MANAGING YOUR MONEY

Safe And Secure: Making Sure Your Money Stays Yours

by Jim Cichy

(NAPSA)—To keep your money safe and secure, you need to understand what you and your financial institution can do to combat security compromises and fraudulent use of your financial information.

Debit Fraud Techniques

When your debit card data is compromised, criminals can produce counterfeit cards an hour later. One of the most common fraud types can be found online. You've likely seen at least one e-mail claiming that you need to provide personal information or your checking account will be placed on hold or shut down completely.

Jim Cichy

Recently, many people got an e-mail falsely notifying them that their credit cards may have been compromised due to fraudulent activity. Along with official-looking information and a false case number, cardholders were threatened with the suspension of online services if they didn't verify their identity over the Web by providing sensitive financial information.

Other types of online scams promise rewards or financial gain for providing such information. A recently circulated e-mail promised that recipients would miss out on economic stimulus funds if they didn't respond immediately and provide the requested information. The e-mail was a hoax, but the promise of wealth or rewards can cause people to not check sources of information as thoroughly as they should.

You can even be taken advantage of without knowing anything is amiss on shopping Web sites. "Phishing" attacks can cause a Web page resembling or identical to a retailer's to appear when a customer visits. The difference is that the sensitive account and financial information isn't processed by the retailer but sent to the thief for fraudulent use.

Another type of fraud occurs over the phone. Some people may be fooled into giving out personal information by official-sounding titles or financial institution names when called. For example, in one case, text messages were sent to cell phone customers requesting them to call a bank and reactivate their debit cards. Callers to the number were prompted to provide personal information, such as a debit card number or personal identification number (PIN). Also, customers of a city utility department received automated calls requesting payment and a late fee for a utility bill. Customers were requested to provide card information over the phone for payment.

Keep in mind that, no matter how official an e-mail looks or a phone call sounds, financial institutions will never contact you over the telephone or Internet to request personal information, including account, card numbers or your PIN.

Fight Against Fraud

To ward off possible scammers and fraudulent use of your personal cards, don't give out your PIN or other personal information. This includes not providing your PIN to tellers, retail customer service representatives or telephone marketers, none of whom should ever ask for it to begin with. Your PIN is yours and shouldn't be shared with anyone, written down or stored with your debit card.

Secondly, monitor your account frequently so you'll discover unauthorized spending quickly. You can work with your financial institution to stop the activity immediately and potentially have most or all of your funds restored. Many financial institutions provide online access to accounts, so you can watch your money daily. This also helps you keep track of your spending.

Financial Institutions' Role

Many institutions and payments networks have rolled out technology-driven solutions that quickly identify and decrease fraudulent use of debit cards.

For example, financial institutions using the PULSE ATM/debit network for processing use the company's fraud detection system, designed to red-flag potentially fraudulent purchases immediately and notify the institution. The system is always adapting to spending habits and will identify purchases outside of regular spending trends.

On top of individual company technology solutions, all firms that handle, store, process or transmit financial data must adhere to the Payment Card Industry Data Security Standard. It's designed to help organizations prevent fraudulent payment card use, hacking and other types of security issues.

Your knowledge of your finances and your financial institution's efforts to stop fraud before it starts can help decrease your risk of attack.

For more information on steps you can take, visit www.debitfacts.org.

• *Jim Cichy is Vice President of Fraud Management for PULSE, one of the leading ATM/debit networks in the country.*