

FDIC Consumer News

Spring 2013

Protecting Your Plastic from High-Tech Criminals

How to help keep your credit and debit cards safe

While many consumers still like to use paper money and coins, more and more people are pulling out credit or debit cards to make purchases. And, as the popularity of payment cards has grown, so has the number of criminals trying to steal very valuable details, including the cardholder's name and the card's account number and expiration date, which are printed on the card itself as well as encoded (for machine readability) in the magnetic stripe or a computer chip.

"No matter how your card information is stored, it is in high demand by criminals who would like to retrieve that data to create a counterfeit version of your card or use the information to make purchases online or over the phone," said Michael Benardo, manager of the FDIC's Cyber Fraud and Financial Crimes Section.

If you're ever the victim or target of credit or debit card theft or fraud, catching it fast and reporting it to your card issuer are key to resolving the situation. And while federal laws and industry practices protect consumers in these situations, there are important differences depending on the type of card.

In general, under the Truth in Lending Act, your cap for liability for unauthorized charges on a credit card is \$50. But under the Electronic Fund Transfer Act, if your debit card or ATM card is lost or stolen or you notice an unauthorized purchase or other transfer using your checking or savings account, your maximum liability is limited to \$50 only if you notify your bank within two business days. If you wait more than two business days, your debit/ATM card losses under the law could go up to \$500, or perhaps much more. With either card, though, industry practices may further limit your losses, so check with your card issuer. To learn more about your consumer protections, see the Fall 2009 **FDIC Consumer News** (www.fdic.gov/consumers/consumer/news/cnfall09/debit_vs_credit.html).

What else can you do to keep thieves away from your cards...and your money?

Never give out your payment card numbers in response to an unsolicited e-mail, text message or phone call, no matter who the source supposedly is. An "urgent" e-mail or phone call appearing to be from a well-known organization is likely a scam attempting to trick you into divulging your card information. It's called "phishing," a high-tech variation of the concept of "fishing" for account information. If they get confidential details, the criminals can use the information to make counterfeit cards and run up charges on your accounts.

Take precautions at the checkout counter, ATM and gas pump. "Be on the lookout for credit and debit card reading devices that look suspicious, such as a plastic sleeve inside a card slot," Benardo said. "Crooks are getting very good at attaching their own devices over legitimate card readers and gathering account information from the cards that consumers swipe through those readers."

Also be alert when you hand your payment card to an employee at a restaurant or retail establishment. For example, if he or she swipes your card through two devices instead of one, that second device could be recording your account information to make a fraudulent card. Report that situation to a manager and your card issuer.

To help combat payment card fraud, many card issuers have turned to the technology known as radio frequency identification (RFID). This uses wireless radio signals to identify people or objects from a distance. It is also being used with items such as highway toll passes, subway fare cards and pay-at-the-pump

cards to add convenience and speed up many routine transactions. While some news reports indicate that payment cards with RFID chips may be more vulnerable to fraud than traditional cards with magnetic stripes on the back, Bernardo said that's not the case.

"Today an RFID card is nearly impossible to breach because the chip in it creates an encrypted signal that is extremely difficult to hack or compromise," he said. "If you have questions or concerns about a payment card that is RFID-enabled, ask your bank about the precautions it takes to safeguard your card information."

Closely monitor your bank statements and credit card bills. "Look at your account statements as soon as they arrive in your mailbox or electronic inbox and report a discrepancy or anything suspicious, such as an unauthorized withdrawal," advised FDIC attorney Richard M. Schwartz. "While federal and state laws limit your losses if you're a victim of fraud or theft, your protections may be stronger the quicker you report the problem." These days, it's also easy to monitor your accounts using online banking or even your mobile phone (see [Using Technology to Remain Financially Fit](#)).

Also, don't assume that a small unauthorized transaction isn't worth reporting to your bank. Some thieves are making low-dollar withdrawals or charges in hopes those will go unnoticed by the account holders. In one recent example, a federal court temporarily halted an operation that allegedly debited hundreds of thousands of consumers' bank accounts and billed their credit cards for more than \$25 million—in small charges— without their consent.

And, contact your institution if your bank statement or credit card bill doesn't arrive when you normally expect it because that could be a sign that an identity thief has stolen your mail and/or account information to commit fraud in your name.

Periodically review your credit reports for warning signs of fraudulent activity. Credit reports, which are prepared by companies called credit bureaus (or consumer reporting agencies), summarize a consumer's history of paying debts and other bills. But if a credit report shows a credit card, loan or lease you never signed up for, this could indicate you are a victim of ID theft.

You are entitled to at least one free credit report every 12 months from each of the nation's three major credit bureaus. To maximize your protection against fraud, some experts suggest spreading out your requests throughout the year, such as by getting one free report every four months instead of all three at the same time. To request your free report, go to www.AnnualCreditReport.com or call toll-free 1-877-322-8228.

For additional information on how to protect your credit or debit card from fraud, start with consumer information about identity theft on the Federal Trade Commission Web site at www.consumer.ftc.gov/features/feature-0014-identity-theft. Resources from other federal agencies can also be found at www.mymoney.gov.