

CONSUMER'S EDGE

CONSUMER PROTECTION DIVISION, MARYLAND OFFICE OF THE ATTORNEY GENERAL

ANTHONY G. BROWN, MARYLAND ATTORNEY GENERAL

HOW TO AVOID CREDIT CARD FRAUD

Credit card fraud in the U.S. takes an annual toll of billions of dollars a year. But who pays the price tag? We all do, in the form of higher finance charges, annual fees, and costs for law enforcement.

Con artists commit fraud by stealing and selling credit cards, using counterfeit cards, and operating online or telemarketing scams. Many scam artists find credit cards and account numbers through phishing and other high-tech means, although some thieves still raid mailboxes and trash cans to get this information.

Although credit card companies are working to design more counterfeit-proof cards, you still need to take some simple precautions to outsmart con artists and avoid becoming another victim of fraud.



Protect Your Credit Card

Don't use your credit card on a website that isn't secure. It's much easier for a hacker to intercept your credit card information that way. Secure websites include an SSL certificate; in other words, a secure website address begins with https, rather than http.

Protect your physical credit cards as well by following these simple tips:

- Be aware of when your renewed cards and billing statements usually arrive so you can contact your card issuer if there's a delay.
- Sign new cards as soon as they arrive. Keep a record of all your card numbers, expiration dates, and phone numbers and addresses of the card issuers in a secure place.
- Periodically check your cards to make sure none are missing.
- Make it a practice not to lend your credit card to anyone.

Guard Your Credit Card Number

A consumer received a phone call from a woman promoting discount vacation packages. All she needed was his credit card number and expiration date, she said, to include him in a "special deal" for a Hawaiian vacation. He found out the offer was phony when he never received his airline tickets although his credit card was charged for them.

- Never give your credit card number over the phone or computer unless you're dealing with a company you know.
- Beware of phishing attempts. Scammers often send emails or texts that look like they're from a bank or credit card company and ask you to confirm information. If you get something like this, only use the contact information you already have for the company to verify whether the request is legitimate. Most likely, it isn't.
- Memorize your PIN (personal identification



number) and don't keep it with your card. Don't select a PIN that someone could easily guess, such as your phone number or birthday.

- Watch for credit card "skimmers" when you use an ATM or pay for gas at the pump. Sometimes thieves install a device that steals your credit card number in places like these.
- Be wary of using a credit card on a public computer or public WiFi network. If you do need to make a purchase on a public computer, make sure it does not store or "remember" your information. It's best to avoid making purchases on unsecured WiFi networks (networks that don't require a password to access), as these are particularly easy for hackers to get into.

Use Your Card Wisely

Another consumer was holiday shopping when her wallet was stolen from her purse. She didn't realize until she got home that all ten of her credit cards had been stolen. She was sorry she hadn't left home the eight cards she rarely uses.

- Carry only the cards you most frequently use, and leave the rest at home. If you don't use certain cards at all, cut them up and throw them away.
- Avoid signing blank receipts. Draw a line through any blank spaces above the total when you sign.
- Save all credit card receipts in a secure place so that you can check them against each statement.
- Notify your card company in advance of your change of address so new cards aren't sent to your old address.
- Set up an email or text alert so you receive a notice whenever your card is used.
- If you lose your card or discover it's been stolen, call the card issuer immediately. Most have a toll-free number. By law, you're not responsible for any unauthorized charges from the time you report the loss or theft, so document the date and time you called. If your debit card is used before you report its loss, the most you'll have to pay is \$50 (per card) as long as you call within two days of its theft. Otherwise, you may be liable for up to \$500 if you call before 60 days after the theft, or the full loss if you call after 60 days. Credit card holders may be responsible for up to \$50 if the card is used before they report the theft.
- If you think someone's used your credit card or account number without authorization, notify the card issuer immediately.



HOW TO CONTACT US

Consumer Protection Division

200 St. Paul Place, 16th Fl., Baltimore, MD 21202

- **General Consumer Complaints:** 410-528-8662
Toll-free: 1-888-743-0023 TDD: 410-576-6372
En español: 410-230-1712
9 a.m. to 3 p.m. Monday-Friday
www.marylandattorneygeneral.gov/Pages/CPD/
- **Health Consumer Complaints:** 410-528-1840
Toll-free: 1-877-261-8807 TDD: 410-576-6372
En español: 410-230-1712
9 a.m. to 4:30 p.m. Monday-Friday
www.marylandcares.org
- **For information on branch offices** in Largo, Salisbury, Hagerstown, and a full list of offices across Maryland, visit:
www.marylandattorneygeneral.gov/Pages/contactus.aspx

The Consumer's Edge is produced by the Maryland Attorney General's Office. Reproductions are encouraged.



MARYLAND
ATTORNEY GENERAL
ANTHONY G. BROWN

www.marylandattorneygeneral.gov

