Preventing Payment Card Fraud

Dos & Don'ts

Federal Reserve Bank of Philadelphia

About the Federal Reserve

The Federal Reserve Bank of Philadelphia is one of 12 regional Reserve Banks in the United States that, along with the Board of Governors in Washington, D.C., make up the Federal Reserve System, the nation's central bank. To ensure a sound financial system and a healthy economy, the Fed conducts monetary policy, supervises and regulates financial institutions, maintains the payments system, and serves as the lender of last resort in a financial crisis.

The Philadelphia Fed is responsible for the Third District, which covers eastern Pennsylvania, southern New Jersey, and Delaware. Like other Reserve Banks, the Philadelphia Fed is involved in conducting monetary policy, supervising and regulating banks, and providing financial services to banks and the federal government.

The Board of Governors, which is accountable to Congress, oversees the Reserve Banks. Fed Governors and Reserve Bank presidents participate in Federal Open Market Committee decisions on national monetary policy.

Payment Cards Center

The Federal Reserve Bank of Philadelphia established a Payment Cards Center to provide insights into developments in consumer credit and payments. The center carries out its mission through an agenda of research and analysis, as well as forums and conferences that encourage dialogue incorporating industry, academic, and public-sector perspectives.

Payment card fraud is the unauthorized use of your cards or card account numbers for financial gain, often by using them to purchase goods and services.

Payment Card Fraud

There are many antifraud tools used by the payment card industry. Among them, artificial neural networks are sophisticated computer programs that help to identify transactions that may be fraudulent. One indicator may be transactions that appear to be out of line with a customer's past usage, for example, transactions occurring in certain foreign countries where the cardholder has never before traveled. These out-of-profile transactions may generate a call from your issuer. Without this notification, victims of payment card fraud may not be aware of fraudulent activity until they review their monthly statements.

Likewise, if you suspect fraudulent activity, you should call your card issuer immediately. (You may also follow up in writing as an abundance of caution, but be sure you note it as a written follow-up to an already reported fraud event.) Depending on the nature of the fraud, a new card number may be issued for your account and new plastic mailed to you, and the issuer will decline any authorizations to the former number.

To protect against payment card fraud, know where your cards are at all times and keep them secure. To protect ATM and debit cards that involve a personal identification number (PIN), keep your PIN a secret. Don't use your address, birth date, or phone or Social Security number as the PIN, and do memorize the number. Following are some additional dos and don'ts for preventing payment card fraud.

Do

1. Sign your payment cards as soon as they arrive. This enables the merchant to compare your signature at checkout with the one on the card. It further validates that you are the true account holder.

2. Carry only those cards you need. Keep them separate from your wallet, in a zippered compartment, business card holder, or small pouch. Keep others secured in a locked safe at home or in a safe deposit box to avoid “friendly fraud,” a form of theft committed by people who know their victims and can gain access to their account information.

3. Keep a record — in a safe place, separate from your cards — of your account numbers, their expiration dates, and the phone number and address of the card-issuing bank so you can quickly report the loss of your card or fraudulent transactions.

4. Keep an eye on your card during transactions and get it back as quickly as possible. This reduces the risk of your card or card number being copied without your knowledge.

5. Save your credit card receipts to compare against your monthly statements. Also, if you have any reason to dispute a transaction, having the credit card draft will expedite the process.

6. Shred or cut up old cards — cutting through the account number — before disposing. Also, shred all mail solicitations for payment cards before discarding. Inform the issuer of any cards you wish to cancel. Don’t assume that just because the plastic card is destroyed, no risk remains. Fraud can be conducted using only information related to an account without having physical possession of the plastic card. Only the issuer can close the account. Some issuers may send you a confirmation, via mail or e-mail, when your account is closed. When you close your account, ask your issuer about procedures.

Sign your payment cards as soon as they arrive. This enables the merchant to compare your signature at checkout with the one on the card.

7. If you receive statements by mail, open them promptly and immediately reconcile them with your receipts. Using your issuer's website, you may monitor your account more frequently. Whether you notice a questionable transaction online or on a paper bill, notify your issuer immediately.

8. Notify your card companies when you have a change of address. If you receive a change of address confirmation and you made no such request, contact your issuer immediately.

9. Check ATM or debit card transactions carefully before you enter the PIN or sign the receipt; funds will be quickly transferred from your checking or other deposit account.

10. Call your credit card issuer immediately if you do not receive your monthly account statement as expected. Undelivered statements may indicate a thief has taken over your account and changed the billing address.

11. Make sure you're using a secure site when making payments over the Internet. Look for a lock icon in the status bar of your web browser; this icon indicates that a site is employing an encryption technology when transmitting sensitive data.

12. Periodically change the PIN on your debit and ATM cards.

13. Contact your card issuer in response to letters or phone messages from them. Federal regulations restrict the amount of information that banks can include in their communications to their customers. Don't assume the return call can wait; contact your bank as soon as possible. To ensure you are calling your issuer, and not someone posing as such, call the number on the back of your card or from your billing statement rather than one left in a message.

Don't

1. Leave your cards unattended anywhere.

2. Leave your payment cards in your vehicle. A very high proportion of payment cards are stolen from motor vehicles.

3. Lend your cards to anyone.

4. Sign a blank receipt. When you sign a receipt, draw a line through any blank spaces above the total.

5. Write your account number or PIN on a postcard or on the outside of an envelope.

6. Give out your account number over the phone unless you're calling a company you know is reputable. If you have questions about a company, check it out with your local consumer protection office or Better Business Bureau.

7. Carry your PIN in your wallet or purse or write it on your ATM or debit card.

8. Reveal financial or personal information unless you have initiated the contact. Remember, thieves may pose as representatives of banks, Internet service providers, and government agencies as a way to get you to divulge personal or financial data that can be used to commit payment card fraud. These types of scams, such as "pretexting" and "phishing," can be perpetrated in person, over the phone, on the Internet, and through e-mail.

If You Are a Victim

If you do become a victim of credit card fraud, your maximum liability under federal law for unauthorized use of your credit card is $50 per card. If you report a card lost or stolen before any fraudulent misuse is attempted, the card issuer cannot hold you responsible for any misuse.

When you receive new credit cards, shred old cards before disposing.

For debit cards, liability protection depends on whether the plastic card itself is stolen and used fraudulently. If it is, a time element is added to the protection: If unauthorized activity is reported within two business days, the liability limit is $50. If unauthorized activity is reported within 60 days, the liability limit is $500. If the fraud is reported more than 60 days after the customer received the statement showing the fraudulent activity, the customer's liability may be unlimited on transfers made after the 60-day period. When thieves steal just the account number and use it either on its own or to produce a counterfeit plastic card, customers have zero liability for 60 days from receipt of the statement on which the fraudulent activity is reported and unlimited liability thereafter. For this reason, it is critical to regularly monitor these accounts and the associated statements for unauthorized use and to quickly notify your issuer.

Card issuers often provide greater protections from fraud than are required by law. Therefore, it is important to check with your issuer to confirm its policies regarding consumer liability limits for payment fraud.

For more information on how to protect yourself from payment card fraud or to report an instance of fraud, go to the Federal Trade Commission's website: www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards. The FTC's site also contains information about other consumer-related issues.

To obtain a free copy of your credit report from one or all three of the national credit bureaus, visit www.annualcreditreport.com or call 1-877-322-8228. To request your report(s) through the mail, visit www.annualcreditreport.com/manualRequestForm.action, download the form, print it, fill it out, and then mail it to:

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281

For More Information

The Federal Reserve Bank of Philadelphia has other brochures on credit topics.

To obtain copies of these brochures, or for additional copies of this one, please contact:

Federal Reserve Bank of Philadelphia
Public Affairs – Publications
P.O. Box 66
Philadelphia, PA 19105-0066

215-574-6113

www.philadelphiafed.org

To view this and other consumer publications produced by the Federal Reserve Bank of Philadelphia, scan this code with your smartphone.

FEDERAL RESERVE BANK
OF PHILADELPHIA

Ten Independence Mall
Philadelphia, PA 19106

8/2015