Let's Talk Finances

Scams Targeting Bank Customers

By Charles Schmalz
President of
East Wisconsin Savings Bank

It is becoming more common to hear from bank customers who believe they may be the victims of financial fraud or theft, and our staff is trained to provide information on where and how to report suspicious activity. Here a list of several scams that you should be aware of:

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. **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 refund the overpayment or forward it along to someone else who is supposedly owed money by the same check writer. In a few days, the check is discovered to be fraudulent, and the depositor may be held responsible for any money withdrawn from the bank account. Victims may end up owing thousands of dollars to their financial institution, and sometimes they've also sent the merchandise to the fraud artists, too.

5. **"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.

While we have described several 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. Next week we will cover some basic strategies you can use to safeguard your personal information and your money.