

# 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.

## **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 card 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.
- Review your accounts regularly for unauthorized charges or other activity.
- 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.



# EAGLE VALLEY BANK

## 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
- Online data

### **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 user names, passwords, social security numbers or other private information.

#### ***Thieves often pose as:***

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

#### ***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 you mouse hovers over the line a web address not associated with the sender displays.

### **Smishing**

Cell phone and other mobile device users 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.



# EAGLE VALLEY BANK

## 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:

1. Never give out any personal information including user names, passwords, social security numbers or date of birth.
2. Create difficult passwords, using letters, numbers and symbols.
3. Do not use personal information for your user names or passwords, such as names of family members, pets or birthdates.
4. Avoid using public computers to access your accounts.
5. Use multiple usernames and passwords. Keep user names and passwords for social networks, online banking, e-mail and online shopping different.
6. Change your password periodically.
7. 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.
8. 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!
9. 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://>.
10. 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.

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.

## 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:

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



# EAGLE VALLEY BANK

## **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 their 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.

## **IF YOU BECOME A VICTIM OF IDENTITY THEFT**

- Contact the fraud department of the three major credit bureaus.
- Contact the creditors of any accounts that have been misused
- File a report with the local police.
- Contact your local Eagle Valley 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/stophinkconnect>

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

Experian – 888-397-3742

Trans Union – 800-680-7289

