protiviti®
Face the Future with Confidence

Compliance Insights

Your monthly compliance news roundup

June
2019

A Framework for OFAC Compliance Commitments

On May 2, 2019, the Department of the Treasury's Office of Foreign Assets Control (OFAC) published guidance to assist organizations in developing an appropriate risk-based sanctions compliance program (SCP). The guidance, titled *A Framework for OFAC Compliance Commitments*, instructs institutions that an effective SCP will vary depending on factors such as their size and sophistication, products and services, customers and counterparties, and geographic locations. However, the guidance also identifies five essential components of compliance OFAC believes each SCP should address. A summary of the components is provided below:

- **Management Commitment.** The guidance identifies senior management's commitment and support as one of the most important factors of an institution's risk-based SCP. Management's commitment and support drive success by facilitating investment in resources, empowering personnel, and promoting a culture of compliance throughout the organization. When evaluating management's commitment and support, OFAC will consider the appointment of a dedicated OFAC sanctions compliance officer, the quality and expertise of supporting personnel, and management responsiveness to infractions of SCP requirements.

- **Risk Assessment.** The guidance recommends that each organization take a risk-based approach to designing its SCP, and recommends a top-to-bottom assessment of all institutional touchpoints to the outside world. The guidance also reminds organizations that OFAC's Economic Sanctions Enforcement Guidelines, found in the Annex to Appendix A to 31 CFR Part 501, provides an OFAC Risk Matrix which may be useful when conducting a sanctions compliance risk assessment.

- **Internal Controls.** An effective OFAC compliance program should have an adequate system of internal controls, including written policies and procedures that

are communicated and enforced. It should also include processes to identify and immediately correct weaknesses in internal controls.

- **Testing and Auditing.** Testing and auditing are critical elements of an SCP as they measure its effectiveness and identify areas in need of updating and enhancement. The testing or audit function should be independent of the functions being tested and should utilize personnel and resources appropriate to the sophistication of the entity.

- **Training.** A successful SCP should include a strong training program, provided periodically, or annually at a minimum. Training should be tailored to high-risk employees and reflect the organization's products and services, client and partner relationships, and the geographic regions in which it operates.

In addition to the essential components, a separate section of the guidance lists 10 root causes of SCP breakdowns based on OFAC's assessment of prior administrative actions. This information is included to assist institutions with designing, updating, and amending their SCPs. The 10 root causes are:

- Lack of a formal OFAC SCP.

- Misinterpreting, or failing to understand the applicability of, OFAC's regulations.

- Facilitating transactions by non-U.S. persons (including through or by overseas subsidiaries or affiliates).

- Exporting or re-exporting U.S.-origin goods, technology or services to OFAC sanctioned persons or countries.

- Utilizing the U.S. financial system, or processing payments to or through U.S. financial institutions, for commercial transactions involving OFAC-sanctioned persons or countries.

- Sanctions-screening software or filter faults.

- Improper due diligence on customers or clients (e.g., ownership and business dealings).

- Decentralized compliance functions and inconsistent application of an SCP.

- Utilizing nonstandard payment or commercial practices.

- Actions of individual employees.

While the OFAC guidance does not differ from long-standing expectations of the financial services' regulators, compliance professionals should use this guidance as a benchmark when reviewing and updating their existing SCPs and should consider whether its current sanctions controls adequately account for the root causes of prior OFAC administrative actions.

CFPB Issues Fair Debt Collections Practices Act (FDCPA) Proposal

On May 7, 2019, the Consumer Financial Protection Bureau (CFPB) issued a much anticipated Notice of Proposed Rulemaking (Proposed Rule or Proposal) to implement the Fair Debt Collection Practices Act (FDCPA). Prior to the CFPB's creation by the 2010 Dodd-Frank Act, no federal agency was authorized to issue regulations to implement substantive provisions of the FDCPA. As a result, since the passage of the FDCPA in 1977, many interpretive questions have arisen and gone unanswered. With this Proposed Rule, the CFPB hopes to provide much needed clarity to the industry.

The Proposed Rule restates the FDCPA's substantive provisions largely in the order they appear in the statute, sometimes without further interpretation. In addition, however, the Proposed Rule includes many new provisions and clarifications to address prior uncertainty and advances in communications technology. The substantive changes focused on debt collection communications and consumer disclosures although noteworthy modifications were made in other areas. The following is a summary of some of the key changes established by the Proposed Rule within the aforementioned categories of debt collection communications, consumer disclosures and other areas:

- **Debt Collection Communications.** Communicating with consumers is a fundamental element of the debt collection process. Because such communications can be false, misleading or abusive, they are also regulated by the FDCPA. In addition, communication technology has evolved considerably since passage of the FDCPA in leaving industry participants to speculate on how to comply. The following are key provisions of the Proposed Rule that are directed at communications with consumers:
    - **Mandatory Opt-Out.** Under the proposal, debt collectors that communicate electronically -- via email address, text message or other electronic medium -- are required to include in such communication a clear and conspicuous statement describing one or more ways the consumer can opt out of further communications to that electronic address or telephone number. Consumers cannot be required to pay any fee for opting out.

- **Limited Content Message.** The FDCPA places strict limitations on communications with third parties in connection with the collection of a debt. These limitations, along with the broad definition of the term *communication*, have led to uncertainty over whether debt collectors can leave voicemails or other messages for consumers while still complying with the FDCPA. The proposal attempts to address this issue by establishing criteria for a "limited content message," which, if adhered to, would not qualify as communication under the FDCPA and would therefore not violate the restriction on disclosure of a debt to a third party. A limited content message must include the consumer's name, a request that the consumer reply to the message, the name and telephone number of a natural person whom the consumer can contact to reply, and the mandatory opt-out notice for electronic communications, if applicable. Other limited additional information can be provided including a salutation, date and time of the message, a statement that it relates to an account, and suggested dates and times for the consumer to reply.
- **Frequency Limits for Telephone Calls.** Excessive phone calls by debt collectors have long been a complaint of consumers targeted by such calls. The proposed rule attempts to address this by establishing specific frequency limits on telephone calls. Under the proposal, a debt collector may contact a consumer no more than seven times within a consecutive seven-day period regarding the collection of a particular debt. Debt collectors are also prohibited from calling a consumer within seven days after having had a telephone conversation with the person in connection with the collection of such debt. It is important to note that the frequency prohibitions apply in connection with a "particular debt," so calls made with respect to one debt owned by a consumer do not count with respect to calls made for that consumer's other debts.

- **Consumer Disclosures.** The FDCPA requires that debt collectors send a written notice to a consumer within five days of initial communication containing certain information about the debt and actions the consumer may take in response unless such information was provided in the initial communication. This is commonly referred to as a validation notice. The Proposal retains the existing content requirements for a validation notice but requires the inclusion of additional information on the nature of the debt to help consumers identify whether it is a debt they owe. Another modification to the validation notice is a requirement that it includes options (or prompts) for a consumer to indicate whether he or she wishes to respond to the notice. This consumer response section must be provided in a format

that can be detached and submitted to the debt collector (i.e., a "tear-off"). Importantly, the proposal includes a model form which provides debt collectors a "safe harbor" if used.

- **Other Requirements.** The proposed rule addresses other topics not previously covered by the FDCPA, including a key provision prohibiting debt collectors from furnishing information to a credit reporting agency about a consumer's debt if the debt collector has not previously communicated to the consumer about the debt. Another key provision prohibits the sale, transfer or placement for collection of debt if a debt collector knows the debt has been paid, settled, discharged for bankruptcy or if an identity theft report has been filed.

The information presented above is an overview of the proposed rule and a summary of some key changes. Debt collectors and other institutions subject to the requirements of the FDCPA should perform a thorough analysis of the Proposal and assess the potential impact on their operations. Those wishing to comment on the Proposed Rule must do so by August 19, 2019. The CFPB has indicated that the effective date of any final rule would be one year after the final rule is published in the Federal Register.

FINRA Issues Anti-Money Laundering Red Flag Guidance for Broker-Dealers

On May 6, 2019, the Financial Industry Regulatory Authority (FINRA) issued Regulatory Notice 19-18 (the "Notice") to provide its members with assistance in meeting their suspicious activity monitoring and reporting obligations under FINRA's anti-money laundering (AML) rule. Regulatory Notice 19-18 provides a general overview of AML requirements applicable to broker-dealers, but its primary purpose is to provide member firms with a comprehensive list of money laundering red flags that they should incorporate into their suspicious activity monitoring processes.

A listing of money laundering red flags applicable to the securities industry was first published by the National Association of Securities Dealers (NASD) as Notice to Members 02-21 in April 2002. Since that time, additional lists of red flags have been published at various times by various government agencies and international organizations including the Financial Crimes Enforcement Network (FinCEN), the Federal Financial Institutions Examination Council (FFIEC), the Securities and Exchange Commission (SEC) and the Financial Action Task Force (FATF), to name the more prominent. Regulatory Notice 19-18 is a compilation of those red flags, and others, contained within a single publication.

The red flags in Regulatory Notice 19-18 fall within the following six categories, based on the types of transactions involved:

- Customer due diligence and interactions with customers.
- Deposits of securities.
- Securities trading.
- Money movements.
- Insurance products.
- Other.

While the list of red flags within Regulatory Notice 19-18 is comprehensive, FINRA warns that it is not exhaustive and monitoring for only these types of transactions will not guarantee compliance with AML program requirements or provide a safe harbor from regulatory criticism. FINRA also reminds members of the need to stay vigilant to areas of emerging risks such as activity associated with digital assets as the nature of emerging risks makes them less likely to be addressed by known red flags.

Broker-dealer compliance with AML requirements should be a continuous focus for a firm. The identification and reporting of suspicious activity are the most significant elements of any AML compliance program and the red flags contained within Regulatory Notice 19-18 is guidance that should be incorporated where appropriate. This may mean reviewing policies and procedures, re-evaluating alert criteria within suspicious activity monitoring software or training personnel that have customer interactions. Broker-dealers should be looking to their compliance professionals to review the guidance and make any necessary updates to help ensure an effective AML program.

DOJ Updates Compliance Program Guidance

On April 30, 2019, the Criminal Division of the U.S. Department of Justice (DOJ) released an updated version of its guidance on the Evaluation of Corporate Compliance Programs (DOJ Guidance). The stated intent of the DOJ Guidance is to assist prosecutors in making informed decisions on the effectiveness of a corporation's compliance program for purposes of determining the appropriate form of prosecution or resolution, monetary penalty, and compliance obligations contained in any corporate criminal resolution. While the guidance is directed towards prosecutors, it broadly addresses the characteristics of effective

corporate compliance programs, a relevant issue for all professionals and industries where compliance with laws and regulations is a necessity.

The DOJ's Fraud Division published the prior guidance in 2017, the first formally issued corporate compliance-related document from the DOJ. The former guidance outlined 11 broad "sample topics and questions" and was presented in a checklist format. The new guidance moves from a checklist format to a narrative that identifies three "fundamental questions" that prosecutors should analyze when evaluating a compliance program's effectiveness. The questions are summarized below:

- **Is the Compliance Program Well-Designed?** This is the first fundamental question and it directs prosecutors to determine whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing and whether management is enforcing the program. The guidance identifies six key hallmarks of a well-designed compliance program including (1) a risk assessment, (2) policies and procedures, (3) training and communications, (4) a confidential reporting structure and investigation process, (5) third-party management, and (6) due diligence in mergers and acquisitions.

- **Is the Program Being Implemented Effectively?** The second fundamental question asks prosecutors to evaluate whether the compliance program is applied in good faith and not merely a "paper program." It advises prosecutors that a program that is being effectively implemented will reflect commitment by senior and middle management, provide autonomy and resources to compliance personnel, and incorporate appropriate incentives and disciplinary measures.

- **Does the Corporation's Compliance Program Work in Practice?** The third fundamental question requires prosecutors to evaluate whether, and to what extent, the corporation's compliance program was effective at the time of the offense and at the time of a charging decision or resolution. Assessing the program's effectiveness at the time of the offense is challenging due to its evaluation of a prior state. In assessing whether the program was effective at the time of the offense, prosecutors are advised to consider whether and how the misconduct was detected, what resources were in place to investigate and detect suspected misconduct, and the extent of the remediation efforts. Assessing the program's effectiveness at the time of charging or resolution requires consideration of the program's risk and control

evolution over time, including whether management completed a root-cause analysis to fully understand the misconduct and the actions taken to prevent similar events going forward.

The updated guidance communicates the DOJ's approach to evaluating corporate compliance programs. This perspective is insightful and sheds light on the weight that a compliance program's design, implementation, and operating effectiveness holds in a prosecution. The guidance also emphasizes the overall importance of a company's corporate compliance program and provides details as to how compliance programs should be structured and operating. For these reasons, compliance professionals and senior management would benefit from a close review of the DOJ guidance and should consider the principles contained therein the next time they re-evaluate their own corporate compliance programs.

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.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work 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.

© 2019 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®