if you need to obtain credit in the future.

How does identity theft work?

Thieves use a variety of tactics to access your personal information. They may pose as someone with a legitimate need to gain access to financial data. Or the criminal could be a roommate, a worker in your home, or a friend who can easily get his or her hands on your documents. Identity thieves may even resort to rummaging through trash for pieces of non-shredded personal information, a tactic known as "Dumpster diving." Data breaches are another way your information may become exposed.

Tips to avoid Identity theft

There are a few basic practices you should follow to increase your card safety.

Monitor your credit card and account statements online on a weekly basis.

Report lost or stolen cards immediately and cancel all inactive accounts. When using your card at checkout, do not volunteer any personal information.

If you've applied for a new card and don't receive it in a timely manner, or if a replacement card is not received prior to your card's expiration date, contact your financial institution immediately. Be sure to sign new cards upon receipt, too.

Shred sensitive documents before disposing of them

Install anti-virus and anti-spyware software on all computers, and change your passwords regularly

Cancel all inactive accounts

Review statements for unauthorized or unusual activity

Try to resolve issues with the merchant first; if unsuccessful, contact your financial institution

MAIL & PHONE FRAUDS

What are common mail and phone frauds?

Identity thieves may send official-looking letters and pose as representatives from Visa or financial institutions. If you're asked to provide your account number or other personal information in a reply envelope or by dialing a number, it could be fraud at work.

How do phone and mail fraud scams work?

Mail and phone frauds can take the form of get-rich-quick schemes, fake charity solicitations, requests for shipping expenses to send a prize, and many other variations in which the victim sends money and receives nothing. Identity thieves may also ask victims to provide account numbers or other personal information in a reply envelope or on the phone

Tips to avoid mail and phone fraud

Consumers should not respond to any e-mails or phone calls with requests for any personal card information and are advised to immediately report the situation to their financial institution that issued their card by calling the number on the back of the card.

You should never give out account or personal information over the phone or in response to a mailing unless you initiated the communication yourself or have positively verified the source.

Notify your financial institution if you change your address

On the phone, don't be afraid to ask questions, including asking for a number to call back. Get details—If the caller can't answer, it's not legitimate

Don't feel obligated to provide card numbers by phone

Did you know your cards have a multi-layered protection?

3-Digit Security Code This code on the back of a Visa card confirms that the card is in a cardholder's physical possession for online and phone purchases.

Verified by Visa Activating Verified by Visa gives online transactions an extra layer of protection by allowing cardholders to select a personal password that confirms their identity at the checkout of participating merchants.