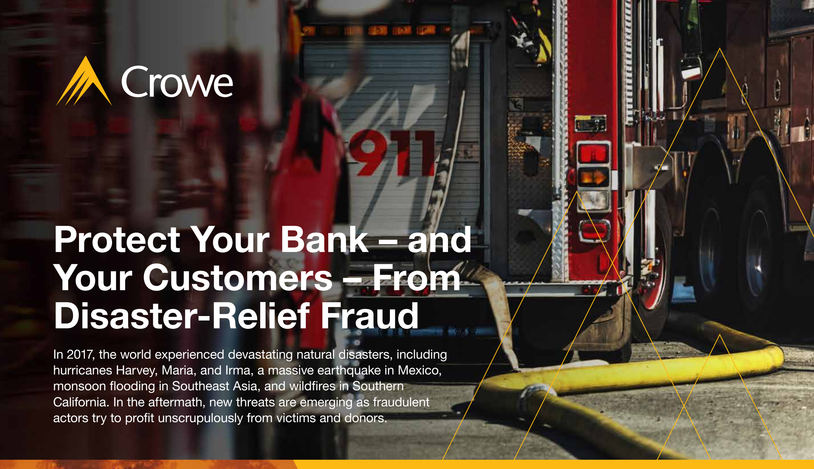

Protect Your Bank – and Your Customers – From Disaster-Relief Fraud

In 2017, the world experienced devastating natural disasters, including hurricanes Harvey, Maria, and Irma, a massive earthquake in Mexico, monsoon flooding in Southeast Asia, and wildfires in Southern California. In the aftermath, new threats are emerging as fraudulent actors try to profit unscrupulously from victims and donors.

16

Number of billion-dollar weather and climate disasters that occurred in the United States in 2017[1]

70,000

Complaints received by the National Center for Disaster Fraud (NCDF) since Hurricane Katrina in 2005[2]

400+

Fraud complaints received by the NCDF within the first month following hurricanes Harvey and Irma[3]

Banks

Banks can play an important role in thwarting disaster fraud schemes. Prepare your disaster fraud mitigation strategy today before the next disaster strikes.

Benefits Fraud

With benefits fraud, bad actors use stolen personal information to receive disaster-relief benefits.

Red Flags for Banks:[4]

- Deposits of multiple emergency assistance checks or funds transfers into the same account, or cashing multiple checks
- Deposits of emergency assistance checks into an account of a retail business when the payee is an individual
- Use of emergency assistance checks to open accounts in names different from those on the checks

Precautions Banks Should Take:

- Be aware of affected areas, and take special precautions to monitor account activity in these areas
- Plan ahead how the bank will handle identity verification for disaster victims who may have lost traditional, formal documents in the disaster
- Prepare a strategy for reissuing lost or inaccessible debit cards
- Consider reducing daily withdrawal limits, but remain flexible as there may be legitimate needs for large amounts of cash

Charities Fraud

In September 2017, shortly after Irma was upgraded to hurricane status, more than 743 domain names were set up containing the name "Irma," including some fake charities that could steal either donated funds or personal information to be used in identity fraud schemes.[5]

Red Flags for Banks:

- Website or charity name is similar to actual charity, but not exactly the same, such as the site name ending in ".net" or ".com" instead of ".org"
- Requested use of money transfer services or crowdfunding platforms for charitable contributions
- Lack of supporting documentation for tax exempt status

Precautions Banks Should Take:

- Regularly monitor higher risk organizations, such as not-for-profits
- Vet charity organizations on independent charity evaluator sites
- Carefully review organizational naming conventions when opening new accounts
- Warn customers to watch for bogus charities that appear to be legitimate

Choose Experience

When you choose Crowe, you can count on receiving practical solutions based on our professionals' many years of experience working with more than 1,800 financial services clients worldwide. Crowe financial services specialists have extensive experience in assisting clients with developing sustainable antifraud programs. Our fraud detection and prevention, regulatory compliance, governance, and technology risk professionals can deliver results quickly and in conformance with industry best practices.

Learn More

Brenda Buetow
+1 317 706 2631
brenda.buetow@crowe.com

Aly Jiwani
+1 312 966 3083
aly.jiwani@crowe.com

Arjun Kalra
Leader, AML and Sanctions
+1 415 946 7449
arjun.kalra@crowe.com

Tom Paar
+1 630 575 4324
thomas.paar@crowe.com

1 "U.S. 2017 Billion-Dollar Weather and Climate Disasters," NOAA National Centers for Environmental Information (NCEI), 2018, https://www.ncdc.noaa.gov/billions/

2 National Center for Disaster Fraud, https://www.justice.gov/disaster-fraud

3 "Four U.S. Attorneys' Offices in Districts Affected by Hurricane Irma Establish Task Forces in Combating Disaster Fraud and Urge the Public to Be Vigilant in Reporting Suspected Fraud," U.S. Department of Justice, Office of Public Affairs, Sept. 14, 2017, https://www.justice.gov/opa/pr/four-us-attorney-offices-districts-affected-hurricane-irma-establish-task-forces-combating

4 "Advisory to Financial Institutions Regarding Disaster-Related Fraud," U.S. Department of the Treasury, Financial Crimes Enforcement Network, Oct. 31, 2017, https://www.fincen.gov/sites/default/files/advisory/2017-10-31/FinCEN%20Advisory%20FIN-2017-A007-508%20Compliant.pdf

5 "Cyber Alert: Cyber Threat Actors Expected to Leverage Hurricane Irma," Center for Internet Security, Sept. 8, 2017, https://www.cisecurity.org/ms-isac/cyber-alert-cyber-threat-actors-expected-to-leverage-hurricane-irma/

crowe.com

RISK-18500-032