Articles + Publications | February 21, 2023

Locke Lord QuickStudy: OFAC Russia Related Sanctions ?Update: ?February 21, 2023?

Locke Lord LLP

WRITTEN BY

Ryan Last

On February 8, 2023, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") published FAQ 1113 related to the ?Russian Harmful Foreign Activities ?Sanctions Regulations, 31 CFR Part 587 (the ???"RuHSR") which clarifies that a transfer of securities issued by non-blocked Russian entities through inheritance to a U.S. Person beneficiary of the decedent's estate is permissible.? On the following day, OFAC, in coordination with the United Kingdom, designated seven individuals who are members of the Russian-based cybercrime Trickbot Group and the Conti gang, pursuant to Executive Order ("EO") 13694, as amended by EO 13757.

FAQs

FAQ 1113 – *If a decedent's estate includes securities issued by non-blocked Russian entities, do the new investment prohibitions in Executive Order ("EO") 14066, EO 14068, or EO 14071 (collectively, the "Executive Orders") prohibit the transfer of such securities, through inheritance, to the relevant beneficiary of the decedent's estate?*

No. If a decedent's estate includes securities issued by non-blocked Russian entities, the new investment prohibitions in Executive Orders do not prohibit the transfer of such securities, through inheritance, to the relevant beneficiary of the decedent's estate. U.S. persons, including U.S. financial institutions, may transfer securities issued by non-blocked Russian entities from a decedent's estate to the account of a relevant beneficiary or beneficiaries, including a successor entity (*e.g.*, a family trust), provided such transfers (i) are part of the ordinary course administration of the decedent's estate, (ii) do not involve an exchange for value, and (iii) have no other sanctions nexus (including the involvement of blocked persons). Blocked securities in a decedent's estate, however, must remain blocked. The administration of a decedent's estate requiring the transfer of blocked securities would still require a specific license from OFAC.

Trickbot Executive Designation

Trickbot, a type of malware operated by a group of cybercriminals based in Russia known as the ("Trickbot Group"), was first discovered in 2016. It has been reported that 2021, the Conti cybercrime gang took over management of Trickbot and has since sunset the Trickbot malware in favor of a new Trojan called "BazarBackdoor." Trickbot was designed to capture sensitive information such as financial and other personal data and allow the cybercriminals to "lock-up" the victim's data until an agreed ransom is paid. BazarBackdoor provides threat actors remote access to an internal device that can be used as a launch-pad for further lateral

movement within a network.

The United States and the United Kingdom jointly took action on February 9, 2023, when both countries sanctioned seven individuals of the Trickbot Group (a/k/a Conti Gang) for their involvement in a range of malicious cyber activities. As a result of the designation, U.S. persons are prohibited from engaging in any transactions or dealing with these seven individuals that are owned or controlled by them. All property and interests in property of these individuals that are in the U.S. or in the possession or control of a U.S. person must be blocked and reported to OFAC. Furthermore, persons that engage in certain transactions with any of the seven designated individuals may themselves be become sanctioned.

Paying ransomware payments to the designated persons, other specially designated nationals ("SDNs") or a comprehensively embargoed jurisdiction such as North Korea, would violate U.S. sanctions, and could also jeopardize the victim's ability to obtain insurance coverage. If payment to unlock ransomeware would be made to a SDN (either directly or indirectly), the victim would be required to obtain a license from OFAC prior to making payment. While OFAC has indicated that it would address any such payment requests in an expedited manner, it does not guaranty grant of the license. Moreover, any delay including the additional time to seek an OFAC license, could result in additional harm to the victim. Finally, the victim usually does not know the ultimate beneficiary of a ransomeware payment; diligence is required to determine if the payment will benefit a SDN such as one of the seven designees mentioned above.

In September 2021, OFAC issued an advisory ("Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments") warning that individuals and entities who facilitate ransomware payments to sanctioned persons may face civil penalties for violating OFAC regulations. The advisory notes that paying a ransom to a sanctioned individual or entity could be interpreted as providing material support to a sanctioned person or entity, which is prohibited under OFAC regulations. Therefore, legal counsel, insurers, digital forensics providers, incident response technicians, financial services and other advisers should also take note that facilitating such payments to SDNs also violates U.S. sanctions laws and regulations.

U.S. Persons are encouraged to implement a risk-based compliance program to mitigate exposure to cybercrime. Recent studies indicate that ransomeware players spend considerable time in a victim's system to learn where data back-ups are stored, and how to defeat the victim's other disaster recovery and mitigation techniques. Therefore, many cybercrime experts are recommending adding external hard drive back-up media in addition to cloud-based back-up systems which can be corrupted by malware. Organizations can also reduce the risk of falling victim to ransomware by a sanctioned actor and mitigate the impact of an attack if one occurs by adopting or improving their internal cybersecurity practices, such as those highlighted in the Cybersecurity and Infrastructure Security Agency's September 2020 Ransomware Guide. This guide is a resource developed by the U.S. government to help organizations prevent, detect, and respond to ransomware attacks.

Conclusion

This paper is intended as a guide only and is not a substitute for specific legal or ?tax advice. ??Please ???reach out to the ?authors for any specific questions. We expect ?to continue to monitor the ??topics ???addressed in this paper and provide ?future ?client updates when useful.?

RELATED INDUSTRIES + PRACTICES

- Corporate
- International
- Sanctions + Trade Controls