FinCEN Issues Historic Order Against Virtual Currency Exchange Facilitating Russian Illicit Finance

By **William Brannan**, **Diana Ingallinera Faillace**, **Jimmy Kang**, and **Samantha Sigelakis-Minski**

On January 18th, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued its first action (the Order) pursuant to Section 9714 of the Combating Russian Money Laundering Act[1] to designate Bitzlato Limited (Bitzlato), a convertible virtual currency (CVC) exchanger and peer-to-peer service provider incorporated in Hong Kong, as a "primary money laundering concern" in connection with Russian illicit finance.

FinCEN determined that Bitzlato played a critical role in laundering CVC by facilitating illicit transactions for ransomware actors operating in Russia. Moreover, Bitzlato did not take meaningful steps to stop abuse of its services, including failing to implement an effective anti-money laundering (AML) compliance program. As a result, covered financial institutions[2] are prohibited from engaging in certain transactions with Bitzlato.

In the Order, FinCEN found Bitzlato to have significant connections to Russian illicit finance and facilitated illicit transactions, which Bitzlato made little effort to prevent. FinCEN documented numerous transactions between known Russia-based ransomware groups and Bitzlato. Between 2019 and 2021, Bitzlato received CVC worth almost half a billion dollars from illicit activity, while two-thirds of Bitzlato's top receiving and sending counterparties were associated with darknet markets or scams. These counterparties included Binance and Hydra, a known Russia-connected darknet market.

Bitzlato also took no meaningful steps to disrupt its users' abuse of Bitzlato's service. Under the Bank

Secrecy Act of 1970 and its amendments, AML compliance programs of financial institutions must be designed to detect and prevent money laundering and any activity that facilitates money laundering or the funding of terrorist activities. Included in these AML compliance programs is the collection and verification of customer information to that end, collectively called "Know Your Customer" (KYC). While Bitzlato publicly purports to maintain an AML/KYC policy and processes to perform KYC, Bitzlato actively advertised its lack of AML compliance controls on its website. Bitzlato, in fact, only requires an email address to open an account and does not require or collect the typical suite of information expected that would facilitate a meaningful KYC analysis.

Given the extent to which Bitzlato is used for Russian illicit finance and the lack of AML compliance controls to combat money laundering, FinCEN determined it appropriate to issue the Order to help insulate the U.S. financial system from international money laundering and other financial crimes. As a result, covered financial institutions are prohibited from transmitting funds from or to Bitzlato or from or to any account or CVC address administered by Bitzlato, except as otherwise set forth in the Order.[3]

Concurrently with the Order, the Department of Justice announced that the founder and majority shareholder of Bitzlato was arrested and charged with conducting an unlicensed money-transmitting business.[4]

In addition to being the first Section 9714 action, the Order reflects the first time FinCEN has identified

---

[1] As amended by section 6106(b) of the National Defense Authorization Act for Fiscal year 2022. Section 9714 actions are intended to address, and can only be invoked for, primary money laundering concerns in connection with Russian illicit finance. For more information, please review FinCEN's FAQs issued with the Order found here.
[2] As defined in 31 C.F.R. §1010.100(t).
[3] See https://www.fincen.gov/sites/default/files/shared/FAQs_Bitzlato FINAL 508.pdf
[4] https://www.justice.gov/usao-edny/pr/founder-and-majority-owner-bitzlato-cryptocurrency-exchange-charged-unlicensed-money

a CVC exchanger as a primary money laundering concern. The Order highlights how FinCEN can use its authority under Section 9714(a) to impose either (i) one or more of the special measures as described in 31 U.S.C. § 5318A(b), commonly known as Section 311 special measures,[5] or (ii) special measures prohibiting or imposing conditions upon transmittal of funds by any covered financial institution. The Order sends a clear message that FinCEN can and will take action against any financial institution, including virtual asset service providers, that facilitate money laundering, terrorist financing, or other financial crimes.

We encourage our clients, particularly those engaged in virtual currency exchange activities or those with exposure to virtual currency partners or vendors, to review FinCEN's Order and assess its impact on your risk profile. Please contact one of the listed authors of this Client Alert or your regular Lowenstein Sandler contact if you require assistance with reviewing or assessing how FinCEN's Order impacts your operations.

---

[5] See Section 311 of the USA PATRIOT Act.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

WILLIAM BRANNAN
Partner
Vice Chair, Lowenstein Crypto
T: 646.414.6977
wbrannan@lowenstein.com

DIANA INGALLINERA FAILLACE
Senior Counsel
T: 646.414.6953
dfaillace@lowenstein.com

JIMMY KANG
Associate
T: 646.414.6916
jkang@lowenstein.com

SAMANTHA SIGELAKIS-MINSKI
Associate
T: 646.414.6934
ssigelakisminski@lowenstein.com

NEW YORK   PALO ALTO   NEW JERSEY   UTAH   WASHINGTON, D.C.