



Factsheet: Avoiding Post-Disaster Scams and Fraud

As disaster victims find themselves in vulnerable financial situations, they can be targets of scammers pretending to be government employees, creditors, mortgage servicers, insurance adjusters, and contractors. Help your clients be alert to and aware of potential scams and fraud after a disaster strikes.

SCAM AWARENESS

Adhere to the following basic practices to avoid scams:

- **Do not be pressured into taking immediate action.** If someone is telling you that you need to act now, they are likely trying to prevent you from verifying whether the business is legitimate. Take your time.
- **Be wary of anyone going door to door.** Scammers may pose as contractors, charity workers, or even government officials. Remember that if someone is trying to sell you something or asking for a donation, you can say no and then do the necessary research.
- **Work with charities and services you know and trust.** Do research before donating to new organizations or using new services.
- **Pay with a credit card whenever possible.** Paying with a credit card gives you the ability to reverse any fraudulent charges, adding an extra layer of protection.
- **Ask for references, licenses, and certifications.** Make sure that anyone you hire is qualified and has all applicable licenses or certifications required by their field.
- **Obtain offers in writing.** Ask for written estimates and contracts before you do business.
- **Initiate communication.** Never make payments or give out personal information to someone on a phone call you did not initiate.

CONTRACTOR SCAMS AND FRAUD

Following a disaster, property owners need to take additional care in hiring contractors to make repairs. The high demand for construction contracts may cause some businesses to misrepresent their qualifications, raise their prices, or otherwise cut corners in the contracting process. Instruct your clients to follow these guidelines when choosing and working with contractors:

- Ask your insurer for a list of approved contractors.
- For major repairs, get at least three estimates, based on the same specifications and materials.



- Check references, licensing, and registration information with the [National Association of State Contractors Licensing Agencies \(NASCLA\)](#), read reviews posted by the [Better Business Bureau](#), and work with a local housing and community development agency to coordinate with local contractors and identify appropriate contractor resources.
- Require written contracts that specify the work to be done, materials to be used, start and end dates, responsibility for hauling away debris, and costs broken down by labor and materials. Verify that the contractor's name, address, phone number, and license number are included, as well as any verbal promises and warranties.
- Never sign a contract with blank spaces. Dishonest contractors sometimes enter unacceptable terms later.
- Read the fine print. Make sure your contract does not include any clauses that allow for substantial cancellation fees if you choose not to use the contractor after your insurance company has approved the claim, or that require you to pay the full price if you cancel after the cancellation period has expired.
- Never pay in full in advance, and do not pay with cash. Have the contract specify a schedule for making payments, and before making the final payment, ask the contractor to provide proof that all subcontractors have been paid; if not, you could be liable for their fees.
- Make sure that anyone you hire is qualified and has all applicable licenses or certifications required by their field.

FINANCIAL SCAMS AND IDENTITY THEFT

After a disaster, con artists may pose as insurance servicers or government employees to obtain your personal information (e.g., Social Security number, bank account number). They may contact you in person or by phone, mail, or email. Keep the following in mind:

- HUD, the Federal Emergency Management Agency (FEMA), and the Small Business Administration do not charge fees to apply for assistance or to receive property damage inspections.
- Always ask to see a government-issued photo ID. Take a picture of it with your cellphone, if possible.
- Government workers will **never** ask for payment to perform their duties, or offer to increase your assistance grant for a fee.
- Beware of anyone claiming to be from FEMA or the state who asks for a Social Security number, bank account number, or other sensitive information. Ensure that anyone you give this information to is a reliable source.
- If someone calls and tells you that you need to make a payment immediately in order to maintain your coverage, check with your insurer directly. Use the phone number provided on your monthly bill or find one directly on your insurer's website rather than trusting someone who calls you.
- If you suspect fraud, call the FEMA Disaster Fraud Hotline at (866) 720-5721.



DONATION SCAMS AND FAKE CHARITIES

Con artists may solicit charitable donations for nonexistent organizations. Some charity scams contact you by phone or by door-to-door visits, but many more begin with text messages, emails, or social media posts to direct would-be donors to scammer-run websites. At the website, personal information and credit card numbers are collected for supposed donations (and possible identity theft). Scammer sites also may infect your computer with information-stealing malware. To avoid fraud, follow these rules:

- Only give to charities and services you know and trust. Do research before donating to new organizations or using new services.
- Contact the charity directly. Do not trust requests that come to you. Stick with names and reputations vetted at [Charity Navigator](#), [Charity Watch](#), and [Give.org](#).
- Ask for the charity's exact name, street address, phone number, and web address. Confirm that the person asking for funds is an employee or volunteer.
- Do not pay with cash. Pay with a check made out to the charity or by using a credit card in case the funds must be stopped later.
- Request a receipt. Legitimate nonprofit agencies routinely provide receipts for tax purposes.
- Do not open any emails or click on any links that seem to be suspicious. Fraudulent emails may include spelling mistakes, list suspicious contact information (e.g., an address in a state in which the institution is not headquartered, a phone number with an unrecognizable area code), or contain urgent or threatening language. Never click on links provided in emails that are sent to you – instead, look them up on the organization's website.

CAR SCAMS

Damaged cars can be resold to unsuspecting consumers. When vehicles damaged by floods are deemed a loss by insurers, owners are paid off and the cars are moved to a salvage yard to be sold for parts. However, roughly half of these "flood cars" are instead purchased, cleaned up, and resold to dealers and individual buyers. Although initially drivable, rust can damage the engine and body; wires that were water-soaked are at risk of cracking; and brakes, door locks, power windows, transmission, and heating and air conditioning units can fail. To avoid buying a flood car:

- Enter the vehicle identification number (VIN) at [VINCheck](#), a free service from the National Insurance Crime Bureau, which could reveal a vehicle's flood damage.
- Have a trusted auto repair person inspect the car prior to purchasing.
- Look for signs of water damage, such as musty smells or fragrances that suggest the seller is trying to cover up smells, and carpeting that looks too new, is discolored, or has water stains.



HOUSING COUNSELING DISASTER RECOVERY TOOLKIT



- Look for mud, silt, or rust. Check engine crevices and exposed screw heads, the glove compartment, door panels, and under seats and the spare tire well for water lines or signs of mud, silt, or rust.
- Look out for water condensation, fogging, or water lines inside headlights, taillights, and dashboard gauges.
- Repeatedly test electrical equipment, such as wipers, turn signals, the heater and air conditioner, and power windows and locks. Also check engine wires; if they do not bend easily, they may soon crack due to water damage.



Acknowledgments and Additional Resources

- [The Consumer Financial Protection Bureau \(CFPB\): Avoiding Loan Scams After a Natural Disaster](#)
- [FEMA: Protect Yourself From Disaster-Related Fraud and Scams](#)
- [National Foundation for Credit Counseling: Avoiding Post-Disaster Scam Artists](#)
- [National Insurance Crime Bureau: Beware Harvey Flood-Damaged Vehicles](#)
- [HUD Exchange Housing Counseling Consumer Protection Toolkit](#)