Regulatory Dispatch

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

July 29, 2026

CSBS Wayback Machine - A Look Back at One Year of GENIUS Implementation

One year ago, President Trump signed the GENIUS Act, creating a comprehensive national framework for stablecoin issuance. A decade prior, dollar-backed stablecoins had developed and began maturing under regulation by state money transmission and virtual currency laws. But growing interest from regulated financial institutions, the difficulty of limiting access to unregulated stablecoins, and the risks posed by a potential stablecoin run all made last year a critical moment for developing a uniform national floor.

The GENIUS Act establishes a central prudential requirement: stablecoins must be backed 1:1 with high quality, short duration reserve assets that may not be rehypothecated. The reserve requirement is buttressed with additional standards, helping promote the safe and sound operations of issuers. Federal regulators and states that choose to establish a substantially similar framework for regulating stablecoin issuers are now tasked with turning those standards into a complete regulatory framework.

Along with setting a federal floor, Congress recognized the role that states have played in the development of stablecoin markets. Beyond retaining a state pathway for approving stablecoin issuers, the GENIUS Act preserves the applicability of state consumer protection law. It also retains state supervisory authority over federally approved issuers that are the subsidiaries of state-chartered banks.

The one-year anniversary of the GENIUS Act isn't just a sentimental milestone. It marks the statutory deadline for Treasury and the federal banking regulators to issue most of the implementing regulations. While the agencies have not met that ambitious goal, they have at least issued proposals for implementing most of the requirements. States have also begun to develop their own frameworks, creating a clearer view of how the system will fit together. The volume of work already completed by regulators makes the one-year mark a good moment for a retrospective on how GENIUS Act implementation has gone so far, what's still to come, and what risks we must carefully monitor.

Comment: The GENIUS system was deployed exactly one year ago to modernize core infrastructure, streamline operational workflows, and establish a single source of truth for organizational data. This retrospective evaluates the system's performance, user adoption rates, financial impact, and strategic value over the past 12 months.

BSA / AML

	FinCEN Issues Alert on Fraud Schemes Targeting Federal Student Aid (07/24/2026) – WASHINGTON—Today, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued an Alert urging financial institutions to detect, prevent, and report suspicious activity connected to fraud schemes targeting student aid programs administered by the Federal government. Today's action is the latest in Treasury's efforts, led by President Trump and Vice President Vance, to eliminate government benefits fraud. "Every dollar stolen from Federal student aid is a dollar taken from taxpayers and deserving students," said Secretary of the Treasury Scott Bessent. "The Trump Administration will not tolerate criminals who exploit government programs for personal gain. Treasury is working with financial institutions and law enforcement to identify these fraud schemes, recover stolen funds, and hold those responsible accountable." Fraud rings use stolen and fraudulent identities, as well as other tactics, to enroll in educational institutions and unlawfully acquire funds from Federal student aid programs. The schemes not only result in losses to Federal student aid programs, but in some cases, real students face difficulties enrolling in classes because of the number of fraudulently enrolled "students." ***Comment: Jointly recognized with the FBI and the Department of Education, the alert details how international rings and artificial intelligence (AI) bots exploit open-admission and online college programs to steal millions in taxpayer funds.***

Deposit / Retail Operations

	FTC A way to spot scams: how someone asks you to pay (07/22/2026) – Let's say someone contacts you unexpectedly and says you have to pay to fix a problem, get a prize, or something else. But then they say the only way to pay is by bank transfer, wire transfer, cryptocurrency, payment app, or gift card. Well, reports to the FTC show that's a scam. ***Comment: Remind your accountholders that if someone insists that they can only pay in a specific way that makes it difficult to get their money back, it is a scam. According to reports from the Federal Trade Commission (FTC), forcing a specific, irreversible payment method is the single fastest way to identify fraudulent activity.***
	Sheppard, Mullin, Richter & Hampton LLP Seventh Circuit Holds TCPA Do-Not-Call Claims Do Not Cover Text Messages (07/16/2026) – Section 227(c)(5) permits a consumer who receives more than one telephone call within a 12-month period in violation of Federal Communications Commission regulations to seek injunctive relief and statutory damages. The Seventh Circuit concluded that the provision does not authorize claims based on unwanted texts. Specifically, the court: • Relied on the statute's original meaning. The court determined that the ordinary meaning of "telephone call" when Congress enacted the TCPA in 1991 referred to sound-based communications and did not encompass text messages.

	• Distinguished calls from messages. Other provisions define “telephone solicitation” as a telephone call or message, while Section 227(c)(5) refers only to telephone calls. The court reasoned that Congress’s use of different terms supported a narrower private right of action. • Declined to follow the FCC’s broader interpretation. Although the FCC has extended National Do-Not-Call Registry protections to text messages, the court explained that those regulations were issued under provisions addressing “telephone solicitations,” not the narrower language in Section 227(c)(5). ***Comment: In summary, the U.S. Court of Appeals for the Seventh Circuit ruled that text messages are not "telephone calls" under the private right of action for Do-Not-Call (DNC) violations. In Steidinger v. Blackstone Medical Services, the court eliminated an avenue for consumers to file private class-action lawsuits over marketing texts under Section 227(c)(5) of the Telephone Consumer Protection Act (TCPA).***

Technology / Security

	CISA Russian State-Supported Cyber Actors Conduct Phishing Campaign Targeting Users of Zimbra Collaboration Suite (07/23/2026) – A group of Russian state-supported cyber actors has been targeting and compromising various Western government and commercial organizations using the Zimbra Collaboration Suite (ZCS) software since at least July 2025. The Russian state-supported advanced persistent threat (APT) group’s activity is tracked in the cybersecurity community under several names (see Cybersecurity industry tracking), primarily as “LAUNDRY BEAR,” a name initially coined by the Netherlands General Intelligence and Security Service (AIVD) and Defence Intelligence and Security Service (MIVD) [1]. LAUNDRY BEAR’s targeting is almost certainly to gather sensitive information for the Russian Federation, with these actors primarily focusing on the covert acquisition of email data. Previous campaigns indicated LAUNDRY BEAR relied on unsophisticated initial access techniques—including password spraying, phishing, and pass-the-cookie—allowing the group to successfully run high-volume operations. The latest campaign targeting ZCS uses a novel exploit that was a zero-day vulnerability when first exploited and continues to be successfully exploited. The vulnerability, Common Vulnerabilities and Exposures (CVE) CVE-2025-66376, was patched in November 2025. This demonstrates LAUNDRY BEAR’s intent and ability to deploy increasingly sophisticated technical capabilities. Unlike traditional phishing campaigns that persuade a user into taking an action, such as clicking a link or opening a file, LAUNDRY BEAR’s latest campaign leverages a view-based exploit that only requires a user to view a malicious email within a vulnerable version of the webmail service. Once viewed, the exploit attempts to exfiltrate the victim’s last 90 days of email communications, the organization email directory (i.e., Global Address List [GAL]), and other sensitive information to servers controlled by LAUNDRY BEAR. The exploit also attempts to establish persistent access to victim accounts through a variety of means as detailed in the Persistence and credential access section. ***Comment: A quick Google search and Zimbra’s own website indicate that some banks – mainly larger banks – are in fact using Zimbra Collaboration Suite.***

Open for Comment

Included only when specific to or relevant for community banks to comment on. Date posted may not be the same as the Federal Register Date.

07.17.2026 **FDIC** Reporting Forms and Instructions Associated with Requirements and Standards for FDIC Supervised Permitted Payment Stablecoin Issuers SUMMARY: The FDIC invites comment on new forms and instructions associated with an Office of Management and Budget (OMB) control number (3064-0225) assigned in connection with a notice of proposed rulemaking. In accordance with the requirements of the Paperwork Reduction Act of 1995 (PRA), the FDIC may not conduct or sponsor, and the respondent is not required to respond to, an information collection unless it displays a currently valid OMB control number. As part of the notice of proposed rulemaking, the FDIC sought a new OMB control number for a new information collection that would include weekly and quarterly reporting forms that must be completed by permitted payment stablecoin issuers. **DATES: Comments must be submitted on or before September 18, 2026.**

07.09.2026 **CFPB** Request for Information Regarding Promoting Access to Mortgage Credit **SUMMARY:** This notice requests information from the public about potential regulatory changes that may reduce regulatory burdens and promote access to mortgage credit, as appropriate and consistent with applicable law. The Consumer Financial Protection Bureau (Bureau or CFPB) seeks to reduce unwarranted regulatory burdens to ensure that creditworthy borrowers can access mortgage credit. Specifically, the CFPB is requesting information on industry and consumer burdens related to the integrated mortgage disclosures under the Truth in Lending Act (TILA) and Real Estate Settlement Procedures Act (RESPA) (TILA-RESPA integrated disclosures or TRID), the right of rescission, and reverse mortgage disclosures. **DATES: Comments must be received on or before August 10, 2026.**

06.22.2026 **Joint** Permitted Payment Stablecoin Issuer Customer Identification Program **SUMMARY**: The Financial Crimes Enforcement Network (FinCEN), together with the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA) are jointly issuing this proposed rule to implement certain provisions of the Guiding and Establishing National and Innovation for U.S. Stablecoins Act (GENIUS Act). Specifically, this rulemaking implements the GENIUS Act's directives to treat permitted payment stablecoin issuers as financial institutions under the Bank Secrecy Act and to require issuers to maintain an effective customer identification program. **DATES: Comments must be received by August 21, 2026.**

06.11.2026 **OCC** GENIUS Act: Reporting Forms and Instructions for Permitted Payment Stablecoin Issuers Subject to the Jurisdiction of the Office of the Comptroller of the Currency **SUMMARY:** The Office of the Comptroller of the Currency (OCC) is proposing a new information collection that would include weekly and quarterly reporting forms that must be completed by permitted payment stablecoin issuers and foreign payment stablecoin issuers registered with the OCC under the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act. **Comments are requested on these forms by August 11, 2026.**