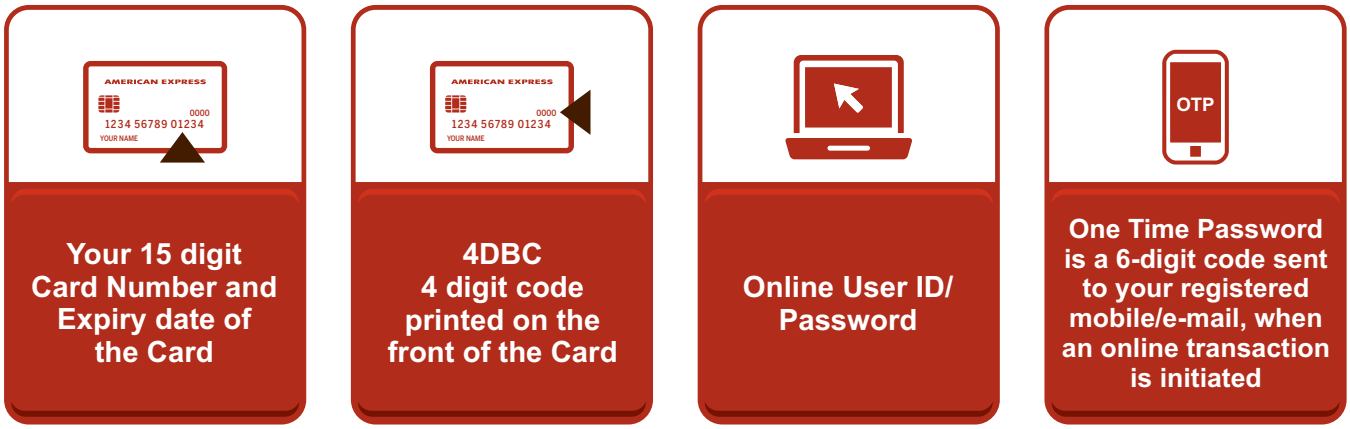
Stay Protected from Fraud

Never share your personal or Card related information when you receive any unsolicited calls, emails or SMS seeking your Card details to offer you an upgrade of your Card, activate or reverse Card transactions or help you redeem your Rewards. Sharing of information listed below could make you a victim of fraud!

Confidential Card information that you should never share via phone, SMS or e-mail:



Your Card security is our top priority. We constantly monitor transactions for out-of-pattern spending for fraud alerts. If you think you may be a victim of fraud, contact the phone number on the back of your Card or you can find other phone numbers in the "contact us" section of our website.

Types of Fraud

Identity Theft

Identity theft occurs when someone uses your name or personal information, such as your PAN number, driving license number, Card number, telephone number or other account numbers, without your permission. Identity thieves use this information to open credit accounts, bank accounts, loan accounts, and make major purchases - all in your name.

How Does Identity Theft Happen?

Identity theft commonly begins with the loss or theft of a wallet or purse. But there are many other ways that criminals can get and use your personal information in order to commit identity theft. The following are some examples:

- Phishing (pronounced "fishing") refers to fraudulent communication designed to deceive consumers into divulging personal, financial or account information. Phishing e-mails continue to be prevalent for individuals and companies. Spoofing well-known companies, these e-mails ask consumers to reply, or "click" a link to a fraudulent web page that will ask for personal information, such as their Card number, PAN number or account password.

  These fraudulent e-mails are often difficult to identify but there are some techniques you can use to protect yourself. Below are some examples:

E-mail Greetings

Always be suspicious of e-mails that do not greet you by name. While not impossible, it is more difficult and costly for phishers to associate an e-mail address with the e-mail owners name on a mass scale. Because of this, phishing e-mails most often are addressed generically like "Dear Customer" or "Dear Cardmember."

If you are concerned about the legitimacy of an e-mail from American Express you can forward the e-mail to phishing@americanexpress.co.in. If the e-mail is fraudulent we will take the appropriate actions.

Sense of Urgency

Phishing e-mails often try to create a false sense of urgency intended to provoke the recipient to take immediate action; for example, phishing e-mails frequently instruct recipients to "validate" or "update" account information or face cancellation. Be very cautious of any e-mail asking you to update sensitive information particularly if it has a generic greeting (see above).

Links in E-mails

Nearly every commercial e-mail today contains a "link to a website," or website address (URL). Links are used by business as a convenience for their customers to help them easily find information the customer is looking for. Unfortunately, phishers also use links to drive customers to "fake" or "spoofed" websites. Look for the warning signs outlined above (generic greetings, sense of urgency). If you are suspicious of the e-mail, do not click on any links contained in it. Instead, go to the website by using your "favorites" if you have it saved, or type the website's URL directly into your browser.

What Should You Do If You Suspect an E-mail Is a Phishing Attempt?

If you are suspicious of an e-mail you receive, you should forward the e-mail to the legitimate company being impersonated. Today, most major brands have an e-mail address where you can forward the suspicious e-mail.

If you receive an e-mail claiming to be from American Express that you believe to be suspicious, please forward the e-mail to phishing@americanexpress.co.in. We will review the e-mail and, if it is fraudulent, we will take appropriate action.

What should you do if you entered sensitive information into a fraudulent website?

If you have already responded to an e-mail with your American Express account information and you believe it to be fraudulent, please contact American Express immediately by calling the number on the back of your Card.

- Phone Phishing (also called "Vishing") is another way fraudsters try to collect sensitive information from you. In this type of fraud, the fraudster will either contact you by telephone or send you a fake e-mail and ask for you to respond by telephone.

If you are ever in doubt about American Express contacting you by phone, simply call the number on the back of your Card or on your account statement. Be sure to enter your account number when prompted and you will be routed to the correct department for assistance.

What Should You Do If You Supplied Sensitive Information over the Phone to a Suspicious Party?

If you have already responded to a suspicious caller with your American Express account information and you believe it to be fraudulent, please contact American Express immediately by calling the number on the back of your Card.

Card Fraud

Card fraud strikes millions of times every year and is one of the fastest growing white-collar crimes. The information and services in the Fraud Protection Center can help reduce your chances of becoming a victim.

Card Fraud happens whenever someone obtains your Card account number, and then uses it to make fraudulent purchases.

This can happen if:

- A dishonest store clerk makes an extra imprint of your Card.
- A thief gets your account number and expiration date from a discarded receipt.
- A restaurant cashier swipes your Card in a small handheld device known as a skimmer, which copies the information on your Card in order to make a counterfeit copy of your Card. This method is called "Skimming".
- You were a victim of a phishing scam.

Remember that when you use your American Express Card, you are not liable for fraudulent purchases. In addition, American Express has sophisticated monitoring systems and controls in place to detect fraudulent activity and protect our Cardmembers' accounts from misuse. If we discover activity on your account that we believe is suspicious, we will contact you.

Protecting Yourself

There are some simple and important steps you can take to help reduce your risk.

- **Monitor Your Account Activity Online.**

Accessing your account online is a great way to stay up to date on recent charges and monitor your account for irregular activity. To enroll to Manage Your Card Account online, go to www.americanexpress.co.in

- **Create Unique Passwords and Personal Identification Numbers**

Avoid using easily available information such as date of birth, or the last four digits of your Birth Year when creating passwords and personal identification numbers. Use different passwords on your various banking accounts, and update all of your passwords regularly.

- **Bookmark the Websites You Visit Most in Your Favorites**

Get in the habit of using your favorites to navigate to the sites you use to perform financial transactions such as your bank or Card.

- **Set Up "Remember Me" on Websites You Visit Regularly**

Have the American Express website remember your User ID on your computer, so when you return your User ID will automatically entered into the Sign In box. A fraudulent website (spoof site) will not be able to display your User ID, le website. Note: You should not use the Remember Me functionality on a public or shared computer, like at a public library.

- **Secure Your Personal Information at Home and at Work**

Consider keeping your sensitive personal information such as bank, mortgage, and Card statements, PAN number, and other documents and passwords, in a safe location accessible only to you both at home and at work.

- **Shred Documents Containing Your Personal Information**

Identity thieves have been known to obtain discarded documents with personal information. Before discarding documents containing personal information, consider shredding them first.

- **Avoid Giving Out Personal Information Over the Phone**

This is especially true when the telephone call is initiated by another party. Identity thieves may pose as a representative of a legitimate organization with whom you do business and may contact you to "verify" your information. If you are contacted by someone who claims to be from American Express, you can call the number on the back of the Card and enter your account number. You will be routed to the appropriate department for assistance.

- **Before Disclosing Any Personal Information**

Make sure you know why it is required and how it will be used. Do not give out your Card number, account number or PAN number to people or companies that you do not know.

- **Carry Only The Information You Need**

Only take with you the Cards you need, and avoid carrying your PAN card, your birth certificate or passport, except when necessary.

HOW WE PROTECT YOU

ONLINE PROTECTION

American Express takes online security very seriously. Below are some examples of the ways we protect your account online.

- **Self-Selected User ID and Password**

When you sign up to manage your account online, American Express lets you create your own User ID and password to access your account. This information is encrypted during transmission using 128-bit encryption technology.

- **Secure Website for Servicing Your Account**

American Express uses 128-bit Secure Sockets Layer (SSL) technology. This means that when you are on our secured website the data transferred between American Express and you is encrypted and cannot be viewed by any other party.

- **Automatic Time-Outs**

When managing your American Express account online, your session will automatically end if you do not perform any transactions for 10 minutes. To continue using the online system, you will need to re-enter your User ID and password.

- **Remember Me**

Have the American Express website remember your User ID on your computer, so when you return your User ID will automatically be entered into the sign in box. A fraudulent website (spoof site) will not be able to display your User ID; this lets you know you are not on the genuine American Express website. Note: You should not use the "Remember Me" functionality on a public or shared computer, for example, at a public library.

Purchase Protection Services

American Express goes to great lengths to protect your Card from fraudulent use. Below are some examples of the ways we protect your card from fraudulent use.

- **American Express SafeKey**

Your online shopping is absolutely safe and secure as SafeKey prompts you with a one-time password for every transaction so that you are protected against online frauds.

- **Fraud Protection Guarantee**

Our Fraud Protection Guarantee means you won't be held responsible for any fraudulent charges when you use your American Express Card. No fine print, no deductible - just pure protection so you can shop with confidence anywhere, online or off.

- **Authorized User Verification**

When you use your American Express Card at some retail or online stores, you may be asked to provide your full billing address and/or "CID" (Card Identification Digits). American Express compares that information with the address or CID on file to help confirm that it is you using the Card. This information is for security purposes only. It will not be used for marketing purposes, and is not retained by the merchant.

- **Monitoring Your Account for Suspicious Transactions**

American Express has sophisticated monitoring systems and controls in place to detect fraudulent activity and protect our Cardmembers' accounts from misuse.

- **Irregular Account Activity Alert**

If we detect a questionable transaction on your account, we will contact you to verify its legitimacy.

- **Account Alerts**

Stay in control of your accounts with Account Alert e-mails or text messages. You can sign up to receive e-mails or text messages to notify you when your payment is due, when your payment is received, and to inform you of your current balance.

If You Are a Victim

What To Do If You Are a Victim of ID Theft

- **Contact the Police**

Contacting the police allows them to start investigating the crime. You should also obtain a copy of the police report. Banks, Card companies, and other agencies may require this information as proof of a crime.

- **Close Suspect Accounts**

Close the accounts you know or suspect involve identity fraud.

- **Credit Accounts and ATM Cards**

Report the incident to all institutions with which you hold Card and ATM cards. Ask the financial institution or agency to send you a fraud dispute form to complete. When reopening new accounts, be sure to use new PINs to reduce the risk of future identity theft.

- **Keep a Record of Your Actions**

Keep a file of documents related to the identity theft. You will want to include documents such as disputed bills, credit reports, police reports, and any correspondence.

Maintain a record of your telephone conversations with the persons and agencies you contact for assistance. Be sure to record the date and time of the call, the name and title of the person you spoke with, and the things you discussed.

Follow up all telephone conversations in writing and send these letters certified with return receipts requested; maintain copies of these written correspondences for your file.

Keep original documents for your file, mail only copies.