protiviti®
Face the Future with Confidence

Compliance Insights

Your monthly compliance news roundup

April
2020

OCC Reinforces Third-Party Risk Management Expectations

Regulatory expectations related to third-party relationships have evolved considerably since 2013, when the Federal Reserve Board and Office of the Comptroller of the Currency (OCC) issued prescriptive guidances SR 13-19 and OCC 2013-29, respectively. To account for this evolution, the OCC published OCC Bulletin 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," on March 5, 2020. This latest FAQ is an update to the previous and now-rescinded version, OCC Bulletin 2017-21, issued by the OCC on June 7, 2017. The questions from the prior bulletin were incorporated as-is into the new FAQ except for one, which was updated to reflect current AICPA Service Organization Control report information.

The new FAQ provides answers to 13 additional questions not previously addressed. It provides guidance on a number of new topics, including risk management measures when banks have limited contractual negotiation power, instances where third parties have limited ability to provide requested documentation, and circumstances when financial institutions leverage third-party models or third-party assistance in model risk management. Relatedly, the FAQ offers more prescriptive guidance for relationships that involve emerging technology activities such as cloud computing and data aggregation. It also clarifies the distinction between critical business activities and critical third parties and explains expectations for the use and oversight of subcontractors, or fourth parties.

The new FAQ also outlines several criteria for providing comprehensive oversight and monitoring of third parties supporting critical financial institution activities, including how a risk-based approach can be incorporated to enhance the program's effectiveness. Critical business activities may differ from a critical vendor risk assessment classification, so it is important to identify not only those third parties that support these critical business activities, but also which vendors introduce critical risk to the organization. Now, more than

ever, it is important for organizations to have a fundamental understanding of their critical business activities and associated resiliency plans, inclusive of third-party relationships.

The updated guidance highlights the importance of the board in approving contracts with third parties that involve critical activities. The updated FAQ notes that the board should receive sufficient information to understand the bank's strategy for use of third parties to support products, services and operations and should understand key dependencies, costs and limitations the bank has with these third parties. It is not a requirement for the board to read and sign each contract related to critical business activities; however, banks are expected to have processes in place to keep the board informed of the pros and cons of relying on third parties to support critical business activities. Banks must fully understand this reliance to appropriately manage potential interruptions to these activities caused by third parties.

As mentioned, the new FAQ clarifies OCC guidance related to a third party's use of subcontractors. Third parties often deploy their own subcontractors, which can introduce additional risk exposure to a bank depending on the volume, type and location of the work the fourth party is performing. In today's climate, where the temporary viability of certain businesses and industries are often dependent on national or even local government's public health guidance, the FAQ highlights the importance for bank management to understand the risk profile of any fourth parties supporting critical business activities. In addition to understanding the third party's ability to identify and control risks from its use of subcontractors, the FAQ provides additional considerations for management when evaluating its fourth-party risks, including, but not limited to:

- The nature and extent of changes to the third party's reliance on, exposure to, or performance of subcontractors
- The location of subcontractors and bank data
- Whether subcontractors provide services for critical activities
- Whether subcontractors have access to sensitive customer information.

Holistically, the revised guidance reiterates that bank management must understand the importance of identifying third-party relationships beyond contractual arrangements and should establish a risk-based framework for managing these relationships through the third-party risk management lifecycle. Specifically, it is imperative that bank leadership can manage the risks associated with using third and fourth parties to support or provide critical business activities.

Risk-Based Transaction Monitoring During Uncertain Times

In the throes of the COVID-19 emergency, financial institutions are turning to their pandemic plans, business continuity plans and regulatory contacts for guidance on how to navigate during these uncertain times. Recently, regulatory agencies have published a succession of guidance documents to help compliance professionals understand expectations on examinations, reporting obligations, innovating responsibly and adjusting risk-based approaches during the crisis.

Although financial institutions are operating in unprecedented times, risk-based controls can be modified to better equip an institution against the risk of opportunistic financial crimes emerging during this crisis. To defend against COVID-19 exploitation scams, compliance professionals should, among other strategies, review their risk-based transaction monitoring programs to help ensure that monitoring controls are addressing new and emerging risks resulting from the pandemic, while remaining mindful of the challenges that the current environment presents to their organizations' customers and workforce.

The Financial Crimes Enforcement Network (FinCEN) issued its initial guidance on the COVID-19 crisis on March 16, 2020, in a notice that urged financial institutions to communicate concerns related to COVID-19 to regulators and to remain vigilant to heightened illicit activity. The notice highlighted an increased risk in criminals attempting to exploit fears of the crisis by, for example, selling sham cures and duping victims into donating to fraudulent charities. FinCEN had previously warned the financial sector about the nexus between disasters and financial crimes, such as the guidance issued in October 2017 (FIN-2017-A007) regarding fraudulent activity related to disaster relief efforts.

As evidence of the concerns expressed by FinCEN, on March 22, 2020, the U.S. Department of Justice (DOJ) announced its first enforcement action related to COVID-19 financial crime for the selling of bogus vaccines. This action by the DOJ was announced on the heels of Attorney General William Barr's recent direction for the DOJ to prioritize the detection and investigation of illicit conduct related to the pandemic. The Financial Action Task Force (FATF) echoed the concerns and focus expressed by FinCEN and the DOJ, and on April 1, 2020, issued a statement encouraging governments to collaborate with financial institutions to leverage their risk-based approaches to pandemic-related challenges, while still remaining vigilant to illicit financial risks.

On April 3, 2020, FinCEN issued a follow-up notice that outlined COVID-19 impacts to Bank Secrecy Act/anti-money laundering (BSA/AML) programs, including considerations for beneficial ownership, suspension of a recently issued administrative ruling (FIN-2020-

R001) relating to currency transaction reporting (CTR) and encouraging financial institutions to explore innovative approaches to meeting BSA/AML obligations in the current environment responsibly.

From the perspective of transaction monitoring, BSA/AML compliance teams are likely operating in unfamiliar territory with a workforce that is likely remote and understaffed as they brace for a potential uptick of transaction monitoring alerts. To help manage changes in alert volumes, compliance teams should review for potential shifts in expected client activity due to the crisis and consider recalibrating their risk-based monitoring programs accordingly. When reevaluating risk-based transaction monitoring programs, institutions should consider the following:

- Conduct a scenario coverage assessment for both money laundering and fraud to assess whether current scenarios reflect typologies observed in historical disasters and new schemes emerging from COVID-19. Leverage results of such analysis to inform risk-based changes to transaction monitoring programs, help ensure that red flags related to disasters are captured and assess reprioritization of alert reviews to align with the institution's revised approach.
- Prior to deploying adjustments related to transaction monitoring, conduct tests of scenarios, rules and thresholds to allow for reasonable deviations in customer behavior. Even minor tweaks may help mitigate against generating excessive unproductive and low-risk alerts as riskier ones emerge. Anticipated changes in behavior may include dips in wire-transfer volumes, spikes in cash withdrawals, and increased use of digital payment methods such as mobile-based payments and virtual currencies.
- For any modification to transaction monitoring programs, ensure that the rationale is properly documented and that modifications adhere to proper change control protocols. Consider developing structures for permitting anticipated exceptions and swift interim approval processes to meet operational demands during the crisis. Financial institutions should expect examiners to request key decision-making evidence supporting risk-based approach changes due to COVID-19.

With the above considerations, many financial institutions still may not know what changes to expect from their customer base or may believe that continuing uncertainty argues against making changes during such radical times. While there is no playbook or blueprint for how to proceed, BSA/AML compliance professionals of all financial institutions, regardless of

size, may benefit from reevaluating their risk-based approaches and determining whether their current transaction monitoring approach is the best path forward.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60% of *Fortune* 1000® and 35% of *Fortune* Global 500® companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

© 2020 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans.
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®