10 Scams Targeting Bank Customers: Plus the basics on how to protect your personal information and your money

The FDIC often hears from bank customers who believe they may be the victims of financial fraud or theft, and our staff members provide information on where and how to report suspicious activity. To help further, ***FDIC Consumer News*** includes crime prevention tips in practically every issue. As part of that coverage, we feature here a list of 10 scams that you should be aware of, plus key defenses to remember.

1. **Government "imposter" frauds:** These schemes often start with a phone call, a letter, an email, a text message or a fax supposedly from a government agency, requiring an upfront payment or personal financial information, such as Social Security or bank account numbers.

   "They might tell you that you owe taxes or fines or that you have an unpaid debt. They might even threaten you with a lawsuit or arrest if you don't pay," said Michael Benardo, manager of the FDIC's Cyber Fraud and Financial Crimes Section. "Remember that if you provide personal information it can be used to commit fraud or be sold to identity thieves. Also, federal government agencies won't ask you to send money for prizes or unpaid loans, and they won't ask you to wire money to pay for anything."
2. **Debt collection scams:** Be on the lookout for fraudsters posing as debt collectors or law enforcement officials attempting to collect a debt that you don't really owe. Red flags include a caller who won't provide written proof of the debt you supposedly owe or who threatens you with arrest or violence for not paying.
3. **Fraudulent job offers:** Criminals pose online or in classified advertisements as employers or recruiters offering enticing opportunities, such as working from home. But if you're required to pay money in advance to "help secure the job" or you must provide a great deal of personal financial information for a "background check," those are red flags of a potential fraud.

   Another variation on this scam involves fake offers of part-time jobs as "mystery shoppers," who are people paid to visit retail locations and then submit confidential reports about the experience. In an example of the fraudulent version, your job might be to receive a $500 check, go "undercover" to your bank, deposit the check into your account there, and then report back about the service provided. But you also would be instructed to immediately wire your new "employer" $500 out of your bank account to cover the check you just deposited. Days later, the bank will inform you that the check you deposited is counterfeit and you just lost $500 to thieves. One warning sign of this type of scam is that the potential employer requires you to have a bank account.
4. **"Phishing" emails:** Scam artists send emails pretending to be from banks, popular merchants or other known entities, and they ask for personal information such as bank account numbers, Social Security numbers, dates of birth and other valuable details. The emails usually look legitimate because they include graphics copied from authentic websites and messages that appear valid.

   "We have also seen emails with links to fake websites that are exact copies of real websites for FDIC-insured banks, except the web addresses are slightly different than the real ones," said Doreen Eberley, director of the FDIC's Division of Risk Management Supervision, which is in charge of the agency's policies and programs related to financial crimes. "These sites are used to trick people into giving up valuable personal information that can be used to commit identity theft."
5. **Mortgage foreclosure rescue scams:** Today, many homeowners who are struggling financially and risk losing their homes may be vulnerable to false promises to refinance a mortgage under better terms or rates. But borrowers should always be on the lookout for scammers who falsely claim to be lenders, loan servicers, financial counselors, mortgage consultants, loan brokers or representatives of government agencies who can help avoid a mortgage foreclosure and offer a great deal at the same time. These criminals will present homeowners with what sounds like the life-saving offer they need. Instead, the homeowner is required to pay significant upfront fees or, even worse, tricked into signing documents that, in the fine print, transfer the ownership of the property to the criminal involved. Common warning signs of fraudulent mortgage assistance offers include a "guarantee" that foreclosure will be avoided and pressure to act fast.

6. **Lottery scams:** You might be told you won a lottery (typically one that you never entered) and asked to first send money to the “lottery company” to cover certain taxes and fees. Similar examples involve bogus prize winnings and sweepstakes. “In one example, a scammer sent a letter to people using falsified FBI and FDIC letterhead telling them they won a popular, well-known lottery but that they needed to send money by wire transfer to a lottery ‘official’ in order to secure the winnings,” Benardo said. “The ‘official’ was really a crook hoping to trick people into sending money.”
7. **Elder frauds:** Thieves sometimes target older adults to try to cheat them out of some of their life savings. For example, telemarketing scams may involve sales of bogus products and services that will never be delivered. Warning signs include unsolicited phone calls asking for a large amount of money before receiving the goods or services, and special offers for senior citizens that seem too good to be true, like an investment “guaranteeing” a very high return. To help seniors and their caregivers avoid financial exploitation, the FDIC and the Consumer Financial Protection Bureau have developed Money Smart for Older Adults, a curriculum with information and resources (see our News Briefs).
8. **Overpayment scams:** This popular scam starts when a stranger sends a consumer or a business a check for something, such as an item being sold on the internet, but the check is for far more than the agreed-upon sales price. The scammer then tells the consumer to deposit the check and wire the difference to someone else who is supposedly owed money by the same check writer. In a few days, the check is discovered to be a counterfeit, and the depositor may be held responsible for any money wired out of the bank account. Victims may end up owing thousands of dollars to the financial institution that wired the money, and sometimes they’ve also sent the merchandise to the fraud artists, too.
9. **"Ransomware":** This term refers to malicious software that holds a computer, smartphone or other device hostage by restricting access until a ransom is paid. The most common way ransomware and other malicious software spreads is when someone clicks on an infected email attachment or a link in an email that leads to a contaminated file or website. Malware also can spread across a network of linked computers or be passed around on a contaminated storage device, such as a thumb drive.
10. **Jury duty scams:** A thief makes phone calls pretending to be a law enforcement official warning innocent people that they failed to appear for jury duty and threating an arrest unless a “fine” is paid immediately. And to pay up, the caller asks for debit account and PIN numbers, allowing the perpetrator to create a fake debit card and drain the account.

What You Can Do: Plus the basics on how to protect your personal information and your money

While we have described many forms of financial scams, the red flags to look out for are often similar. And so are the things you can do to help protect yourself and your money. Here are some basic precautions to consider, especially when engaging in financial transactions with strangers through email, over the phone or on the internet.

Avoid offers that seem “too good to be true.” As Eberley noted: “If someone promises ‘opportunities’ that are free or with surprisingly low costs or high returns, it is probably a scam. Be especially suspicious if someone pressures you into making a quick decision or to keep a transaction a secret.”

No matter how legitimate an offer or request may look or sound, don’t give your personal information, such as bank account information, credit and debit card numbers, Social Security numbers and passwords, to anyone unless you initiate the contact and know the other party is reputable.

Remember that financial institutions will not send you an email or call to ask you to put account numbers, passwords or other sensitive information in your response because they already have this information. To verify the authenticity of an email, independently contact the supposed source by using an email address or telephone number that you know is valid.

Be cautious of unsolicited emails or text messages asking you to open an attachment or click on a link. This is a common way for cybercriminals to distribute malicious software, such as ransomware. Be especially cautious of emails that have typos or other obvious mistakes.

Use reputable anti-virus software that periodically runs on your computer to search for and remove malicious software. Be careful if anyone (even a friend) gives you a thumb drive because it could have undetected malware, such as ransomware, on it. If you still want to use a thumb drive from someone else, use the anti-virus software on your computer to scan the files before opening them.

Don’t cash or deposit any checks, cashier’s checks or money orders from strangers who ask you to wire any of that money back to them or an associate. If the check or money order proves to be a fake, the money you wired out of your account will be difficult to recover.

Be wary of unsolicited offers “guaranteeing” to rescue your home from foreclosure. If you need assistance, contact your loan servicer (the company that collects the monthly payment for your mortgage) to find out if you may qualify for any programs to prevent foreclosure or to modify your loan without having to pay a fee. Also consider consulting with a trained professional at a reputable counseling agency that provides free or low-cost help. Go to the U.S. Department of Housing and Urban Development website for a referral to a nearby housing counseling agency approved by HUD or call 1-800-569-4287.

Monitor credit card bills and bank statements for unauthorized purchases, withdrawals or anything else suspicious, and report them to your bank right away.

Periodically review your credit reports for signs of identity theft, such as someone obtaining a credit card or a loan in your name. By law, you are entitled to receive at least one free credit report every 12 months from each of the nation’s three main credit bureaus (Equifax, Experian and TransUnion). Start at AnnualCreditReport.com or call 1-877-322-8228. If you spot a potential problem, call the fraud department at the credit bureau that produced that credit report. If the account turns out to be fraudulent, ask for a “fraud alert” to be placed in your file at all three of the major credit bureaus. The alert tells lenders and other users of credit reports that you have been a victim of fraud and that they should verify any new accounts or changes to accounts in your name.

Contact the FDIC’s Consumer Response Center (CRC) if you have questions about possible scams or you are the victim of a scam experiencing difficulty resolving the issue with a financial institution. The CRC answers inquiries about consumer protection laws and regulations and conducts thorough investigations of complaints about FDIC-supervised institutions. If the situation involves a financial institution for which the FDIC is not the primary federal regulator, CRC staff will refer the matter to the appropriate regulator. Visit our webpage on submitting complaints or call 1-877-ASK-FDIC (1-877-275-3342) Monday - Friday, 8am to 8pm (EST).

To learn more about how to avoid financial scams, search by topic in back issues of ***FDIC Consumer News*** and the FDIC's multimedia presentation Don't Be an Online Victim. Also find tips from the interagency Financial Fraud Enforcement Task Force.