CLIENT ALERT

FinCEN Director Identifies Virtual Currency Compliance Risks and COVID-19 Related Issues at Consensus 2020 Conference

May.20.2020

On May 13, 2020, the Director of the Financial Crimes Enforcement Network (FinCEN), Kenneth Blanco, delivered remarks during the first virtual Consensus Blockchain Conference. Blanco called for continued cooperation between the government and the virtual currency industry, cautioning that cybercriminals predominantly use virtual currencies to launder the proceeds of their criminal activities and to purchase the tools needed to conduct them. He stated that since 2013, FinCEN has received almost 70,000 suspicious activity reports (SARs) related to virtual currency exploitation, and financial institutions have provided additional information regarding illicit financial flows involving virtual currency. This information, he said, is critical to law enforcement and FinCEN, which use the information to identify typologies of illicit virtual currency use. FinCEN then disseminates these to industry through advisories. Blanco also highlighted two specific areas for consideration in the virtual currency space:

1. Whether companies have appropriate anti-money laundering/countering the financing of terrorism (AML/CFT) controls in place for anonymity-enhanced cryptocurrencies, or privacy coins, such as Monero, Zcash, Bitcoin, and Grin, noting that the Internal Revenue Service (IRS) is also focused on this issue; and
2. Whether "businesses located outside the United States continue to try to do business with U.S. persons without complying with" Bank Secrecy Act (BSA) rules, including "registering, maintaining a risk-based AML program, and reporting suspicious activity, among other requirements."

Blanco also re-emphasized FinCEN's expectation that virtual currency companies be in compliance with the BSA's Travel Rule, which requires money services businesses (MSBs) that transmit funds to also transmit information about the sender and recipient, noting that "the United States has maintained this expectation to understand who is on the other side of a transaction for years."

Although he commended the creative and collaborative approach to technical solutions on this topic from the industry, he suggested that adequate technologies had been developed at this point to allow compliance, and that the main challenges remaining related instead to governance and process. He encouraged companies to move forward with implementing available solutions, and pointedly noted that recordkeeping violations are among the most cited AML violations in IRS exams of MSBs, which include most virtual currency exchanges.

Blanco applauded a similar, international standard for the transfer of such information established by the Financial Action Task Force (FATF) last June, and that body's interpretive guidance that this obligation should apply to virtual currency businesses.

Separately, Blanco identified the forms of cybercrime that are on the rise during the COVID-19 pandemic: (1) using COVID-19 information as a lure; (2) targeting vulnerabilities in applications that support remote work, such as virtual private networks and remote desktop software, to steal information and compromise transactions; (3) exploiting COVID-19 by scams, extortion,

ransomware, and the sale of fraudulent medical products; and (4) taking advantage of a greater reliance on remote customer onboarding and verification processes to undermine customer due diligence, for example "deepfake" manipulation of digital images and the use of "credential stuffing" attacks to facilitate account takeovers. Blanco encouraged financial institutions to "proactively" notify FinCEN if the pandemic is likely to impact compliance with their BSA reporting obligations, and referenced FinCEN's March 16 and April 3 notices addressing the COVID-19 pandemic. Blanco also noted that FinCEN plans to publish a series of advisories highlighting specific crime typologies relating to the pandemic to encourage better defenses and reporting. FinCEN issued its first advisory in the series on May 18, addressing medical scams related to COVID-19.

Practical Considerations

Director Blanco's remarks suggest practical issues that virtual currency firms may wish to consider, including:

- Whether they have mechanisms to comply with the Travel Rule in place;
- Whether they have appropriate AML/CFT controls in place with respect to "anonymity enhanced" virtual currencies like those identified by Director Blanco. In particular, processes that will allow the institution to understand "normal" customer activity and to properly identify suspicious activity.

More broadly, financial institutions should keep an eye out for additional guidance from FinCEN regarding typologies used in fraud and criminal activity during the pandemic, and to incorporate this information, along with FinCEN's previous guidance surrounding COVID-19, into their AML programs.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Caroline E. Brown
Partner – Washington, D.C.
Phone: +1 202.624.2509
Email: cbrown@crowell.com

Michelle Ann Gitlitz
Partner – New York
Phone: +1 212.895.4334
Email: mgitlitz@crowell.com

Carlton Greene
Partner – Washington, D.C.
Phone: +1 202.624.2818
Email: cgreene@crowell.com

Jorge Pesok
Counsel – New York
Phone: +1 212.803.4073
Email: jpesok@crowell.com

Nicole Sayegh Succar
Counsel – New York

Phone: +1 (212) 803-4031
Email: nsuccar@crowell.com