FinCEN FACT SHEET

FIN-2022-FCT1 **February 11, 2022**

Fact Sheet on the Rapid Response Program (RRP)

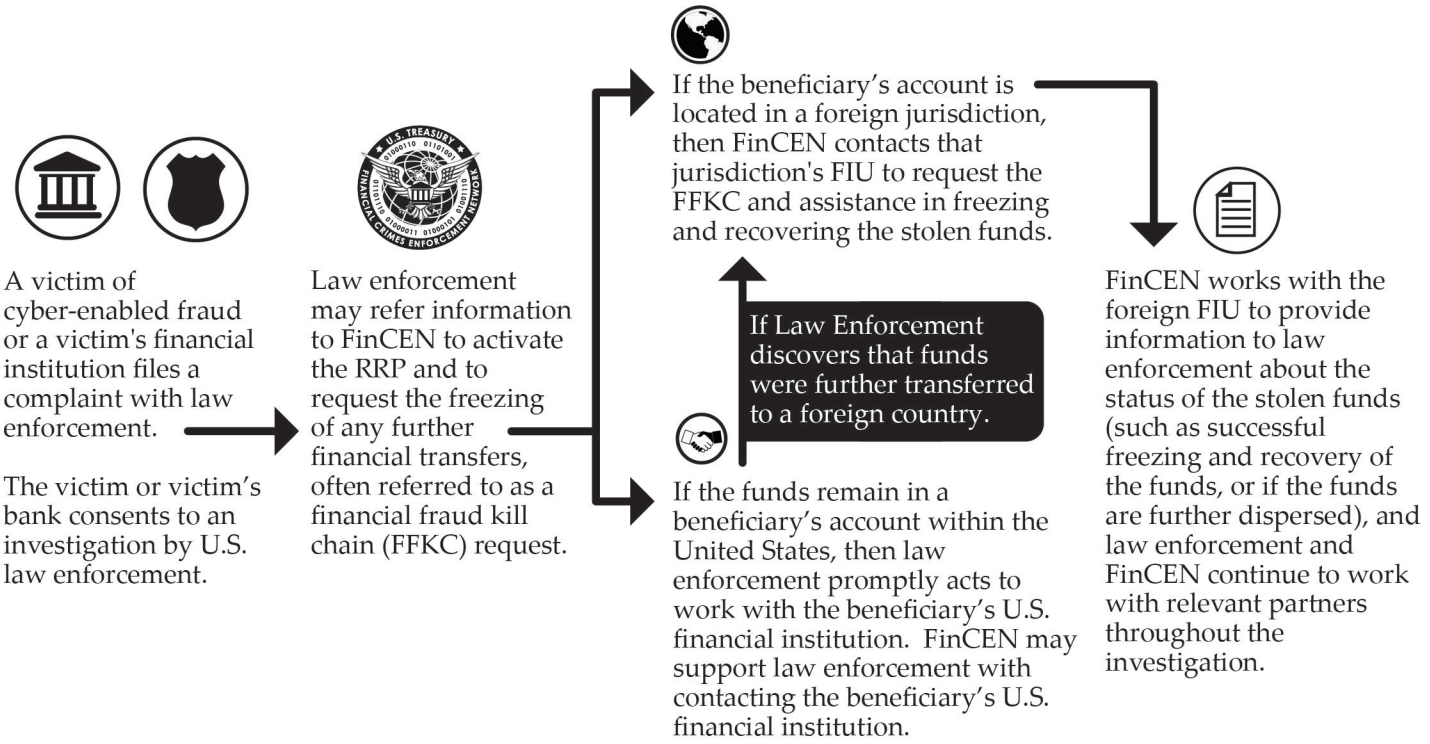
Since the RRP's inception in 2015, the program has facilitated the recovery of more than $1.1 billion for U.S. victims.

The Financial Crimes Enforcement Network (FinCEN) plays several key roles in preventing financial crime. Through the Rapid Response Program (RRP), FinCEN helps victims and their financial institutions recover funds stolen as the result of certain cyber-enabled financial crime schemes, including business e-mail compromise (BEC).[1]

This RRP is a partnership between FinCEN; U.S. law enforcement (including the FBI, the U.S. Secret Service (USSS), Homeland Security Investigations (HSI), and the U.S. Postal Inspection Service (USPIS)); and, foreign partner agencies that, like FinCEN, are the financial intelligence units (FIUs) of their respective jurisdictions.[2] FinCEN uses its authority to share financial intelligence rapidly with counterpart FIUs and encourages foreign authorities to interdict the fraudulent transactions, freeze funds, and stop and recall payments using their authorities under their own respective legal and regulatory frameworks. The RRP has been used to confront cyber threats involving approximately 70 foreign jurisdictions to date, and has the capacity to reach more than 160 foreign jurisdictions through FIU-to-FIU channels. Through these collaborative efforts, FinCEN has successfully assisted in the recovery of over $1.1 billion.

1. BEC fraud involves schemes in which criminals compromise the email accounts of victims either to (1) send fraudulent payment instructions to financial institutions or other business associates in order to misappropriate funds; or (2) cause data to be transmitted fraudulently to conduct financial fraud. *See* FinCEN Advisory, FIN-2016-A003, "Advisory to Financial Institutions on E-mail Compromise Fraud Schemes" (September 6, 2016); FIN-2019-A005, "Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes" (July 16, 2019).
2. As the FIU of the United States, FinCEN serves as the United States' national center that receives and analyzes suspicious transaction reports (a.k.a., suspicious activity reports) and other information relevant to money laundering, associated predicate offences, and terrorist financing, and disseminates the results of its analysis to competent authorities. FinCEN obtains information from reporting entities pursuant to the Bank Secrecy Act (*see* 31 U.S.C. 5311-5314; 5316-5336 (reporting authorities under the BSA)) and collaborates with foreign FIUs and law enforcement (domestic and foreign), among other things, to detect and deter financial crime (*see* 31 U.S.C. 310(b)(2)(H)). FinCEN is a member of The Egmont Group, which is a global network of FIUs that exchanges financial intelligence and other information to combat money laundering, associated crime, and terrorist financing. For more information, see the Financial Action Task Force's (FATF) *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations* (Recommendations 29 and 40 and the respective Interpretive Notes).

Operational Flow of RRP



Activating the RRP

A victim of a cyber-enabled crime, or the victim's financial institution, ***must file a complaint with law enforcement*** to initiate the RRP. To request assistance from law enforcement, a victim or the victim's financial institution may file a complaint with the FBI's Cyber- and Internet-related Crime Complaint Center (IC3)[3] or the nearest USSS field office (www.secretservice.gov/field_offices.shtml).[4] Victims should also expeditiously contact their financial institution at the time that they file a complaint with law enforcement. Victims should not directly contact FinCEN.

As depicted in the flow chart above, the activation of the RRP begins with a complaint to law enforcement. After law enforcement receives the consent of a victim, it will open an investigation and may request FinCEN's assistance to share financial intelligence with foreign FIUs in an attempt to recover the proceeds of the crime.[5]

3. *See* the FBI's IC3 website, http://www.ic3.gov.
4. The U.S. Department of Homeland Security (including HSI and Immigration and Customs Enforcement) encourages the reporting of cyber and import/export fraud via its Cybersecurity and Infrastructure Security Agency National Cybersecurity Communications and Integration Center (NCCIC). See DHS's CISA reporting form: https://us-cert.cisa.gov/report.
5. FinCEN also processes inbound requests from foreign FIU partners regarding proceeds of fraud sent to the United States and works with U.S. law enforcement to activate the FFKC with U.S. financial institutions.

Information to Provide to Law Enforcement to Activate the RRP

When requesting law enforcement assistance, the victim or the victim's financial institution should provide as much transactional detail and cyber-related information surrounding the scheme as possible. While FinCEN does not ensure the recovery of stolen funds, the RRP has had greater success in recovering funds when victims or financial institutions report fraudulently induced wire transfers to law enforcement within 72 hours of the transaction.

The following information should be provided at the time of filing a complaint with law enforcement:

- Victim's name
- Victim's financial institution's name
- The country location (full address helpful, but not required) of the branch of the victim's financial institution that originated the transaction
- Victim's account name (which may be different than the victim's name)
- Victim's account number
- Beneficiary's/Recipient's financial institution's name
- The country location of the beneficiary's/recipient's financial institution's branch that received the funds.
- Beneficiary's/Recipient's account name
- Beneficiary's/Recipient's account number
- Date of wire transaction
- Currency and amount transferred

Time is of the essence to successfully recover funds! Do not delay in providing the required information above to law enforcement to activate the RRP.

In addition to the information listed above, the following information is useful in recovering funds and detecting and preventing future illicit transactions.[6] FinCEN encourages the victim's financial institutions to provide this secondary information at the time of filing the complaint (**if it does not cause any delay in filing the required information to activate the RRP**), or in subsequent communications with law enforcement, or in filing any obligatory suspicious activity reports:

6. The data collected through the RRP aids government authorities in the recovery of stolen funds on behalf of victims of cyber-enabled crime, and assists FinCEN and law enforcement in detecting trends and criminal networks.

Additional Secondary Information Useful in Recovering Funds but Not Required to Activate the RRP:

- Additional financial transaction information:
  - Victim's bank's address
  - Victim's bank's Society for Worldwide Interbank Financial Telecommunication (SWIFT) Identifier
  - Beneficiary's bank's SWIFT identifier
  - Beneficiary's bank's address
  - Correspondent and intermediary financial institutions' information
  - Wire or currency transfer instructions from cyber actors
- Additional information on the fraud:
  - Summary of the fraud
  - Fake names used by the bad actors, including authors of attached documents to correspondences with the victim
  - Fake credibility method: e.g. pretended to be government representative, NGO, friend, technology company, etc.
  - Text (SMS) communication phone number(s) and messages
  - Stated location of the sender or messages, or beneficiary of funds
- Any other pertinent information that the partners of RRP can use to trace the funds and identify the bad actors

Additional Optional Information Useful for Intelligence, Enforcement, and Detecting Trends and Typologies:

- Additional information on the victim:
  - Victim's age
  - Victim's profession, or if an entity, the type of business
- Additional information on the fraud:
  - Sender email address and associated Internet Protocol (IP) addresses, with their respective timestamps, if possible
  - Sender email domain
  - Reply to email address
  - Email receive date

- Type of request from bad actor
- Subject of email
- Attached document file name
- Self-deleting emails or other communication

- Additional cyber indicators
  - Malware hashes; MD5 Hash Values: The 128-bit value which acts as a fingerprint for a message or file and is used to verify its contents after transfer
  - Infection vector: Method used to evade network security in order to install a malicious program
  - C2 Beacon Address: IP address of server(s) attackers use to establish outbound communications with compromised hosts
  - Login information with location and timestamps
  - Blockchain identifiers (e.g. virtual currency wallet addresses and transaction hashes)
  - Ingress and egress data of suspicious fund movements from identified wallets
  - Mobile device information (such as device International Mobile Equipment Identity (IMEI) numbers)
  - Malicious domains
  - Virtual private network (VPN) information
  - Encrypted Chat Services Used
  - P2P payment details, such as handles, usernames, QR codes, etc.

Reminder of Regulatory Obligations for U.S. Financial Institutions Regarding Suspicious Activity Reporting Involving Cyber-enabled Crime

Suspicious Activity Reporting

Financial institutions play an important role in protecting the U.S. financial system from these threats by complying with their obligations under the Bank Secrecy Act (BSA). Financial institutions should determine if filing a suspicious activity report (SAR) is required or appropriate, as will likely be the case in an incident of cyber-enabled crime conducted *by, at, or through* the financial institution. SAR obligations apply to both *attempted and successful* transactions. Contacting law enforcement does not relieve a financial institution from its SAR-filing obligations. Financial institutions are required to file complete and accurate reports that incorporate *all relevant information available*, including the information required to activate the RRP and cyber-related information.[7]

If the victim or the victim's financial institution activated the RRP through a law enforcement complaint, then FinCEN requests that financial institutions reference the key terms **"Rapid Response Program," "RRP,"** and, if received, include the **RRP case number**. Moreover, for cyber events, FinCEN requests that financial institutions continue to use the SAR filing instructions issued in relevant FinCEN advisories. For instance, in SAR field 2 (Filing Institution Note to FinCEN). Financial institutions should also select SAR field 42 (Cyber event) as the associated suspicious activity type, as well as select SAR field 42z (Cyber event - Other) while including "RRP" as a keyword in SAR field 42z. Additionally, financial institutions should include any relevant technical cyber indicators related to the activity and associated transactions within the available structured cyber event indicator SAR fields 44(a)-(j), (z).

When filing is not required, institutions may file a SAR voluntarily to aid law enforcement in protecting the financial sector.

7. For information on filing a high-quality SAR, *see e.g.* FinCEN Advisory, FIN-2016-A003, "Advisory to Financial Institutions on E-mail Compromise Fraud Schemes," (September 6, 2016); FinCEN Advisory, FIN-2019-A005, "Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes," (July 16, 2019); FinCEN Advisory, FIN-2020-A005, "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic," (July 30, 2020); FinCEN Advisory, FIN-2021-A004, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," (November 8, 2021); FinCEN Financial Trend Analysis, "Ransomware Trends in BSA Data between January 2021 and June 2021," (October 15, 2021); and FinCEN Frequently Asked Questions (FAQs), "FAQs regarding the Reporting of Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through SARs," (October 25, 2016).

Information for Financial Institutions Sharing Information

Financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT ACT are reminded that they may share information relating to transactions that the institution suspects may involve the proceeds of one or more specified unlawful activities (SUAs) under the section 314(b) safe harbor. The SUAs listed in 18 U.S.C. 1956 and 1957 include an array of fraudulent and other criminal activities, including fraud against individuals or the government. The financial institution need not have specific information indicating that the activity directly relates to an SUA and money laundering; rather, it is sufficient for the financial institution to have reasonable basis to suspect that the information being shared may involve money laundering or terrorist activity, and is sharing for the purpose of identifying and, where appropriate, reporting possible money laundering or terrorist activity.[8]

For Further Information

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

8. *See* FinCEN Section 314(b) Fact Sheet (December 2020).