

FIN-2017-A007

October 31, 2017

Advisory to Financial Institutions Regarding Disaster-Related Fraud

Financial Institutions should be aware of potential fraudulent activity related to disaster relief efforts.

This Advisory should be shared with:

- Chief Risk Officers
- Chief Compliance Officers
- Legal Departments
- AML/BSA Departments
- AML/BSA Analysts
- Fraud Departments

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to warn financial institutions about the potential for fraudulent transactions in the wake of disasters, including recent hurricanes and wild fires. This advisory is not intended to deter legitimate donations and relief assistance efforts. Rather, the purpose is to help financial institutions identify and prevent fraudulent activity that may interfere with legitimate relief efforts.

The U.S. Department of Justice established the National Center for Disaster Fraud (NCDF) to investigate, prosecute, and deter fraud in the wake of Hurricane Katrina, when billions of dollars

in federal disaster relief poured into the Gulf Coast region.¹ Its mission has expanded to include suspected fraud from any natural or manmade disaster, including Hurricanes Harvey, Irma, and Maria. More than 30 federal, state, and local agencies participate in the NCDF, which allows the NCDF to act as a centralized clearinghouse of information related to disaster relief fraud of all types. Financial institutions are encouraged to use the resources made available by the NCDF to help identify and mitigate their potential for all types of disaster fraud risks.

Potential Frauds





While there are many indicators of general fraud, financial institutions should pay particular attention to benefits fraud, charities fraud, and cyber-related fraud.

Benefits Fraud

Benefits fraud typically occurs when individuals apply for emergency assistance benefits to which they are not entitled. Financial institutions are at risk when fraudsters seek to deposit or obtain cash derived from the emergency assistance payments. FinCEN has noted an increase in the use of wire transfers to perpetrate these frauds. In those situations, requests for withdrawals are made and funds are wired to bank accounts, where the fraudster immediately withdraws the funds.

1. See <https://www.justice.gov/usao-sdtx/pr/authorities-announce-formation-working-group-fight-hurricane-harvey-related-illegal>

The NCDF has identified certain possible signs of fraudulent activity that may assist financial institutions in identifying and combating hurricane-related benefit fraud, including the following red flags:



-  Deposits of multiple [Federal Emergency Management Agency](#) (FEMA), Red Cross, or other emergency assistance checks or electronic funds transfers into the same bank account, particularly when the amounts of the checks are the same or approximately the same (e.g., \$2,000 or \$2,358);
-  Cashing of multiple emergency assistance checks by the same individual;
-  Deposits of one or more emergency assistance checks, when the accountholder is a retail business and the payee/endorser is an individual other than the accountholder; and
-  Opening of a new account with an emergency assistance check, where the name of the potential accountholder is different from that of the depositor of the check.

The presence or absence of a red flag in any given transaction is not by itself determinative of whether a transaction is suspicious. Financial institutions should take into account all relevant details of a customer or transaction and should not necessarily presume suspicious activity based on a single red flag.

Charities Fraud

Charities provide a vehicle for donations to assist hurricane victims. However, during times of disaster, criminals seek to exploit these vehicles for their own gain. Both legitimate and fraudulent contribution solicitations and schemes can originate from social media, e-mails, websites, door-to-door collections, flyers, mailings, telephone calls, and other similar methods. In the coming weeks and months, it is likely that millions of aid dollars will flow to areas affected by Hurricanes Harvey, Irma, and Maria.


To ensure those contributions end up where donors intend, and not in the hands of criminals, the NCDF has identified possible signs of fraudulent activity to assist financial institutions in identifying and combating hurricane-related charities fraud,² which may include the following red flags:


-  Financial institutions may be able to identify potential fraudulent transactions where the payee organization's name is similar to, but not exactly the same as, those of reputable charities; or
-  The use of money transfer services for charitable collections – generally, legitimate charities do not solicit donations via money transfer services.

2. See <https://www.justice.gov/opa/pr/tips-avoiding-fraudulent-charitable-contribution-schemes>

Cyber-Related Fraud

Cyber actors take advantage of public interest during natural disasters in order to conduct financial fraud and disseminate malware. The Center for Internet Security expects this trend to continue as new and recycled scams emerge involving financial fraud and malware related to Hurricanes Harvey, Irma, and Maria. As of September 2017, the Multi-State Information Sharing and Analysis Center (MS-ISAC) observed the registration of more than 743 domain names containing the word “Irma,” and most include a combination of the words “help,” “relief,” “victims,” “recover,” “claims,” or “lawsuits.” They believe more domain registrations related to Hurricanes Harvey, Irma, and Maria are likely to follow.³ Financial institutions may want to be aware of public reporting on hurricane-related or wild fire phishing campaigns, malicious websites, and associated malware. Institutions should be aware of the following red flags for potential cyber-related fraud:

 Crowdfunding platforms also can be exploited by criminal elements. While many crowdfunding efforts are legitimate and have platforms with the appropriate protections in place, some platforms have limited policies and procedures in place to protect customer funds and identification. In these circumstances, financial institutions should be aware of the risk this can present for potential identity theft vulnerabilities of account holders who are donors. Information security units in financial institutions may have access to information that may help in the detection and reporting of such activity.

 Some illicit crowdfunding sites are set up expressly to defraud donors. Cyber actors often create such sites using web designs or names that are virtually identical to legitimate charities and relief organizations to induce unwitting donors into making donations to criminal enterprises through these fraudulent sites. These fraudulent websites often end with a “.com” or a “.net”, while most legitimate charities’ websites end in “.org”. For example, [www.\[charity\].org](http://www.[charity].org) (legitimate) versus [www.\[charity\].net](http://www.[charity].net) (potentially not legitimate). Payments to such websites may indicate fraudulent activity.

Financial institutions can report any internet-based fraud and crimes to the FBI’s Internet Crime Complaint Center at <https://www.ic3.gov/>.

Suspicious Activity Reporting

Consistent with suspicious activity reporting requirements in 31 CFR Chapter X, if a financial institution knows, suspects, or has reason to suspect that a transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, the financial institution should file a Suspicious Activity Report (SAR).⁴

3. See <https://www.cisecurity.org/ms-isac/cyber-alert-cyber-threat-actors-expected-to-leverage-hurricane-irma/>

4. 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.

As noted above, the presence or absence of a red flag in any given transaction is not by itself determinative of whether a transaction is suspicious. Financial institutions should consider additional factors such as a customer’s overall financial activity and whether it exhibits multiple red flags, as well as the specifics of their own risk profiles and business models as those relate to the information and red flags outlined in this advisory.

When evaluating potential suspicious activity, financial institutions should also be mindful that some red flags may be observed during general transactional monitoring, whereas others may be more readily identified during in-depth case reviews.

FinCEN requests, though does not require, that financial institutions reference this advisory and include the key term, “*Disaster-related Fraud*” in the SAR narrative and in SAR field 31(z) (Fraud-Other) to indicate a connection between the suspicious activity being reported and possible misuse of relief funds. Financial institutions should provide a detailed description of the known or suspected criminal violation or suspicious activity in the narrative sections of Suspicious Activity Reports.

If financial institutions encounter any of these situations, or other situations that they suspect may involve hurricane or other disaster-related benefit fraud or other potentially illicit transactions, they should complete and file a Suspicious Activity Report and, in these instances, also contact their local office of the Federal Bureau of Investigation or the United States Secret Service.⁵

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at FRC@fincen.gov. *Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day)*. The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

FinCEN’s mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

5. See 31 CFR §§ 1020.320(e)(1)(ii)(A)(2)(i), 1021.320(e)(1)(ii)(A)(2), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2)(i), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), and 1030.320(d)(1)(ii)(A)(2) regarding joint SAR sharing. See Pub. L. No. 107-56, § 314(b) promulgated under 31 CFR § 1010.540 regarding Section 314(b) voluntary information sharing.