DORSEY

DORSEY+WHITNEY LLP

U.S. Treasury Department Takes Action Against Russian Darkmarket Entity as Latest Government Move Against Cybercrime

by Lawrence Ward, Beth Forsythe, John Marti, Nicole Engisch, and Alex Hontos

On April 5, the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") in the U.S. Department of the Treasury named **Genesis Market** to OFAC's Specially Designated Nationals List ("SDN List").[1] Genesis Market is considered one of the world's largest "dark" marketplaces involved in the theft and illegal sale of device credentials and other stolen valuable confidential personal or business information. OFAC acted in close coordination with the U.S. Department of Justice and law enforcement agencies in another dozen countries.

In this action, OFAC placed Genesis Market, believed to be located in Russia, on the SDN List under Executive Order 13694[2] ("EO 13694"), as amended by Executive Order 13757[i3] ("EO 13757") because the U.S. Government considers it as being directly or indirectly responsible for cyber activities enabling a significant threat to U.S. national security, foreign policy, or economic health or financial stability and involving the significant misappropriation or theft of money, trade secrets, personal identifiers, or economic information for illicit advantage or financial gain. The Genesis Market methodology is to obtain unauthorized access to certain valuable information, to steal or copy that information and then to offer that data, including usernames and passwords, for sale.

Once a person is named an SDN, that designated person's property or interests in property in the United States or in the possession or control of U.S. persons are legally blocked (frozen) and must be reported to OFAC. Generally speaking, a U.S. person is prohibited from engaging in any transaction related to property or interests in property of a person on the SDN List without separate OFAC authorization. Moreover, any person who engages in certain transactions with an Entity List person without such OFAC authorization may then find itself liable to similar sanctions in the future.

Background of Genesis Market & Other Darknet Markets

According to OFAC, Genesis Market has both a clearnet (traditional internet) and a

Related People

- Lawrence Ward
- Beth Forsythe
- John Marti
- Nicole Engisch
- Alex Hontos

Related Capabilities

- Asia-Pacific
- Privacy & Social Media
- Europe
- Government Enforcement & Corporate Investigations
- International Arbitration & Litigation
- International Trade
- National Security Law

darknet presence and is one of world's largest marketplaces for illegally obtained credentials and other confidential information. It targets vulnerable individual and corporate computer systems to gain illicit access and then sells such access to cybercriminals for their further illegal purposes. The Genesis Market site collates such stolen data from victims (e.g., computer or mobile device identifiers, email addresses, usernames, passwords, and other credentials illegally obtained from malware-infected computer systems) and offers such data for sale to other criminals.

OFAC reported that, as of early 2023, close to half a million packets of such stolen data from hacked computer systems of victims are now freely available for purchase on Genesis Market. Each packet of data being offered for sale is comprised of stolen passwords and personal or business information related to various email, video streaming and social media accounts belonging to significant U.S. and non-U.S. companies. As one graphic illustration of the dangers presented by Genesis Market, OFAC cited a June 2021 breach of a U.S. company's computer system by hackers who then were able to steal that company's software engine and source code using a cookie purchased through Genesis Market. OFAC also asserts that cybercriminals and other malign actors use Genesis Market to attack and penetrate U.S. Government computer systems.

The Alarming Growth of Cybercrime

In 2022, the Federal Bureau of Investigation ("FBI") reported that it had gotten more than 800,000 cybercrime-related complaints involving some $10.3 billion in losses according to the FBI's Internet Crime Complaint Center ("ICCC") in its 2022 Internet Crime Report[4], up from only $6.9 billion in reported 2021 losses. Since 2017, the ICCC has received over three million complaints totaling some $28 billion in losses.

Furthermore, the Treasury Department's February 2002 National Money Laundering Risk Assessment[5] noted that darknet markets allow criminals to sell stolen personal or business data obtained by their unauthorized access to victim computers or computer networks. They then offer such stolen data to other criminals who can readily profit from its further misuse. Furthermore, the Treasury Department's Financial Crimes Enforcement Network ("FinCEN") has also cautioned[6] that criminals frequently use darknet markets to sell illegal or stolen goods and services and accept cryptocurrency payments to thwart detection by law enforcement.

OFAC's Latest Action in Context

This latest OFAC action should be viewed in the context of multiple U.S. Government actions to combat cybercrime and corporate crime across several agencies, including the following:

- On March 2, 2023, U.S. Deputy Attorney General Lisa Monaco announced significant resource commitments by the Department of Justice ("DOJ") to address the intersection of corporate crime and national security.[7] The surge in resources will include the recruitment of 25 new prosecutors in the DOJ's National Security Division

("NSD") as well as the hiring of the NSD's first-ever Chief Counsel for Corporate Enforcement. The NSD will also increase its capacity to prosecute corporate violations through new partnerships with the U.S. Attorneys' Offices and the DOJ'S Criminal Division. Similar to guidance issued on the Foreign Corrupt Practices Act ("FCPA") by the Securities and Exchange Commission ("SEC"), the NSD will now issue joint advisories with the Departments of Commerce and the Treasury to inform the private sector about national security-related compliance and enforcement trends. DAG Monaco also announced an investment in the Bank Integrity Unit housed in the Criminal Division's Money Laundering and Asset Recovery Section. Significantly, she emphasized that, although economic santions and export controls were once only of concern for select U.S. businesses, they "should now be at the top of every company's risk compliance chart," and she reiterated that "sanctions are the new FCPA."

- In April 2022,[8] OFAC had designated the Hydra Market, another darkmarket based in Russia, to its SDN List after German Federal Criminal Police officials had also moved against that entity and its servers in Germany and seized some $25 million in bitcoin. Significantly, OFAC's notice of that SDN designation included some 100 different alternative cryptocurrency addresses for Hydra Market to alert the public. According to media reports, as of 2021, Hydra Market alone had represented about 75% of the world's darkmarket transactions and had cleared some $1.7 billion in annual illicit revenue.
- Also in April 2022, OFAC added a cryptocurrency exchange based in Russia, Guarantex, to the SDN List for its related role in money laundering.[9] OFAC had previously applied[10] the SDN List sanction in November 2021 against two other cryptocurrency exchanges, based in Russia, SUEX and CHATEX, which were accused of heavy involvement in processing cryptocurrency payments of ransomware payments by victims of cybercrime who needed to restore the operations of their hacked and disabled computer systems.
- In July 2022, the DOJ announced[11] that it had seized and forfeited $500,000 in bitcoin payments that a North Korean state-sponsored cybercrime group had extorted from healthcare providers in Kansas and Colorado using the "Maui" ransomware to block those providers from accessing their critical patient care records.
- The Federal Communications Commission ("FCC") has warned consumers that criminals have also found ways to penetrate public charging stations for mobile phones or laptops at airports, hotels and other such areas to install malware and to steal sensitive business or personal information from such devices while they are being charged, a practice known as "juice jacking." Such stolen information can then be sold illicitly through darkmarkets.[12] The FBI's Denver field office has recently added its own urgent warning to consumers to avoid the use of public charging stations due to the same cyber risks to such personal electronics.[13]
- In October 2021, U.S. DAG Lisa Monaco had also announced[14] that the DOJ was launching its Civil Cyber-Fraud Initiative to apply the False Claims Act ("FCA") against fraud by government contractors and grant recipients who fail to protect information gathered or generated through the expenditure of federal funds. The FCA is the government's main civil tool to deal with false claims to obtain federal funds and property in government programs and operations, and that statute includes a unique provision allowing private parties to assist the DOJ to identify and address such fraudulent conduct and then to share in any eventual government recovery.During 2022, DOJ reported that, under that initiative it had already obtained some $10 million in FCA settlements with government contractors who had failed to protect their data systems containing government-related data against cybercrime and cyberthreats after giving inaccurate assurances to federal funding agencies that such security measures were in effect.

OFAC Sanctions Guidance Available

OFAC also recently updated its entire website to make public access to its resources and information more intuitive and convenient. Among those official resources for sanctions compliance purposes are:

Frequently Asked Questions (FAQs) about Sanctions – a lengthy and searchable compilation of FAQs across all of the various OFAC sanctions regimes

Civil Penalties and Enforcement Information – an explanation of OFAC's enforcement powers and policies, including guidelines for voluntary self-disclosures

Report Blocked and Rejected Transactions to OFAC – OFAC instructions and forms on reporting of any blocked property or rejected transactions involving blocked property

Sanctions Compliance Guidance for the Virtual Currency Industry – OFAC advice on cryptocurrency transactions and sanctions compliance

Updated Advisory on Potential Sanctions Risk for Facilitating Ransomware Payments – OFAC guidance on the mitigating factors specific to an OFAC enforcement action with regard to ransomware payments that pose a potential sanctions risk

# # #

If you have any questions regarding this eUpdate, please contact the attorneys profiled below. Dorsey's attorneys have had substantial experience counseling clients to address cybercrime and comply with U.S. economic sanctions and other federal laws applicable to government contracts and grants.

[1] https://home.treasury.gov/news/press-releases/jy1388

[2] 80 Fed. Reg. 18077 (April 2, 2015).

[3] 82 Fed. Reg. 1 (Jan. 3, 2017).

[4] https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics#:~:text=IC.

[5] https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf

[6] https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf

[7] https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-monaco-delivers-

remarks-american-bar-association-national

[8] https://home.treasury.gov/news/press-releases/jy0701

[9] *Id*.

[10] https://home.treasury.gov/news/press-releases/jy0471

[11] https://www.justice.gov/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware-actors

[12] https://www.fcc.gov/juice-jacking-dangers-public-usb-charging-stations

[13] https://thehill.com/policy/technology/3942399-dont-use-public-phone-charging-stations-fbi/

[14] https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative