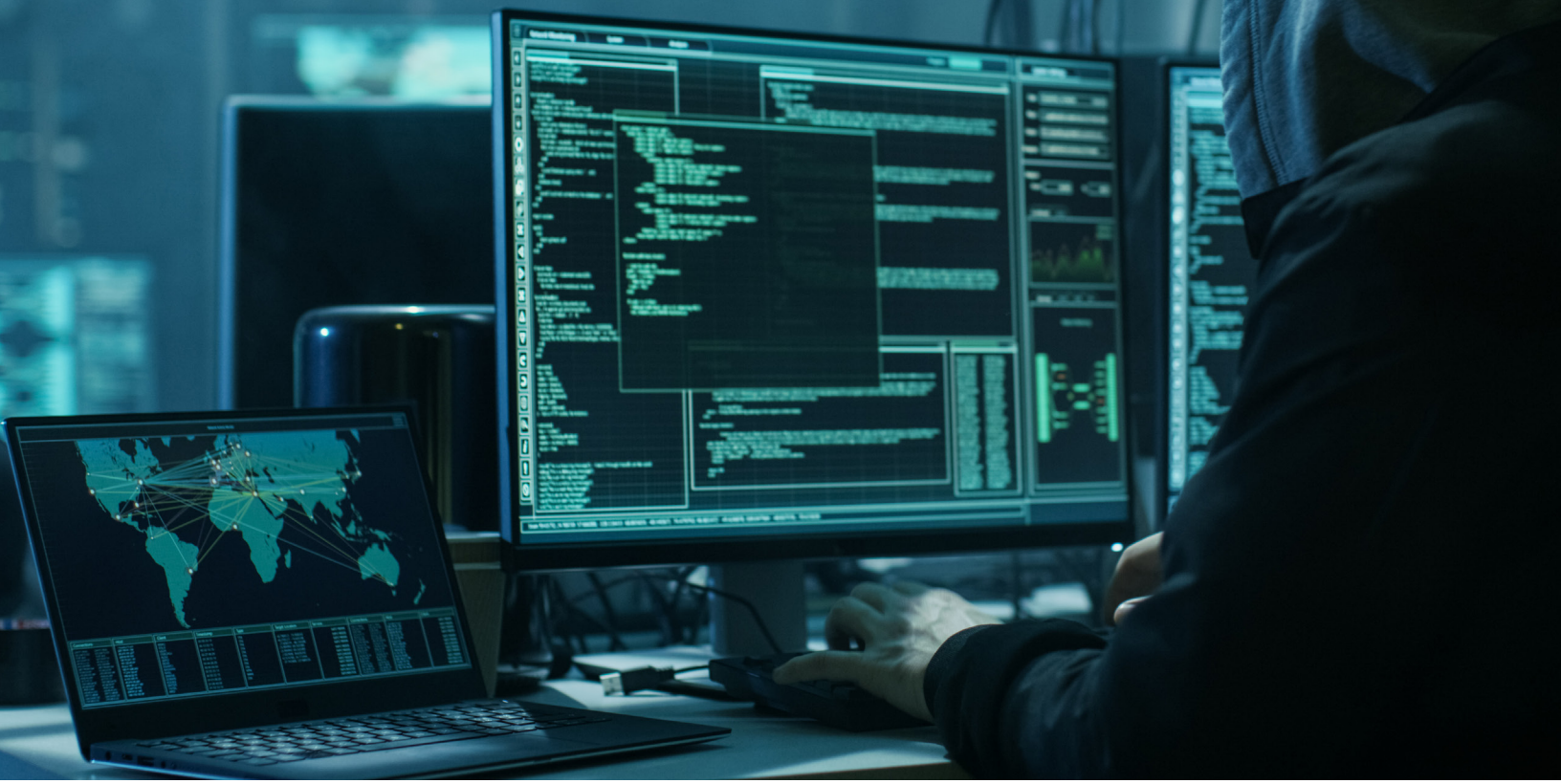
CRDFGLOBAL

Building Your Compliance Toolbox:

Latest Updates for Financial Institutions & Their Role in Countering WMD Proliferation Financing

Gabrielle Green and Brian Boone



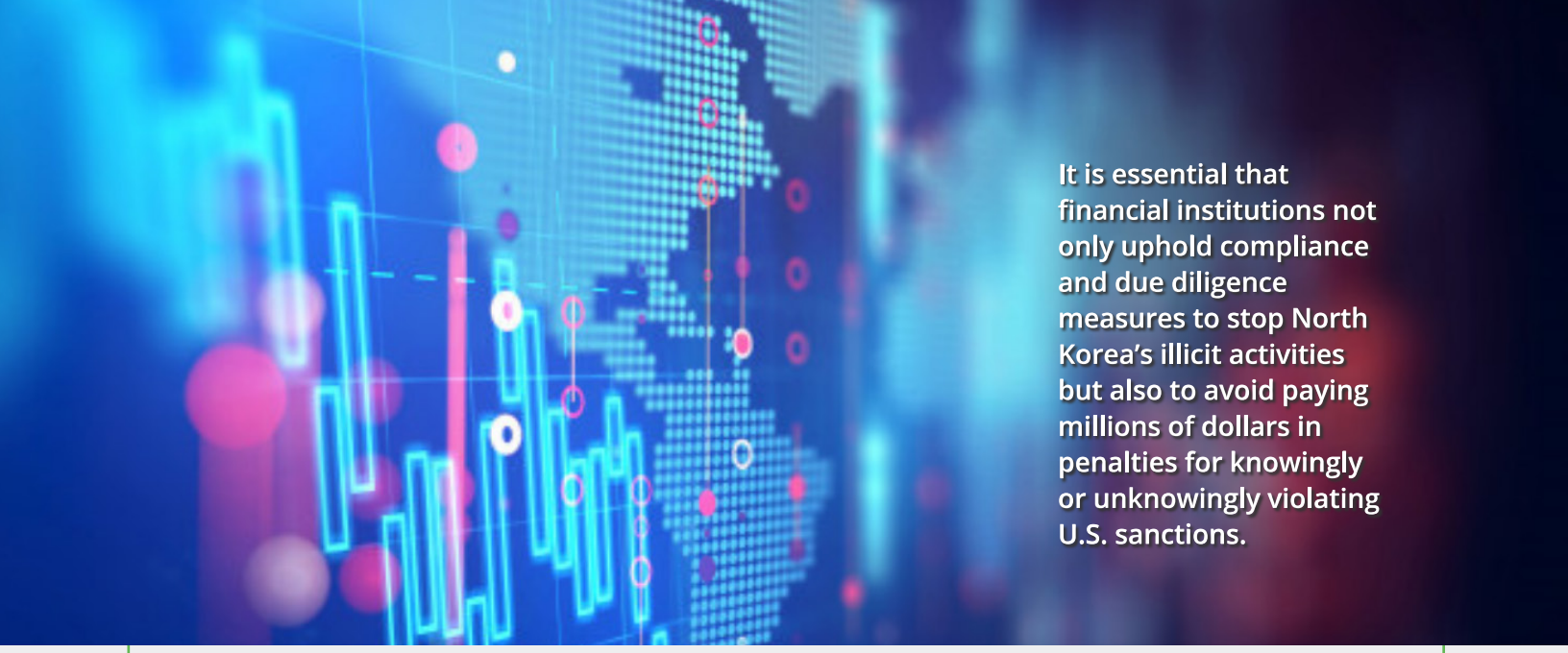
$1.3 billion—That is how much three North Korean hackers stole in money and cryptocurrency from financial institutions and companies since as early as September 2009, according to a recently unsealed U.S. Department of Justice federal indictment.[1]

With North Korean cyberattacks becoming "increasingly sophisticated," financial institutions need to incorporate the latest sanctions enforcement guidance...

Since North Korea's gross domestic product (GDP) was estimated to be only $18-28 billion[2] with defense spending accounting for 21.9%–24.4%[3] of its GDP, the billion dollar virtual heist is a significant contribution to North Korea's financial activities, especially in combination with a 2019 confidential U.N. report detailing that North Korea had stolen an estimated $2 billion for its weapons of mass destruction (WMD) program through targeting banks and cryptocurrency exchanges.[4] With North Korea continuing to threaten and exploit financial institutions and cryptocurrency exchanges with cyberattacks, the question remains of how financial institutions can strengthen their compliance programs and stay up-to-date with the latest due diligence information.

As virtual financial threats from North Korea accelerate, the U.S. Office of Foreign Assets Control of the Treasury Department (OFAC), the U.S. Financial Crimes Enforcement Network (FinCEN), and the intergovernmental Financial Action Task Force (FATF) provide regular updates on individuals and entities linked to North Korea as well as further guidance on the necessary compliance and due diligence measures financial institutions should uphold. With North Korean cyberattacks becoming "increasingly sophisticated,"[5] financial institutions need to incorporate the latest sanctions enforcement guidance from OFAC, FinCEN, FATF and online tools into their compliance programs to ensure their virtual environment and cryptocurrencies are protected and avoid significant civil penalties.

*Footnotes are hyperlinks unless noted.



It is essential that financial institutions not only uphold compliance and due diligence measures to stop North Korea's illicit activities but also to avoid paying millions of dollars in penalties for knowingly or unknowingly violating U.S. sanctions.

Case Study in Civil Penalties: BitPay

Financial institutions must protect themselves. One illustrative example is the February 2021 OFAC settlement against BitPay,[6] a cryptocurrency payment processing service that paid $507,375 to settle its potential civil liability for knowingly facilitating 2,102 transactions in 2013-2018 with individuals in sanctioned jurisdictions such as North Korea, Iran, and Syria.[7] While BitPay had Know Your Customer (KYC) measures such as screening in place, it did not fully analyze or assess the information it received on user identification, location, or IP addresses, allowing individuals in known sanctioned locations to continue using the company's services to conduct transactions in virtual currencies. These violations could have resulted in a maximum civil monetary penalty of over $600 million. The case underscores the business risk associated with failing to use IP address and other location data to screen customers as a compliance measure.[8] It is essential financial institutions not only uphold compliance and due diligence measures to stop North Korea's illicit activities but also to avoid paying millions of dollars in penalties for knowingly or unknowingly violating U.S. sanctions.

There are numerous publicly available resources from OFAC, FinCEN, and FATF for financial institutions to better understand their obligations under international sanctions and to meet robust due diligence requirements.

OFAC: The Latest Lists of Sanctioned Entities and Typologies of Sanctions Evasion

The U.S. Office of Foreign Assets Control of the Treasury Department (OFAC) administers and enforces U.S. economic and trade sanctions. OFAC publishes lists of sanctioned individuals and companies linked to targeted countries as well as lists of individuals, groups, and entities linked to terrorists, those involved with activities related to WMD proliferation, and other threats to U.S. national security, foreign policy, or the economy.[9] In addition to sanctions lists, OFAC regularly provides updates or additions to sanctions lists, including identifiable personal information and associated bank account or cryptocurrency addresses.[10]

In September 2020, OFAC added two Russian individuals, Daniel Potekhin and Dmitrii Karasavidi, to its Specially Designated Nationals (SDN) list in an update, providing the digital addresses linked to cryptocurrencies such as Ether (ETH; cryptocurrency associated with the Ethereum blockchain) and

Bitcoin (XBT; also abbreviated as BTC).[11] According to OFAC, the individuals were a part of a $16.8 million phishing campaign in 2017 and 2018 that targeted customers, individuals, and businesses of three virtual asset service providers.[12] The sanctioned individuals used two primary tactics to access and obfuscate their monetary gain: 'spoofing,' or the use of fake websites of legitimate companies to gain access to login credentials by unsuspecting customers; and laundering the cryptocurrency through multiple account and multiple virtual currency blockchains (e.g., exchanging currency types frequently).[13] While not linked to North Korea, this update offers an example of guidance financial institutions should be aware of as well as similar tactics that are used by North Korean cyberattackers. In addition to adding cryptocurrency addresses to its SDN List, OFAC recently added "privacy coins" (e.g., Zcash, Dash), which are cryptocurrencies built on a private blockchain (versus using a public blockchain like Bitcoin) to increase anonymity.[14]

Specially Designated Nationals List Update

The following individual has been added to OFAC's SDN List:

KARASAVIDI, Dmitrii (Cyrillic: КАРАСАВИДИ, Дмитрий) (a.k.a. KARASAVIDI, Dmitriy), Moscow, Russia; DOB 09 Jul 1985; Email Address 2000@911.af; alt. Email Address dm.karasavi@yandex.ru; Gender Male; Digital Currency Address - XBT

1Q6saNmqKkyFB9mFR68Ck8F7Dp7dTopF2W; alt. Digital Currency Address - XBT 1DDA93oZPn7wte2eR1ABwcFoxUFxkKMwCf; Digital Currency Address - ETH 0xd882cfc20f52f2599d84b8e8d58c7fb62cfe344b; Digital Currency Address - XMR 5be5543ff73456ab9f2d207887e2af87322c651ea1a873c5b25b7ffae456c320; Digital Currency Address - LTC LNwgtMxcKUQ51dw7bQL1yPQjBVZh6QEqsd; Digital Currency Address - ZEC t1g7wowvQ8gn2v8jrU1biyJ26sieNqNsBJy; Digital Currency Address - DASH XnPFsRWTaSgiVauosEwQ6dEitGYXgwznz2; Digital Currency Address - BTG GPwg61XoHqQPNmAucFACuQ5H9sGCDv9TpS; Digital Currency Address - ETC 0xd882cfc20f52f2599d84b8e8d58c7fb62cfe344b; Passport 75 5276391 (Russia) expires 29 Jun 2027 (individual) [CYBER2].

SDN List Identifiers

1. General Identifier for digital currency addresses
2. Type of digital currency (e.g., Ethereum)
3. Unique digital currency address associated with the sanctioned individual or entity
4. SDN program tags; [CYBER2] is pursuant to Executive Order 13694 and Executive Order 13757

Such [cryptocurrency] activities contributed to an estimated $571 million stolen in cryptocurrency by North Korea as of 2019.

In March 2020, OFAC sanctioned two Chinese nationals, Tian Yinyin (田寅寅) and Li Jiadong (李家东), who were engaged in laundering stolen cryptocurrency from a 2018 cyberattack on a cryptocurrency exchange. These individuals were linked to the Lazarus Group, which has been designated by the U.S. as a North Korean state-sponsored malicious cyber group. The cyberattack occurred when an employee of the exchange unknowingly downloaded North Korean-linked malware via email and exposed exposed customers' access keys. The stolen cryptocurrency was then laundered through additional bank and cryptocurrency accounts. Such activities contributed to an estimated $571 million stolen in cryptocurrency by North Korea as of 2019.[15]

To protect themselves—and to comply with OFAC sanctions and FinCEN regulations—financial institutions, including cryptocurrency exchanges, should take at a minimum the following steps:

a. Register the business with FinCEN as a money services business,

b. develop a risk-based compliance and anti-money laundering (AML) program, including conducting KYC and other due diligence prior to providing service,

c. create protocols for recordkeeping and reporting (e.g., filing Suspicious Activity Reports (SARs)),

d. conduct routine compliance examinations to identify vulnerabilities and to ensure compliance,

e. ensure one is not conducting business with individuals or entities on OFAC's sanctions lists, transfers to sanctioned jurisdictions, or transfers to prohibited digital currency addresses, and

f. communicate such compliance expectations to the customer as related to one's transactions and activities.[16]

OFAC's Toolbox

- ✓ Specially Designated Nationals and Blocked Persons List (SDN)
- ✓ Search OFAC's Sanctions Lists
- ✓ OFAC'S Recent Actions: Sanctions Designations & Removals
- ✓ Frequently Asked Questions on Virtual Currencies

FinCEN: Advisories and Best Practices to Safeguard the Financial System

FinCEN is the U.S. Financial Intelligence Unit safeguarding the financial system from illicit use by regularly publishing advisories to combat money laundering, terrorism financing, and proliferation of WMD. On March 11, 2021, FinCEN issued its latest advisory highlighting FATF's updated list of jurisdictions with "strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing." Importantly, the notice reaffirms its February 2020 notice that both Iran and North Korea remain "High-Risk Jurisdictions Subject to Call for Action."[17] For financial institutions, this means "enhanced scrutiny," as defined by special attention to the DPRK and its linked entities or individuals and the application of effective counter-measures, is required to protect their financial sectors from such risks.

The purpose of the [proposed] rule would be to strengthen anti-money laundering efforts and close regulatory gaps within virtual currency and digital asset transactions.

On the cryptocurrency side, FinCEN extended the comment period in late January 2021 for a proposed rule which would require financial institutions to report and verify the identity of customers conducting transactions over a certain threshold involving virtual wallets.[18] The purpose of the rule would be to strengthen anti-money laundering efforts and close regulatory gaps within virtual currency and digital asset transactions. FinCEN has not released further updates on the status of the rule beyond stating it will review additional information submitted in the extended comment period. *Note, the content of the comments on the rule is not publicly available.* [19]

A FinCEN study of the anti-money laundering act that began in 2019 and consulted with 65 domestic and foreign firms has released its report: "Emerging Themes and Future Role of AML Act Implementation (March 2021). Key themes highlighted by the report include:

1. Financial institutions may not be aware of the existing solutions available to strengthen gaps in AML/CFT compliance, especially related to virtual currencies.
2. Reluctance to innovate among financial institutions is primarily due to concern with reactions from federal/state examiners or internal/ auditors, not due to Bank Secrecy Act (BSA)[20] requirements.
3. Industry solutions exist to address increasing account hacking via email, ransomware attacks, and cybertheft, especially in relation to crimes using virtual currencies.

FinCEN's Toolbox

- ✓ Money Services Business (MSB) Registration
- ✓ Recent Advisories and Notices
- ✓ Report on "Emerging Themes and Future Role in AML Act Implementation" (March 2021)

[18] The rule would apply to transactions involving convertible virtual currency (CVC) or digital assets with legal tender status (LTDA) not hosted by a financial institution or CVC/LTDA wallets hosted by a financial institution within jurisdictions identified by FinCEN.

FATF: Watchdog for the Global Financial System

The Financial Action Task Force (FATF) is an intergovernmental body providing anti-money laundering guidance to countries around the world. FATF does not enact law and regulations or impose penalties and fines. Instead, FATF creates and monitors, through its FATF 40 Recommendations, the international standard for combating money laundering. FATF Recommendations now require that Virtual Asset Service Providers be regulated, licensed, registered, and subjected to effective systems for monitoring and supervision to meet its standard.

FATF urged its members to apply effective countermeasures, and targeted financial sanctions in accordance with applicable United Nations Security Council Resolutions,...

In September 2020, FATF issued a report on Virtual Assets Red Flag Indicators of money laundering and terrorist financing. The report highlights how terrorists and other criminal users operate as unregistered/unlicensed virtual asset service providers on peer-to-peer (P2P) exchange websites and the anonymous peer to peer transactions enables criminals to avoid detection.

Another indicator comes from transaction size and frequency. North Korean sanction evaders often structure virtual assets in small amounts or quantities under record-keeping or reporting thresholds. These reporting thresholds follow the same typologies as structuring cash transactions, and the red flag is indicated by the transaction patterns. Transactions with new users conducting a large initial deposit to open a new relationship with a Virtual Asset Service Providers and funding the entire deposit the first day it is opened is an immediate red flag. These irregularities can be identified by following FATF's recommended prescreening procedures.

On February 21, 2021, FATF, issued a call for action against two high risks jurisdictions—North Korea and Iran—with significant strategic deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation. FATF urged its members to apply effective countermeasures, and targeted financial sanctions in accordance with applicable United Nations Security Council Resolutions, to protect their financial sectors from money laundering, financing of terrorism, and WMD proliferation financing risks emanating from the North Korea. The lack of transparency or

FATF's Toolbox

- ✓ FATF Draft Guidance on a Risk-Based Approach to Virtual Assets and Virtual Assets Service
- ✓ Virtual Assets Red Flag Indicators Report
- ✓ Mutual Evaluation Reports: Analysis of Countries' Financial Systems

On top of OFAC, FinCEN, and FATF compliance requirements and updates, financial institutions must also review guidance and regulations from organizations such as the Office of the U.S. Comptroller of Currency, U.S. Securities and Exchange Commission, U.S. Department of Justice, U.S. Commodity Futures Trading Commission, and U.S. Internal Revenue Service. The burden of responsibility laid on financial institutions, not only to prevent illicit use, but also to avoid paying millions in penalties is severe. Yet, it is also necessary. When state actors exploit seams in the global financial system to violate international law and pursue destabilizing WMD, there is no choice other than demanding enhanced diligence and scrutiny of the entire system for as long as the threat continues.

CRDFGLOBAL

Established in 1995, CRDF Global is an independent nonprofit organization that promotes safety, security, and sustainability through international development and foreign assistance missions across the globe.

1776 Wilson Blvd., Suite 300
Arlington, VA 22209 USA

Phone: 703-526-9720
Email: Info@CRDFGlobal.org

Linkedin.com/company/CRDF-Global
Facebook.com/CRDFGlobal
Twitter.com/CRDFGlobal
Instagram.com/CRDFGlobal

CRDFGLOBAL.ORG