protiviti®
Face the Future with Confidence

Compliance Insights

Your monthly compliance news roundup

September
2020

Agencies Update Guidance on BSA/AML Compliance Program Expectations

On August 13, 2020, the Federal Reserve Board, the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA) and the Office of the Comptroller of the Currency (OCC) released a joint statement that explains the enforcement of certain Bank Secrecy Act (BSA)/anti-money laundering (AML) requirements.

The statement identifies instances in which an agency may issue a mandatory cease and desist order to address compliance failures with certain requirements under section 8(s) of the Federal Deposit Insurance Act and section 206(q) of the Federal Credit Union Act (FCUA). The guidance also outlines scenarios in which an agency may use discretion to issue formal or informal administration actions or other supervisory measures to address violations or deficiencies.

Enforcement Actions for BSA/AML Compliance Program Failures

The guidance details that a cease and desist order will be issued to depository institutions in cases where an institution:

- Fails to have a written BSA/AML compliance program, including a customer identification program (CIP), that adequately covers the required program components or pillars (i.e., internal controls, independent testing, designated BSA/AML personnel, and training)
- Fails to implement a program that adequately covers the required components
- Has defects in its BSA/AML program in one or more components that indicate that either the written compliance program or its implementation is not effective.

A cease and desist order will be issued whenever an institution fails to correct a previously reported problem with its BSA/AML compliance program. This decision, however, will depend on the following factors:

- A reported issue is considered a "problem" when it involves substantive deficiencies in one or more of the required components or pillars of the institution's BSA/AML compliance program or implementation thereof. The problem must have been documented in a report of examination or other supervisory communication to the institution's board of directors or senior management as a violation of law or regulation that is not isolated or technical, or as a matter that must be corrected.
- Ordinarily, a cease and desist order will not be issued for failure to correct a BSA/AML compliance program problem unless the problems subsequently found by the agency are substantially the same as those previously reported to the institution.

Updates to the 2007 Interagency Statement

The guidance updates the joint statement issued in 2007 in the following key aspects:

- Specifies that financial institutions must have a risk-based customer identification program. This program should enable the institution to understand the nature and purpose of customer relationships to develop customer risk profiles, conduct ongoing monitoring to identify and report suspicious transactions, and maintain and update customer information, which includes beneficial ownership information.
- Provides additional information associated with the individual components, often referred to as pillars, of a BSA/AML compliance program as well as certain examples of related compliance failures that may or may not result in a cease and desist order.
- Clarifies that isolated or technical violations or program deficiencies likely will not necessitate a cease and desist order.

Summary

Financial institutions should take the opportunity to review their current BSA/AML compliance programs and ensure that they address the updated details provided in this latest joint regulatory statement adequately. Prudent next steps should include refreshing the testing program, evaluating the institution's risk-based approach to compliance management, reviewing the audit program, ensuring that the issue management program is comprehensive, and identifying and tracking issues related to BSA/AML through root cause analysis and resolution.

Although the latest guidance does not create new foundational requirements, it provides insight into aspects of a BSA/AML program that the agencies investigate in order to classify and mitigate violations. It also reflects the continued commitment that each agency holds toward identifying and clarifying the expectations of financial institutions' compliance programs.

Fintechs Continue to Challenge Status Quo as Firm Launched in 2015 Becomes First to Receive Full Service National Bank Charter

Fintechs have been disrupting the banking industry since the financial crisis. Most do not need a banking charter to operate; they exist in a hybrid space, where technology-enabled startups and traditional financial service companies meet, a place of ambiguity that shields them from the prying eyes of prudential regulators. The same characteristics that give financial service regulators the authority to supervise do not apply to many fintechs.

However, despite their unique business and strategic models, fintechs still face many compliance risks and challenges associated with serving consumers in a safe and sound manner. Take the case of Varo Money Inc., a fintech that began operation in 2015. In July 2020, the company was granted a full national banking charter by the Office of the Comptroller of the Currency (OCC). Prior to receiving the charter, Varo partnered with a small U.S. bank based in Delaware and used that bank's charter to build a user front-end system, while the bank provided the infrastructure, and traditional bank products and services (i.e., checking, savings, and credit accounts).

Although Varo will rely heavily on the bank during the transition period, Varo will now be able to offer FDIC-insured nationwide banking services (i.e., traditional loan and deposit products) through its mobile and online platform, allowing consumers the same access to products as a traditional bank. It paves the way as the first fintech to receive a full-service national bank charter. In addition to customer interest, Varo will benefit from the bank charter, with direct access to customers, higher liquidity through deposit products, and lower compliance costs as it transitions away from being subject to multiple state regulators to falling under national OCC oversight, which preempts state law.

The National Bank Act was established in 1863 with the intention of creating a national banking system, paying war loans, and establishing a currency. This allows the OCC to grant charters to national banks and interpret authorization for special purpose national banks (i.e., trust banks and credit card institutions). In December 2016, the OCC announced it

would issue special purpose national bank charters to fintechs, as their innovative services were interpreted as equivalent to traditional banking product offerings (i.e., issuing debit cards or offering an electronic payment platform similar to paying checks). Going forward, the OCC will determine fintech eligibility for special purpose charters or full national bank charters case by case to maintain high supervisory standards and fair access and treatment of customers for fintech products and services.

In the United States, there is no fintech-specific regulatory compliance framework standard. However, as fintechs receive charters via prudential regulators such as the OCC, the standards and expectations held for traditional banks will apply. Bank-fintech partnerships are generally cohesive, as their functions are still relatively separate and different. With Varo as the first nationally chartered fintech bank, it is possible those lines will blur as competition increases.

The financial services industry is seeing a transition towards a sharing economy as more consumers turn to fintech firms for banking needs. Varo can now operate with complete independence and offer full deposit banking services, making it a direct competitor to other insured financial institutions. Fintech partnerships with banks may look different than they did in the past. Where fintech business models continue to overlap in function with banks, these relationships will put more pressure on traditional banks to quickly provide new and innovative services.

Considering the legal battles to block the OCC special purpose charter designed for fintechs oversight and a number of fintechs operating in niche markets without a desire for FDIC-backed deposit products, it is unclear whether an influx of national bank charters for fintechs is on the horizon. Although the future of fintechs looks bright, these institutions can expect increased regulatory engagement to mitigate risks to the financial services industry and ensure fair and responsible delivery of banking products to an even broader segment of the population.

Final CCPA Regulations Approved: An Overview of Changes

The California Consumer Privacy Act (CCPA) was passed in June 2018 with the purpose of granting California residents additional rights over their data privacy. The rights granted by the CCPA include the ability to know what information has been collected about consumers and whether consumers' information has been sold or disclosed to another party. It also grants consumers the ability to access, and request that a business delete, their collected

information without discrimination for exercising their rights under the law. Shortly after the CCPA was passed, amendments were proposed to clarify certain provisions.

In August 2020, the California attorney general announced that the state Office of Administrative Law (OAL) had approved updates to the CCPA. The OAL was responsible for reviewing the attorney general's submission of the final proposed CCPA regulations and their respective addendum. Overall, the changes approved by the OAL were deemed "non-substantial" and "without regulatory effect."

Overview of Changes

Below is a list of the "non-substantial" changes made to the final regulations:

- The phrase "Do not sell my info" was removed from various sections in an attempt to eliminate shorthand wording. Instead, businesses are required to use the phrase "Do not sell my personal information."
- The requirement that the identification of sources from which personal information is collected "be described in a manner that provides consumers a meaningful understanding of the information being collected" in the privacy policy has been removed from Section 999.308 in an effort to reduce duplications of requests.
- The severability provision, formerly Section 999.341, was deemed unnecessary and removed.

In addition to the non-substantial changes, the following provisions were withdrawn from the regulations but may be resubmitted after further review and possible revisions:

- The language from Section 999.305(a) regarding the requirement that businesses provide consumers a direct notice and receive explicit consent when the business intends to use personal information for a materially different purpose was removed.
- The offline opt-out notice requirement from Section 999.306(b)(2) that declared that a business that substantially interacts with consumers offline must also provide a notice to the consumer offline was removed. However, businesses still should note that they have an obligation to inform consumers of their right to opt out offline under sections 999.308 and 999.305.
- The ease of consumer opt-out requirement from Section 999.315(c) that stated the business's methods for submitting the request to opt-out must "be easy for

consumers to execute" was removed. Nevertheless, institutions are still required to consider ease of use when implementing an opt-out method.

- The provision formerly in Section 999.326(c) that permits a business to deny a request from an authorized agent if the agent fails to submit proof of authorization from the consumer was also removed.

The aforementioned updates came into effect on August 14, 2020. While the changes are described as non-substantial and without regulatory effect, financial institutions subject to the CCPA should take note of the regulatory changes and ensure that any policies and procedures impacted are reviewed and updated as needed. The changes also signal to the industry that the CCPA and the protection of consumer's right continues to be a priority. With broad information available across search engines and social media platforms that institutions may engage with for marketing purposes, the industry can expect additional states to follow California's model and consider implementing their own state-specific requirements as well.

About Protiviti

Protiviti (www.protiviti.com) 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 independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk, and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent 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.

protiviti®