Regulatory Dispatch

Timely news and resources community bankers can use to better stay on top of a rapidly changing world.

October 30, 2025

Strategic Considerations for Banks to Keep Pace During the Latest Wave of Technology Innovation - *BankNews*

Regulatory compliance and ethical considerations

Banks should be aware that complying with new AI laws and regulations is not sufficient. Because they operate in a highly regulated space, banks must ensure AI technology is used in compliance with existing financial laws and regulations, consumer protection laws, as well as ethical standards. For example, under the Equal Credit Opportunity Act and the Fair Credit Reporting Act, an AI system must have the ability to provide specific and accurate reasons for an adverse action taken relating to a consumer application. AI is also widely used in Anti-Money Laundering and Know-Your-Customer compliance under the Bank Secrecy Act and must be accurate and capable of explaining why fraud was detected or suspicious activity flagged. AI technology can also pose risks under federal and state unfair, deceptive, or abusive acts or practices laws, such as chatbots that may inadvertently provide inaccurate information.

AI technology that handles large volumes of nonpublic financial information must be designed with data security and privacy management controls in compliance with the federal Gramm-Leach-Bliley Act. States are also highly active with regards to AI in financial services. For example, the New York State Department of Financial Services issued guidance warning of the increased cybersecurity risks that arise from the use of AI — phishing attacks and overreliance on vendors that may introduce vulnerabilities and supply-chain risks.

Comment: Community banks certainly have technological opportunities but must adopt practical strategies that balance innovation and responsible implementation.

Bank Management

	FRB Embracing New Technologies and Players in Payments - Governor Christopher J. Waller (10/21/2025) – *Before we hear from these innovators, I would like to touch on the roles that the Federal Reserve plays to support the private sector. These include serving as a convener to solve coordination problems and operating core payment and settlement infrastructure. We are also looking ahead, conducting hands-on research on tokenization, smart contracts, and the intersection of AI and payments for use in our own payment systems. We do this to understand the innovation happening within the payment system as well as to evaluate whether these technologies could provide opportunities to upgrade our own payment infrastructures and to enable us to have deeper conversations with the industry on these new technologies.*

While this is a good start, I believe we can and should do more to support those actively transforming the payment system. To that end, I have asked Federal Reserve staff to explore the idea of what I am calling a "payment account." Today, Federal Reserve Banks provide access to master accounts and financial services to legally eligible entities following our Guidelines for Evaluating Account and Services Requests. The payment account would be available to all institutions that are legally eligible for an account and could be beneficial for those focused primarily on payments innovations.

This payment account concept would be targeted to provide basic Federal Reserve payment services to legally eligible institutions that right now conduct payment services primarily through a third-party bank that has a full-fledged master account. There are many eligible firms engaged in substantial payments activities that may not want or need all the bells and whistles of a master account, or access to the full suite of Federal Reserve financial services, to successfully innovate and provide services to their customers. The idea is to tailor the services of these new accounts to the needs of these firms and the risks they present to the Federal Reserve Banks and the payment system. Accordingly, and importantly, these lower-risk payment accounts would have a streamlined timeline for review. Payments innovation moves fast, and the Federal Reserve needs to keep up.

To be more concrete, let me describe a possible prototype for this type of payment account or, as I sometimes call it, a "skinny" master account. The account would provide access to the Federal Reserve payment rails while controlling for various risks to the Federal Reserve and the payment system. To control the size of the accounts and associated impacts on the Fed's balance sheet, the Reserve Banks would not pay interest on balances in a payment account, and balance caps may be imposed. These accounts would not have daylight overdraft privileges—if the balance hits zero, payments will be rejected. They would not be eligible for discount window borrowing or have access to all Federal Reserve payment services for which the Reserve Banks cannot control the risk of daylight overdrafts. I want to be clear that this is just a prototype idea to provide some clarity on how things could change. The upshot is that, in my view, the payments landscape, as well as the types of providers, has evolved dramatically in recent years, and, accordingly, a new payments account could better reflect this new reality.

BSA / AML

FinCEN Identifies $9 Billion of Iranian Shadow Banking Activity in 2024 (10/23/2025) – WASHINGTON—Today, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued a Financial Trend Analysis (FTA) identifying approximately $9 billion of potential Iranian shadow banking activity that occurred through U.S. correspondent accounts in 2024, based on reporting from U.S. financial institutions. This FTA, which supports President Trump's maximum pressure campaign on Iran, will help to ensure financial institutions are tracking and countering the threat posed by Tehran's shadow banking activity.

Tehran relies on shadow banking networks of Iran-based exchange houses and foreign companies to evade sanctions, sell oil and other commodities abroad, launder money, sustain its regional terrorist proxies, and fund its military and weapons programs. Iranian shadow banking networks are connected across continents—most prominently through the United Arab Emirates (UAE), Hong Kong, and Singapore—by a diverse array of Iranian front companies. This includes oil companies, shell companies, shipping companies, investment companies, and technology procurement companies, which transact billions of

dollars with each other and with unrelated companies, who may be witting or unwitting counterparties.

"Identifying Iran's complex financial lifelines and shadow networks is an essential part of cutting off the funding for their military, weapons programs, and terrorist proxies," said **FinCEN Director Andrea Gacki**. "By issuing this public analysis, we hope to draw attention to Iran's shadow banking activity and encourage financial institutions to be vigilant."

On February 4, 2025, President Trump announced a maximum pressure campaign against Iran with the goals of denying Iran nuclear weapons and intercontinental ballistic missiles; countering its development of other weapons capabilities; neutralizing Iran's network and campaign of regional aggression; and disrupting, degrading, and denying Iran and its terrorist proxies access to the resources that sustain their destabilizing activities.

FinCEN's analysis is based on information pertaining to transactions that occurred before the announcement of the maximum pressure campaign and further supplements the information within FinCEN's June Advisory on the Iranian regime's illicit oil smuggling activities, shadow banking networks, and weapons procurement efforts. FinCEN's analysis includes case studies and infographics to highlight its significant findings, including that:

Foreign Shell Companies Operating Outside the United States Appear to Play the Largest Role in Iranian Shadow Banking Networks

- Shell companies—which exist only on paper with no meaningful business activities—transacted approximately $5 billion in 2024.

Iran-Linked Oil Companies Transacted Billions of Dollars, Potentially for Illicit Oil Sales

- FinCEN identified dozens of foreign oil companies that appear to be Iranian front companies, including oil companies primarily based in the UAE and Singapore that transacted approximately $4 billion in 2024.

Potential Technology Procurement Companies Received Funds from Iran-Linked Entities

- Companies potentially facilitating Iranian procurement of export-controlled technology engaged in approximately $413 million in transactions in 2024.

FinCEN's FTA is available online at: https://www.fincen.gov/system/files/2025-10/FTA-Iranian-Shadow-Banking.pdf

Questions or comments regarding the contents of the FTA should be addressed to the FinCEN Regulatory Support Section by submitting an inquiry at www.fincen.gov/contact. Members of the media may contact press@FinCEN.gov.

Comment: Not the first release from FinCEN regarding Iran this year. Back in June, FinCEN issued Advisory Highlighting Iranian Oil Smuggling, Shadow Banking, and Weapons Procurement Typologies.

Deposit / Retail Operations

Levenfeld Pearlstein Cyberattack and the Risk to Wire Transfers (10/23/2025) – October is Cybersecurity Awareness Month, the perfect time to provide some common-sense tips to avoid a common risk facing businesses: business email compromise and wire fraud. Businesses of all shapes and sizes use email, and those accounts are susceptible to attempts to trick employees into providing sensitive information or sending money.

The perpetrators of business email compromise scams send authentic-looking messages and use a sense of urgency to trick an employee into acting quickly without verifying the sender's identity. With respect to wire fraud, bad actors have made a business of hacking into corporate email systems, perpetrating the "man in the middle attack" whereby the bad actor jumps into a conversation between individuals communicating by email. Often, this conversation involves discussion of a scheduled transaction, and the bad actor modifies wire instructions so the payment, which may be substantial, ends up with the bad actor, not the intended recipient. Typically, before anyone notices the fraud, the money is long gone. These scenarios often lead to litigation, with both parties pointing the finger and both feeling wronged.

Loss, like the above, is real and growing. In 2022, the Federal Bureau of Investigation published "Business Email Compromise and Real Estate Wire Fraud," a report stating that "[its] Internet Crime Complaint Center (IC3) received [business email compromise] related complaints with losses exceeding $2.4 billion." Imagine, for instance, that your business wires payment of $10,000,000 and it goes missing due to this type of scheme – businesses are frequently unable to recover misdirected wire or ACH transfers. While these losses are already substantial, changes to technology, including the rise of AI deepfakes, will make detecting and avoiding business email compromise scams more challenging in the next several years.

Comment: Fraud is a constant and evolving threat, but community banks can take important steps to reduce their risk by being vigilant and educating both employees and customers about the latest fraud trends and tactics. On the topic of fraud, IBAT friend Brent Farley of Farley Law published Fraud Mitigation White Paper – Community Banks in April of this year that is also an informative read.

Technology / Security

CISA Microsoft Releases Out-of-Band Security Update to Mitigate Windows Server Update Service Vulnerability, CVE-2025-59287 (10/24/2025) – Microsoft released an update to address a critical remote code execution vulnerability impacting Windows Server Update Service (WSUS) in Windows Server (2012, 2016, 2019, 2022, and 2025), CVE-2025-59287, that a prior update did not fully mitigate.

CISA strongly urges organizations to implement Microsoft's updated Windows Server Update Service (WSUS) Remote Code Execution Vulnerability guidance, 1 or risk an unauthenticated actor achieving remote code execution with system privileges. Immediate actions for organizations with affected products are:

1. Identify servers that are currently configured to be vulnerable to exploitation (i.e., affected servers with WSUS Server Role enabled and ports open to 8530/8531) for priority mitigation.

	2. Apply the out-of-band security update released on October 23, 2025, to all servers identified in Step 1. Reboot WSUS server(s) after installation to complete mitigation. If organizations are unable to apply the update immediately, system administrators should disable the WSUS Server Role and/or block inbound traffic to ports 8530/8531, the default listeners for WSUS, at the host firewall. Of note, do not undo either of these workarounds until after your organization has installed the update. 3. Apply updates to remaining Windows servers. Reboot servers after installation to complete mitigation. CISA added CVE-2025-59287 to its Known Exploited Vulnerabilities (KEV) Catalog on October 24, 2025

Selected federal rules – proposed

Proposed rules are included only when community banks may want to comment. Date posted may not be the same as the Federal Register Date.

10.06.2025 **OCC** Fair Housing Home Loan Data System SUMMARY: The Office of the Comptroller of the Currency (OCC) invites public comment on a notice of proposed rulemaking (proposed rule) to rescind its Fair Housing Home Loan Data System regulation codified at 12 CFR part 27. The OCC has determined that the regulation is obsolete and largely duplicative of and inconsistent with other legal authorities that require national banks to collect and retain certain information on applications for home loans. Moreover, part 27 imposes asymmetrical data collection requirements on national banks compared to their other depository institution counterparts, and the data collected has limited utility. For these reasons, rescinding the regulation would eliminate the regulatory burden attributable to part 27 for national banks without having a material impact on the availability of data necessary for the OCC to conduct its fair housing-related supervisory activities. **DATES: Comments must be received on or before December 5.**

10.05.2025 **Joint** Unsafe or Unsound Practices, Matters Requiring Attention SUMMARY: The Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC) propose to define the term "unsafe or unsound practice" for purposes of section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818) and to revise the supervisory framework for the issuance of matters requiring attention and other supervisory communications. **DATES: Comments must be received by December 4.**

09.19.2025 **Treasury** GENIUS Act Implementation SUMMARY: The Department of the Treasury (Treasury) is issuing this advance notice of proposed rulemaking (ANPRM) to solicit public comment on questions relating to the implementation of the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act. The GENIUS Act tasks Treasury (and various other federal agencies) with issuing regulations that encourage innovation in payment stablecoins while also providing an appropriately tailored regime to protect consumers, mitigate potential illicit finance risks, and address financial stability risks. Through this ANPRM, Treasury is seeking public comment on potential regulations that may be promulgated by Treasury, including regarding regulatory clarity, prohibitions on certain issuances and marketing, Bank Secrecy Act (BSA) anti-money laundering (AML) and sanctions obligations, the balance of state-level oversight with federal oversight, comparable foreign regulatory and supervisory regimes, and tax issues, among other things. Treasury is seeking comment on all aspects of the ANPRM from all interested parties and also requests commenters to identify other issues that Treasury should consider. **DATES: Comments on this ANPRM must be received on or before November 4, 2025.**