

# 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. The Board writes bank and consumer protection regulations to implement many laws passed by Congress. Fed Governors and Reserve Bank presidents participate in Federal Open Market Committee (FOMC) 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*

Payment card issuers have had some success in limiting payment card fraud by employing sophisticated computer software that helps to identify fraudulent transactions. One indicator may be transactions that appear to be out of line with a customer's past behavior, for example, spending originating in Russia on a payment card never used overseas. Many times, card issuers will call customers to confirm whether suspected fraudulent transactions were made by the cardholder. Without notification from the card issuer, victims of payment card fraud typically recognize the fraudulent activity only when they review monthly statements.

If you suspect fraudulent activity, immediately notify your card issuer and follow up in writing. The card issuer can cancel your card account and send you a new card and number to safeguard your account from further misuse.

The best protection against payment card fraud is to know where your cards are at all times and to 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.
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. Void incorrect receipts and destroy all copies or carbons of receipts so that they do not fall into the wrong hands. Save original receipts to compare against your monthly statements.
6. Shred or cut up old cards — cutting through the account number — before disposing. Also, shred all mail solicitations for payment cards before discarding.

*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. Open monthly statements promptly and reconcile with your receipts, as you would your checking account. If you bank online, check activity in each of your financial accounts regularly. Report any questionable charges immediately by calling the card issuer and follow up such calls in writing.
8. Notify card companies in advance of a change in address.
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.

## *Don't*

1. Leave your cards unattended at work. There are more payment card thefts in the workplace than in any other single location.
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

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



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 the loss before your credit cards are used, the card issuer cannot hold you responsible for any unauthorized charges.

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 liability is potentially unlimited. 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.

Many times, your issuer may provide incremental liability protection above what is 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.ftc.gov/ftc/consumer.htm](http://www.ftc.gov/ftc/consumer.htm). 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 reporting agencies (Equifax, Experian, and TransUnion), visit [annualcreditreport.com](http://annualcreditreport.com); call 1-877-322-8228, or print the Annual Credit Report Request Form from [www.ftc.gov/credit](http://www.ftc.gov/credit), complete it, and mail it to:

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



FEDERAL RESERVE BANK OF PHILADELPHIA

---

Ten Independence Mall, Philadelphia, PA 19106

[www.philadelphiafed.org](http://www.philadelphiafed.org)