INDUSTRY ADVISORY

FROM Treliant RISK ADVISORS

Financial Institutions and Donors Face Risk of Post-disaster Fraud

DECEMBER 2017

When natural or man-made disaster strikes, there is typically a rush of aid in the form of personnel, supplies, and financial funds. The sources of such aid may include federal, state, and local governments, non-governmental organizations, disaster aid groups, and charities, as well as private donors acting directly or through these vehicles. Since purse strings are sometimes loose during the early stages of relief and recovery, money and materiel may flow at high volumes with limited supervision and review.

Too often, there is an unfortunate consequence of this confluence of the need for assistance and the availability of money and other resources. Waste, fraud, and abuse may result, depleting the reserves of available funds for the intended recipients and projects. Disaster-related fraud or criminal activity can take a number of different forms, including benefits fraud, antitrust schemes such as bid-rigging, and outright theft.

Extreme and catastrophic damage has been caused in recent times by events ranging from Hurricane Katrina in 2005, to the Gulf of Mexico oil spill in 2010, to this year's Hurricanes Harvey, Irma, and Maria and the wildfires in the West. These disasters have seen massive responses—but also incidents of fraud.

Donor Awareness

While eager to help, donors to relief funds—be they private individuals or businesses—should exercise the appropriate level of caution when contributing. Minimum due diligence warrants checking the credentials of those soliciting and collecting donations and contributions, asking questions that include the following:

- Is the organization a well-known, "household name" in relief efforts or among charities?
- Does it have a robust, commercially reasonable public and/or internet presence? (Be wary of websites that present as "bare bones" or "off-the-shelf" sites.)
- Are there complaints or other advisories concerning the organization, such as with the Better Business Bureau or the Federal Trade Commission (FTC)?
- Does the organization have readily, publicly-available records that document the utilization of collected funds? Where does the money go? What percentage of collected funds go to "administrative costs" or "overhead?"
- In general, does the organization appear to lack legitimacy?

The FTC's website has an entire section with guidance for giving to charities as well as information on charity scams. Post-disaster relief periods may also see increased cybercrime activity, such as fraudulent or fake charities soliciting donations via spam or targeted emails. Donors should be cautious if receiving email solicitations, and it may be more prudent for them to donate directly through a reputable charity's website.

Bank Monitoring

The compliance departments of financial institutions, including those portions responsible for the monitoring, investigation, and reporting of potential money laundering and fraud, should also be cognizant of ill-gotten gains flowing through their organizations as a result of disaster-related fraud.

After Hurricane Katrina, the National Center for Disaster Fraud (NCDF) was established to improve the detection and ultimate prosecution of fraud related to natural and man-made disasters, by means including a hotline. The Financial Crimes Enforcement Network (FinCEN) recently issued an advisory to financial institutions describing some classic types of disaster-related frauds and their attendant red flags. The primary types of frauds include benefits fraud and, as noted above, charities fraud.

Much like public assistance fraud, benefits fraud related to disasters arises when someone seeks and receives benefits to which they are not otherwise entitled. Incidents of this during the Gulf oil spill recovery included parties claiming losses that did not actually occur. A fraudster may also "double-dip" in order to receive multiple benefits for the same loss, through name variations or aliases. Other examples may involve simple theft of benefit checks, cashed or deposited through forgery.

Financial institutions are in a good position to detect and, when appropriate, report potential benefits fraud, when instruments such as checks are cashed or deposited, or funds are transferred via wire. Through their monitoring, they may see instances of multiple benefit payments being deposited by the same individual, or multiple benefit payments under different names going into the same account.

Pursuant to the Bank Secrecy Act, financial institutions should file suspicious activity reports (SARs) if they observe these "red flags" or generally find a transaction to be suspicious. FinCEN requests that SARs potentially related to disasters clearly state that linkage in their narrative.

Financial institutions that assist in the detection of disaster-related fraud are also potentially mitigating their own operational, reputational, and legal risk. So compliance departments, anti-money laundering personnel, and fraud units need to be aware of the red flags and typologies associated with these activities, especially in the wake of large disasters.

This Advisory was provided by Timothy A. Westrick.

- **Timothy Westrick, Senior Manager, has over 20 years of domestic and international experience as a white-collar attorney and compliance professional in both the public and private sectors, including government, industry, and advisory services. twestrick@treliant.com**