

# FOCUS ON FRAUD!

AREN'T THEY GREAT? Our debit cards surely have made life a lot better, right? You use them to get ATM cash anywhere for the lowly cost of a half a buck (if you use the freebie terminals we've identified), make purchases all over the world without writing a check, and yet pay no fees for having these conveniences!

"Yes they are," you say! BUT they also EXPOSE YOUR FUNDS to all kinds of FRAUDULENT actors! And neither the theft of your funds or the hassle involved in trying to resolve your fraudulent charges is anything you want to face. So, here are some precautions you can take to protect your funds!

YOUR FIRST STEP is to fill out the form on the back of this newsletter so you'll have details if your card is lost or stolen! THEN, on a regular basis—

- Check your **account** balance and **activity** frequently. (Thank heaven for "CU-at-Home" on-line access!)
- **CHECK YOUR STATEMENTS!**
- Be careful **where you use** your card—perhaps you should use a credit card instead at stores where you don't regularly shop or websites you might not trust.
- **Keep receipts** or other records of your card activity.
- **NEVER WRITE YOUR PIN** on or near your card!
- **NEVER GIVE YOUR CU account information** by phone/internet unless YOU initiate the contact or you trust the other party. WE WON'T ASK; don't fall for calls from others who ask you to "verify such information"!
- On the rare occasion when you use your PIN, be careful! **Shield your number** selections from view.
- When you give your card to wait staff/clerk, keep your eye on how your card is used. Thefts occur if your card is swiped in a second scanner; extra copies of sales slips are made, or numbers/codes are written to **SKIM** your card info. A debit card swipe without a PIN is called an "off-line" transaction; and when such transactions also don't require a signature, a thief who has merely your card information **can drain your checking account—even if your card itself or PIN hasn't been stolen!**
- **PURCHASES ON LINE** make your debit card particularly vulnerable. When you order online, check if you are on a **secure server** by looking for a security symbol such as an unbroken key or padlock symbol at the bottom of your internet browser window. Also make sure that you look for "**checkboxes**" of any kind that, if ignored, could enroll you in a "partner" company's 'membership,' with its monthly card billings!
- Sometimes fraudulent charges appear *no matter how careful you are!* In that event, you should IMMEDIATELY CALL Fifth-Third Bank at **800-927-0395, Extension 1**. You must have your card details on hand to give the operator, so we hope you've taken our advice and recorded those details.
- IF YOU GET NABBED BY FRAUDULENT ACTORS, be sure that YOU CALL THE PHONE NUMBERS that appear on your statement to demand your money back; but, *more importantly*, to CANCEL ANY MEMBERSHIPS that were probably created by the fraudulent charge!

NOW, go ahead and fill in the form below. If your card is STOLEN, you'll be happy that you did! (Or photocopy both sides & keep your copies in a safe place!)

My card's "Security Code" is \_\_\_\_\_

If compromised, call 800-927-0395 X1  
then 800-869-8920, then either CU  
office at 836-4809 or 945-4000.

