scam, government impostor scam, bank impostor scam, business impostor scam, relative/family/friend scam* or *other trusted party scam.*

80

80



81

81

2025 Global eCommerce

Payments & Fraud Report

In partnership with the Merchant Risk Council [MRC], the Visa Acceptance Solutions and Verifi teams are proud to present the results of the 2025 Global eCommerce Payments & Fraud survey.

The purpose of this report is to convey transparent, unbiased research on merchants' views regarding current trends and challenges in the realm of eCommerce payments and fraud.



82

82

2025 Global eCommerce Payments & Fraud Report

3. Fraud attacks and metrics

Fraud rates are down, with significant declines in first-party misuse, card testing & triangulation schemes

- Fraud rates are down across the board, reversing a multi-year trend of increasing incidence.
- Significant declines reported in incidence of first-party misuse, card testing, and triangulation schemes.
- The dip in first-party misuse is notable, as this form of fraud has risen rapidly over the past two years.
- Real-time payment fraud, refund/policy abuse, phishing attacks, first-party misuse and card testing are the top five threats. These attacks each impact between one-third and half of all merchants globally.
- 98% of merchants report experiencing one or more types of fraud in the past 12 months.
- MRC members over-index significantly on experiencing these types of fraud, while non-MRC members over-index only when it comes to identity theft.

83

83

2025 Global eCommerce Payments & Fraud Report

Other fraud-related metrics also show improvement

- Additional fraud metrics show marginal year-over-year improvements.
- Order rejection rates declined significantly over the past year.
- Merchants also made progress cutting down on false positive (or "customer insult") rates, with a significant decline in the share reporting rates above 10%.

MRC members lead the way in fraud prevention, reporting better metrics despite registering more attacks

- Despite experiencing more attacks each year, MRC members report significantly better fraud metrics than non-MRC enterprises, including:
  - Lower fraud rates by order and by revenue
  - Lower rejection rates
  - Higher dispute win rates
  - Lower false positive rates

84

84

2025 Global eCommerce Payments & Fraud Report

Refund/policy abuse now on the rise, adding to merchants' post-purchase problems

- Over half (57%) report increasing rates of refund/policy abuse, with over one-fifth (22%) citing increases of 50% or more over the past year.
- Merchants say this is mainly driven by false claims that goods were never received, as well as attempted returns of used, damaged, or incorrect items.
- This form of fraud is significantly more likely to affect merchants in APAC, as well as enterprise.

85

85

Payments Fraud Liability Matrix

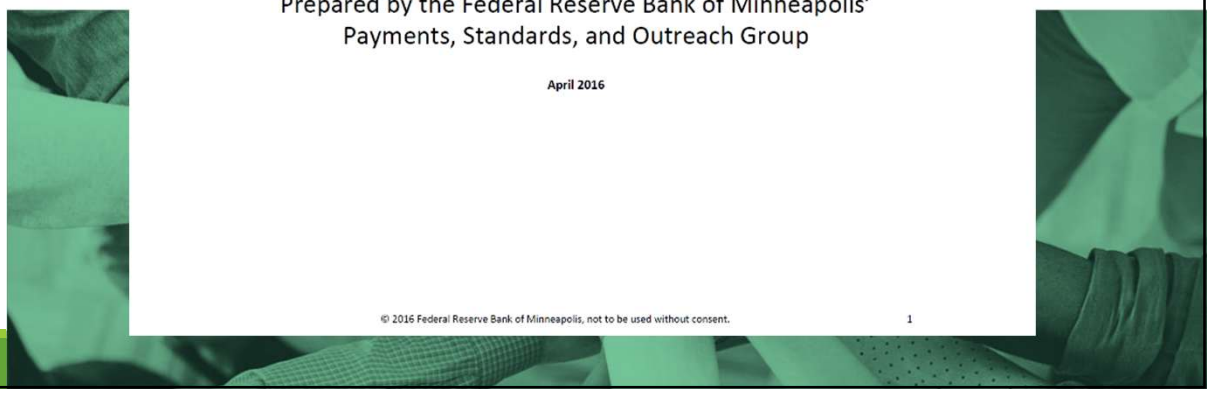
*** Disclaimer*** The information in this document dates to April 2016 and may not be the most current information available. The document is for informational purposes only and does not constitute legal advice. Please consult an attorney about a particular case, problem, or question. Any embedded links are being provided as a convenience and for informational purposes only; they do not constitute an endorsement or an approval by the Federal Reserve Bank of Minneapolis of any of the products, services or opinions of the corporation or organization or individual. The Federal Reserve Bank of Minneapolis has no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

https://fedpaymentsimprovement.org/wp-content/uploads/payments-fraud-liability-matrix.pdf

Payments Fraud Liability Matrix

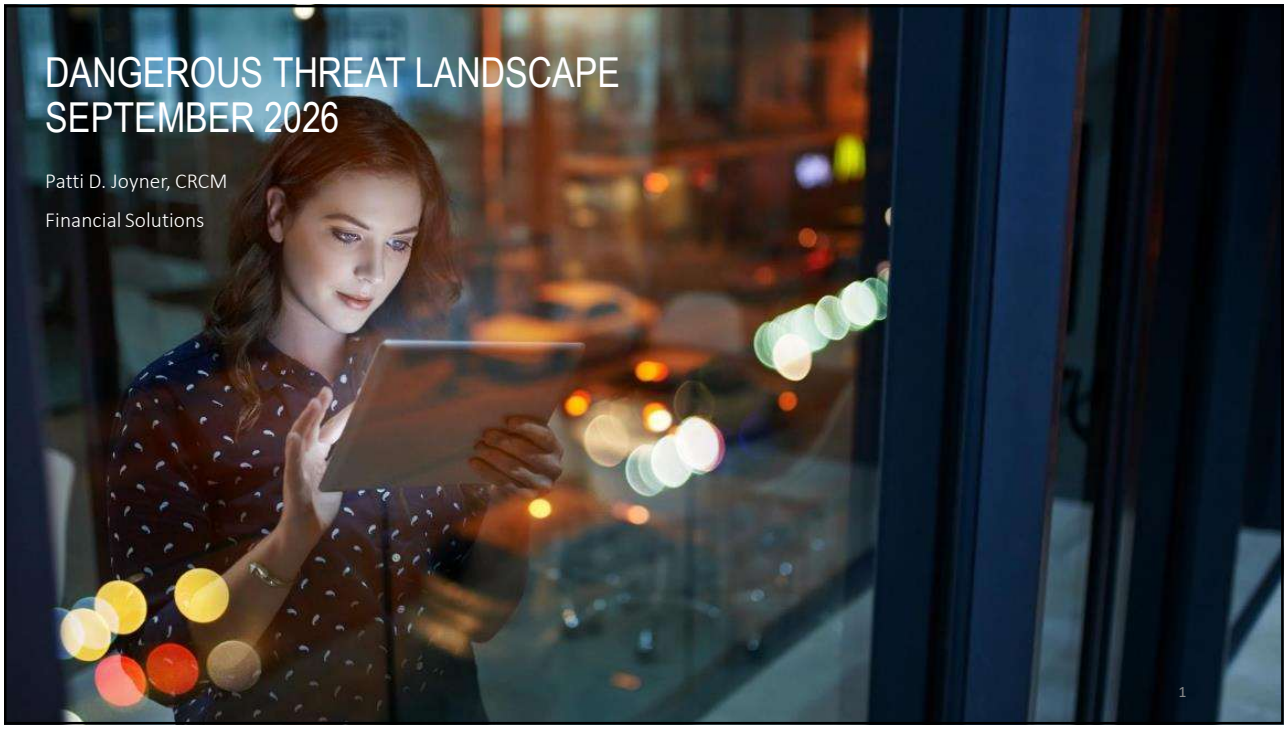
Prepared by the Federal Reserve Bank of Minneapolis' Payments, Standards, and Outreach Group

April 2016



© 2016 Federal Reserve Bank of Minneapolis, not to be used without consent. 1

86



1

Nasdaq
Verafin

FRAUD TRENDS AND TECHNOLOGY: 5 TRENDS TO WATCH IN 2026

JANUARY 5, 2026

BY COREY LYNCH

2

1. BUSINESS EMAIL COMPROMISE (BEC) & AUTHORIZED PUSH PAYMENT (APP) FRAUD

Authorized Push Payment (APP) fraud losses grew in the U.S. in 2024, as fraudsters increasingly exploited new technologies to target vulnerable customers and bypass heightened Business Email Compromise (BEC) controls.

In 2026, the race will continue as more scammers use AI to scale into more convincing virtual kidnapping and family emergency scams, compelling financial institutions to respond with more robust, AI-enabled solutions. Institutions can further bolster their defense by using a consortium solution, in tandem with AI, to quickly identify high-risk payee accounts.

Nasdaq Verafin

3

3

2. ACH FRAUD & NEW NACHA RULES

As BEC and APP fraud grow, ACH payments are continually exploited in these scams. Nacha's total ACH payment value is increasing by $1 trillion each year — and fraudsters are following the money. This is exacerbated by high BEC volumes. Since more companies are using ACH for payroll and supplier payments, fraudsters who gain access to their account will transfer funds using the same payment method. Institutions using consortium analytics will identify these criminal payees before the funds clear.

Nacha has issued new rules to strengthen their network against APP scams, promoting detection across an entire ACH payment — from origination to receipt. Institutions will be working to implement new processes in time to meet the March 20, 2026 deadline and engaging vendor solutions to ensure compliance.

Nasdaq Verafin

4

4

3. HOLISTIC DEFENSE AGAINST CHECK FRAUD

Check fraud has been a challenge for centuries, but the scale of the problem remains immense. An estimated $21 billion, or 80%, of global check fraud, took place in the Americas in 2023. More recently, 62% of financial institutions reported increased check fraud losses last year. While point solutions exist, their fragmented and disparate nature leaves financial institutions vulnerable.

In 2026, financial institutions will need a holistic check fraud solution to keep pace with evolving risk. An approach that combines real-time analysis, machine learning, and consortium analytics into one holistic solution will be necessary to ensure your institution can detect check fraud accurately while making funds available to customers quickly.

Nasdaq Verafin

5

5

4. FRAUD DETECTION EFFICIENCY & ARTIFICIAL INTELLIGENCE

Financial institutions must embrace AI-powered solutions in 2026. Fraudsters are using AI to scale their typologies and deploy increasingly convincing social engineering tactics. This means institutions must also use AI to their advantage. In 2025, over 85% of financial firms were actively applying AI in areas such as fraud detection. AI can improve fraud detection by identifying uncharacteristic customer behavior while reducing false positive alerts — allowing investigators to focus on truly high-risk activity.

Nasdaq Verafin

6

6

5. USING CONSORTIUM ANALYTICS TO YOUR ADVANTAGE

With high fraud risk across wire, check, ACH and instant payments, it was imperative in 2025 that institutions use consortium analytics to improve fraud detection. Consortium analytics review hundreds of millions of counterparties across thousands of financial institutions and identify when a payment is destined for a high-risk recipient or account. In 2026, more institutions will need to harness this approach as a difference-maker in fraud prevention.

Nasdaq Verafin

7

7

CONSORTIUM ANALYTICS

In the last decade, consortium data has become the cornerstone of financial crime prevention.

Large high-quality datasets are now essential for our industry to confront and stem the $3.1 trillion scourge of illicit activity threatening the global financial system. Information is fundamental to ensuring confidence, continuity, and resilience in the face of this ever-evolving threat.

As criminals have evolved, the efficacy of spreadsheets and isolated datasets in the fight against financial crime has weakened. Complex networks of money mules, cross-border payments fraud, surging AI-enabled scams and brazen cooperation between bad actors are now commonplace. Insights from a vast consortium network have the power to expose these distributed crimes to investigators.

Nasdaq Verafin

8

8

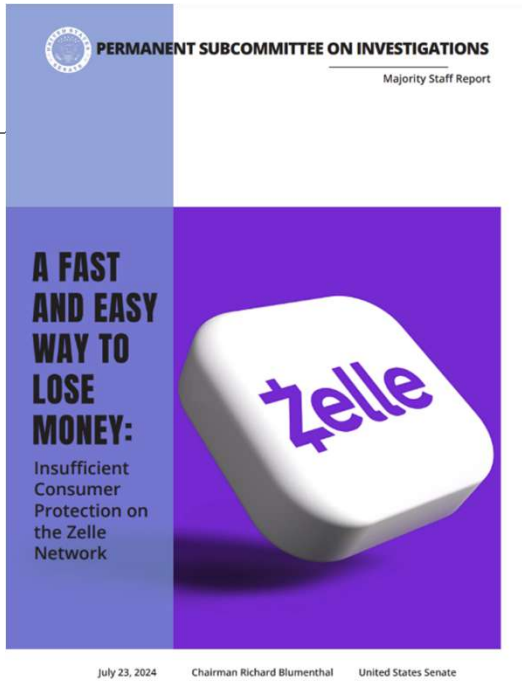
FRAUD OR A SCAM?

9

On June 16, 2023, the US Senate Permanent Subcommittee on Investigations ("PSI" or "the Subcommittee") launched an inquiry into Early Warning Services, which operates the Zelle Network, and the three largest banks that offer Zelle and co-own EWS, 73% of all Zelle 2023 payments.

Finding: In most cases, by the time a consumer realizes they have been targeted, their money is already gone. **Instances in which consumers have been victimized by scams and fraud on Zelle generally fall in two categories:**

- **Unauthorized transactions, in which a consumer Loses control of their account (such as through hacking) [Fraud], and**
- **Authorized transactions, in which the consumer is somehow tricked into authorizing a payment under false pretenses [Scam]**.



10

US SENATE PSI RECOMMENDATIONS

Over the course of PSI's 13-month investigation, the Subcommittee identified multiple opportunities that Congress, regulators, and the Zelle participants could take to improve consumer protection. The report includes the following recommendations:

1. Congress should amend the Electronic Fund Transfer Act to consumer reimbursement for "fraudulently induced" authorized transactions amidst a surge in increasingly sophisticated scams and fraud.
2. The CFPB should update Reg. E to require greater transparency in disputed transaction processes by providing clarity on what constitutes a "reasonable" investigation," giving banks a minimum set of requirements for thorough disputed claims' investigations.
3. Where commercial P2P payments, payment platforms should be required to provide purchase protections provided for other payment methods, such as credit cards.
4. EWS and banks that offer Zelle should implement a robust framework to share specific and real time information regarding scams and fraud with law enforcement and other financial institutions.
5. Congress and the CFPB should further limit the use of consumer financial data collected by payment platforms to help protect consumers from unwanted harvesting of their data.
6. EWS should require banks that offer Zelle to allow parents to disable Zelle in their child's online banking app and to notify parents of large transactions initiated by their child.
7. Congress should amend the Electronic Fund Transfer Act to clarify that EWS, and any other financial services companies that play a central role in facilitating electronic fund transfers, are considered a "financial institution" under the statute.

11

11

Figure 3: EFTA Definitions of Authorized and Unauthorized Payments

	Unauthorized a/k/a "Fraud" or Other[99]	Authorized a/k/a "Scam"
Definition	"[A]n electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit."[100]	EFTA does not define "authorized" electronic fund transfer, however, instances in which a consumer initiates an electronic fund transfer for a good or service, even if they do not receive the value they paid for, are considered authorized.[101]
Example	Unauthorized user hacks into a consumer's bank account and transfers money out of the account without consumer's knowledge.	Bad actor impersonates a landlord offering to rent an apartment and a prospective tenant transfers what they believe is a security deposit.
Reimbursement Obligation	EFTA generally requires the financial institution to reimburse the consumer.[102]	EFTA does not address authorized payments. Courts have interpreted the statute to provide that financial institutions are not required to reimburse the consumer.[103]

12

12

The Zelle website similarly differentiates between authorized and unauthorized transactions, making a distinction between transactions it categorizes as "fraud" and those that it categorizes as "scams" in its approach to reimbursement.[107] According to the Zelle website:

- A "scam" is when a consumer is knowingly involved in the transaction and authorizes a payment to be sent.[108] Scams include instances when a consumer is tricked or persuaded into authorizing a payment for a good or service that is never provided.[109]
- "Fraud" is when someone gains access to a consumer's account and makes a Zelle payment without the consumer's permission, and the consumer is not involved with the transaction.[110] For example, this would include instances when someone gains access to a consumer's account and steals or sends money without the consumer's permission.[111]

13

13

Figure 4: Examples of Common Scams and Fraud

Scams
Me-to-Me Scams: Bad actors, claiming to be bank employees, successfully change settings on a consumer's bank account, and then instruct victims to transfer money to themselves with Zelle, which sends the money to a separate bank account.[112] A San Francisco woman received a text message that seemed to come from Wells Fargo's fraud department, asking her to verify recent payments she did not make on Zelle.[113] The bad actor then told her that she had to Zelle the $3,500 back to herself. The money was routed to the bad actor's account.[114] **AI Voice Cloning Scams:** Bad actors search for potential victims through social media and learn about their family. Then, using artificial intelligence, the bad actors clone a loved one's voice, call the consumer using the artificial voice, and contrive a crisis that persuades the consumer to transfer money out of a sense of urgency.[115] A senior couple in Pittsboro, North Carolina, wired $5,000 to a bad actor impersonating their grandson with voice cloning technology.[116] The "grandson" claimed that he had just been in a car accident and needed bail money to get out of jail.[117] **Romance Scams:** Bad actors initiate contact with a consumer through an online dating site or elsewhere and impersonate a potential love interest. Over the course of a fake relationship, the bad actor requests money for gifts or contrived needs.[118] An 82-year-old man from Houston was scammed by a woman he met on a dating site.[119] The woman sent him photos and requested that he send her money through Zelle. The man was scammed out of more than $100,000 as a result.[120]

14

14

Employment Scams: Bad actors find a consumer in the process of a job search. The bad actor conducts a fake virtual job interview and extends a fraudulent job offer. As part of the fake onboarding, the bad actor sends a forged check to the consumer and instructs them to use the "funds" to Zelle money to various accounts to buy supplies for the job.[121]

A college graduate received a fake job offer via LinkedIn.[122] As a part of the onboarding process, they were sent a fraudulent $2,400 check and instructed to Zelle the amount to the office's equipment employee for her work laptop, phone, and printer.[123] However, the check bounced, and the college graduate was scammed out of $2,400.[124]

Puppy Scams: A bad actor places a fake item on an online forum or marketplace such as Facebook Marketplace or Craigslist. A consumer pays money for an item they never receive.[125]

A Florida woman responded to a Facebook listing for mini-Goldendoodles.[126] She paid the breeder a $300 deposit through Zelle. The breeder then asked for an additional $660 for "puppy insurance."[127] The consumer never received a puppy.[128]

15

15

Fraud

Hacking: A bad actor gains access to a consumer's bank account without any form of authorization, through deception or otherwise, provided by the consumer.

A Houston woman receives a notice from her bank notifying her that a new user had been added to her The new user immediately withdrew $1,000. Over the next three days, the hacker continuously attacked her account, ultimately withdrawing $8,000.

Robbery or Threat of Force: A bad actor obtains a user's phone through theft or threat of violence. After gaining access to the consumer's mobile device, the bad actor transfers funds away.

In January 2024, Manhattan District Attorney Alvin Bragg sent letters to Zelle and other P2P platforms relating to a wave of robberies in New York, in which bad actors used theft or force to obtain access to consumer's P2P account and transferred money to themselves.[130]

16

16

Figure 6: Total Dollar Value of all Zelle Payments Disputed as Fraud at the Three Banks 2019-2023[154]

	2019	2020	2021	2022	2023
Total	$82,235,513	$127,618,310	$189,438,794	$215,211,008	$165,842,411
Reimbursed	$53,706,680	$77,191,918	$86,928,146	$99,285,420	$63,546,270
Unreimbursed	$28,618,833	$50,426,393	$102,510,647	$115,925,588	$102,296,141

Figure 8: Total Dollar Value of all Zelle Payments Disputed as Scams at the Three Banks 2021-2023[168]

	2021	2022	2023
Total	$194,052,969	$241,596,948	$206,783,481
Reimbursed	$27,745,695	$16,200,671	$38,575,254
Unreimbursed	$166,307,273	$225,396,277	$168,208,227

17

PROPOSED PROTECTING CONSUMERS FROM PAYMENT SCAMS ACT

On August 2, 2024, Congresswoman Maxine Waters (D-CA), the top Democrat on the House Financial Services Committee, **Senator Richard Blumenthal (D-CT)**, Chairman of the Senate Permanent Subcommittee on Investigations, and **Senator Elizabeth Warren (D-MA)**, Chair, Senate Banking, Housing, & Urban Affairs Subcommittee on Economic Policy, announced the **introduction of their bill**, the "Protecting Consumers from Payment Scams Act."

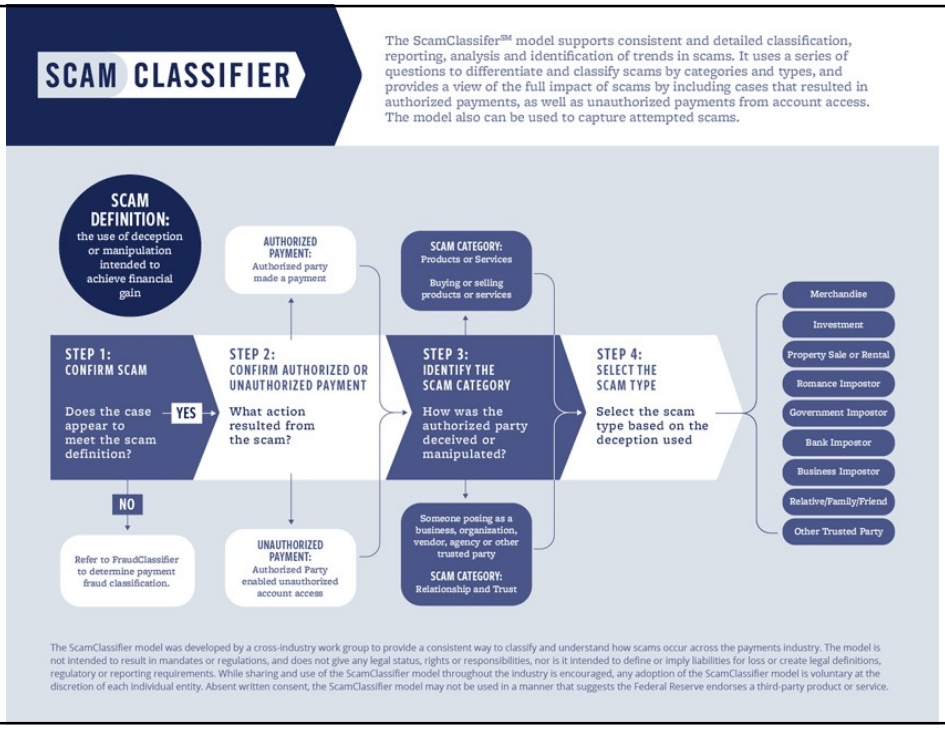
They state: "As payment fraud skyrockets, the bill would update the Electronic Fund Transfer Act (EFTA) to clarify ambiguities and strengthen the law to better protect consumers harmed when they make payments. Specifically, it would protect consumers when they are defrauded into initiating a payment sent to a bad actor, when they lose funds through fraudulent bank wire transfers, and when their accounts are inexplicably frozen or closed."

Proposal seeks to clarify that protections also apply to bank wire transfers and telephone-authorized transfers.

The proposed bill has not progressed further as of this presentation.

18

18



19

19

https://fedpaymentsimprovement.org/news/blog/stomp-out-scams-with-the-scamclassifier-model/



20

20

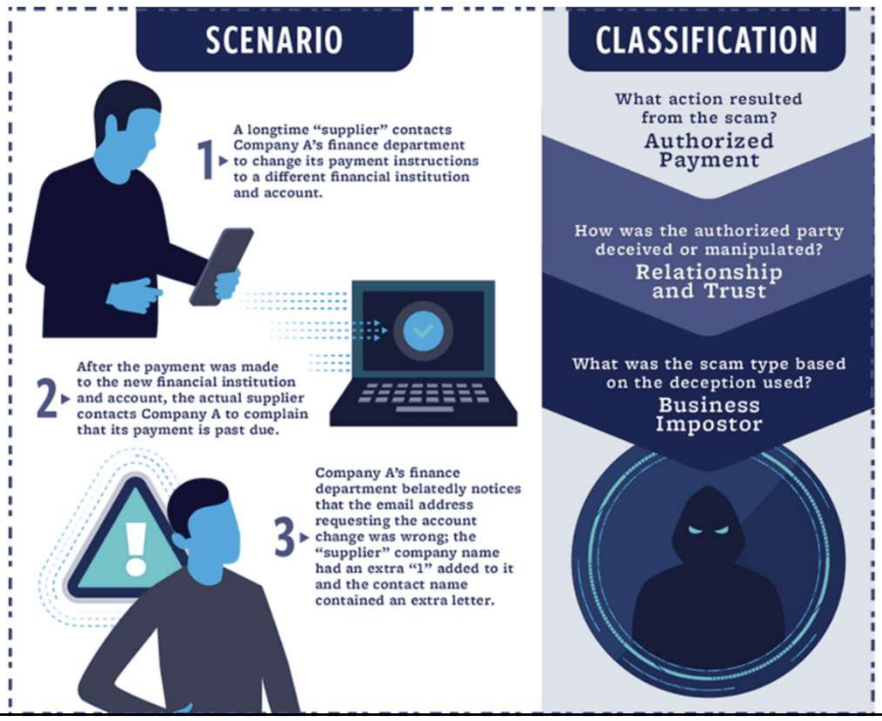
How to Use the ScamClassifier Model

https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/scams/scamclassifier-model/

- **Step 1: Does the incident meet the definition of a scam: the use of deception or manipulation intended to achieve financial gain?**
- **Step 2: What action resulted from the scam?**
  - Either an authorized party was tricked into making the payment, OR the authorized party was tricked into enabling the fraudster to access the account.
- **Step 3: How was the authorized party deceived or manipulated?**
  - Answers to this question are used to categorize the incident as either a *products or services scam* (e.g., to buy or sell something), OR as a *relationship and trust scam* (e.g., someone posing as a business, organization, vendor, agency or other trusted party). Incidents that are suspected of being fraudulent but not classified as scams can be further investigated using the FraudClassifier model.
- **Step 4: Classify the scam type based on the type of deception.**
  - The nine scam types in the ScamClassifier model focus on characteristics of the impostor and desired outcome: *merchandise scam, investment scam, property sale or rental scam, romance impostor scam, government impostor scam, bank impostor scam, business impostor scam, relative/family/friend scam* or *other trusted party scam.*

21

21



22

22





Synthetic identity fraud (SIF) is the use of a combination of personally identifiable information (PII) to fabricate a person or entity in order to commit a dishonest act for personal or financial gain.

The following graphic reflects personally identifiable information elements that may be used to create a synthetic identity. These are solely examples and do not represent an exhaustive list.

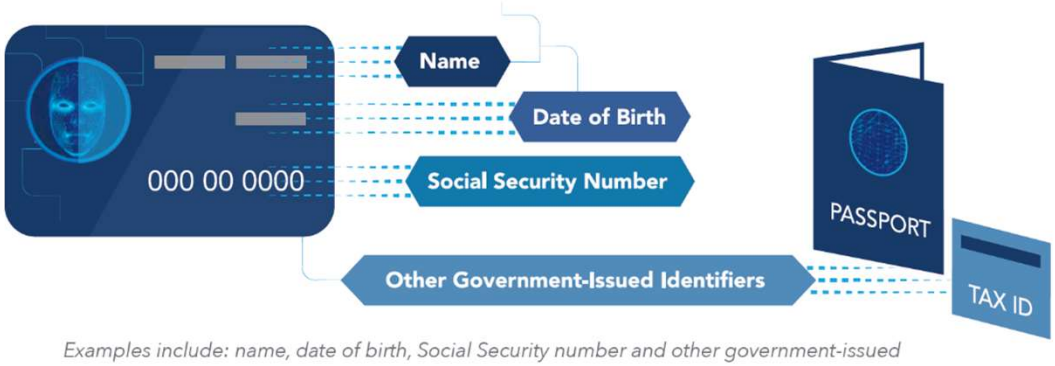
FedPaymentsImprovement.org

23

23

PRIMARY ELEMENTS

Identity elements that are, in combination, typically unique to an individual or profile:



Examples include: name, date of birth, Social Security number and other government-issued identifiers (such as a passport or tax identification number)

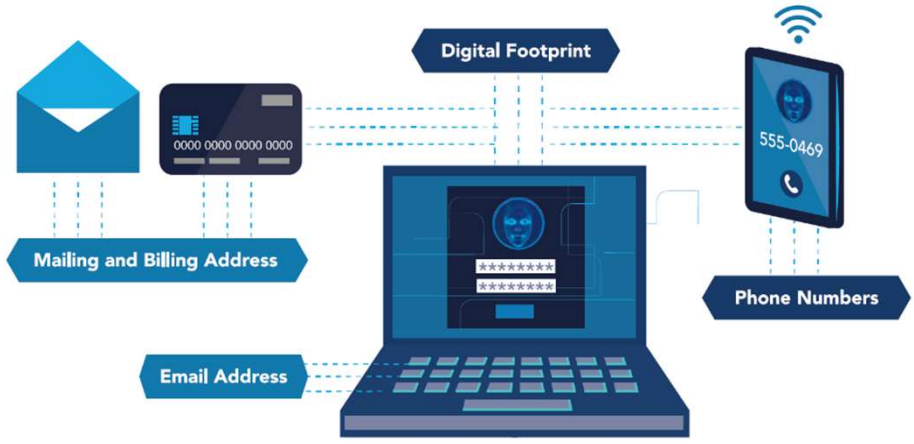
FedPaymentsImprovement.org

24

24

SUPPLEMENTAL ELEMENTS

Elements that can help substantiate or enhance the validity of an identity but cannot establish an identity by themselves:



Examples include: mailing or billing address, email address, phone number(s), and digital footprint (such as device ID or IP address)

25



FRAUD FOR LIVING

This occurs when a synthetic identity is used to apply for employment or services such as utilities, housing or bank accounts. This is done because an individual is unwilling or unable to establish or secure employment or services with his/her own PII elements. Typically, the individual has no intent to default on payment.

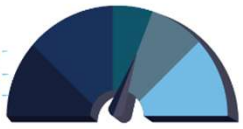
Example: does not have a Social Security number (SSN) – An individual immigrated to the U.S. and sought honest employment to provide for his family. As a non-citizen, he did not have an SSN issued by the Social Security Administration. He purchased an SSN from an organization claiming to help provide employment services for immigrants. The SSN he purchased rightfully belongs to an elderly person who was not actively using credit. The immigrant applied for and secured employment, earning wages under his name and the purchased SSN.

Example: unwilling to use SSN – An individual who was the victim of domestic violence left home for a fresh start. She attempted to hide her new address from being discovered by using a fake name and made-up SSN to apply for housing and set up a new bank account. She didn't realize the made-up SSN is a real SSN that rightfully belongs to another individual.

26



CREDIT REPAIR



An individual may want to qualify for a large purchase or line of credit – or simply rebuild credit for future use – but cannot do so due to a previous negative credit history or bad debt. To appear more creditworthy, the individual created a synthetic identity and began building a more positive credit history and/or increased purchasing power through this new identity.

Example: Following a personal bankruptcy, an individual sought help for rebuilding his credit. An organization posing as a credit repair agency guided the individual to rebuild his credit by applying for new credit under his full name, date of birth and a randomized nine-digit number instead of his actual SSN. This number, called a Credit Profile Number or Credit Privacy Number (CPN), is positioned as a legitimate way to disassociate the individual from his bad credit history. Often unbeknownst to the individual, these CPNs are really SSNs belonging to other individuals and using them is illegal. Often unbeknownst to the individual, many CPNs are SSNs not tied to an active credit file, such as those belonging to children or the elderly. There is nothing legitimate about CPNs and if using one for credit repair, that consumer has engaged in identity theft. Using a CPN on a credit application is a violation of federal law and can result in prison time and/or substantial fines.

FedPaymentsImprovement.org 27

27



PAYMENT DEFAULT SCHEME



A common use of synthetic identities is to obtain goods, cash or services with no intent to repay over a period of time. This could take the form of a large, one-time purchase or a series of purchases that often total a substantial amount.

Example: fraud conducted over time – An individual opened a consumer credit card using a synthetic identity. For several years, the individual made small, frequent purchases and paid off the balance on time and in full every month. Because of the long, positive payment history, the credit line on the card increased to $20,000. At this point, the individual maxed out the credit line and ceased to make any payments. The credit card company was left with no "real" individual from whom to seek payment.

Example: fraud that occurs up front – An individual secured an auto loan using a synthetic identity. He purchased a new car and drove it off the lot. No payments were made on the loan and there was no "real" individual from whom to seek payments, so this essentially became a stolen vehicle.

FedPaymentsImprovement.org 28

28



OTHER CRIMINAL ACTIVITY



Synthetics can be used to facilitate a means to an end as part of other illegal acts.

These acts are pervasive in nature and impact many industries outside of the payments industry, such as the insurance, healthcare, government and telecommunications industries.

Examples of illegal acts:

- Avoiding legal responsibilities (e.g., paying child support)
- Conducting money laundering
- Defrauding insurance companies to receive payouts or services
- Facilitating human and/or narcotics trafficking
- Organizing and financing terrorist attacks

Criminals conducting these illegal activities range from individuals to transnational organized crime groups.

FedPaymentsImprovement.org 29

29



GENERATIVE ARTIFICIAL INTELLIGENCE INCREASES SYNTHETIC IDENTITY FRAUD THREATS

To make synthetic identities appear legitimate, Gen AI can:

- Create authentic-looking documents to present along with a credit application to corroborate personal information, such as birth certificates, Social Security cards, pay stubs, bank statements, utility or phone bills.
- Use photos available online to create authentic-looking driver's licenses that include personal details required for credit approvals.
- Produce fake images, videos, or misleading voice recordings, called deepfakes. These digitally altered results can be sophisticated and may convincingly appear to be real people because of realistic Gen AI characteristics such as hand gestures and unique speech patterns. Real-time deepfakes are scripted but flexible enough to respond to unexpected questions or requests as part of an account opening process. The images or videos may be set up by fraudsters as an authentication factor to access accounts in the future using facial recognition.

These Gen AI features increase the number of accounts opened with synthetic identities that then can be used to steal money by making credit card purchases or overdrawing an account with no intent to repay. Fraudsters may choose to let accounts mature to obtain higher credit limits or apply for loans to increase the amount available to steal. The accounts can be used to receive and transfer money to support other criminal activities, such as fraud, scams and money laundering.

FedPaymentsImprovement.org 30

30



FIGHTING FRAUD WITH AI AND GEN AI

AI tools and Gen AI can:

- Search for corroborating evidence that an applicant has an established history of credit, utility payments, related phone numbers and other inputs.
- Examine IDs and documents for missing or blurred wording and images, as well as check for special features, such as holograms.
- Scan for a live person and identify discrepancies, including incomplete hands and faces, missing lines or perspectives that appear to be inconsistent with the image.
- Generate fraud scenarios and data to improve model risk scores, enabling financial institutions to more quickly adapt to evolving fraud patterns without requiring human intervention. This feature allows fraud detection strategies to continually update based on new information.
- Support investigations by analyzing details to identify cases of synthetic identity fraud that may have been classified as credit losses or first-party fraud. Improved detection, even after the fact, increases financial institutions' understanding of the occurrence and impact of synthetic identity fraud. The value of this information to benefit detection and mitigation tactics can be magnified when shared with other organizations.

31



The relentless nature of check fraud growth and the challenges that remain year after year beg the question: *why is check fraud still around?* Although there is not a single contributing factor, check fraud continues to be a concern within the payments industry because it is:

- A **lucrative opportunity** for criminals
- Relatively **simple to perpetrate**
- **Not easy to detect:** often manual and fraudulent items can be indistinguishable from legitimate items

A deeper understanding of these challenges may help drive changes that will prevent check fraud.



OPPORTUNITY MAKES CHECKS A LUCRATIVE TARGET

The continued use of checks – with billions processed each year – provides many opportunities for criminals to target this payment method. Before checks can be fraudulently created, altered or forged, a check – or the data needed to create a fake check – needs to be obtained or fictitiously created. Criminals can gain access to data and checks in a multitude of ways, such as mail theft, data compromises and social engineering.

32

https://www.icba.org/check-fraud-a-practical-guide#appendix1

I. Summary of Defenses Issues - The following table summarizes the relevant defenses available when check fraud results in a loss, including the time periods to provide notice or return an item.

Allegation	Defense	Comment
Forged drawer signature	Drawer was negligent by allowing access to blank checks.	Comparative negligence rules apply. Customer negligence can reduce the amount of damages, but unlikely to eliminate bank liability.
Forged drawer signature	Customer failed to promptly notify the paying bank.	The UCC provides a one-year requirement after receiving monthly statement. But this can be shortened by agreement.
Forged drawer signature	Action was brought after the three-year statute of limitations.	Time limit begins when the customer knew or should have known of the fraud.
Forged Endorsement	Negligence in the handling of the check allowing fraudster to gain access.	Comparative negligence rule applies.
Forged Endorsement	Person who forged the endorsement was a "trusted" employee of the payee.	Comparative negligence rule applies.
Forged Endorsement	Claim barred by relevant statute of limitations.	Check individual state law to see if three-year rule applies.

33

https://www.icba.org/check-fraud-a-practical-guide#appendix1

I. Summary of Defenses Issues - The following table summarizes the relevant defenses available when check fraud results in a loss, including the time periods to provide notice or return an item.

Allegation	Defense	Comment
Name of Payee Changed	Maker negligence, customer failed to promptly notify bank, statute of limitations expired.	Check individual state law to see if UCC three-year limitation has been changed.
Amount altered	Maker negligence, customer failed to promptly notify bank, statute of limitations expired.	Check individual state law to see if UCC three-year limitation has been changed.
Check made to a fictitious payee or imposter	No bank liability unless bank failed to exercise "ordinary care."	Banks should be suspicious of potential imposter ruses.
Common Law claim against bank	Common law preempted by UCC and federal regulations.	Confirm that this rule applies in your state.
Signature on Substitute Check is forged	Under regulation CC, the presumption is that the check was altered, and not a forged maker's signature.	Presumption may be overcome by a "preponderance of the evidence."

34

PNC BANK SUES SOFTWARE ENGINEER FOR $27.3 MILLION IN KITING LOSSES

In August 2025, PNC filed a lawsuit against Dan Herbatschek, the founder of several companies including Ramsey Theory Capital and Ramsey Theory Group. The lawsuit seeks to recover its losses though claims of fraud, conversion, unjust enrichment, and breach of contract.

The lawsuit claims the check-kiting scheme took place over a 2-week period in July 2025. Herbatschek allegedly deposited $77 million in bad checks from accounts at other banks into his PNC accounts. During that time he also wired $370 million out of the PNC accounts to other banks.

The fraud was discovered when 3 checks he deposited, totaling $2.9 million were returned NSF

PNC closed the accounts, leaving them with an enormous negative balance of over $27.3 million

The lawsuit calls into question Heratschek's lifestyle, noting a spending spree earlier in 2025 including purchase of a luxury Manhattan condo for over $12 million.

35

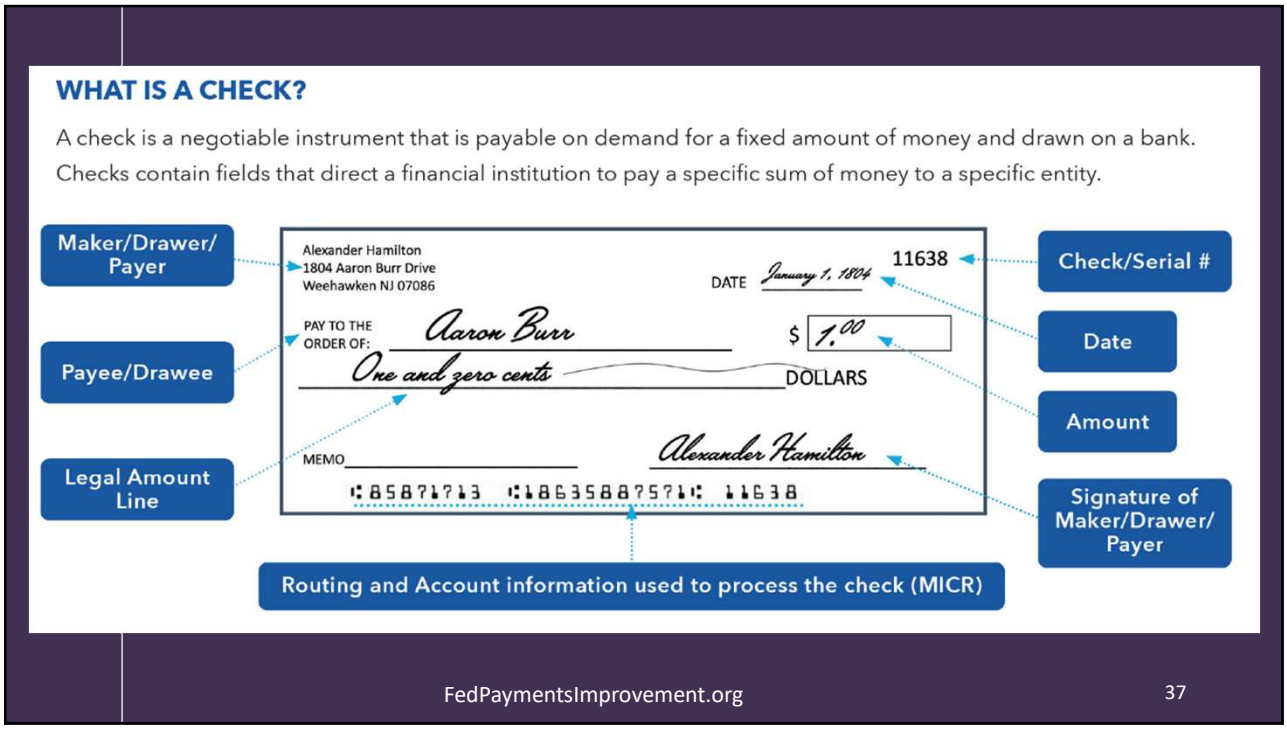
35



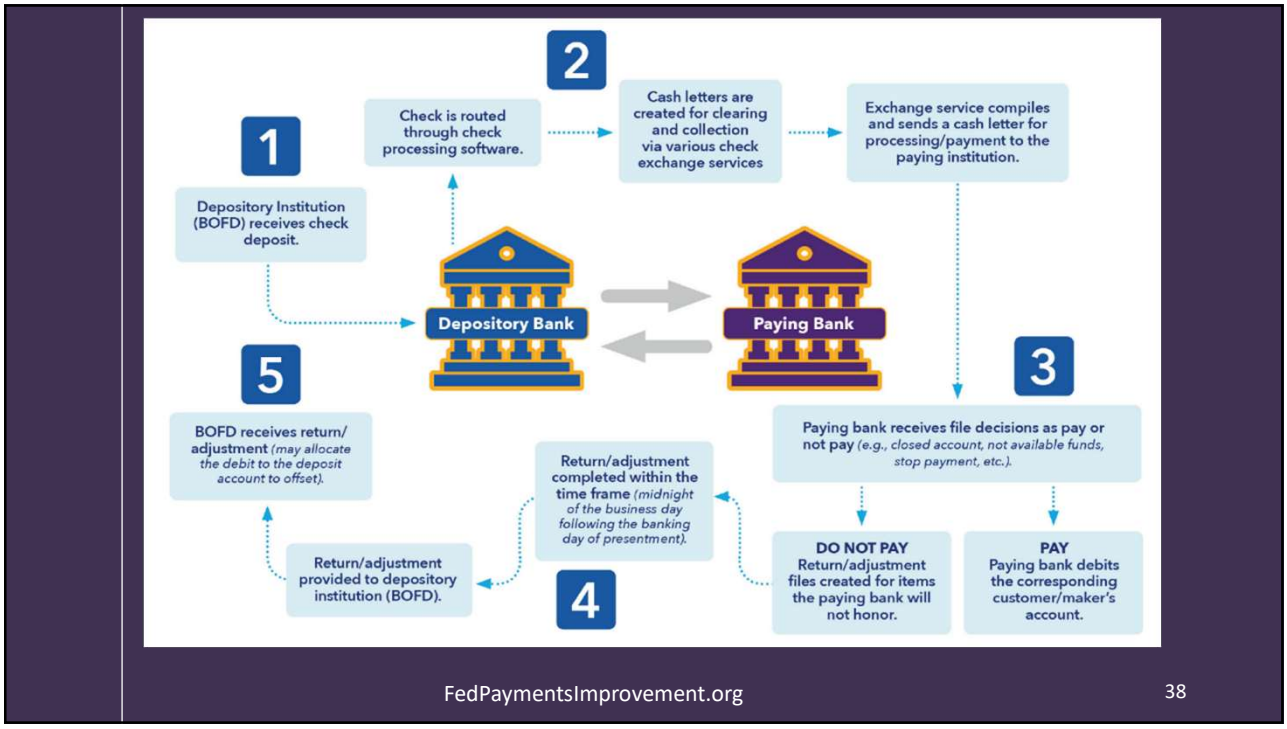
https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/money-mules

36

36

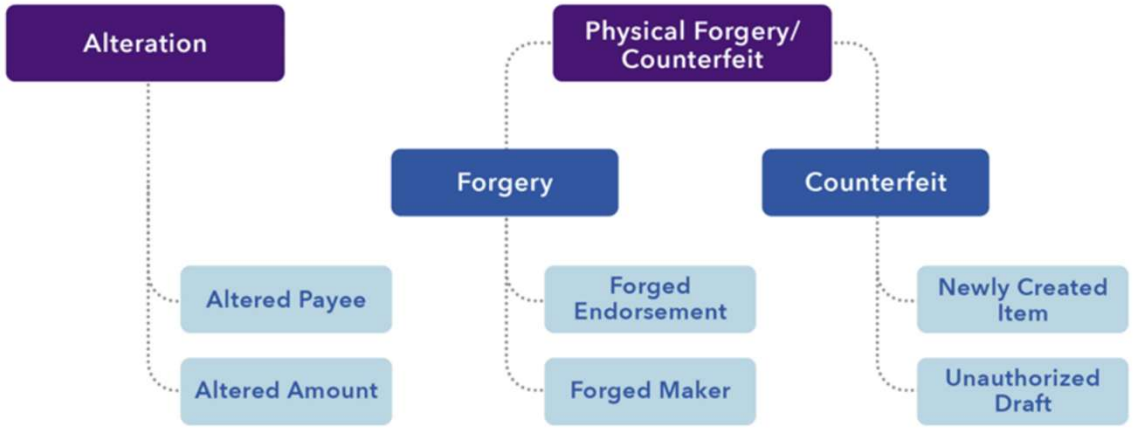

WHAT IS A CHECK?
A check is a negotiable instrument that is payable on demand for a fixed amount of money and drawn on a bank.
Checks contain fields that direct a financial institution to pay a specific sum of money to a specific entity.
Maker/Drawer/ Payer
Payee/Drawee
Legal Amount Line
Alexander Hamilton
1804 Aaron Burr Drive
Weehawken NJ 07086
DATE January 1, 1804
11638
PAY TO THE ORDER OF: Aaron Burr
$ 1.00
One and zero cents DOLLARS
MEMO
Alexander Hamilton
⑆858?1?13 ⑆186358857?1⑆ 11638
Check/Serial #
Date
Amount
Signature of Maker/Drawer/ Payer
Routing and Account information used to process the check (MICR)
FedPaymentsImprovement.org
37

37


1
Depository Institution (BOFD) receives check deposit.
2
Check is routed through check processing software.
Cash letters are created for clearing and collection via various check exchange services
Exchange service compiles and sends a cash letter for processing/payment to the paying institution.
Depository Bank
Paying Bank
3
Paying bank receives file decisions as pay or not pay (e.g., closed account, not available funds, stop payment, etc.).
DO NOT PAY
Return/adjustment files created for items the paying bank will not honor.
PAY
Paying bank debits the corresponding customer/maker's account.
4
Return/adjustment completed within the time frame (midnight of the business day following the banking day of presentment).
Return/adjustment provided to depository institution (BOFD).
5
BOFD receives return/ adjustment (may allocate the debit to the deposit account to offset).
FedPaymentsImprovement.org
38

38

Primary Types of Fraudulent Checks



FedPaymentsImprovement.org 39

39

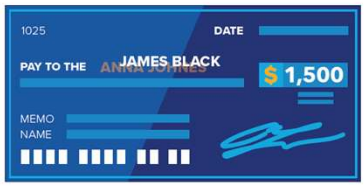
ALTERATION

An alteration is an unauthorized change in a check that modifies in any respect the *obligation* of a party, or an unauthorized addition of words or numbers, or another change to an incomplete check related to the party's obligation.

What this means: *A check is a paper instrument authorizing the payee to the amount of funds indicated on the check. Paper checks are altered if unauthorized changes to a legitimate instrument modify the obligation of the party (i.e., who the funds are intended for or the amount of the funds).*

Indicators of an altered paper check:

- Erasure, washing, dried liquid marks
- Uneven or faded printing or color
- Font type, color, type size is different than other fields, especially if payee or amount differs from the date or memo line
- Handwriting is inconsistent with other writing on the check or other items known to be valid



FedPaymentsImprovement.org 40

40

COUNTERFEIT

A fictitious check can be created to imitate a legitimate negotiable item, which may or may not contain legitimate maker (payer) and account information. (Note that case law has used the terms "forgery" and "counterfeit" interchangeably.)



Indicators of a counterfeit paper check:

- Font style, size or capitalization does not match known legitimate items
- Check stock or alignment on the check differs from known legitimate stock
- Smooth edges, as checks typically are torn from a book or a check stub
- Back of the check is blank or does not match other known valid items
- Printed ink on the check runs or becomes distorted if it gets wet
- Magnetic ink character recognition (MICR) – the numbers and characters that appear at the bottom of a check to show the bank routing number, account number and check number – is raised or glossy
- Serial number is low or out of range for current check usage
- Issuing bank information (name, address and/or routing number) listed on the check is fictitious, does not match or cannot be found
- Poor quality or missing security features

FedPaymentsImprovement.org 41

41

FORGED MAKER

Check fraud also may involve an unauthorized signature of the maker (payer) on the check.

What this means: *The signature is not from an authorized payer. Forged checks generally are created using legitimate check stock, but the maker's signature has been forged, copied or is otherwise unauthorized.*

Indicators of a forged check:

- Signature on the maker line does not match known valid signatures
- Light or inconsistent pressure in signature compared to other writing on the check, which may be noted during visual inspection or when holding the check up to the light
- Erasure marks, retraces or irregularities on the signature line
- Exact match (i.e., a copy of previous items), even though the maker usually signs freehand



FedPaymentsImprovement.org 42

42

IMPROPER OR FORGED ENDORSEMENT

In this case, the payee's signature and/or the endorsement on the back of the check is forged, missing or otherwise improper.

What this means: *The intended payee did not sign or authorize the endorsement on a check. This also could include blank endorsements, where the check was deposited into an account the payee did not have access to.*



Indicators of an endorsement concern:

- Signature on the endorsement line is similar to the handwriting on the front of the check
- Endorser signature does not match known valid signatures
- Endorsement font or wording matches other known bad items

FedPaymentsImprovement.org 43

43

UNAUTHORIZED ITEMS

Unauthorized Electronically Created Item (UECI): when any of the following were not authorized by the account holder – the electronically created item itself, the amount stated on the item or the payee stated on the item.

Unauthorized Remotely Created Check (URCC): a remotely created check that was not authorized in the amount stated on the check to the payee indicated on the check and does not bear a signature applied by the account holder. (This is not intended to include buyer's remorse or other instances where the maker authorizes the payment but then retracts it.)

What this means: *The paper draft was not authorized by the account holder whose account was debited and, the check does not bear a signature and instead, indicates the signature is "on file" or "pre-approved." This type of fraud also may be called Demand Draft Fraud or Unauthorized Remotely Created Check.*

FedPaymentsImprovement.org 44

44

Indicators of an unauthorized item:

- Inconsistent and/or new activity compared to the account history
- A non-typical maker for remotely created items
- Customers report they did not authorize debits from their accounts and the draft checks do not contain a signature
- Missing or incorrect information – for example, the name and account do not match
- Velocity of items presented across multiple accounts is inconsistent with prior activity

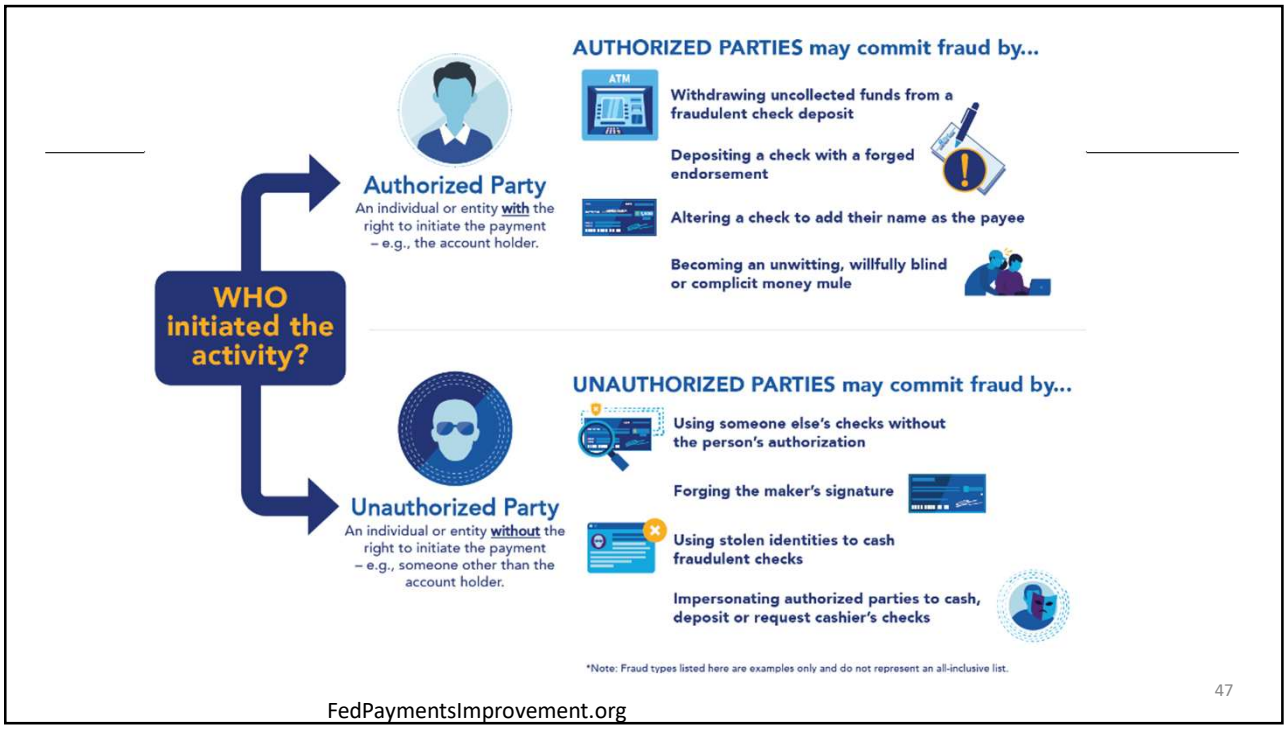
The indicators included here are not all-inclusive and may not always be evident. Criminals use technology and other resources to create very legitimate-looking fraudulent checks.

FedPaymentsImprovement.org 45

45



46



FedPaymentsImprovement.org

47



48

Unsophisticated Methodologies

- **Fraudulently endorsing a check without modifying any information on the check**: This involved someone signing their name on the back of a stolen check and attempting to deposit it.
- **Altering the payee or dollar amount without washing the check**: Some perpetrators crossed out the payee and added their own name or changed certain letters or numbers to change the payee and/or amount. Others used white out to alter the information.
- **Third-party payments[19] with no check modifications**: Instead of modifying a check, criminals attempted making it appear as though the intended payee signed it over to them and attempted negotiating the check.

49

49

Moderately Sophisticated Methodologies

- **Check washing**: Perpetrators wash check information using available chemicals to remove original ink and replace it with new information.
- **Selling information from a stolen check online**: Some criminals attempted monetizing the check beyond its original amount by selling the check on dark web marketplaces or online forums, according to BSA reports and open-source research.[20]
- **Using compromised check information to create counterfeit checks**: Criminals took stolen checks and used them as a framework to create counterfeit checks with the victim's banking information. Some criminals used more sophisticated technology to make high-quality counterfeit checks.
- **Stealing newly ordered checks from the mail**: Some criminals stole newly ordered blank checks from the mail, forged the rightful account holder's signature, and then issued the checks to themselves or others.

50

50

Sophisticated Methodologies

- **New account fraud**: New account fraud involved criminals opening new accounts, typically online, specifically designed to negotiate stolen checks.[21] This most frequently occurred when stolen checks were made out to businesses. Some criminals opened accounts either in the name of the payee or a name that is nearly identical. The company that opened the account may not actually exist and may use a fraudulent address during the account opening process. Perpetrators may open these accounts using compromised identifying information or synthetic IDs comprising of information from several people.
- **Mail theft-related check fraud as part of a larger scam, mostly romance and employment scams**: In these cases, scammers engaged victims in a scam and convinced them to negotiate a check and then send the funds elsewhere, using the victims as money mules to move stolen funds.
- **Insider involvement**: Sophisticated operations have enlisted insider assistance at financial institutions or the USPS.[22] In one case, federal prosecutors charged a USPS employee with stealing more than $1.6 million in checks from the U.S. mail, altering the checks, and depositing them into his own account.[23]

51

51



52

FBI'S 2025 INTERNET CRIME REPORT

WWW.FBI.GOV/NEWS/PRESS-RELEASES/CRYPTOCURRENCY-AND-AI-SCAMS-BILK-AMERICANS-OF-BILLIONS

FBI released its annual internet crime complaint report on April 6, 2026.

For the past quarter-century, IC3 has been the primary connection between the FBI and the public for information related to cyber-enabled criminal activity.

In 2025, the FBI Internet Crime Complaint Center (IC3) celebrated its 25th anniversary as the central hub for reporting cyber-enabled crime. This milestone signifies the FBI's enduring commitment to fighting the ever-evolving cyber threat. Their success in protecting individuals and organizations is driven by public participation and robust data analysis.

IC3 now averages almost 3,000 complaints per day!!!

53

53

FBI'S 2025 INTERNET CRIME REPORT

WWW.FBI.GOV/NEWS/PRESS-RELEASES/CRYPTOCURRENCY-AND-AI-SCAMS-BILK-AMERICANS-OF-BILLIONS

The IC3 received approximately 453,000 cyber-enabled fraud complaints, with reported losses exceeding $17.7 billion. **Investment fraud remains the primary driver, accounting for nearly 49% of all scam-related losses.**

Americans who submitted complaints involving cryptocurrency reported the highest losses, with 181,565 complaints totaling more than $11 billion. In 2024, the FBI launched Operation Level Up, a proactive initiative to identify and notify people who are currently falling victim to cryptocurrency investment fraud. Since its inception, the initiative has surpassed 8,000 total victims notified and reduced losses by more than $500 million. In 2026, the FBI launched Operation Winter SHIELD, highlighting concrete steps organizations can take to bolster their digital security.

Costly tactics used by scammers also include compromised corporate e-mails, tech support fraud, and personal data breaches. For the first time in its nearly 25-year history, the IC3 report features a section on artificial intelligence, which accounts for 22,364 complaints, costing Americans nearly $893 million. Scammers rely on pressure techniques to defraud Americans while deploying fake social profiles, voice clones, identification documents, and believable videos depicting public figures or loved ones.

54

54

Operation Level Up

The FBI's proactive approach to identify and notify victims of cryptocurrency investment fraud and prevent further financial loss

Operation Level Up began in January 2024 to identify victims of cryptocurrency investment fraud and notify them of the scam. The operation was initiated with the support of agents from the FBI and the United States Secret Service (USSS).

Cryptocurrency investment fraud, also known as pig butchering, is a confidence-based scam. In these types of scams, subjects target victims online and develop a friendship or relationship before introducing a fraudulent investment opportunity in cryptocurrency. Victims are coached to invest more and more money into what appears to be an extremely profitable platform, only to be unable to withdraw their funds.

Operation Level Up has also identified victims of other types of scams, such as work-from-home scams, where scammers pose as employees of legitimate companies and recruit victims for work-from-home, online-only positions. When a victim expresses interest, the scammer provides online training. Once trained, the victim will begin to perform a series of tasks that require the victim to deposit their own money, via cryptocurrency or money transfers, into a platform for the job to be completed.



- www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/operation-level-up

55

55

ABA BANKING JOURNAL, APRIL 7, 2026
FBI: CYBERCRIME LOSSES INCREASED 26% IN 2025

The elderly remain the primary target for fraudsters, with victims aged 60 or over reporting more than $7.7 billion in losses. Victims aged 50-59 reported more than $3.6 billion in losses, with younger age groups reporting less. The average loss among all victims was $20,699. That average increased to $62,604 when crypto was involved.

Complaints involving cryptocurrency accounted for more than $11 billion in total losses, a 22% increase from 2024.

For the first time this year, the IC3 report included a section on AI-facilitated fraud, which accounted for more than 22,000 complaints and nearly $893 million in losses.

"Scammers rely on pressure techniques to defraud Americans while deploying fake social profiles, voice clones, identification documents, and believable videos depicting public figures or loved ones," the agency said.

56

56



Adoption Fraud

Unethical adoption service providers can take advantage of an emotionally charged process to deceive and defraud prospective adoptive parents or birth parents considering adoption. Learn what to look out for, how to protect yourself and your family, and what to do if you're a victim.



Business and Investment Fraud

Scammers are always looking to separate you from your money in business transactions. If it sounds too good to be true, it is. Common scams include advance fee schemes, Nigerian letter or 419 schemes, Ponzi schemes, pyramid schemes, and telemarketing fraud schemes.



Business Email Compromise

Business email compromise (BEC) is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business—both personal and professional.



Charity and Disaster Fraud

Charity fraud scams can come in many forms: emails, social media posts, crowdfunding platforms, cold calls, etc. They are especially common after high-profile disasters. Always use caution and do your research when you're looking to donate to charitable causes.



Consumer Fraud Schemes

Learn more about common fraud schemes that target consumers, including identity theft, non-delivery scams, online car buying scams, and theft of ATM/debit and credit cards.



Cryptocurrency Investment Fraud

Cryptocurrency investment fraud, which the media commonly describes as pig butchering, is one of the most prevalent and damaging fraud schemes today.



Cryptocurrency Job Scams

These scams begin when scammers, masquerading as employees of legitimate companies, recruit victims and require them to deposit their own money in order to complete the job.



Elder Fraud

Each year, millions of elderly Americans fall victim to some type of financial fraud or confidence scheme. Common scams that target older citizens include romance scams, tech support scams, grandparent scams, government impersonation scams, sweepstakes and lottery scams, home repair scams, and TV/radio scams.

- The FBI has lots of useful content to help increase awareness of common frauds!
- //www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams

FINANCIAL SOLUTIONS FOR GROWING COMPANIES, INC.

57

57



Election Crimes and Security

Fair elections are the foundation of our democracy, and the FBI is committed to protecting the rights of all Americans to vote. If you suspect a federal election crime, contact the FBI.



Health Care Fraud

Health care fraud is not a victimless crime. It affects everyone and causes tens of billions of dollars in losses each year. The FBI is the primary agency for investigating health care fraud, for both federal and private insurance programs.



Holiday Scams

When shopping online during the holiday season—or any time of year—always be wary of deals that seem too good to be true, and do your part to avoid becoming a scammer's next victim.



Money Mules

A money mule is someone who transfers or moves illegally acquired money on behalf of someone else. Some money mules know they are supporting criminal enterprises; others are unaware that they are helping criminals profit. Don't be a mule.



Operation Level Up

The FBI's proactive approach to identify and notify victims of cryptocurrency investment fraud and prevent further financial loss.



Ransomware

Ransomware attacks are becoming more targeted, sophisticated, and costly. Learn more about this type of malware, including how to respond and report if it happens to you.



Romance Scams

Protect your heart—and your wallet—by learning to spot and prevent romance scams.



Sextortion

Sextortion is a crime that involves adults coercing kids and teens into sending explicit images online. The FBI has several resources to help caregivers and young people better understand what sextortion is, how to protect against it, and how to talk about this growing and devastating threat.

- The FBI has lots of useful content to help increase awareness of common frauds!
- //www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams

FINANCIAL SOLUTIONS FOR GROWING COMPANIES, INC.

58

58



- The FBI has lots of useful content to help increase awareness of common frauds!
- //www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams

59

59

- www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams



60

60

Identity Theft and Deep Fakes

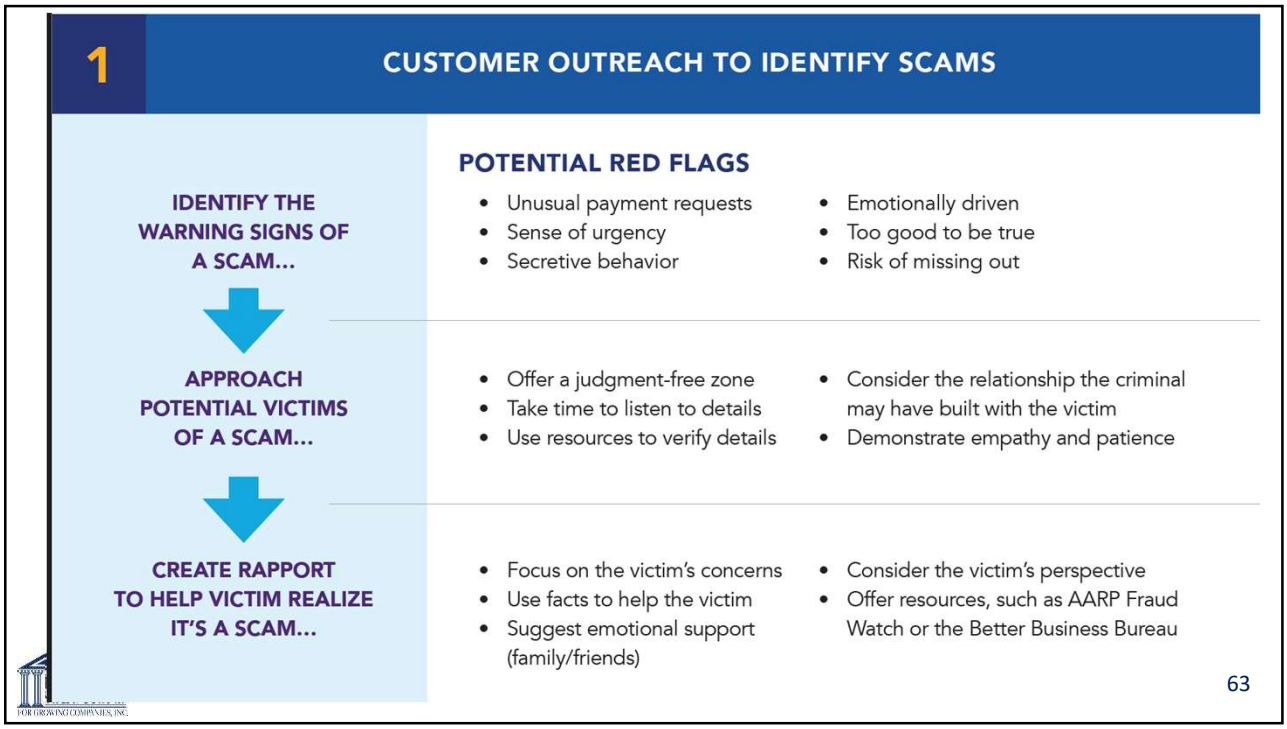
- Complex landscape for compliance:
  - TAKE IT DOWN Act (May 2025)
  - The DEFIANCE Act (S. 1837; introduced in 2025, passed Senate 2026, pending in House)
  - Roughly 47 states also have enacted some form of deepfake legislation, but criminal penalties, civil remedies, and platform obligations vary significantly by jurisdiction.
- According to FTC data, consumers lost more than $12.5 billion to fraud in 2024, and nearly 60% of companies reported increased fraud losses from 2024 to 2025.
- Global losses from identity fraud exceeded $50 billion in 2025, with deepfakes a significant contributing factor.
- Overall trend is clearly toward more enforcement, higher damages, and broader liability — both for individual bad actors and for platforms and companies that fail to act on deepfake content.

61

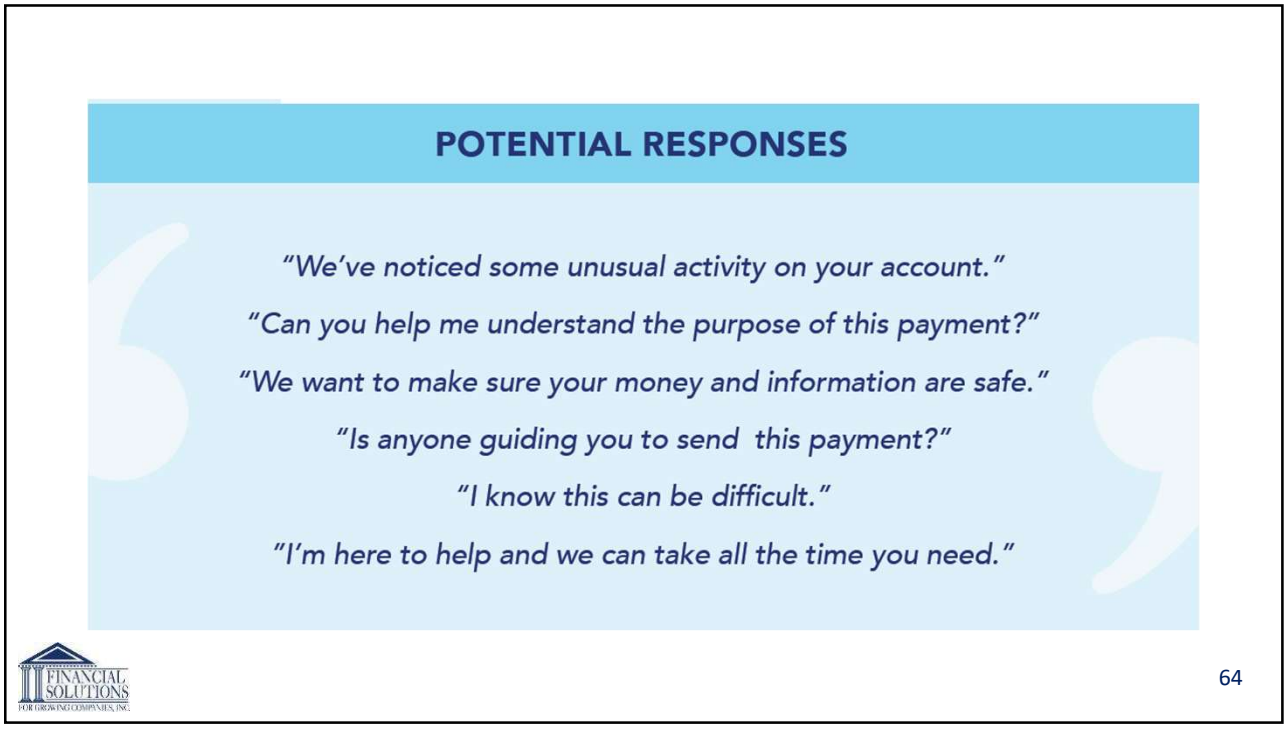


62

62


1
CUSTOMER OUTREACH TO IDENTIFY SCAMS
IDENTIFY THE WARNING SIGNS OF A SCAM...
POTENTIAL RED FLAGS
Unusual payment requests
Sense of urgency
Secretive behavior
Emotionally driven
Too good to be true
Risk of missing out
APPROACH POTENTIAL VICTIMS OF A SCAM...
Offer a judgment-free zone
Take time to listen to details
Use resources to verify details
Consider the relationship the criminal may have built with the victim
Demonstrate empathy and patience
CREATE RAPPORT TO HELP VICTIM REALIZE IT'S A SCAM...
Focus on the victim's concerns
Use facts to help the victim
Suggest emotional support (family/friends)
Consider the victim's perspective
Offer resources, such as AARP Fraud Watch or the Better Business Bureau
63

63


POTENTIAL RESPONSES
"We've noticed some unusual activity on your account."
"Can you help me understand the purpose of this payment?"
"We want to make sure your money and information are safe."
"Is anyone guiding you to send this payment?"
"I know this can be difficult."
"I'm here to help and we can take all the time you need."
64

64

2 RESPONSES TO HELP CUSTOMERS AND REMEDIATE SCAMS

PROVIDE SUPPORT TO THE VICTIM...

- Acknowledge the shock that the victim is feeling
- Reiterate to the customer that this could happen to anyone
- Offer reassurance

TAKE STEPS TO PROTECT THE VICTIM...

- Pause sending the transaction
- Prevent the criminal from accessing the account
- Identify any scam payments sent and request recovery
- Help the customer add security features
- Answer questions patiently

HELP THE VICTIM FEEL IN CONTROL WITH NEXT STEPS...

- Advise the victim to cut off all contact with the criminal
- Recommend reporting the scam to local police, FTC and IC3
- Prioritize the victim's well-being, as the impact is emotional, not just financial

65

65

POTENTIAL RESPONSES

"Scams are widespread and can impact anyone."

"These scams can feel very personal."

"I suggest we add a security feature to your account, if you agree."

"This is a lot to take in at once. I'm going to email this information, too."

"Do you have any questions that I can help answer?"

"It helps to have someone to talk to about this. Do you have someone you can reach out to?"

"Criminals are persistent, so stay strong."

66

66

Thank you for your participation!

Patti D. Joyner, CRCM
www.finsolinc.com
Patti.Joyner@finsolinc.com



67