FinCEN Rapid Response Program Fact Sheet

April 15, 2026

Since its inception in 2015, the U.S. Department of the Treasury's Financial Crimes Enforcement Network's (FinCEN) Rapid Response Program (RRP) has facilitated the interdiction of $1.8 billion and the recovery of over $1 billion in stolen proceeds on behalf of 5,790 U.S. victims. RRP is a partnership between FinCEN, U.S. law enforcement, and foreign partners working together to help victims and their financial institutions recover stolen funds sent abroad as the result of cyber-enabled fraud.

As the financial intelligence unit (FIU) of the United States, FinCEN uses its authority to share financial intelligence rapidly with counterpart FIUs and encourages foreign authorities to stop and repatriate the fraudulent transactions using authorities under their respective legal and regulatory frameworks. To date, the RRP has confronted cyber threats involving 96 foreign jurisdictions.

Are you a victim of a cyber-related fraud?

TIME IS OF THE ESSENCE!

A victim should immediately contact their **financial institution** to report fraudulent activity and request assistance. Please do not contact FinCEN directly.

A victim or their financial institution should file a complaint with the FBI's Internet Crime Complaint Center (IC3) (www.IC3.gov) and/or contact the nearest USSS field office (www.secretservice.gov/contact/field-offices).

RRP'S IMPACT SINCE JANUARY 20, 2025

More than $268.2 million in stolen funds interdicted and $157.3 million recovered on behalf of U.S. victims.

Phone Scams	Business E-mail Compromise	Investment Fraud
$33.9 million interdicted	$120.5 million interdicted	$40.2 million interdicted

Activating the RRP

Once law enforcement refers a victim's complaint involving a foreign beneficiary account to FinCEN, the RRP will contact the foreign FIU to encourage the interdiction and repatriation of the stolen funds and will work with the foreign FIU to provide status updates, financial intelligence, and procedural information to law enforcement.

1. The victim or their financial institution must file a complaint with law enforcement.
2. Law enforcement reviews the complaint and refers the case to FinCEN, activating the RRP.
3. RRP shares the financial intelligence with the foreign FIU in an attempt to recover the proceeds and provides information back to law enforcement.

Information to Provide to Law Enforcement to Activate the RRP

FinCEN encourages individuals to report fraudulent activity to law enforcement as quickly as possible. FinCEN is most likely to be able to interdict or recover funds when fraudulently induced wire transfers are reported to law enforcement within 72 hours of the transaction. When requesting law enforcement assistance, the victim or their financial institution should provide as much detail about the scheme and transactions as possible.

The following information *is required* to be provided at the time of filing a complaint with law enforcement:

- Victim's account name and number
- Victim's financial institution's name
- The country of the branch of the victim's financial institution that originated the transaction
- Summary of the fraud
- Beneficiary's account name and number
- Beneficiary's financial institution's name
- The country of the beneficiary's financial institution's branch that received the funds
- Date of wire transaction
- Currency and amount transferred

FinCEN encourages financial institutions to provide secondary information, where available, at the time of filing the complaint, in subsequent communications with law enforcement, and in any suspicious activity reports.[1]

While ***not required*** to activate the RRP, FinCEN recommends financial institutions provide the following additional information if available:

Additional financial institution information, including but not limited to:

- Society for Worldwide Interbank Financial Telecommunication (SWIFT) payment reference code from the victim bank
- Correspondent and intermediary financial institution information

Additional fraud details, including but not limited to:

- Fake names and credentials, including government-issued identification numbers, used by fraud actors
- Mobile application names used by fraud actors, including encrypted chat applications or any social networking sites exploited in the fraud scheme
- Filenames and/or hash values of documents, images, videos, or other digital files sent from the fraud actor
- Emails, unique hashtags, or other unique descriptive information
- Peer-to-peer (P2P) payment details, such as handles, usernames, QR codes, or other unique identifying information associated with fraud actors
- Virtual currency wallet addresses and transaction hashes

Additional cyber indicators, including but not limited to:

- Descriptive information involving any methods of cyber compromise, such as a Common Vulnerabilities and Exploits (CVE) record ID
- Mobile device information (such as device International Mobile Equipment Identity or IMEI numbers) associated with fraud actors.

1 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.