Fraud and Your Responsibilities

You're in Charge

Credit Union members are responsible for every check they deposit. That means fraud victims MUST repay the Credit Union for bad checks. Credit Unions are required by law to make the funds from checks you deposit available to you quickly. This "hold" period is no guarantee that a check is good. It may not be long enough to reveal that a check is fraudulent. Credit Unions often release funds from a cashier's check or money order before it clears.

Remember: Just because you can withdraw the money does not mean the check is good. In any case, the victim of fraud must refund the full amount to the Credit Union.

Checking Scams

Although they vary in the details, fake check scams involve stolen, forged, or counterfeit checks or money orders. The victim deposits the check into a personal checking account, sometimes as payment, sometimes as a favor to the fraudster. When the money is available and posted to the account, the victim wires the money to the criminals, usually keeping a small percentage as payment.
Cashier's checks and postal money orders are often considered to be as good as cash. In reality, they're only as good as the person sending it to you, whether it's a legitimate buyer or an online acquaintance.

Growing Fraud Schemes

Deposit Fraud

In deposit fraud, the victim opens a new bank account at the request of the con artist. This account's sole purpose is to process the crook's fake or stolen check. In return, the victim is promised a commission or a percentage of the money. The victim is instructed to withdraw the funds and transfer them to another account once the check or money order is deposited into this account. When the check is returned to the credit union unpaid, the funds are long gone and the victim must repay whatever amount the criminal stole.

Fee Fraud

This ever-evolving scheme has many variations. In essence, the victim pays money or provides something of value in anticipation of receiving something of greater value, such as a gift, loan, investment, or contract. The victim receives little or nothing in return.

Often, the con artist may promise the victim a payoff that involves lottery winnings, "found money," an inheritance, or some other vague opportunity that sounds too good to pass up. The victim may be asked to sign documents and pay a "finder's fee" in advance of receiving a service, such as a financing agreement or a "foreclosure rescue." Victims find that they are ineligible for this service or that the service does not exist – only after the victim has paid the fees.

The Rent Scam is another a type of Advance Fee fraud to be aware of. In this scam, a "landlord," often advertising on an online classified ad site, hooks potential renters

on the perfect property at a great price. The red flags start when the potential renter is not able to see the inside of the property yet is asked to pay the rent in advance, possibly by wiring funds or sending them through services, such as Money Gram. Only after the money is gone, the renter then finds out that the "landlord" is in no way authorized to rent the property.

To avoid falling prey to an Advance Fee scheme, look for telltale signs. You should rarely pay for services before they are rendered. Offers that appear too good to be true are often just that. Legitimate business is rarely conducted in cash or on the street. Research a business or individual to verify credentials. Check the Better Business Bureau and consult your credit union or an attorney. Be sure you understand any business agreement that you enter into before signing anything. If the terms are complex, have an attorney review them.

Online Auction Overpayment Scam
You sell or auction a product over the internet. The buyer "overpays" in error. He requests that you wire the excess amount to the buyer or to a third party. In turn you send them product and the excess funds, only to find out the check is no good and you are responsible for the entire check, as well as, the merchandise you lost.

Internet Relationship Scam
There are various versions of these scam. However, they all involve an online relationship established via Facebook or an online dating site. As the relationship progresses, the scammer tells of hardships and money needed in order for them to come to visit. Money is wired or account information is given in order for counterfeit checks or money orders to be deposited via remote deposit capture.
In all such cases, the credit union will discover that the check or money order is counterfeit or stolen and the item is returned unpaid. The member will discover they've been duped when their online acquaintance doesn't come to visit.

Ways You Can Protect Yourself

- Verify the source of all checks that you deposit into your account. Fake money orders are common con artist tools.
- Be wary of offers that require you to wire money or transfer funds.
- There is no legitimate reason someone would give you a check or money order and ask you to wire money anywhere in return.

What to Do if You've Been the Victim of Fraud

Contact Bayer Heritage FCU Immediately!
If you think unauthorized access or fraud has occurred in connection with your Bayer Heritage FCU accounts, report such incidents to your closest Bayer Heritage FCU branch or call the Fraud Squad at **1-800-272-6003 x1493**.

File a complaint with the Federal Bureau of Investigation's Internet Crime Complaint Center at: www.ic3.gov

Contact the Federal Trade Commission's Consumer Sentinel Center at: www.ftc.gov/sentinel