Data Privacy and Cybersecurity

United States Department of Justice Announces National Cryptocurrency Enforcement Team and Civil Cyber-Fraud Initiative

By: David Bitkower, Shoba Pillay, Aaron R. Cooper, and Ashwini Bharatkumar

Ransomware attacks have become increasingly common and, according to the NSA Director, are projected to continue growing in prevalence.[1] Amidst the rise in ransomware attacks, last week the United States Department of Justice (DOJ) announced two cybersecurity-related enforcement initiatives: the National Cryptocurrency Enforcement Team and the Civil Cyber-Fraud Initiative. The initiatives aim to bolster the DOJ's capabilities to investigate and prosecute cybercrimes such as ransomware attacks and to enforce cybersecurity requirements aimed at mitigating the risk of such attacks.

National Cryptocurrency Enforcement Team

The National Cryptocurrency Enforcement Team (NCET) will investigate and prosecute criminal use of cryptocurrency. The team will focus on criminal activity *by* cryptocurrency platform providers and money laundering infrastructure providers, as well as crimes *using* cryptocurrency platforms — such as ransomware demands and dark web market exchanges of illegal drugs, weapons, and hacking tools. Prosecutors from the DOJ's Money Laundering and Asset Recovery Section (MLARS) and Computer Crime and Intellectual Property Section (CCIPS), and Assistant US Attorneys (AUSAs) on detail from US Attorneys' Offices throughout the country will comprise the initial NCET. The head of the NCET will report to the Assistant Attorney General of the Criminal Division.

The NCET will also seek to track and recover ransomware payments and assets otherwise lost to fraud and extortion. The DOJ has recognized cryptocurrency as the primary means by which ransomware payments are collected.[2] In October 2020, the DOJ released a Cryptocurrency Enforcement Framework that will be used and augmented by the NCET.[3] In June 2021, the DOJ announced a Ransomware and Digital Extortion Task Force to coordinate and focus its ransomware investigation and prosecutorial capabilities, and to identify and mitigate the root causes of ransomware attacks. The NCET initiative is yet another component of the DOJ's efforts to combat ransomware, digital extortion, and other criminal activity that may be facilitated by cryptocurrency platforms. These initiatives are further supplemented by the Department of the Treasury's Office of Foreign Assets Control (OFAC) September 21, 2021 updated ransomware advisory. The advisory highlights the sanctions risks companies may face for making or facilitating ransomware payments related to malicious cyber-enabled activities. For more information, see Jenner & Block's recent article on the OFAC Ransomware Guidance.

In addition to carrying out investigative and prosecutorial tasks, the NCET will also seek to cultivate relationships with federal, state, local, and international law enforcement agencies that investigate and prosecute cryptocurrency cases; will provide training and advice to federal prosecutors and law enforcement agencies on matters such as search and seizure, restraining orders, forfeiture allegations, and indictments, as they pertain to cryptocurrency crimes; facilitate information- and evidence-sharing between law enforcement offices; and consider ways in which to collaborate with private sector actors that have cryptocurrency expertise.

Civil Cyber-Fraud Initiative

The Civil Cyber-Fraud Initiative, announced the same day as the NCET, will attempt to use the civil False Claims Act to penalize government contractors for failure to comply with cybersecurity mandates. The initiative seeks to enhance accountability for "knowingly providing deficient cybersecurity products or services, knowingly misrepresenting. . . cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches."[4] For more information, see Jenner and Block's recent client alert on the Civil Cyber-Fraud Initiative.

Multiple ongoing policy efforts, within both the executive and legislative branches, seek to define cybersecurity reporting requirements for government contractors. The May 12, 2021 Executive Order on Improving the Nation's Cybersecurity (see Jenner & Block's client alert on the Executive Order) initiated the development of cybersecurity monitoring and incident reporting requirements for all providers of information technology and operational technology services to the federal government. The Executive Order established a requirement for information and communication technology service providers that have contracted with federal agencies to promptly report cyber incidents to those agencies and to the Cybersecurity and Infrastructure Security Agency (CISA).[5] The Executive Order also directed updates to contract requirements and language in the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) to facilitate cybersecurity information collection and reporting.[6]

In July, the Cyber Incident Notification Act of 2021 was introduced in the United States Senate (see Jenner & Block's client alert on the proposed legislation). The bill proposes cyber intrusion reporting requirements applicable to federal contractors, owners or operators of critical infrastructure, nongovernmental entities providing cybersecurity incident response services, and potentially additional covered entities defined by CISA. The Civil Cyber-Fraud Initiative seeks to equip the DOJ with capabilities to enforce these cybersecurity reporting requirements.

Jenner & Block will continue to monitor the development of the National Cryptocurrency Enforcement Team and Civil Cyber-Fraud Initiative.

Contact Us

David Bitkower

dbitkower@jenner.com | Download V-Card

Shoba Pillay

spillay@jenner.com | Download V-Card

Aaron R. Cooper

acooper@jenner.com | Download V-Card

Ashwini Bharatkumar

abharatkumar@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

David Bitkower
Co-Chair
dbitkower@jenner.com
Download V-Card

Madeleine V. Findley
Co-Chair
mfindley@jenner.com
Download V-Card

[1] *See, e.g.*, Maggie Miller, *NSA director expects to be facing ransomware attacks 'every single day' in five years*, The Hill (Oct. 5, 2021), https://thehill.com/policy/cybersecurity/575386-nsa-director-expects-to-be-facing-ransomware-attacks-every-single-day-in (noting the NSA Director's prediction that ransomware attacks will not diminish in frequency in the next five years, while noting the view of the Deputy National Security Advisor for Cyber and Emerging Technology that the US will face fewer ransomware attacks in five years).
[2] *See, e.g.*, Press Release, Department of Justice, *Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team* (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team.
[3] DOJ Office of the Deputy Attorney General, Cyber-Digital Task Force, *Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework* 6 (Oct. 8, 2020), https://www.justice.gov/archives/ag/page/file/1326061/download.
[4] Press Release, Department of Justice, *Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative* (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.
[5] White House, Executive Order on Improving the Nation's Cybersecurity, § 2(f) (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.
[6] Executive Order on Improving the Nation's Cybersecurity, § 2.