# Hopewell Federal Credit Union
# Federal Financial Institutions Examination Council (FFIEC)
# Member Education

Hopewell Federal Credit Union (HFCU) is committed to preserving your privacy and security. With more consumers using the internet to conduct banking transactions, unscrupulous individuals are busy developing new scams targeting the unsuspecting public. One of the best ways to avoid fraud is to become an educated consumer and we would like to help you in this endeavor. Please take a moment to read this important information on how to keep yourself safe when conducting business online.

**Protections under Regulation E**

Regulation E, also known as the Electronic Funds Transfer Act, outlines the rights, liabilities, and responsibilities of consumers that use electronic services as well as the financial institutions that offer electronic services. Electronic Fund Transfer services include, but are not limited to, debit card, MAGIC, Hopewell Online Banking, Bill Pay, Mobile Banking, Automated Clearing House (ACH), and Automated Teller Machine (ATM) transactions. These rights, liabilities, and responsibilities are described in the Electronic Funds Transfer Agreement and Disclosure that you received at account opening.

**Contact with HFCU**

Hopewell Federal Credit Union is committed to preserving your privacy and security. Please remember, HFCU and its affiliate partners will **NEVER** request your sensitive account information via text, phone or email. HFCU will **NEVER** contact you and ask for your user name, password, other online banking credentials, credit or debit card number, or PIN.

Our Fraud Prevention provider, Card Services, may contact you on behalf of HFCU to verify unusual credit or debit card transactions. Card Services will **NEVER** ask for your card number, expiration date, security code, PIN number or online banking credentials. They may ask to verify your address, the last four digits of your Social Security Number, the last four digits of your card number, and/or the amount of your last valid transaction or payment. If you are uncomfortable with the call, please hang up and call them back on the 1-800 number of the back of your card.

**Tips for Keeping Your Information Safe**

- **Set good passwords.** A good password is a combination of upper and lower case letters and numbers and one that is not easily guessed. Change your password frequently. Don't share your password with others.
- **Safeguard you PIN.** Never keep your PIN with your debit card as you may be liable for unauthorized use.
- **Don't reveal personal information via email.** Emails and text messages can be masked to look like they are coming from a trusted sender when they are actually from

someone else. Play it safe, do not send your personal information such as account numbers, social security numbers, passwords etc. via email or texting.

- **Don't download that file!** Opening files attached to emails can be dangerous especially when they are from someone you don't know as they can allow harmful malware or viruses to be downloaded onto your computer. Keep your home and work computers safe with current technology solutions, including gateway routers and virus/malware/spyware detection software, which will help prevent virus infections and warn when you are attempting to access a known phishing site.
- **Links aren't always what they seem.** Don't use links in messages, even if the message appears to come from HFCU. Enter HFCU's web address in the browser yourself. Phishers can make links look like they go one place, but it actually send you to their legitimate-looking fake site. Ignore e-mails or pop-up messages that request personal or financial information.
- **Web sites aren't always what they seem.** Be aware that if you navigate to a website from a link you don't type, you may end up at a site that looks like the correct one, when in fact it's not. Take time to verify that the web page you're visiting matches exactly with the URL that you would expect.
- **Logoff from sites when you are done**. When you are ready to leave a site you have logged in to, logoff rather than just closing the page.
- **Monitor account activity.** Review credit card and account statements, as well as online transaction, as soon as they are available to check for unauthorized charges and report any unauthorized transactions immediately.
- **Assess your risk.** We recommend periodically assessing your online banking risk and put into place increased security controls where weaknesses are found, particularly for members with business accounts. Some items to consider when assessing your online banking risk are:
    - Who has access to your online business accounts?
    - How and where are user names and passwords stored?
    - How strong are your passwords and how often are they changed? Are they changed before or immediately after terminating an employee who had access to them?
    - Do you have dual controls or other checks and balances with respect to access to online banking transactions?
    - Do you have antivirus protection on your computer?

**Additional Resources**

If you've been scammed, visit the Federal Trade Commission's Identity Theft Web site at www.ftc.gov/idtheft for assistance. Also, file a complaint on the Federal Bureau of Investigation's Internet Crime Complaint Center Web site, www.ic3.gov/.

Please check out the following websites for additional information:

www.staysafeonline.com
www.usa.gov
www.idtheft.gov
www.onguardonline.gov

If you should notice any suspicious account activity or experience any information security-related events, please contact Hopewell Federal Credit Union immediately at (740) 522-8311.