# EAGLE VALLEY BANK

## EAGLE VALLEY BANK'S COMMITMENT TO YOUR SECURITY

Eagle Valley Bank understands that your trust in us depends in part on keeping your personal, business and account information confidential and secure.

As the number of consumers who fall victim to ID theft and electronic fraud increases, the staff and management of Eagle Valley Bank have pledged to take steps to safeguard your confidential information and give you guidance on how you can protect yourself against ID theft, electronic fraud, and other common threats encountered by today's banking customers.

Eagle Valley Bank will follow security guidelines to minimize threats to you. We will never request personal information by email or text messaging, including account numbers, passwords, personal identification information or any other confidential customer information. Do not respond to any email communications that appear to be from Eagle Valley Bank which request any type of personal or confidential information and do not go to any links listed on that email.

Never give callers information that the Bank already has via phone, text messages or email senders. The Bank will not contact you to ask for your debit card number or your full social security or tax ID number.

If we contact you, we will do so by means that protect your personal or confidential information.

Please report any suspicious calls, e-mails or telephone messages to Eagle Valley Bank by calling (800-840-2144) or your local branch office.

## IDENTITY THEFT

Identity theft is illegally using another person's name, social security number, driver's license number, birth certificate, credit card, address, telephone number or any other form of identifying information to obtain credit, money, goods, services or anything else of value without that person's consent.

## HOW DOES IT HAPPEN

Thieves can obtain personal information through several sources including:

- Theft of a wallet or purse
- Dumpster diving
- Inside sources
- Mail theft
- Submitting change of address forms
- Taking information while inside your home
- Shoulder surfing or eavesdropping
- Data Breach

### Phishing

Phishing is a common method used for identity theft. This is when thieves represent themselves as an organization in an attempt to gather personal or confidential information. Thieves trick consumers and businesses in providing personal or account access information such as usernames, passwords, social security numbers or other private information.

**Thieves often pose as:**

- Financial institutions
- Credit card companies
- Utility companies
- Government agencies
- Prospective employers



14800 Galaxie Avenue, Suite 100
Apple Valley, MN 55124
952-431-3232

1946 Washington Avenue S
Stillwater, MN 55082
651-351-1200

2206 Glacier Drive
St. Croix Falls, WI 54024
715-483-5016

www.eaglevalleybank.com

9/2017

**Clues that an email may be Phishing:**

- A call to act such as, "We are updating our records," "We've identified fraudulent activity on your account," "Information was lost due to a computer error." This type of email encourages people to act now!
- Typos or poor grammar.
- Greeting that may not refer to the customer by name.
- A link that points to a different website than the alleged sender. The link looks good in the email, but when your mouse hovers over the line, a web address not associated with the sender displays.

### Smishing

Cell phone and other mobile devices can be targets! Smishing is the use of these types of devices to gain personal information. Text messages are sent asking a recipient to register for a service. When following the link in the message a virus, worm or other malware can spread to the device which will gain access to private data.

### Vishing

Vishing refers to attempts to use phone calls or voicemails to gain personal information. Often consumers receive a pre-recorded call identifying a specific location financial institution. The message informs the consumer that their bank accounts have been frozen. The message then tells the recipient to input their ATM or debit card number, expiration date and PIN to reactivate their account.

## TIPS FOR SAFEGUARDING YOUR INFORMATION

- Immediately report lost or stolen checks, credit cards, etc.
- Don't give your social security number or other personal account information to anyone who calls you – unless you verify who you are speaking with.
- Don't carry your social security number with you.
- Do not leave your purse or wallet unattended.
- Shred unneeded receipts, bank statements, paystubs, medical billings, and old checks. Also shred any credit card offers received – don't just throw them in the trash or recycling.
- Don't mail bills from your own mailbox.
- Use anti-virus and anti-spam software as this may help to detect, block, or disable some malicious software and phishing emails. Keep your anti-virus software up to date.
- Order copies of your credit report at least annually to ensure accuracy.
- Don't open emails from unknown sources.
- Use up-to-date anti-virus software.
- Protect your PIN's and passwords; don't carry them with you.
- Use a combination of letters and numbers for your passwords, change them frequently.
- Report suspected fraud to the bank and the fraud department of the credit reporting agencies immediately.
- Practice email safety; don't click on links in emails or open attachments unless the email was expected and verified; confirm a message is legitimate by contacting the sender directly via pre-determined contact information.
- Be suspicious of email or phone requests to update or verify personal information.
- Be wary of offers that are too good to be true, require fast action or instill a sense of fear.
- Be on guard against fraudulent checks, cashier's checks, money orders or electronic fund transfers with a request to return part of the funds via wire transfer.
- Use security and privacy settings on social network sites and beware of random contacts from strangers.
- Research "apps" before downloading, only download from an "app" store (iTunes, Play Store, Windows Store), and don't assume an "app" is okay because the icon resembles that of a bank.
- Beware of disaster-related scams where scammers claim to be from legitimate charitable organizations.



14800 Galaxie Avenue, Suite 100
Apple Valley, MN 55124
952-431-3232

1946 Washington Avenue S
Stillwater, MN 55082
651-351-1200

2206 Glacier Drive
St. Croix Falls, WI 54024
715-483-5016

www.eaglevalleybank.com

9/2017
Member FDIC

**PROTECTING YOURSELF AND YOUR ACCOUNTS**

Eagle Valley Bank is committed to protecting your personal information. The Bank's internet banking system uses several methods to protect your information. In addition to these, you can take further precautions to protect your information.

- Never give out any personal information including usernames, passwords, social security numbers or date of birth.
- Do not use personal information for your usernames or passwords, such as names of family members, pets or birthdates.
- Avoid using public computers to access your accounts.
- Use multiple usernames and passwords. Keep user names and passwords for social networks, online banking, e-mail and online shopping different.
- Remain at your computer until your online banking transactions are completed and you are logged out. Log out of internet banking prior to visiting other websites.
- Be mindful of the security level of the websites requesting personal data, financial or otherwise. The web address should start with https:// ("s" for security) rather than the usual http://.
- If a phishing email references a telephone number that you suspect to be related to a VoIP (voice over internet protocol) scam, please report the number to your local federal law enforcement agency. Most agencies now have cyber threat units that are well-versed in investigating these claims.
- Review monthly bank and credit card statements closely and contact the financial institution immediately if any unknown transactions occur; better yet, if online or mobile banking is available for deposit and credit card accounts, make a habit of reviewing every few days to ensure immediate actions can be taken.
- Safeguard credit cards, social security numbers and other personal information:
    - Only provide sensitive information over secure websites or emails;
    - Do not provide personal information or log onto critically sensitive accounts (email, online banking, etc.) via public computers, like a hotel or library kiosk, or while using public WiFi.
- Wherever possible, utilize two-factor authentication to provide an additional layer of account logon protections; two-factor authentication requires two pieces of information to login to an account, usually the password and a code from an SMS text message or approving the login via phone call.
- Use password protections:
    - Create long passwords with at least 10 characters and using a mix of alpha-numeric characters (A, b, 1, 99) and symbols (@, $, %, *);
    - Instead of a password, use a passphrase, a long (15-25 char) phrase or sentence that only makes sense to you and is easy for you to remember; do not use something common like "Maryhadalittlelamb." And use something uncommon like "MichaelWhassocceronThursdays.".
    - Use a password checker to verify the strength of the selected password; do NOT put a valid password into an online password checker; instead, use a variation that is similar but not the same;
    - Do not use the same password for two critical websites or online accounts, do not share passwords with others and do not use the "Remember My Password" feature in web browsers;
    - Unless you use a very long and difficult password, change passwords often; and
    - Use a password manager to enable longer passwords without having to write them down.
    - Change all passwords periodically.
- Protect postal mail by locking the mailbox, if possible; monitor postal mail closely and act quickly if bills don't arrive when expected or if a "new" credit card or account statement arrives; ask the post office to hold mail if traveling for a long period of time.
- Shred bills, bank statements, pre-approved financial solicitations and other confidential information before discarding them; check for local free "shred events" to securely dispose of documents.

If you believe your internet banking access information has been lost or stolen or that someone has accessed your account(s) without your authorization, call us immediately at 800-840-2144 during business hours.



14800 Galaxie Avenue, Suite 100
Apple Valley, MN 55124
952-431-3232

1946 Washington Avenue S
Stillwater, MN 55082
651-351-1200

2206 Glacier Drive
St. Croix Falls, WI 54024
715-483-5016

9/2017
Member FDIC

## LEVERAGE FINANCIAL INSTITUION SAFEGUARDS:

Check with your financial institution for these additional account protections:

- A security challenge pass-phrase must be selected before any changes are made to account(s); restriction to only perform secure withdrawals or transfers to pre-specified accounts;
- Account alerts, the institution offers to monitor online or phone transactions, wire transfers, international transactions, new payees added to bill pay and address or profile changes to accounts;
- Account notes and travel protections if going on vacation, especially out of the country; account notes for active duty military on assignment overseas, that they are not stateside;
- Destroy sensitive documents via a cross-out shredder.

## DEBIT AND CREDIT CARD FRAUD

Debit and credit cards have become an accepted way to purchase items for our daily needs. To protect you from card fraud:

- Carry only cards that you frequently use.
- Do not leave your wallet or purse in your vehicle.
- Never give your card or card numbers to anyone else.
- Memorize your PINs, do not write them on the card or in your checkbook.
- Choose a PIN for your ATM or Debit Card that is different from your address, telephone number, social security number or birthdate.
- Take your receipt with you at the end of each transaction. Check your receipts to your statements.
- Be aware of your surroundings when using an ATM. Consider using another machine or coming back later if you notice something suspicious.
- Report all crimes related to ATM activity to the owner of the machine and to local law enforcement.
- Do not provide any personal information to web sites that do not use secure methods for protecting your information.

## IF YOU BECOME A VICTIM OF IDENTITY THEFT

- Contact the fraud department of the four credit bureaus.
- Contact the creditors of any accounts that have been misused.
- File a report with the local police.
- Contact your local Eagle Valley Bank Branch to cancel any existing accounts or services with your name.

## IDENTITY THEFT RESOURCES

Federal Trade Commission – Consumer Information
http://www.consumer.ftc.gov/

Federal Trade Commission – Identity Theft
http://www.consumer.ftc.gov/features/feature-0014-identity-theft

National Cyber Security Alliance
http://staysafeonline.org

Department of Homeland Security
http://www.dhs.gov/stopthinkconnect

Office of the Comptroller of the Currency:
http://www.occ.treas.gov/topics/consumer-protection/fraud-resources/index-fraud-resources.html

**Credit Bureau Information:**

Equifax – 800-525-6285
https://www.equifax.com/personal/

Experian – 888-397-3742
https://www.experian.com/

Trans Union – 800-680-7289
https://www.transunion.com/

Innovis – 800-540-2505
https://www.innovis.com/



14800 Galaxie Avenue, Suite 100
Apple Valley, MN 55124
952-431-3232

1946 Washington Avenue S
Stillwater, MN 55082
651-351-1200

2206 Glacier Drive
St. Croix Falls, WI 54024
715-483-5016

www.eaglevalleybank.com

9/2017
Member FDIC

## CORPORATE ACCOUNT TAKEOVER

Business accounts are as vulnerable to fraud as are personal accounts. There continues to be an increase in fraud where thieves gain access to a business' finances, conducting unauthorized transactions, including wire or ACH transactions, creating new employees to payroll and stealing other sensitive information.

Criminals use various methods to obtain access to the legitimate banking credentials from businesses, including mimicking a bank website, using viruses or malware to compromise a system, or social engineering to trick employees to giving security credentials.

**Business systems may be compromised by:**

- An infected document or email
- A link in an email to a malicious website
- Employees visiting legitimate websites and clicking on infected documents
- Use of an infected flash drive

**How to protect your business:**

- Conduct a risk assessment of your business risk and controls.
- Develop a security training program for all employees.
- Use of firewalls, virus protection, anti-malware and other security tools.
- Pay attention to suspicious activity. Look for unexplained account or network activity. If detected, contact the Bank immediately and stop all online activity. Remove systems that may have been compromised.
- Dedicate one computer exclusively to online banking and cash management. Do not allow this computer to be used in a Wi-Fi hotspot. Do not allow general web browsing on any online banking workstation.
- Create financial transaction files using dual control.



14800 Galaxie Avenue, Suite 100
Apple Valley, MN 55124
952-431-3232

1946 Washington Avenue S
Stillwater, MN 55082
651-351-1200

2206 Glacier Drive
St. Croix Falls, WI 54024
715-483-5016

9/2017
Member FDIC