A New Way of Stealing Your Credit/Debit Card

If you've owned a few credit or debit cards, you know exactly how different they look depending on the brand. One day, you decide to go out to eat at a restaurant. You've finished your meal and the bill arrives at your table. You decide to pay using either a debit or credit card. The server picks up your check and credit/debit card and walks away to authorize the card for payment. The server returns to your table with your receipt to sign, and a credit or debit card. You sign the receipt, and slip the card back into your wallet, same as always.

The next time you attempt to use your credit or debit card, it's declined and you notice, that although it is the same brand and looks the same, it's not your card. You call your card company and learn the maximum limit has been spent on your card since the last time you used it.

This is one of the latest scams in card fraud and it's called a "card switch".

The scammer has a collection of cancelled or declined cards and waits for someone to give him or her an identical brand card. When a customer pays with a card similar in appearance, the scammer steals the new card and substitutes a cancelled or declined card. If the victim fails to notice at the time of payment, the thief is able to go on a shopping spree.

Develop the habit of checking your credit or debit card each time it is returned to you after a transaction to make sure it is yours.

Check the name on the card every time you sign for something and/or the card is taken away for even a short period of time.

Make sure the credit and debit cards in your wallet are yours.

If need be, cancel your current card with your credit union and have a new card re-issued.

Using your Debit/Credit Card Safely

As the new year begins, so do the opportunities for fraudsters to take advantage of unsuspecting consumers while using their debit and credit cards.

Using your credit or debit card in public places doesn't always mean you are safe. Information/identity theft can take place just about any time or anywhere – at an ATM, in your favorite coffee house or eatery, or when you're buying something online.

You don't have to lose your debit or credit card to become a victim of card fraud. Thieves have their clever ways and have become proficient at skimming and copying your card information from a machine at a merchant. The scary thing is that card fraud can take place without you or store employees even knowing it. Once your card number has been copied, the thieves will then be able to obtain this information from a remote location and produce a fraudulent copy of your card.

Here are some tips for protecting your credit and debit cards:

Keep Your Card in Sight. When using your debit or credit card at a merchant/store, keep it in sight at all times. A common way to steal debit or credit card information is called 'skimming' or 'swiping,' where thieves pass your card through a device that reads and records the information from the magnetic swipe.

Keep Your PIN a Secret. Never write it on your card or store it with your card. Don't give your PIN over the telephone. No company or person should ever ask for your PIN. If you use your debit card to make a purchase by phone, never disclose your PIN.

Watch Your Email. Don't provide your debit or credit card number, PIN or other personal information in response to an unsolicited email or online request. It is highly recommended to have different PINs for different accounts. And it's a good idea to change your PINs often.

Be Smart Online. When shopping online look for secure transaction symbols, such as the little 'lock' logo in the lower right-hand corner of your browser window and web addresses that start with 'https'. Log off from a site after you complete a purchase, and if you can't log off, close your browser to protect your personal information.

Don't Wait. If your card is lost or stolen, report it to your credit union right away. By notifying your credit union immediately, you can reduce the chance that your card will be used improperly. And, you can limit your potential liability – the money you actually lose for unauthorized transactions by scammers or hackers.

Keep an Eye on Your Money. **Review account statements from your credit union when you get them.** Or better yet, sign up for electronic banking to get secure online access to your account day or night. Report any problems, including transactions you think may be unauthorized, right away. Quick action can limit misuse and save you money.

Cardholder Prevention Strategies

- Close all unused card accounts
- Review credit report frequently
- Review all monthly statements
- Do not give account numbers over the phone without knowing caller
- Keep personal records in a secure location
- Do not provide personal information on solicitations
- Destroy all pre-approved applications
- Be aware of when to expect new plastics and report when they have not been received
- Report all mail theft to a postal inspector
- Carry only cards that are used frequently
- Do not write your PIN on your card
- Keep a list of account number with their lost/stolen numbers
- Do not leave plastics with another person
- Use one card for internet purchases
- Check for secure websites
- Keep a record of all internet transactions
- Pick up mail promptly
- Inform the Post Office when planning out of town trips

Tips to Avoid Being Skimmed

- Inspect the ATM, gas pump, or credit card reader before using it. Look for anything that may be loose, cracked, or damaged, or if you notice scratches or adhesive tape residue
- Block the keypad with your other hand when entering your PIN number to avoid any possible hidden cameras from recording your number
- Get in the habit of using the same ATM machine for your transactions
- Try to use an ATM at an inside location rather than on the street. It may be less accessible for criminals to install skimmers
- Never use an ATM when other people are lingering
- If your card is not returned after processing the transaction, immediately contact your financial institution

- Retain your ATM receipts and check them against your monthly statements each month. If anything looks irregular or if there are any unauthorized transactions report them to your financial institution immediately.

For Pay-at-the-Pump Fuel Dispensers

- Do not pay at the pump
- Only pay at pumps that are well monitored, well lit and busy locations
- Observe individuals using the pump prior to your use to ensure they haven't tampered with it
- Always check pump for evidence of tampering

Cell Phone Camera Scam

- While paying for a purchase with your card, someone could be nearby using their cell phone to take a picture of your card number, expiration date and name

Card Switch

- After making a purchase, the wrong card was intentionally returned to you. It's been replaced with a cancelled or declined card, and if unnoticed at the time of the transaction, the fraudster can go on a shopping spree with your card.

Restaurant and Store Skimming

- Small, pocketable skimming devices, which can be used by restaurant servers and store cashiers. Do not let your card out of your sight