MASTER YOUR CARD

A public education campaign brought to you by MasterCard

SLEEP EASY: CARD SECURITY NEVER SLEEPS

Given recent data breaches at major retailers, it's understandable that you might feel anxious about using cards, but rest easy—cards are still your safest choice, far safer than cash or checks.

The network has you covered. MasterCard's electronic payment technology works tirelessly to ensure that every transaction made on its network is safe, smart and simple. In fact, breaches don't happen at the network level—they happen when businesses, banks or cardholders make errors. In the unlikely event your card data is compromised through someone else's errors, you're covered by MasterCard and other networks with a zero-liability policy guaranteeing you won't be responsible for any fraudulent charges.

Businesses are required to keep you covered. MasterCard and other networks require that each business using the networks is required to meet security standards to keep your account and identity safe. Breaches happen when businesses don't follow these guidelines or make an error. Networks work constantly with businesses and banks to make them aware of new scams and attacks, often preventing or stopping them before anyone else even realizes what is happening. Businesses are held accountable for their errors, paying fines and higher rates when they expose their customers to fraud and crime.

You can cover yourself. The first thing you can do is use credit, debit and prepaid cards wisely to protect yourself. Credit cards provide the best protection—your money cannot be stolen because credit transactions don't involve your bank account. Federal law limits your liability for fraudulent purchases on cards—but MasterCard and others go a step further with zero-liability policies that protect you completely. When it comes to checks, payment cards are safer because they never expose your account information and address to criminals. Prepaid cards are completely anonymous and can be frozen if lost or stolen so you can recover your funds on a new card. Unlike cash, payment cards leave a trail and allow you to recover funds if lost or stolen—not only that, card security often prevents unauthorized purchases in the first place.

TIPS TO HELP YOU COVER YOURSELF.

- Keep an eye on your card during the transaction and get it back as quickly as possible.
- Check your bank statement frequently—you can typically monitor this online or from your phone. Report any questionable charges promptly and in writing.
- Monitor your credit history at www.annualcreditreport.com and dispute any inaccuracies immediately.
- Change the PIN on your credit and debit cards periodically.
- Guard the personal information stored on your phone and computer with complex passwords that are difficult to guess.
- If someone phones or emails saying they are from your bank and need personal or account information, call your bank directly. Banks and card companies won't make requests by email or over the phone, so verify payment and information requests and get them in writing.
- Do not volunteer details or fill in the blanks (name, relationship, financial or personal information) if someone calls asking for help from family or friends. Fraudsters use this information to guess your passwords and steal your identity.
- Keep a record of your account numbers, expiration dates and the contact information of each card company in a secure place.
- Avoid sending checks in the mail and never write your account number on a postcard or the outside of an envelope.
- Don't sign a blank receipt. When you sign a receipt, draw a line through any blank spaces above the total.
- Don't conduct financial transactions over public Wi-Fi or Internet connections that are not protected by a password.
- Only make purchases on websites that look reputable. You can check a site's validity at www.siteadvisor.com.

If you think you've been scammed or targeted by a fraudster, report it immediately to the Federal Trade Commission (FTC). You can forward spam emails to spam@uce.gov. You should also report fraud to the authorities, such as the police and postal inspector, and the credit reporting bureaus.