FinCEN Issues Guidance on the Customer Due Diligence Rule and Advisory on Cyber Crimes

August 7, 2020

On August 3, 2020, the Financial Crimes Enforcement Network ("FinCEN") issued three new frequently asked questions ("FAQs") regarding the requirements of its customer due diligence (the "CDD Rule"), the first such guidance in more than two years. Although helpful, FinCEN's new guidance does not address a number of outstanding industry questions about the application of the CDD Rule's requirements to various types of products; instead, FinCEN explains its risk-based expectations regarding customer on-boarding, creating a customer risk profile and on-going customer monitoring.

A few days prior, on July 30, 2020, FinCEN issued an "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic,"[1] alerting financial institutions to potential indicators of cybercrime and cyber-enabled crime during COVID-19. It is the third advisory that FinCEN has issued to financial institutions to be watchful for illicit activities related to the COVID-19 pandemic.[2]

New CDD Rule FAQs. FinCEN's newly issued FAQs provide some helpful clarity regarding the scope of CDD-related obligations. In the first FAQ, FinCEN explains its information-collection expectations at on-boarding. In particular, FinCEN explains that

---

1 FinCEN, Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic (July 30, 2020) FIN-2020-A005, *available* here.

2 FinCEN, Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19) (July 7, 2020) FIN-2020-A003, *available* here; FinCEN, Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19) (May 18, 2020) FIN-2020-A002, *available* here. We have previously written about guidance issued by FinCEN and other federal regulators regarding supervisory expectations for anti-money laundering compliance during the COVID-19 crisis. *See* BSA/AML and KYC in a Crisis: Treasury and Supervisory Agencies Provide Guidance as Financial Institutions Respond to the COVID-19 Pandemic (Apr. 13, 2020) *available* here.

the CDD Rule does not impose categorical requirements on covered financial institutions to:

- collect particular CDD information, other than the required beneficial ownership information and that which is necessary to develop a customer risk profile and conduct monitoring;
- perform media searches or news screenings of customers; or
- collect information regarding a financial institution customer's underlying customers.

FinCEN further explains that, for a customer determined to be low risk, a financial institution is not expected to collect information (beyond required elements) to inform its understanding of the nature and purpose of that customer's account.

The second FAQ clarifies that covered financial institutions are not required to use a specific methodology to establish customer risk profiles or to "automatically categorize as 'high risk' products or customer types listed in government publications" as having characteristics that could pose risks. Instead, covered financial institutions should independently evaluate the money laundering risk posed by their customers and develop a customer risk profile accordingly.

The third FAQ asks whether the CDD Rule requires financial institutions to update customer information on a specific schedule. FinCEN clarifies that no requirement exists to update customer information on any particular cadence; rather, the requirement is to update customer information on a risk basis and as a result of "normal monitoring." The language contained in this FAQ largely tracks the guidance provided in the preamble to the CDD Rule.[3]

FinCEN Cyber-Crime Advisory. FinCEN's cyber-crime advisory warns that illicit actors are engaged in an array of fraudulent schemes to exploit vulnerabilities created by the pandemic and contains descriptions of COVID-19-related malicious cyber activity and scams, associated financial red flags and information on reporting suspicious activity. The advisory is intended to aid financial institutions in detecting, preventing and reporting potential COVID-19-related criminal activity. FinCEN identifies three types of scenarios and provides numerous red flags for each type of scenario.

- *Exploitation of Remove Platforms and Processes*. FinCEN notes the COVID-19 pandemic has seen a migration towards remote access and has led to bad actors

[3] 81 Fed. Reg. 29398, 29399 (May 11, 2016).

targeting vulnerabilities in remote applications and virtual environments to steal information, compromise financial activity and disrupt business operations. FinCEN warns that criminals often seek to undermine online identity verification processes through fraudulent identity documents, which can be created by manipulating digital images of legitimate government-issued identity documents. FinCEN also notes that cybercriminals commonly undermine weak authentication processes in attempted account takeovers via methods such as credential stuffing attacks.

- *Phishing, Malware and Extortion*. FinCEN notes significant increases in phishing campaigns, which often reference COVID-19 themes, such as payments related to the CARES Act, in the subjects and bodies of emails. FinCEN also notes that instances of extortion have grown in the wake of the COVID-19 pandemic. FinCEN cites the receipt of numerous suspicious activity reports ("SARs") involving ransomware, which typically encrypts data on systems in the interest of extorting payment from victims in exchange giving victims access to their systems again. FinCEN explains that criminals are targeting entities that are vulnerable due to their involvement in pandemic response, such as researchers working on medical treatments or manufacturers of personal protective equipment. According to FinCEN, in almost all cases, criminals require ransomware-related extortion payments to be made in convertible virtual currency ("CVC"), and FinCEN warns institutions dealing in CVC to be "especially alert to the laundering of proceeds affiliated with cybercrime, illicit darknet marketplace activity, and other CVC-related schemes."

- *Business E-Mail Compromise ("BEC") Schemes*. FinCEN explains that bad actors have increasingly exploited the COVID-19 pandemic by using BEC schemes, targeting municipalities and healthcare industry supply chains in particular. FinCEN cites a common BEC scheme involving criminals convincing companies to redirect payments to new accounts, claiming the modification is due to pandemic-related changes in business operations. FinCEN also notes that criminals may impersonate critical players in a business relationship or transaction to intercept or fraudulently induce payments.

FinCEN urges financial institutions to file SARs as appropriate when detecting such illicit activities. FinCEN requests that the SARs reference its advisory by including the term "COVID19-CYBER FIN-2020-A005" in SAR field 2 (Filing Institution Note to FinCEN) and that the SAR narrative indicate a connection between the suspicious activity being reported and the activities highlighted in the advisory.

* * *

For more information regarding the legal impacts of the coronavirus, please visit our Coronavirus Resource Center.

Please do not hesitate to contact us with any questions.

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com

Satish M. Kini
smkini@debevoise.com

Jim Pastore
jjpastore@debevoise.com

NEW YORK

David G. Sewell
dsewell@debevoise.com

Zila Reyes Acosta-Grimes
zracostagrimes@debevoise.com