IDENTITY THEFT AND FRAUD

Safeguarding Your Private Information

Safeguarding your private information

How to Identify Scams and Fraud

RiverWind Bank has reported a significant increase in fraud and is currently on a mission to warn the public. Fraud and scams are very active in our area in several different forms, including lottery scams, fraudulent postal money orders, internet sale scams, bank employee impersonation and identity theft.

What is a Lottery Scam?

In a lottery scam, a consumer is sent a letter that claims that they have won a lottery or sweepstakes. They are told that taxes, handling fees or conversion fees on the winning must be paid by wiring a large sum of money to a location outside of the United States before they can receive their jackpot. In a variation of the scheme, a consumer receives a "certified" check in the mail for a large sum of money, which they deposit to their account. The "certified" check turns out to be counterfeit and is charged back to the victim's account. Legitimate lotteries never ask for money. They don't have to and there are not fees of any kind. The only tax you pay is paid directly to the government.

Fraudulent United State Money Orders

Another common scam is fraudulent United State Postal Money Orders. In many cases, victims are often contacted by an email message or in an online chat room and are deceived into accepting them as payment for items they are selling or into cashing the money orders in "return" for a fee.

Postal officials say that the best way to identify a genuine postal money order is to look for the watermark, which, when held up to a light will reveal a repeating image of Benjamin Franklin. Genuine postal money orders also have a security strip running alongside the watermark, just to the right. If held to a light, a micro fiber strip will show the letters "USPS" along its length.

If there is any doubt on the validity of a money order, visit your local post office or call 866-459-7822.

Internet Sale Scams

An internet sale scam is a scam in which a legitimate consumer advertises an item for sale on the internet and a buyer offers the consumer's asking price. They are told that a check will be sent in advance to pay for the item. When the check is received it is for more than the agreed upon sale price. The consumer contacts the buyer who states that the bank made a mistake and askes for the consumer to send back the difference via a wire transfer. Then the money is sent back, the bank check comes back as fraud, and the full amount is deducted from the consumer's bank account. The consumer is left with a large negative account balance and the buyer cannot be located.

Bank Employee Impersonation

Bank employee impersonation is when a consumer receives a telephone call of email from someone claiming to be a bank employee with a request to provide account information for verification purposes. The consumer later discovers that funds are missing from their bank account.

There is no reason for your bank to contact you and request your account number or social security number because they already have this information.

You should call or visit your financial institution to determine the legitimacy of the request before giving out ANY information.

Identity Theft

Identity Theft occurs when someone uses your personal information without your permission to commit fraud or other crimes. While you cannot control whether you will become a victim, there are steps you can take to minimize your risk.

Security and Identity Theft Tips

The Federal Trade commission recommends the following steps:

- Order a free copy of your credit report annually.
- Place passwords on your credit card, bank and phone accounts.
- Secure your personal information in your home.
- Don't give out personal information on the phone, through the mail, or on the internet unless you have initiated the contact or are sure you know with whom you are communicating.
- Treat your mail and trash carefully.
- Deposit your outgoing mail in post office collection boxes or at your local post office.
- Give your Social Security Card only when necessary.

What to do if you are a Victim of Identity Theft

Take steps quickly if you have lost personal information or identification, or if it has been stolen.

- Close account immediately and place passwords on new accounts
- Cancel your driver's license or other government issued identification and get a replacement. Ask the agency to flag your file so no one else can get identification with your name.
- Place an initial fraud alert on your credit report by calling one of the three nationwide consumer reporting agencies:

Equifax
Mailing Address: PO Box 74021 Atlanta, GA 30374-0241
Report Fraud: 800-525-6285
Web site: www.equifax .com

Experian
Mailing Address: PO Box 949 Allen, TX 75013-9049

Report Fraud: 888-EXPERIAN (397-3742)
Web site: www.experian.com

Trans Union
Mailing Address: Fraud Victim Assistance Division, PO Box 6790, Fullerton, CA 92634
Report Fraud: 800-680-7289
Web site: www.tuc.com

Helpful Websites

Access these websites for additional information about how to protect yourself from identity theft or obtain assistance if you have been a victim.

Federal Trade Commission National Resource on Identity Theft which is a one-stop resource for information about identity theft.

http://www.consumer.gov/idtheft

Identity Theft Resource Center which is a non-profit organization helping people recover from identity theft.

http://www.idtheftcenter.org

Free Annual Credit Report

http://www.annualcreditreport.com

Fraud Protection

General Precautions

- **Carry only necessary information with you.** Leave items such as your Social Security card at home. Keep photocopies of vital information and store them in a secure place, such as a home safe or a safety deposit box.
- **Never provide your Social Security Number (SSN) unless you determine it is necessary.** If you asked to provide your SSN for any service, confirm that it is really needed or ask if you can provide another piece of identifying information.
- **Discontinue paper statements.** Receiving online statements will help prevent identity theft. The less personal information you receive through the mail, the less chance there is for identity theft or fraudulent activity against you.
- **Shred documents containing personal or financial information before discarding.** Most fraud and identity theft incidences happen as a result of mail and garbage theft also known as "dumpster diving."
- **Review your credit report.** At least yearly request a copy of your credit report and review it for erroneous and/or fraudulent information or inaccuracies. You can request free credit report

once a year from each of the three major credit bureaus at **www.annualcreditreport.com**. You may also obtain a copy from the credit bureaus directly. Note that there may be a small fee associated:

- Equifax: 1-800-685-1111 or www.equifax.com
- Experian: 1-888-397-3742 or www.experian.com
- TransUnion: 1-800-916-8800 or www.transunion.com

Limit the credit offers you receive. Contact the National Consumer Credit Reporting Agencies at 1-888-5-OPTOUT (1-888-567-8688) to limit the credit offers you receive; this will also limit the information companies share about you. Contact the National Consumer Reporting Agency at www.ncrainc.org

Computer Security Tips

- **Protect and memorize your passwords.** Never write your password down or share them with anyone. Change passwords regularly and use combinations of letters, numbers, and "special characters". Do not use your Social Security Number or birthday as a username or password. Never use your username as a password.
- **Keep your computer operating system up to date.** Ensure that your own personal computer has updated anti-virus and firewall protections. Apply security patches for all your programs and operating systems regularly.
- **Use a current web browser.** RiverWind Bank continually upgrades our online services to provide you with the most secure online services. An outdated web browser may prevent you from accessing your online banking account.
- **Antivirus Software.** Protect your computer by using anti-virus software and a firewall and keeping them up to date.
- **Use secure websites for transactions and shopping.** Make sure the web page you are viewing offers encryption of your data. If you see a lock symbol in the lower right-hand corner of your browser window, or if the web address of the page you are viewing begins with https://, this indicates that web page is secure and uses encryption. When necessary, RiverWind Bank provides 128-bit encryption, the highest level available today.
- **Do not download programs from unknown sources.** Sometimes hidden programs or viruses are contained on downloaded programs which can compromise your computer. Use caution when downloading from an unfamiliar site.
- **Terminate the Internet when not in use.** Always log off from your online banking session. Take an additional precaution by terminating your internet session when not in use. This will help to avoid unwanted access to your computer and its data.
- **Remember that RiverWind Bank will never contact you by email requesting personal information such as your social security number, credit, debit or ATM card numbers, PIN numbers, passwords, usernames or account numbers.**

Please be aware that legitimate calls from RiverWind Bank are often made, but we will only ask for confirmation of certain information. No personal information is requested.

If you believe you are a victim of fraud or have been the recipient of suspicious communication contact RiverWind Bank immediately at 870-347-2511 or support@riverwindbank.com

ATM/Debit Card Security Tips

- Before you approach the ATM, have your ATM card out and ready to use.
- Use care when inputting your Personal Identification Number (PIN) to prevent someone from looking over your shoulder.
- Know your surroundings. If anything looks suspicious when you are the ATM, come back later or use another ATM.
- Some ATMs are in enclosed areas. Before entering an enclosed ATM vestibule, look around before entering and never hold the door for someone else.
- Whenever possible, have someone accompany you when you use at an ATM at night.
- Keep your car doors locked if using a drive-up ATM.
- Do not count your cash at the ATM. Count it later when in a secure place.
- Take your receipts with you.
- Never allow a stranger to assist you with using an ATM.
- Do not use your name, your birth date, phone number, or address, etc. when selecting a PIN.
- Don't write your PIN down anywhere and never share it with anyone.
- Review your account statements on a regular basis. Notify RiverWind Bank immediately if you determine there are discrepancies.
- Never provide your card information over the phone unless you initiated the call.
- When you receive a replacement card, destroy your old card.
- If you forget your PIN or would like to select a new one, please visit your nearest RiverWind Bank Branch.
- Always keep your card in a safe place, as you would cash, checks, or credit cards.
- Report lost or stolen cards and checks immediately.
-

Contact RiverWind Bank immediately:

- At 1-870-347-2511 during business hours Monday thru Friday 8:30 AM to 5:30 PM CST if you suspect unauthorized use or to report your lost or stolen card
- At 1-870-347-2511 to "hot card" your lost or stolen card i.e. to immediately cancel the card; message is also given to merchants that the card has been lost or stolen

Regulation E and Accounts with Internet Access

What is Regulation E?

Regulation E protects individual customers using electronic funds transfers (EFT). Non-consumer accounts are not protected by Regulation E.

What is an EFT?

An EFT is any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing or authorizing a financial institution to debit or credit a consumer's account. The term includes but is not limited to:

- Point of sale transfers
- Automated teller machine transfers
- Direct deposits or withdrawals of funds
- Transfers initiated by telephone
- Transfers resulting from debit card transactions, whether or not initiated through an electronic terminal
- Transfers initiated through internet banking and bill pay

How does Regulation E apply to a consumer using Online Banking and/or Bill Pay?

Regulation E is a consumer protection law for accounts such as checking or savings, established primarily for personal, family or household purposes. Non-consumer accounts, such as Corporation, Trust, Partnerships, LLCs, etc. are excluded from coverage. Regulation E provides consumers a means to notify their financial institution that an EFT has been made to their account without their permission. If you are unsure if your account is protected by Regulation E contact us.

What protections are provided to consumers under Regulation E for consumers who use Online Banking and/or Bill Pay?

If you believe an unauthorized EFT has been made to your account, contact us immediately. If you notify us within two business days after you learn of the unauthorized transaction the most you can lose is $50. Failure to notify the bank within two business days may result in losses up to $500.

No liability limit:

Unlimited loss to a consumer can occur if:

- The periodic statement you receive reflects an unauthorized transfer of money from your account, and
- You don't report the unauthorized transfer to the bank within 60 days after the statement was mailed, and
- The loss could have been avoided if you had given timely notice.

How does Regulation E apply to a non-consumer using Online Banking and/or Bill Pay?

A non-consumer using Online Banking and/or Bill Pay is not protected under Regulation E. Because the customer is not protected by Regulation E special consideration should be made by the customer to review the controls in place to ensure that they are commensurate of the risk level that the customer is willing to accept.

What precautions should a non-consumer take because they are not protected by Regulation E?

As a non-consumer customer you should perform a risk assessment and periodically evaluate the controls you have in place. The risk assessment should be used to determine the risk level associated with any internet activities you perform and any controls in place to mitigate these risks.