

**Plastic card fraud continues to escalate, and all cardholders, whether credit or debit, are vulnerable. You probably won't end up paying the bill, but stolen card or account information can still cost you big- in time and aggravation. Here's how to protect yourself.**

### **Protect Your Account**

- ☠ **Beware of “phishing” e-mails or phone calls.** These are made to look as if they're coming from your financial or credit card issuer and usually urge you to take “immediate action” so that your card or account isn't deactivated. The link in the e-mail takes you to a criminal's web site, where you're encouraged to input your account number and other personal financial details. MCCU, VISA<sup>®</sup>, or any legitimate company will NEVER contact you via email, mail, or phone to ask you to confirm your account number and especially your password or PIN number. DO NOT respond to emails, or pop-ups asking for information, even if it looks legitimate. Contact us, or the company being referred to, with a contact number that you have record of.
- ☠ **Beware of pop-ups on web sites.** These pop-up's may ask for personal information, or to re-enter your account number or password. MCCU will NEVER have a pop-up appear on the Internet Account Access or Express Pay programs. DO NOT respond to these.
- ☠ **Be cautious shopping with unknown Web sites.** If you're making a transaction be sure to look for the secure padlock on the lower part of your browser, and the web site address starts with “https” rather than just “http”, (s stands for secure).
- ☠ If you feel that you may have inadvertently entered your account information or password on a bogus site, or merchant—contact your financial institution ASAP. You will receive help to protect your account and identity before losses occur.

Be sure that all of your financial institutions have the appropriate numbers to contact you. Your credit union will do its best to protect your account and if something does not look right, we will attempt to contact you.

## Protecting Your Account

- **Don't forget your card.** You might be rushed or distracted, or involved in an interesting chat with the clerk. Whatever. Keep your eye on your card and make sure it goes back into your wallet.
- **Shield your card.** Using a camera phone, it would be a easy to snap a picture of your card if it were left in plain view.
- **Don't give your number out to solicitors.** If a solicitor contacts you by phone to offer you a “great deal”, be sure you know they are legitimate.
- **Consider carrying fewer cards.** Reduce your exposure by limiting the number of cards a thief could potentially steal.
- **Know what you carry.** Every once in a while, make a list or copy of the card numbers and the contact information of the issuers in case your card is lost or stolen. Be sure to keep this list in a secure place, not in your purse or wallet.
- **Know when your statements should arrive.** Missing statements could indicate that someone has stolen your mail or redirected it to a new address. Your MCCU account statement should arrive by mail within the first 10 days of the new month, or the first business day of the month by email. Your MCCU VISA<sup>®</sup> statement should arrive by mail around the 25th of the month, regardless of account activity.
- **Review your records and statements.** At the very least, scan each charge to make sure the merchant and the amounts are correct.
- **Report any suspicious or unauthorized charges.** Call the issuer promptly and follow up in writing. Use the company's address for “billing inquiries”, which you'll find printed on your statement or in your account agreement; it's usually different from the place you send your payment. Keep copies of all correspondence with the issuer and any merchants involved.
- **Shred, Shred, Shred.** Even a basic \$20 shredder will do the job. Destroy all old credit card receipts, applications and anything that includes sensitive financial information, such as your Social Security number.