NEWSLETTER – OCTOBER 2026

RGS PERSPECTIVES

Commentary regarding Recent Significant BSA/AML Fines

On October 8 and October 13, 2026, the Office of the Comptroller of the Currency (OCC) announced a $350 million and $750 million civil money penalty against American Express National Bank[1] and Bank of America, N.A.[2], respectively, for violations of the Bank Secrecy Act and related regulations. The OCC action against Bank of America was done in coordination with a Consent Order issued on the same day by the Financial Crimes Enforcement Network (FinCEN), which assessed a $1.2 billion fine on Bank of America for similar violations. The OCC's $750 million penalty will be credited against the $1.2 billion FinCEN fine.

In the American Express case a key failure was that the BSA/AML Risk Assessment did not adequately address main money-laundering risks in the credit and charge card business. Whereas for Bank of America a key focus was on the transaction monitoring system as it failed to adequately identify and escalate suspicious activity involving billions of dollars. Deficiencies included the design, thresholds, data coverage, and testing of the transaction monitoring system. In addition, the BSA audit function failed to identify long-standing BSA concerns that examiners subsequently uncovered.

RGS considers the above actions as a reminder of the importance of periodically assessing a BSA/AML Program to ensure that it is current and relevant to latest developments and business initiatives that may be occurring. The following are key areas to review.

- Confirm that the BSA/AML Risk Assessments include all material products, customers, geographies, transaction types, and delivery channels.
- Review the transaction monitoring system and evaluate the history of rule changes including, as applicable, thresholds, risk weights, alert -suppression rules, outcomes of recent independent system validations.

[1] https://occ.gov/news-issuances/news-releases/2026/nr-occ-2026-87.html
[2] https://www.fincen.gov/system/files/2026-10/BoA-Consent-Order-Execution-Final.pdf

- Determine the level of alert backlogs, false positive alerts, alert decisioning and escalation process.
- Test the timing of alerts to escalation to SAR filing including the quality and accuracy of SAR documentation.
- Review the CIP/CDD/EDD processes including, as applicable, beneficial ownership, risk ratings, expected activity and ongoing due diligence for high-risk accounts.
- Determine whether staffing levels, qualifications and overall BSA/AML training meet the specific needs of the bank.
- Evaluate the independent audit process to make sure that it is risk-based and designed to cover all aspects of the BSA/AML/OFAC operations.

Commentary regarding AI Model Governance

As the usage of AI models continues to become more prevalent, it is important to consider the oversight and controls implications. Firstly, it may be a challenge to recognize what qualifies as a model using traditional model risk management norms. For example, a generative AI Chatbot, an AI feature embedded in a loan-origination system, or a machine-learning credit underwriting application, could be overlooked as a model and therefore not subjected to model risk management.

RGS suggests that banks review AI usage in the context of their model risk management programs. And, depending on how AI is being used, it may require a separate set of controls and monitoring within the framework that governs and oversees the bank's traditional models. The following are three areas to review for potential enhancements related to AI:

- AI Governance that will identify who is authorized to approve the use of AI and who is evaluating the risks.
- AI model and vendor risk management, which should outline how the bank assesses, tests, and monitors AI applications and systems.
- Operational controls designed to: i) detect AI errors and inaccurate decisions, ii) prevent the disclosure of confidential information, and iii) detect fraud and violations of law.

From a regulatory perspective, the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC)

issued revised model risk management guidance in April 2026[3]. The guidance focuses on certain key principles, requirements, and best practices that set expectations for model risk management practices. Underlying the guidance is that banks should tailor their model risk management practices to their risk profile, business lines, and model usage. Key elements include governance and controls, model inventory, vendor management, model validation, and performance monitoring.

REGULATORY RULES AND GUIDANCE

GENIUS Act – on October 21, 2026, OCC[4] issued a final rule to implement the U.S. Stablecoins Act (GENIUS Act) addressing all applicable regulations other than those related to the Bank Secrecy Act (BSA), Anti-Money Laundering (AML) and Office of Foreign Assets Control (OFAC) that would have to be addressed primarily by FinCEN and OFAC agencies of the Department of Treasury. The OCC rules related to GENIUS Act are addressed in a new code, 12 CFR 15[5]. The final rule will apply to permitted payment stablecoin issuers and foreign payment stablecoin issuers under the OCC's jurisdiction, and includes various standards and requirements, including those related to risk management, audit, reporting, applications, examinations, capital, reserve assets, etc.

Digital Assets Proposal Withdrawn – on October 5, 2026, the Financial Crimes Enforcement Network (FinCEN)[6] withdrew its proposed rules that would have imposed certain regulatory requirements on financial institutions related to certain digital assets, which would have imposed recordkeeping, verification, and reporting requirements.

Comptrollers Handbook concerning Credit Concentrations – on September 30, 2026, the OCC issued version 3.0 of the "Concentrations of Credit" booklet of the *Comptroller's Handbook*[7]. The booklet provides information to inform and educate examiners about concentrations of credit in banks of all sizes with emphasis on ranges of practices for varying sizes, complexities, and risk profiles. Examiners should determine which expanded procedures to use, if any, based on risk determinations.

[3] https://www.fdic.gov/model-risk-management-revised-guidance.pdf
[4] https://www.occ.gov/news-issuances/bulletins/2026/bulletin-2026-50.html
[5] https://www.occ.gov/news-issuances/news-releases/2026/nr-occ-2026-92a.pdf
[6] https://www.fincen.gov/news/news-releases/fincen-announces-withdrawals-proposed-digital-asset-related-rules
[7] https://occ.gov/news-issuances/bulletins/2026/bulletin-2026-49.html

NYSDFS Additional Cybersecurity Guidance – risk assessments being the foundation of programs implemented by banks, the New York State Department of Financial Services ("DFS)[8] issued additional guidance on September 10, 2026 to clarify regulatory requirements and highlight best practices when designing, conducting, and updating Risk Assessments. Such risk assessments are required in conjunction with the requirements under Cybersecurity Regulation ("Part 500") which requires regulated entities to understand and address cybersecurity risks to maintain cybersecurity programs that protect the confidentiality, integrity, and availability of data in their Information Systems.

Examination Cycles – on September 10, 2026, the OCC[9] published an interim final rule that raises the asset threshold for certain supervised institutions with less than $6 billion in total assets to qualify for an 18-month on-site examination cycle, thereby reducing regulatory burden on these smaller banks.

Regulatory Enforcement and Supervisory Actions – on August 27, 2026, - the OCC and FDIC[10] issued a final rule to clarify how enforcement and supervisory authority will be exercised going forward. The final rule requires prioritizing issues that present material financial risks over matters regarding policies, processes, documentation, and other nonfinancial risks. Also, the final rule establishes uniform standards for when and how Matters Requiring Attention (MRAs), other supervisory observations, and other violations of laws and regulations should be communicated.

Bank Accounting Advisory Series (BAAS) - on August 14, 2026, the OCC[11] released the 2026 edition of BAAS that contains staff responses to frequently asked questions from the banking industry and bank examiners on a variety of accounting topics.

Other/In Process Matters

Regulation O Changes – on October 2, 2026, FRB[12] announced that it will extend the comment period for its proposal to modernize Regulation O, (rules governing the extension of credit by a bank to its "insiders"—bank executives, board members and major shareholders), from October 5th until November 4th.

[8] https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20260910

[9] https://occ.gov/news-issuances/news-releases/2026/nr-ia-2026-75.html
[10] https://occ.gov/news-issuances/news-releases/2026/nr-occ-2026-72.html
[11] https://occ.gov/news-issuances/bulletins/2026/bulletin-2026-38.html
[12] https://www.federalreserve.gov/newsevents/pressreleases/bcreg20261002a.htm

GENIUS Act Proposals – on September 24, 2026, FRB[13] requested public comment on two proposals related to establishing a regulatory framework for Board-supervised payment stablecoin issuers under the GENIUS Act. The first proposal would require that Board-supervised payment stablecoin issuers to fully back their stablecoins with certain permissible reserve assets, such as short-term Treasury bills and certain other high-quality, liquid assets. The second proposal would establish a tailored application process for Board-supervised banks applying to issue payment stablecoins. These applicants would be required to submit a business plan and financial information, among other documents.

Additionally, the OCC issued guidance regarding waivers and application submission under the GENIUS Act on October 21, 2026[14], reminding that, without submission of waiver application, payment stablecoin issuers in US must comply with the GENIUS Act beginning January 18, 2027

Bank Merger Act Reform – on September 17, 2026, FDIC[15] approved a notice of proposed rulemaking that would modernize and reform the process by which the FDIC reviews merger transactions under the Bank Merger Act. The proposed rule is intended to reduce regulatory burden and facilitate a more efficient and tailored approval process related to merger transactions.

Third-Party Risk Management Proposed Guidance – on September 11, 2026, the FDIC, FRB, OCC, and the National Credit Union Administration (NCUA)[16], requested comments on proposed updated guidance related to managing risks associated with third-party relationships. The proposal is intended to assist banks and credit unions to better align and tailor their third-party risk management practices to the risks of individual third-party relationships.

BSA/AML/OFAC UPDATES

Digital Identity Credentials – on September 8, 2026, the FinCEN, OCC, FRB, FDIC and NCUA[17], provided clarity through answers to frequently asked questions (FAQ) related to the use of state-

[13] https://www.federalreserve.gov/newsevents/pressreleases/bcreg20260924a.htm
[14] https://www.occ.gov/news-issuances/bulletins/2026/bulletin-2026-51.html
[15] https://www.fdic.gov/news/press-releases/2026/fdic-board-directors-approves-proposed-rule-modernize-and-reform-fdics
[16] https://occ.gov/news-issuances/news-releases/2026/nr-ia-2026-77a.pdf
[17] https://occ.gov/news-issuances/bulletins/2026/bulletin-2026-44a.pdf

issued mobile driver's licenses and other government-issued verifiable digital credentials (VDC). The answers to these FAQs clarify how banks may use such VDCs to comply with the Customer Information Program (CIP) Rule. For example, the FAQ clarified that a mobile driver's license, which is in essence a VDC format of a driver's license or identity card that is issued by a state government and which contains all of the same information as a physical driver's license is acceptable to be used to meet the requirements of the CIP Rule.

Another example, as one of the methods used to verify a customer's identity, included electronic credentials, such as a digital certificate or a verifiable digital credential, which are considered acceptable but subject to the bank's or credit union's CIP policies. However, despite these electronic forms of identity, there is no substitute under the CIP Rules for an institution to have a reasonable belief that it knows the true identity of the customer.

Confidentiality and Suspicious Activity Reports – on September 2, 2026, FinCEN, OCC, FRB, FDIC, and NCUA[18] issued a statement to clarify confidentiality requirements related to Suspicious Activity Reports (SAR), particularly communications with customers regarding potentially fraudulent transactions. The joint statement highlights:

- The Bank Secrecy Act prohibits the disclosure of a SAR or information that would reveal the existence of a SAR.
- SAR confidentiality requirements do not prohibit banks from communicating with an individual when such communication involves the underlying facts, transactions, and documents upon which a SAR is based.
- Customer communication should be considered on a case-by-case basis and take precautions when discussing information that could reveal the existence of a SAR.

For further guidance or assistance contact us at: info@RGSGlobalAdvisors.com

[18] https://occ.gov/news-issuances/bulletins/2026/bulletin-2026-43a.pdf