FinReg Round-Up

July 2024

As summer 2024 gets underway, the financial services industry has three new guides aimed at managing a variety of risks. The Treasury Department released guidance on halting illicit financing and addressing artificial intelligence (AI) cybersecurity risks, while the bank regulatory agencies produced a third-party relationship risk management guide aimed at community banks.

Treasury Department Unveils 2024 Illicit Financing Prevention Strategy

On May 16, the U.S. Department of the Treasury issued the "2024 National Strategy for Combating Terrorist and Other Illicit Financing," which outlines the federal government's goals and priorities to stop and prevent illicit financial activities. The strategy is based on the 2024 National Risk Assessments on Money Laundering, Terrorist Financing, and Proliferation Financing, published by the department in February.

The 2024 strategy identifies four priorities and recommends 15 supporting actions to guide the federal government's efforts. The four priorities are 1) closing legal and regulatory gaps in the U.S. anti-money laundering/ countering the financing of terrorism (AML/CFT) regime; 2) promoting a more effective and risk-focused U.S. AML/ CFT regulatory and supervisory framework for financial institutions; 3) enhancing the operational effectiveness of law enforcement and other U.S. government agencies, to combat illicit financing; and 4) realizing the benefits of responsible technological innovation in the U.S. by developing new payment technology, among other initiatives. (Read the Treasury Department press release here.)

Attorney Advertising

LOEB & LOEB LLP

Agencies' Third-Party Risk Management Guide Targets Community Bank Relationships

The Federal Reserve System Board of Governors, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency released a guide on May 3 to help community banks develop and implement third-party risk-management practices. Third-party relationships offer community banks access to new technology, products, services and markets. However, the partnerships may introduce operational, compliance, financial and strategic risks for the banks due to decreased control over certain activities. (Read the press release here.)

The guidance, "Third-Party Risk Management: A Guide for Community Banks," covers risk management, the third-party relationship life cycle and governance issues.

Community banks' third-party relationships pose a variety of risks that must be managed to ensure compliance with laws on consumer protection and financial crimes, among others. The guidance is not a substitute for the "Interagency Guidance on Third-Party Relationships: Risk Management," issued in June 2023, according to the agencies.

This guidance and the June 2023 guidance should be read together to fully understand regulatory expectations with respect to third-party risk management. In addition, the plain-language approach of the new guidance may be more comprehensible for fintechs and other service providers to banks, and therefore more useful when negotiating new or renewed service contracts with banks.

Treasury Department Report Outlines Ways To Manage AI Cybersecurity Risks in Financial Services

The U.S. Treasury has identified opportunities and challenges that AI presents to the security and resiliency of the financial services sector in a new report called "Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector." The report outlines steps to address current AI-related operational cybersecurity and fraud risks.

Steps include addressing the widening gap between large and small financial institutions' in-house AI systems; addressing the widely varying amounts of data available to financial institutions for training models; increasing coordination between financial institutions and regulators; and developing a common AI lexicon for the financial sector.

The report further recommends expanding the National Institute of Standards and Technology (NIST) AI Risk Management Framework to include more applicable content on AI governance and risk management related

to the financial services sector. It also recommends aligning existing digital identity solutions to help financial institutions combat fraud and strengthen cybersecurity with an emerging set of international, industry and national digital identity technical standards.

Related Professionals

Anthony Pirraglia . . . . apirraglia@loeb.com
Melissa Hall . . . . mhall@loeb.com