FinCEN ADVISORY

FIN-2020-A005 July 30, 2020

Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic

Detecting, preventing, and reporting illicit transactions and cyber activity will help protect legitimate relief efforts for the COVID-19 pandemic and help protect financial institutions and their customers against malicious cybercriminals and nation-state actors.

This Advisory should be shared with:

- *Chief Executive Officers*
- *Chief Operating Officers*
- *Chief Compliance Officers*
- *Chief Risk Officers*
- *AML/BSA Departments*
- *Legal Departments*
- *Cyber and Security Departments*
- *Customer Service Agents*
- *Bank Tellers*

SAR Filing Request:

FinCEN requests financial institutions reference this advisory in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: "**COVID19-CYBER FIN-2020-A005**" and select SAR field 42 (Cyber Event). Additional guidance on filing SARs appears near the end of this advisory.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to potential indicators of cybercrime and cyber-enabled crime observed during the COVID-19 pandemic. Many illicit actors are engaged in fraudulent schemes that exploit vulnerabilities created by the pandemic. This advisory contains descriptions of COVID-19-related malicious cyber activity and scams, associated financial red flag indicators, and information on reporting suspicious activity.

This advisory is intended to aid financial institutions in detecting, preventing, and reporting potential COVID-19-related criminal activity. This advisory is based on FinCEN's analysis of COVID-19-related information obtained from Bank Secrecy Act (BSA) data, open source reporting, and law enforcement partners. FinCEN will continue issuing COVID-19-related information to financial institutions to help enhance their efforts to detect, prevent, and report suspected illicit activity on its website at https://www.fincen.gov/coronavirus, which also contains information on how to register to receive FinCEN Updates.

Financial Red Flag Indicators of Cybercrime and Cyber-Enabled Crime Exploiting COVID-19

This advisory addresses the primary means by which cybercriminals and malicious state actors are increasingly exploiting the COVID-19 pandemic in cyber-enabled crime through malware and phishing schemes, extortion, business email compromise (BEC) fraud, and exploitation of remote applications, especially against financial and healthcare systems.[1]

FinCEN has identified the following red flag indicators of COVID-19 cyber-enabled crimes[2] to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with the COVID-19 pandemic. As no single financial red flag indicator is necessarily indicative of illicit or suspicious activity, financial institutions should consider additional contextual information and the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple indicators, before determining if a transaction is suspicious or otherwise indicative of potential fraudulent COVID-19-related activities. In line with their risk-based approach to compliance with the BSA, financial institutions are also encouraged to perform additional inquiries and investigations where appropriate. Additionally, some of the financial red flag indicators outlined below may apply to multiple COVID-19-related fraudulent activities. Given that many scammers may be directly targeting customers, financial institutions should remain on the alert for potential suspicious activities involving their customers.

Targeting and Exploitation of Remote Platforms and Processes

The significant migration toward remote access in the pandemic environment presents opportunities for criminals to exploit financial institutions' remote systems and customer-facing processes. Cybercriminals and malicious state actors are targeting vulnerabilities in remote

1. *See* Department of Justice (DOJ) Press Release, "Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams," (April 22, 2020); the United Kingdom (U.K.) National Cyber Security Centre (NCSC) Press Release, "Public Urged to Flag Coronavirus Related Email Scams as Online Security Campaign Launches," (April 21, 2020); Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Notification, "Defending Against COVID-19 Cyber Scams," (March 6, 2020); Europol Report, "Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis," (March 27, 2020); DHS CISA and Federal Bureau of Investigation (FBI) Public Service Announcement, "People's Republic of China (PRC) Targeting of COVID-19 Research Organizations," (May 13, 2020); FBI's Internet Crime Complaint Center (IC3) Public Service Announcement, "Increased Use of Mobile Banking Apps Could Lead to Exploitation," (June 10, 2020); and DHS CISA, National Security Agency, NCSC, and Canada Communications Security Establishment Joint Advisory, "APT29 Targets COVID-19 Vaccine Development," (July 16, 2020).
2. For the purpose of this advisory, cyber-enabled crime refers to illegal activities (e.g., fraud, identity theft, etc.) carried out or facilitated by electronic systems and devices, such as networks and computers. *See* FinCEN Advisory, FIN-2016-A005, "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," (October 25, 2016).

applications and virtual environments to steal sensitive information, compromise financial activity, and disrupt business operations.[3] Remote identity processes[4] also face significant risks, which may include:

- *Digital Manipulation of Identity Documentation*: Criminals often seek to undermine online identity verification processes through the use of fraudulent identity documents, which can be created by manipulating digital images of legitimate government-issued identity documents to alter the information and/or photos displayed.[5]
- *Leveraging Compromised Credentials Across Accounts*: Cybercriminals commonly undermine weak authentication processes in attempted account takeovers via methods such as credential stuffing attacks. In these attacks, cybercriminals generally use lists of stolen account credentials (typically usernames or email addresses, and associated passwords) to conduct automated login attempts to gain unauthorized access to victim accounts.

Financial red flag indicators of this sort of activity may include:[6]

1. The spelling of names in account information does not match the government-issued identity documentation provided for online onboarding.
2. Pictures in identity documentation, especially areas around faces, are blurry or low resolution, or have aberrations. Pictures in identity documentation or other images of persons in remote identity verification[7] show visual signs indicating possible image manipulation (e.g., incongruences in coloration near the edge of the face, or double edges or lines on delineated facial features).
3. Images of identity documentation have visual irregularities that indicate digital manipulation of the images, especially around information fields likely to have been changed to conduct synthetic identity fraud (e.g., name, address, and other identifiers).

3. For information related to publicly disclosed cybersecurity vulnerabilities and exposures, *see* U.S. Department of Commerce, National Institute for Standards and Technology (NIST), "National Vulnerability Database;" MITRE, "Common Vulnerabilities and Exposures: CVE List Home;" and FBI IC3 Public Service Announcements, "Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments," (April 1, 2020) and "Increased Use of Mobile Banking Apps Could Lead to Exploitation," (June 10, 2020). *See also* FinCEN Director Kenneth A. Blanco's, prepared remarks delivered at the Consensus Blockchain Conference, "Consensus Blockchain Conference (Virtual)," (May 13, 2020).
4. For the purposes of this advisory, "remote identity processes" include remote processes for customer onboarding and identity verification, as well as authentication of customers for account access purposes. For more information on digital identity standards, *see* NIST, "Digital Identity Guidelines," (December 1, 2017), and the Financial Action Task Force (FATF), "Guidance on Digital Identity," (March 6, 2020).
5. Criminals exploiting identity verification processes will typically use either information associated with a real individual's identity (i.e., identity theft) or create a new fabricated identity that usually consists of a real identifier, such as a social security number or driver's license number, with other fake information (i.e., synthetic identity fraud). For more information on example typologies and financial red flag indicators involving identity theft and identity fraud, *see* FinCEN Report, "Identity Theft: Trends, Patterns, and Typologies Reported in Suspicious Activity Reports," (October 2010).
6. *Id*. *See also* Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation, 16 CFR Part 681, app. A.
7. Images in identity verification other than identity documentation may include pictures or video of the customer (e.g., "selfie" images) taken as part of the financial institution's onboarding process.

4. A customer's physical description on identity documentation does not match other images of the customer.

5. A customer refuses to provide supplemental identity documentation or delays producing supplemental documentation.

6. Customer logins occur from a single device or Internet Protocol (IP) address across multiple seemingly unrelated accounts, often within a short period of time.

7. The IP address associated with logins does not match the stated address in identity documentation.

8. Customer logins occur within a pattern of high network traffic with decreased login success rates and increased password reset rates.

9. A customer calls a financial institution to change account communication methods and authentication information, then quickly attempts to conduct transactions to an account that never previously received payments from the customer.

Phishing, Malware, and Extortion

FinCEN and U.S. law enforcement have observed significant increases in broad-based and targeted phishing campaigns that are attempting to lure companies, especially healthcare and pharmaceutical providers, with offers of COVID-19 information and supplies.[8] Phishing scams target individuals with communications appearing to come from legitimate sources to collect victims' personal and financial data and potentially infect their devices by convincing the target to download malicious programs.[9] Cybercriminals usually send these phishing communications by email but may also use phone calls or text messages.

In these new schemes, phishing scammers will often reference COVID-19 themes, such as payments related to the Coronavirus Aid, Relief, and Economic Security (CARES) Act,[10] in the subjects and bodies of emails. Some phishing emails lure victims by advertising ways to make money, such as through investing in convertible virtual currencies (CVCs) or via domain names that mimic names of organizations, including those that provide or enable teleworking capabilities.[11] Cybercriminals

8. The U.S. Secret Service (USSS) and DHS CISA have noted an increase in malware, phishing, and extortion campaigns related to COVID-19. *See* USSS Press Release, "Secret Service Issues COVID-19 (Coronavirus) Phishing Alert," (March 9, 2020).

9. *See* DHS CISA and U.K. NCSC Joint Alert (AA20-099A), "COVID-19 Exploited by Malicious Cyber Actors," (April 8, 2020); and DHS, "Common Scams: Know How to Spot a Fake."

10. Pub. L. 116–136, 116th Congress (2020).

11. Since January 2020, tens of thousands of new domains have been registered with terms related to COVID-19 and/or disaster and healthcare response efforts (e.g., "quarantine," "vaccine," and "CDC"), many including or mimicking names of companies that provide or enable teleworking capabilities. U.S. law enforcement agencies have disrupted hundreds of malicious domains used to exploit the pandemic. *See* FinCEN Advisory, FIN-2020-A003, "Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)," (July 7, 2020). *See also*, FBI Press Release, "FBI Expects a Rise in Scams Involving Cryptocurrency Related to the COVID-19 Pandemic," (April 13, 2020).

are also distributing malware,[12] including ransomware, through phishing emails, malicious websites and downloads, domain name system (DNS) hijacking or spoofing attacks, and fraudulent mobile applications. These techniques can be applied in broader campaigns involving social media, such as the recent exploit targeting Twitter and prominent users of the platform.[13] Financial institutions dealing in CVC should be especially alert to the potential use of their institutions to launder proceeds affiliated with cybercrime, illicit darknet marketplace activity, and other CVC-related schemes and take appropriate risk mitigating steps consistent with their BSA obligations.

FinCEN assesses that instances of extortion will also continue to grow in the wake of the COVID-19 pandemic. So far in 2020, FinCEN has received numerous suspicious activity reports (SARs) involving ransomware[14] targeting medical centers and municipalities. Much of this ransomware was delivered by exploiting the COVID-19 lures described above. We expect criminals to continue targeting entities that are vulnerable due to their involvement in pandemic response, such as researchers working on medical treatments or manufacturers of personal protective equipment. In other instances of extortion, criminals are threatening to expose victims and their families to COVID-19 if they do not pay the extortion fee. In almost all cases, criminals require ransomware-related extortion payments to be made in CVC.[15]

Financial red flag indicators of this sort of activity may include the following:

10 Information technology enterprise activity related to transaction processes or information is connected to cyber indicators that have been associated with possible illicit activity. Malicious cyber activity may be evident in system log files, network traffic, or file information.[16]

11 Email addresses purportedly related to COVID-19 do not match the name of the sender or the corresponding domain of the company allegedly sending the message.

12. Malware can enable criminals to access compromised computers and computer systems to steal credentials, exfiltrate sensitive information through mechanisms like screenshots or keylogging, alter account information, and conduct fraudulent transactions.

13. *See* FinCEN Alert, FIN-2020-Alert001, "FinCEN Alerts Financial Institutions to Convertible Virtual Currency Scam Involving Twitter," (July 16, 2020).

14. Ransomware, a specific type of malware, typically encrypts data on systems in the interest of extorting ransom payment from victims in exchange for decrypting the information and giving victims access to their systems again.

15. Financial institutions dealing in CVC should be especially alert to the laundering of proceeds affiliated with cybercrime, illicit darknet marketplace activity, and other CVC-related schemes. *See* FinCEN Advisory, FIN-2019-003, "Advisory on Illicit Activity Involving Convertible Virtual Currency," (May 9, 2019).

16. Because cyber indicators are helpful red flag indicators that financial institutions can use to identify related suspicious financial activity, FinCEN, DHS CISA, and the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) offer a broad range of helpful cyber indicator resources, including, but not limited to: FinCEN's Cyber Indicator Lists (CILs), shared through the FinCEN Secure Information Sharing System; OCCIP's CILs and circulars, available upon request; and DHS CISA's cyber analytic products and services, including a comprehensive list of COVID-19-related indicators of compromise in CSV or STIX-formatted XML formats, the Cyber Information Sharing and Collaboration Program (CISCP), and the Automated Indicator Sharing (AIS) program. Public-private and industry partnerships, such as the Financial Services Information Sharing and Analysis Center, and open source and commercial cyber threat feeds can also be useful resources.

12 Unsolicited emails related to COVID-19 from untrusted sources encourage readers to open embedded links/files or to provide personal or financial information, such as usernames and passwords or other account credentials.

13 Emails from untrusted sources or addresses similar to legitimate telework vendor accounts offer remote application software, often advertised at no or reduced cost.

14 Emails contain subject lines identified by government or industry as associated with phishing campaigns (e.g., "Coronavirus Updates," "2019-nCov: New confirmed cases in your City," and "2019-nCov: Coronavirus outbreak in your city (Emergency)").

15 Text messages have embedded links purporting to be from or associated with government relief programs and payments.

16 Embedded links or webpage addresses for purported COVID-19 resources have irregular uniform resource locators (URLs) that do not match that of the expected destination site or are similar to legitimate sites but with slight variations in the domain (e.g., variations in domain extensions like ".com," ".org," and ".us") or web address spelling.

Business Email Compromise (BEC) Schemes

Cybercriminals have increasingly exploited the COVID-19 pandemic by using BEC schemes, particularly targeting municipalities and the healthcare industry supply chain. A common BEC scheme involves criminals convincing companies to redirect payments to new accounts, while claiming the modification is due to pandemic-related changes in business operations. BEC criminals often use spoofed or compromised email accounts to communicate these urgent, last-minute payment changes. In the COVID-19 environment, criminals insert themselves into communications by impersonating a critical player in a business relationship or transaction, typically posing as providers of healthcare supplies, to intercept or fraudulently induce a payment for critically needed supplies.[17]

Financial red flag indicators of this sort of activity may include the following:[18]

17 A customer's transaction instructions contain different language, timing, and amounts in comparison to prior transaction instructions, especially regarding transactions involving healthcare providers or supplies purchases.

17. *See* FBI Press Release, "FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic," (April 6, 2020). *See also* Europol Press Release, "Corona Crimes: Suspect Behind €6 Million Face Masks and Hand Sanitisers Scam Arrested Thanks to International Police Cooperation," (April 6, 2020).

18. For general BEC-scheme financial red flag indicators, *see* FinCEN Advisories, FIN-2016-A003, "Advisory to Financial Institutions on E-mail Compromise Fraud Schemes," (September 6, 2016), and FIN-2019-A005, "Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes," (July 16, 2019).

18 Transaction instructions, typically involving a healthcare-sector counterparty or referencing purchase of healthcare or emergency response supplies, originate from an email account closely resembling, but not identical to, a known customer's email account.

19 Emailed transaction instructions direct payment to a different account for a known beneficiary. The transmitter may claim a need to change the destination account as part of a COVID-19 pandemic response, such as moving the account to a financial institution in a jurisdiction less affected by the disease, and assert urgency to conduct the transaction.

20 Emailed transaction instructions request to move payment methods from checks to ACH transfers as a response to the pandemic.

Information on Reporting Suspicious Activity

Suspicious Activity Report (SAR) Filing Instructions

SAR reporting, in conjunction with effective implementation of due diligence requirements by financial institutions, is crucial to identifying and stopping financial crimes, including those related to the COVID-19 pandemic. Financial institutions should provide all pertinent available information in the SAR and narrative. Adherence to the filing instructions below will improve FinCEN and law enforcement's ability to effectively identify and pull actionable SARs and information from the FinCEN Query system to support COVID-19-related cases.

- FinCEN requests that financial institutions reference this advisory by including the key term "**COVID19-CYBER FIN-2020-A005**" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory.
- Financial institutions that suspect fraudulent COVID-19-related activity should mark all appropriate check boxes on the SAR form to indicate a connection between COVID-19 and the suspicious activity being reported. For example, if the activity includes a COVID-19-related account takeover involving an ACH transfer, financial institutions can select SAR field 38a and 38z, and note in the "other" box, "COVID-19 account takeover fraud – ACH."[19]
- Financial institutions should also include any relevant technical cyber indicators related to cyber events and associated transactions reported in a SAR within the available structured cyber event indicator fields. For example, for a COVID-19-related cyber event against a financial institution, financial institutions can select SAR fields 42a and 42z (noting in the

19. For additional guidance on identifying account takeover activity and related SAR filing instructions, *see* FinCEN Advisory, FIN-2011-A016, "Account Takeover Activity," (December 19, 2011).

"other" box the COVID-19-related cyber event), and SAR fields 44(a)-(j), (z), including email or CVC wallet addresses, malicious domains or URLs, and any other known cyber event indicators.

- For cyber-enabled crime involving fraud driven by COVID-19, financial institutions should select SAR field 34z (Fraud – other) as the associated suspicious activity type. Additionally, financial institutions should include the type of cybercrime or scheme as a keyword (e.g., "COVID 19 BEC Fraud," "EAC fraud," or "BEC data theft") in SAR field 34(z).
- Please refer to FinCEN's May 18, 2020 Notice Related to the Coronavirus Disease 2019, which contains information regarding reporting COVID-19-related crime and FinCEN's Rapid Response Program, and reminds financial institutions of certain BSA obligations.

For Further Information

Financial institutions should send questions or comments regarding the contents of this advisory to the FinCEN Regulatory Support Section at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.