ROYAL CREDIT UNION

FRAUD: MEMBER ACTION PACKET

INDEX

BASICS OF IDENTITY THEFT

Know the basics. Know how to minimize your risk.

You may have fallen victim to fraud and this document is intended to help you resolve that. We want to help you know what to do when you are a victim of fraud. Part of that is knowing how to better safeguard yourself against all forms of fraud, including identity theft, in the future so that you never again have to experience a situation like this.

At Royal Credit Union, we're dead serious about protecting the non-public information we have gathered from you, our Member. We do many things to protect our Members information both technically and through controls within our operation.

Though Royal is committed to protecting your information, there are other ways for your information to get in the wrong hands. We have the appropriate controls in place to protect your private information from being leaked from us, but that is only half the battle when it comes to Identity Theft.

You need to do a number of things to help protect yourself from having your personal information put in the wrong hands. Below are some of the steps Members should follow to help protect themselves:

- **Mail bill payments at the Post Office or secure postal station**
- **Don't leave mail in your mailbox any longer than necessary**
- **Be aware of surroundings when you use credit/ debit card**
- **Don't give personal information over phone or electronically**
- **Shred your junk mail**
- **Look at statements for unauthorized transactions**
- **Review your credit report at least annually**
- **Know the companies you do business with**
- **Be skeptical about unsolicited contacts**
- **Only keep what you need in your wallet**

Remember: Should you become a victim, we're here to assist you in the proper steps necessary to minimize the damage.

SECURE YOUR ONLINE IDENTITY: PASSWORDS

Maybe you've already taken all of these steps, or the nature of the fraud wasn't physical. In an ever-changing world, more and more everyday activities, both personal and financial, are conducted electronically or online.

Because of that, it more important than ever before that you take the necessary steps to protect yourself by strengthening your online security. The best way to do that is by reviewing any/all passwords that you use to access any sensitive information, personal or financial, when you're online.

Passwords may be a hassle, but they are one of the best defenses against identity theft. The problem is, all too often we take the easy way out and use a weak password that is easily guessed by cyber thieves. The key to a strong password, according to Microsoft, is to use a variety of characters and make it both random and lengthy. The greater the variety, the better:

- **Combine letters, numbers, and symbols.** Each character you add increases your protection from fraud. A password without symbols needs to be considerably longer to have the same degree of protection as an eight-character password with symbols.
- **Randomly capitalize some letters.** Sprinkle them throughout your password.
- **Stray from typical symbols.** Don't forget about punctuation marks, slashes, dashes and brackets – symbols not on the upper row of your keyboard.
- **Use a phrase or sentence to help you remember.** Here's one example, "My #1 dog is a cross between Boxer/Lab," becomes the password "m#1diacbB/L." Remember this phrase and you won't forget this seemingly random combination of letters, numbers and symbols.
- **Avoid easy-to-guess passwords.** This includes your login name, sequences (123456789), or look-alike characters (M@ddie).

If you have any questions or want more specific information you can either contact Royal Credit Union Member Service at *member_services@rcu.org*, or call 1-800-341-9911.

IDENTITY THEFT

Identity theft is a very serious problem that is more common than most people realize. It can cause the victim to be unsure of what will happen next. Here are a few steps you should take if you become a victim of identity theft:

- Place a fraud alert with **Experian**, **Equifax** and **TransUnion** by visiting their websites. These are the three largest consumer credit reporting agencies in the U.S., and their websites are an excellent source of information about identity theft.
- **File a police report** with your local police department.
- **File a complaint** with the **Federal Trade Commission** by calling 1-877-438-4338 or visiting them online at *ftc.gov*
- **Close** any affected accounts
- Consider using a **credit monitoring service**
- Consumers are eligible to **receive one free credit report** yearly at *annualcreditreport.com*

ATM, DEBIT, AND CREDIT CARD SECURITY

Debit and credit card theft or fraud are among the most common forms of those types of crimes that a person may experience. Fortunately, the process a victim should follow is fairly straight forward.

If you have a lost or stolen card that has been issued through Royal Credit Union, or if you have concerns about fraud on a card that has been issued through Royal Credit Union, contact us right away.

During regular business hours, if you're experiencing an issue with your **ATM or debit card issued through Royal**, call 715-833-8111 or toll free 1-800-341-9911. If your card is lost or stolen after hours, call 1-833-231-6514.

ATM, DEBIT, AND CREDIT CARD SECURITY (CONT.)

If you're experiencing an issue with your **credit card issued through Royal**, you should call 1-800-853-0872. That is your point of contact 24 hours a day for issues with your Royal credit card.

If you need to complete a **Debit Card Dispute Form**, you can access that on the Royal Credit Union website by visiting *rcu.org/Forms* and clicking on the link for the Debit Card Dispute Form. Once you have completed that form, you can bring it to any office, fax to 715-552-3030 or email to *PSSCardServicesActivity@rcu.org*.

If you believe that your ATM, debit or credit card has been compromised or stolen and is through another institution, we would recommend the following actions:

- **Close the card**
- **Dispute unauthorized transactions**
- **File a police report**

Each financial institution and company has a different process for contact and forms to be completed. You should make sure you are aware of the financial institution that issued each ATM, debit or credit card that you have.

COUNTERFEIT AND FAKE CHECKS

At Royal, we know that fraud isn't always obvious. While electronic fraud and fraud involving credit and debit cards is common, we know that checks are still a major source of fraudulent activity. The number one rule of check fraud is that if it sounds too good to be true, it is.

If you have fallen victim to a **check scam using counterfeit checks**, here are the steps you need to take:

- **Contact Western Union/Money Gram** and see if the wire can be stopped
- **File a complaint** on *IC3.gov* if the scam originated online
- **Visit the Federal Trade Commission's website** at *ftc.gov*
- If your online banking credentials were obtained by the scammer, you should immediately **set up a new user name and password, then close the compromised accounts** because the account numbers available through your online banking will be considered compromised.
- If the account involved in the scam incurred a negative balance due to the item being returned, **establish payment arrangements** to avoid an account closure which would be reported to Chex Systems

If you have fallen victim to f**orged checks because of lost or stolen checks**, here are the steps you need to take:

- **Sign an Affidavit of Forgery**
- **Close the account or place a Stop Payment action on missing checks**
- **File a police report**

If you have completed the above steps, you are well on your way to correct the situation. Next, you should review your security practices to help prevent this type of event from happening again.

If someone you don't know wants to pay you by check but wants you to wire some of the money back, be aware that this is a common scam technique.

There are many variations of the **fake check scam**. It could start many different ways:

- **Offering to buy something you advertised**
- **Pay you to do work at home**
- **Give you an "advance" on a sweepstakes you've supposedly won**
- **Pay the first installment** on the millions that you'll receive for agreeing to have money in a foreign country transferred to your bank account for safekeeping

Fake check scammers hunt for victims. They scan newspaper and online advertisements for people listing items for sale, and check postings on online job sites from people seeking employment. They place their own ads with phone numbers or email addresses for people to contact them. And they call or send emails or faxes to people randomly, knowing that some will take the bait. **Here's what to know:**

- **They often claim to be in another country.** The scammers say it's too difficult and complicated to send you the money directly from their country, so they'll arrange for someone in the US to send you a check.
- **They tell you to wire money that you deposited** or if you're selling something, they claim they'll pay you by having someone in the United States send you a check. It will be for more than the sale price; you deposit the check, keep what you're owed, and wire the rest to them. If it's a work-at-home scheme, they may say that you'll be processing checks from their "clients." You deposit the checks and then wire them the money minus your "pay." Or they may send you a check for more than your pay "by mistake" and ask you to wire them the excess.
- **The checks are fake but they look real**, even bank tellers may be fooled. Some are phony cashiers checks, or look like they're from business accounts. The companies whose names appear may be real, but the checks are not.
- **Quick and easy access to funds from scams doesn't mean that the checks they are using are legitimate.** Under federal law, banks have to make the funds you deposit available quickly— usually within one to five days, depending on the type of check. It doesn't mean the check is good, even if it's a cashier's check. It can take weeks for the forgery to be discovered and the check to bounce.

You are responsible for the checks you deposit. That's because you're in the best position to determine the risk—you're the one dealing directly with the person who is arranging for the check to be sent to you.

When a check bounces, the financial institution deducts the amount that was originally credited to your account. If there isn't enough to cover it, the financial may be able to take money from other accounts you have at that institution, or sue you to recover the funds.

In some cases, **law enforcement authorities could bring charges against the victims** because it may look like they were involved in the scam and knew the check was counterfeit.

There is no legitimate reason for someone who is giving you money to ask you to wire money back. If a stranger wants to pay you for something, insist on a cashiers check for the exact amount, preferably from a local bank or a bank that has a branch in your area.

Don't deposit it! Report fake check scams to **National Consumer League's Fraud Center**. That information will be transmitted to the appropriate law enforcement agencies.

KEEPING AN EYE ON YOUR CREDIT REPORT

Fraudulent activity can damage your credit report, but much of that potential damage can be corrected if you catch it right away.

The best way to catch that activity quickly is to continue paying attention to your credit report by monitoring it regularly and understanding what a good credit score is and how that differs from a poor credit score. Also, it's good to know what comprises your credit score and what you can do to manage each of those factors.

At Royal, we place a high value on making sure that our Members are knowledgeable and informed when it comes to their credit.

Just like you, Royal also keeps an eye on things. We know that identity theft can be scary and is a very serious issue that can have lasting, damaging effects on the financial well being of our Members. Here's how Royal does it.

We have several security measures in place to protect you when you use your Royal Credit Union debit card or Platinum Rewards Visa.

- **We track your typical spending patterns and alert you if there is a purchase outside of that pattern**
- **We look for large unusual purchases and suspicious activity, and notify you if either one occurs**
- **We protect your online purchases with Verified by Visa**

Because of these security features, it is important to notify Royal if you plan to travel outside of the country. Please give us a call before your trip so you can continue to use your card without concern!

MEMBER PAPERWORK

Often, it will require more than just a phone call to resolve fraudulent activity. **More than likely, there will be paperwork that needs to be filled out.**

If you experienced fraud on an ATM/debit card, you will need to call **Member Service** or stop at one of our offices to pick up or complete a form that must be filled out and submitted in order for the appropriate processes to be completed.

If you experienced fraud due to a forged check, you will need to complete an **Affidavit of Forgery**. That form can be picked up at an office or you can have a form sent to you by calling **Member Service**.

If you experienced fraud on a credit card account, you should call 800-853-0872 to report your lost or stolen card or to dispute a fraudulent charge.

MEMBER ACTION CHECKLIST

Actions to complete in all instances of fraud:

___ Contact Royal Credit Union or Other Financial
___ Change Passwords
___ Verify Password Strength
___ Check Credit Report
___ Update Pre-Authorized Transaction Account Numbers

If You Experienced Identity Theft:

___ File Police Report
___ Place Fraud Alert with Experian, Equifax and TransUnion
___ File Complaint with Federal Trade Commission
___ Determine Need for Credit Monitoring
___ Close Affected Accounts

If Lost or Stolen ATM, Debit, or Credit Card:

___ Close/Block the Account
___ Dispute Unauthorized Transactions
___ File Police Report

If You Experienced A Check Scam:

___ Contact Western Union/Moneygram to see if payment can be stopped
___ If originated online, file report at IC3.gov
___ Visit FTC.gov
___ Change passwords
___ Close impacted accounts
___ If caused negative account balance, make arrangements for repayment to avoid further action

If You Had A Stolen/Forged Check Situation:

___ Sign Affidavit of Forgery
___ Place stop action on checks
___ Close compromised account
___ File police report

ROYAL
CREDIT
UNION®

1-800-341-9911 • rcu.org

Your savings federally insured to $250,000

NCUA National Credit Union Administration, a U.S. Government Agency

MFD 0823