



FIRST AMERICAN

B A N K

HOW TO USE YOUR CARD SAFELY AND SECURELY

Questions & Answers

Q: What should I do to help prevent fraudulent use on my card?

A: Here are some helpful steps you should take to help prevent fraud:

- Sign new cards as soon as you receive them.
- Keep your card account numbers and personal identification number (PIN#) in a confidential place and separate from your cards.
- Check your cards periodically to make sure none are missing.
- Destroy and dispose of copies of receipts, airline tickets, travel itineraries, and anything that displays your card numbers.
- Memorize your PIN.
- Check out unfamiliar companies by calling your local consumer protection agency.
- Don't provide information that you're uncomfortable giving.
- NEVER give anyone the password that you use to log on to your online account or Internet Service Provider.
- Don't provide financial account information unless you are paying for a purchase using that account.

Q: I am worried that fraudsters may now call me since they might have my phone number.

A: Cardholders should be on high alert for suspicious calls. These calls are known as phishing calls.

Q: What is skimming?

A: Skimming is the theft of credit card information used in a legitimate transaction. The thief can use small electronic device (skimmer) to swipe and store credit card numbers. Instances of skimming have been reported where the perpetrator has put a device or group of devices illicitly installed on an ATM. Recently-made ATMs now often run a picture of what the slot and keypad are supposed to look like as a background, so that consumers can identify foreign devices attached.

If you suspect skimming you should get in touch with First American Bank at their toll free number 1-877-537-0531.

Q: What is phishing?

A: Phishing refers to scams that attempt to trick consumers into revealing personal information, such as bank account numbers, passwords, payment card numbers, or Social Security numbers. These scams can be done by phone, email, regular mail and even via text message. In addition to seeking bank information, phishers may also try to obtain your ATM PIN or any other bits of data that can help them build a more complete profile from which they can operate in your name.

Most commonly, phishers target unsuspecting users with fake Internet sites or email messages that look legitimate. This is sometimes referred to as "spoofing." Scammers also may leverage social networking sites, where users are already accustomed to sharing information with others.

Q: How does phishing work?

A: Phishing emails and websites typically use familiar logos and graphics to deceive consumers into thinking the sender or website owner is a government agency, bank, retailer or other company they know or do business with. Sophisticated phishers may include misleading details, such as using the company CEO's name in the email "from" field. Another common phishing tactic is to make a link in an email (and the fake website where it leads) appear legitimate by subtly misspelling URLs or changing the ".com" to ".biz" or another easily overlooked substitution.

Some phishing scams even lure victims by telling them that their information has already been jeopardized. For example, potential victims may receive an email that appears to come from a major bank warning that their account has recently been exposed to fraudulent activity. Users are asked to click a link within the message so they can "confirm" their bank account information. Instead of going to the bank's legitimate website, however, victims are taken to a clever lookalike, where their information actually is routed to the scammer.

If you receive any message asking you to confirm account information that has been "stolen" or "lost" or encouraging you to reveal personal information in order to receive a prize, it may be a form of phishing.

It is important for consumers to know that MasterCard will not call or e-mail cardholders to request their personal account information, and Visa call centers do not initiate outbound telemarketing calls.

Q: How can I reduce my risk of phishing?

A: Always view any phone or email requests for financial or other personal information with suspicion, particularly any "urgent" requests. When in doubt, do not provide any information without first verifying the legitimacy of the request by calling the number printed on the back of your payment card. Find more tips for protecting yourself at <http://www.mastercard.com/hk/consumer/fraud-protection.html>.

Q: If I become a victim of identity theft, how will you help to restore my good name?

A: Working with MasterCard, **First American Bank** offers consumers multiple layers of security protection against fraud, including MasterCard's Zero Liability coverage, the cardholders' ultimate protection. With Zero Liability, consumers are not responsible for any unauthorized purchases made on the MasterCard's Cards.

Q: What can I do to ensure this doesn't happen to me again?

A: While we employ the latest systems and technology to monitor and prevent card fraud and merchants also take the necessary precautions to protect your card information, there are some practical steps you can take to help protect your card information:

- Shop with merchants you know. If a deal seems too good to be true, it probably is.
- Check your account statement promptly and immediately report any transactions that you don't recognize.
- Guard your card-don't use it as collateral or give out your card number to someone calling on the phone, unless you initiated the call for the purchase.
- Check your credit report at least annually to ensure its accuracy.

Q: How do I shopping safely online with MasterCard?

A: MasterCard continues to implement and enforce strict security features for online shopping. For consumers and merchants we have developed MasterCard SecureCode®. When you see the MasterCard SecureCode logo below in a web-shop, it means that you as the cardholder can use a one-time code or security device to purchase. If you have not received information about this, contact your card issuer. In addition, here are steps you can take:

- Check the seller's reputation.
- Learn as much as you can about companies or individuals before you do business with them.
- Check with consumer agencies to find out about complaints.
- See if the seller's Web site has a feedback forum where other people who have done business with the seller can put information about their experience with that seller.
- Ask your friends about their favorite online merchants.
- Stay vigilant. Just because a seller has no complaints or a good reputation doesn't guarantee that things will go smoothly for you.
- Before entering card details;
- Look for padlock symbol.
- Look for MasterCard SecureCode™ sign as an endorsement of retailer's security.

To learn more about an organization:

- Check their Web site for a feedback page where customers can offer complaints or praise.
- Ask others about online merchants and other organizations that they've dealt with.

Q: What should I do if I experience fraud on my account?

A: Please monitor your account, both your monthly statement and/or online statements, and let us know immediately if you see unauthorized purchases. **Our toll free number is 1-877-537-0531.**

Q: Are there any other tips you can provide to reduce my chances of card fraud?

A: Yes. There are several actions you can take to protect your personal information. These tips are also available at <http://www.mastercard.com/hk/consumer/fraud-protection.html>.

*MasterCard's Zero Liability coverage covers U.S.-issued cards only and does not apply to:

- i.* MasterCard BusinessCards or Debit MasterCard BusinessCards issued for commercial, business or agricultural purposes (PLEASE NOTE: Zero Liability does apply to MasterCard credit and debit cards for small businesses); or
- ii.* MasterCard's issued or sold "anonymously" (for example, a prepaid card purchased in a store), until such time as the identity of the cardholder has been registered with the financial institution that issued the card; or
- iii.* If a PIN is used for the unauthorized purchase.

For additional details visit <http://www.mastercard.us/zero-liability.html>. If you have questions regarding Zero Liability coverage or you suspect unauthorized use of your card, **contact your bank IMMEDIATELY** at 1-877-537-0531.