ALERTS

Treasury Issues Reports and Guidance to Assist Industry In Addressing Threats Posed by Certain Virtual Currency Transactions and Ransomware Payments

Oct 28, 2021, 12:00 AM

On Oct. 15, 2021, the U.S. Department of the Treasury's ("Treasury") Office of Foreign Assets Control ("OFAC") issued guidance clarifying the application of sanctions laws to virtual currency activity ("VC Sanctions Guidance").[1] Among other topics, the VC Sanctions Guidance outlines recommended best practices for compliance with OFAC's sanctions regulations.[2] OFAC's issuance of the VC Sanctions Guidance follows steps OFAC took last month in the ransomware payments space. On Sept. 21, 2021, OFAC (1) issued an updated advisory ("2021 Ransomware Advisory")[3] highlighting the potential sanctions risks associated with making and/or facilitating ransomware payments; and (2) designated a virtual currency exchange, SUEX OTC, S.R.O. ("SUEX"), as well as its associated digital currency addresses, for facilitating financial transactions for ransomware actors.[4]

Relatedly, pursuant to the Anti-Money Laundering Act of 2020, Treasury's Financial Crimes Enforcement Network ("FinCEN") published its first report ("Report") examining patterns and trends from financial institutions' Suspicious Activity Reports ("SARs"), with the Report focusing on trends relating to ransomware payments.[5]

Finally, on Oct. 18, 2021, Treasury released a report ("2021 Sanctions Review")[6], which, among other matters, details the results of a review of its sanctions programs and outlines recommendations to "preserve and

enhance" the programs' effectiveness going forward with respect to digital currencies.[7]

OFAC's Sanctions Guidance Compliance to the Virtual Currency Industry

Stressing the "increasingly critical role" the virtual currency industry plays in "preventing sanctioned persons from exploiting virtual currencies to evade sanctions," OFAC's VC Sanctions Guidance sets forth best practices for the virtual currency industry to mitigate risk, highlights several industry case studies, and identifies a series of "red flags" to help the industry fashion their compliance programs.[8] Broadly, the VC Sanctions Guidance reiterates that all U.S. persons — including virtual currency companies — are required to comply with OFAC regulations and that U.S. persons are prohibited from transacting with sanctioned individuals or entities.[9] The VC Sanctions Guidance also reminds industry participants that the U.S. sanctions regime follows the concept of strict liability; U.S. persons may be civilly liable for certain sanctions violations even if such persons did not know or have reason to know they were violating OFAC regulations.[10]

With respect to best practices for the virtual currency industry, the VC Sanctions Guidance details certain recommendations that align with the five components OFAC identifies as "essential" to a compliance program: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.[11]

- *Management Commitment*. Stressing that senior management's commitment to compliance is "one of the most important factors in determining the [sanctions compliance] program's success," the VC Sanctions Guidance notes that many virtual currency companies do not implement OFAC sanctions policies and procedures until "months, or even years, after commencing operations."[12] Warning that such a delay can expose virtual currency companies to a variety of risks, the VC Sanctions Guidance recommends that companies (1) review and "endorse" compliance policies and procedures, (2) make available adequate resources to support the compliance program, (3) "[d]elegate sufficient autonomy and authority to the compliance unit," and (4) name a particular sanctions compliance officer with the "requisite technical expertise."[13]

- *Risk Assessment*. Virtual currency companies developing a sanctions program should conduct a routine risk assessment to "identify potential sanctions issues the company is likely to encounter."[14] Notably, the VC Sanctions Guidance does not indicate how frequently a virtual currency company should conduct a risk assessment. The VC Sanctions Guidance also suggests that such a risk assessment exercise include a total review of the company in order to identify and evaluate its "touchpoints to foreign jurisdictions or persons."[15] In addition, the VC Sanctions Guidance encourages virtual currency companies to assess their exposure to OFAC sanctions prior to providing services to customers.[16] Lastly, highlighting OFAC's action designating a virtual currency exchange last month, discussed further below, the VC Sanctions Guidance underscores that a comprehensive risk assessment should include "understanding who is accessing a company's platform or services" as it may "help members of the virtual currency industry identify the appropriate screening standards to set for each of its products and services."[17]

- *Internal Controls*. Noting that an effective sanctions program will "enable a company to conduct sufficient due diligence on customers, business partners, and transactions and identify 'red flags,'" the VC Sanctions Guidance sets forth several recommendations to strengthen virtual currency companies' internal controls.[18]

- *Geolocation Tools*. Industry participants are urged to employ geolocation tools to "identify and prevent IP addresses that originate in sanctioned jurisdictions from accessing a company's website and services for activity that is prohibited by OFAC's regulations."[19] Further, the VC Sanctions Guidance points out that alerts regarding a potentially sanctioned transaction can come from other sources, including address information provided by a customer or counterparty, information contained in email addresses, or invoice or other transactional information.[20] The VC Sanctions Guidance encourages companies to incorporate the review of such types of information.

- *Know Your Customer ("KYC") Procedures.* The VC Sanctions Guidance urges companies to obtain information about their customers during their onboarding process as well as throughout the customer relationship and evaluate that information for potential sanctions-related risk. At both the individual and entity level, such information could include legal/entity name, physical and email address, bank

information, IP addresses associated with transactions and logins, and relevant government documents.[21]

- *Transaction Monitoring and Investigation.* Virtual currency companies should employ transaction monitoring and investigation software in order to pinpoint transactions that involve virtual currency addresses or other identifying information.[22] The VC Sanctions Guidance notes that this control helps companies "prevent transfers to addresses associated with sanctioned persons and avoid violations of U.S. sanctions."[23]

- *Implementing Remedial Measures.* The VC Sanctions Guidance also urges industry participants, upon discovering any weakness in a compliance program, to take immediate action to implement "compensating controls" until the origin of the weakness can be identified and rehabilitated.[24] It notes that, in a potential enforcement action, OFAC may consider an entity's implementation of remedial measures in reaction to a perceived violation of OFAC regulations as a mitigating factor.[25]

- *Testing and Auditing*. The VC Sanctions Guidance encourages the use of a "comprehensive, independent, and objective" testing and auditing function to assess the effectiveness of a company's sanctions compliance program.[26] Such procedures include: (1) ensuring that screening the Specially Designated Nationals ("SDN") list is functional and effective; (2) ensuring that screening tools are properly flagging geographic keywords in connection with KYC-related and transactional screening; (3) ensuring that IP address software is effectively blocking users from sanctioned jurisdictions from accessing the company's products and services; and (4) evaluating procedures for investigating transactions for a potential sanctions nexus as well as reporting rejected transactions to OFAC.[27] The VC Sanctions Guidance does not, however, indicate the frequency at which virtual currency companies should test or audit their sanctions compliance program.

- *Training*. Finally, the VC Sanctions Guidance notes that OFAC training should be given to all "appropriate employees, including compliance, management, and customer service personnel" of a virtual currency company.[28] An effective training program, according to the VC Sanctions Guidance, covers the sanctions compliance responsibilities of employees as well as "hold[s] employees accountable for meeting training requirements through the use of assessments."[29] Notably, the

VC Sanctions Guidance indicates that training should be conducted on a "periodic basis, and, at a minimum, annually."[30]

The VC Sanctions Guidance also highlights two new virtual currency-related FAQs released by OFAC. The first FAQ addresses the definitions of "digital currency," "digital currency wallet," "digital currency address" and "virtual currency."[31] The second FAQ outlines how a U.S. person blocks digital currency, requiring U.S. persons who determine they hold a virtual currency that must be blocked to "deny all parties access to that virtual currency, ensure that they comply with OFAC regulations related to the holding and reporting of blocked assets, and implement controls that align with a risk-based approach."[32] OFAC will not require U.S. persons holding blocked virtual currency to convert it into traditional fiat currency, and U.S. persons will not need to hold the blocked virtual currency in an interest-bearing account.[33] U.S. persons must report blocked virtual currency to OFAC within 10 business days and, as long as the virtual currency remains blocked, on an annual basis.[34]

OFAC's 2021 Ransomware Advisory

As discussed above, OFAC's issuance of the VC Sanctions Guidance follows steps taken last month in the ransomware payments space, including OFAC's issuance of the 2021 Ransomware Advisory and its designation of a virtual currency exchange to the SDN list for facilitating transactions for ransomware actors. The 2021 Ransomware Advisory makes many of the same points made by OFAC in an advisory released in October 2020 regarding the potential risks for facilitating ransomware payments,[35] but it also provides clearer examples of strong cybersecurity practices and more forcefully suggests that companies should not pay ransoms.

The 2021 Ransomware Advisory (1) reminds the public that U.S. persons are prohibited from transacting with sanctioned entities or individuals, (2) stresses that the U.S. sanctions regime incorporates the concept of strict liability, and (3) reiterates that the U.S. government strongly discourages private companies and citizens from paying cyber ransom or extortion demands.[36]

The 2021 Ransomware Advisory recommends that companies should focus on strengthening their cybersecurity protocols because preventing a ransomware attack can negate the need to pay a ransom.[37]

Specifically, OFAC suggests that companies institute cybersecurity training, develop incident response plans, utilize authentication protocols, and regularly update antivirus and anti-malware software.[38] Companies should also maintain offline data backups — which would allow the company to continue operating without having to pay the ransom — and, in the event of a ransomware attack, contact appropriate law enforcement agencies, such as the Cybersecurity and Infrastructure Security Agency, a local FBI field office or a local U.S. Secret Service office.[39] Lastly, the 2021 Ransomware Advisory strongly encourages full and ongoing cooperation with the relevant agencies both during and after a ransomware attack.[40] OFAC notes that these types of measures will be considered as mitigating factors in any potential cyber-related enforcement action.[41]

Finally, if a company is considering paying a ransom, the 2021 Ransomware Advisory reminds companies that various ransomware groups and other malicious cyber actors have been sanctioned, and so facilitating or making payments to these actors constitutes a violation of U.S. sanctions laws and could result in civil penalties.[42]

First Designation of a Virtual Currency Exchange

Last month, OFAC designated SUEX, a virtual currency exchange based in the Czech Republic and Russia associated with ransomware groups and other criminal organizations, by adding SUEX and its associated digital currency addresses to OFAC's SDN list.[43] As a result, all property and interests in property of the designated target under U.S. jurisdiction are blocked, and U.S. persons are generally prohibited from engaging in transactions with the designated target.[44]

In previous designations, OFAC has identified certain virtual currency wallet addresses and persons involved in virtual currency transactions as SDNs.[45] Notably, however, the addition of SUEX to the SDN list is the first time OFAC has designated a virtual currency exchange.[46]

FinCEN Report on Ransomware Payments Trends

Also on Oct. 15, 2021, FinCEN released a Report examining trends relating to ransomware payments, pursuant to a mandate in the Anti-Money

Laundering Act of 2020 that the agency "periodically publish threat pattern and trend information derived from financial institutions' [SARs]."[47] Among other things, the Report finds that:

- Covered institutions filed 635 ransomware-related SARs in the first half of 2021 alone, as compared to 487 reported SARs in the entire 2020 calendar year (a 30% increase);
- The total value of suspicious activity reported in ransomware-related SARs was $590 million;
- The average monthly value of ransomware transactions in the first half of 2021 was $66.4 million, and Bitcoin was the most common ransomware payment method; and
- Several money laundering typologies were common among ransomware variants, "including threat actors increasingly requesting payments in Anonymity-enhanced Cryptocurrencies (AECs) and avoiding reusing wallet addresses, 'chain hopping' and cashing out at centralized exchanges, and using mixing services and decentralized exchanges to convert proceeds."[48]

Treasury's 2021 Sanctions Review

On Oct. 18, 2021, Treasury released its 2021 Sanctions Review, which evaluates the "framework guiding imposition of economic and financial sanctions" as well as "potential operational, structural, and procedural changes to improve Treasury's ability to use sanctions now and in the future."[49] Among other findings, the 2021 Sanctions Review warns that technological innovations like digital currencies and alternative payment platforms "potentially reduce the efficacy of American sanctions" and "offer malign actors opportunities to hold and transfer funds outside the traditional dollar-based financial system."[50] Accordingly, Treasury concludes that it should "invest in deepening its institutional knowledge and capabilities in the evolving digital assets and services space to support the full sanctions lifecycle of activities."[51]

Conclusion

Together, Treasury's recent pronouncements indicate a concerted effort to counter the increasing threat of ransomware incidents and to better protect the public against these threats which are frequently tied to

transactions in virtual currency. These statements also clarify the application of current sanctions regulations to certain virtual currency transactions and industry participants. Persons engaged in virtual currency transactions should be aware of these actions and published guidance and should, if necessary, take appropriate measures to ensure that their sanctions compliance programs are robust and adequate to resist these threats.

Schulte Roth & Zabel lawyers are available to assist you in addressing any questions you may have regarding these developments. Please contact your attorney at Schulte Roth & Zabel or any of the following:

Betty Santangelo – New York (+1 212.756.2587, betty.santangelo@srz.com)

Gary Stein

Kelly Koscuiszka – New York (+1 212.756.2465, kelly.koscuiszka@srz.com)

Donald J. Mosher – New York (+1 212.756.2187, donald.mosher@srz.com)

Kara A. Kuchar – New York (+1 212.756.2734, kara.kuchar@srz.com)

Jessica Sklute – New York (+1 212.756.2180, jessica.sklute@srz.com)

Melissa G.R. Goldstein – Washington, DC (+1 202.729.7471, melissa.goldstein@srz.com)

Adam J. Barazani – New York (+1 212.756.2519, adam.barazani@srz.com)

Jessica Romano – New York (+1 212.756.2205, jessica.romano@srz.com)

Hadas A. Jacobi – New York (+1 212.756.2055, hadas.jacobi@srz.com)

Steven T. Cummings – New York (+1 212.756.2251, steven.cummings@srz.com)

---

[1] Office of Foreign Assets Control, U.S. Dep't of Treasury, "Sanctions Compliance Guidance for the Virtual Currency Industry," October 2021, available here; *see also* Press Release, U.S. Dep't of Treasury, "Treasury Continues Campaign to Combat Ransomware as Part of Whole-of-Government Effort," Oct. 15, 2021, available here ("October Press Release").

[2] VC Sanctions Guidance, *supra* note 1, at 10.

[3] Office of Foreign Assets Control, U.S. Dep't of Treasury, "Updated Advisory on Potential Sanctions Risk for Facilitating Ransomware Payments," 2021, available here ("Ransomware Advisory"); *see also* Press Release, U.S. Dep't of Treasury, "Treasury Takes Robust Actions to Counter Ransomware," Sept. 21, 2021, available here ("September Press Release").

[4] *See* Office of Foreign Assets Control, U.S. Dep't of Treasury, "Publication of Updated Ransomware Advisory; Cyber-related Designation,"2021, available here (listing digital addresses added to SDN List).

[5] Financial Crimes Enforcement Network, U.S. Dep't of Treasury, "Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021", available here ("Report").

[6] U.S. Dep't of Treasury, "The Treasury 2021 Sanctions Review," October 2021, available here ("2021 Sanctions Review").

[7] Press Release, U.S. Dep't of Treasury, "U.S. Department of the Treasury Releases Sanctions Review," October 18, 2021, available here.

[8] VC Sanctions Guidance, *supra* note 1, at 1, 12, 13.

[9] *Id.* at 6.

[10] *Id.*

[11] *Id.* at 10; *see also* Office of Foreign Assets Control, U.S. Dep't of Treasury, "A Framework for OFAC Compliance Commitments," available here.

[12] VC Sanctions Guidance, *supra* note 1, at 11.

[13] *Id.*

[14] *Id.* at 12.

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.* at 13.

[19] *Id.* at 14.

[20] *Id.*

[21] *Id.* at 14–15.

[22] *Id.* at 15.

[23] *Id.*

[24] *Id.* at 16.

[25] *Id.*

[26] *Id.* at 18.

[27] *Id.*

[28] *Id.* at 19.

[29] *Id.*

[30] *Id.*

[31] U.S. Dep't of Treasury, "Frequently Asked Questions, Questions on Virtual Currency, #559," Oct. 15, 2021, available here.

[32] U.S. Dep't of Treasury, "Frequently Asked Questions, Questions on Virtual Currency, #646," Oct. 15, 2021, available here.

[33] *Id.*

[34] *Id.*

[35] Office of Foreign Assets Control, U.S. Dep't of Treasury, "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," Oct. 1, 2020, available here. The 2021 Ransomware Advisory notes that it updates and supersedes the advisory released in 2020. 2021 Ransomware Advisory, *supra* note 3, at 1 n.2.

[36] 2021 Ransomware Advisory, *supra* note 3, at 1, 3, 4.

[37] *Id.* at 1.

[38] *Id.* at 5.

[39] *Id.* at 5–6.

[40] *Id.* at 5.

[41] *Id.* at 4–5.

[42] *Id.* at 3.

[43] September Press Release, *supra* note 3.

[44] *Id.*

[45] *See, e.g.*., Press Release, U.S. Dep't of Treasury, Treasury Sanctions Russian Cyber actors for Virtual Currency Theft (Sept. 16, 2020), available here; Press Release, U.S. Dep't of Treasury, Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Digital Currency Addresses (Nov. 28, 2018), available here.

[46] September Press Release, *supra* note 3.

[47] Report, *supra* note 5, at 1.

[48] *Id.* at 1–2.

[49] 2021 Sanctions Review, *supra* note 6, at 3.

[50] *Id.* at 2.

[51] *Id.* at 6.

Related People

Betty Santangelo

New York

Kelly Koscuiszka

Partner

New York

Donald Mosher

Partner

New York

Kara Kuchar

Partner

New York

Melissa Goldstein

Partner

Washington, DC

Adam Barazani

Special Counsel

New York

Jessica Romano

Special Counsel

New York

Practices

BANK REGULATORY

BROKER-DEALER REGULATORY AND ENFORCEMENT

FINANCE

INVESTMENT MANAGEMENT

SECURITIES LITIGATION AND CLASS ACTION

Attachments

Download Alert