"Identity Theft Awareness: Don't Fall Victim to these Common Scams"

We want you to understand what identity theft is, how it happens, and how to protect yourself. Please read and familiarize yourself with these common methods of identity theft and account takeover. Keep yourself up-to-date with identity theft methods as they are sophisticated and constantly changing. **Remember, vigilance on your part is critical in deterring, detecting and avoiding identity theft.**

WHAT IS IDENTITY THEFT?

Identity theft occurs when someone uses another's personally identifiable information without permission to commit fraud or other crimes.

WHAT IS PERSONALLY IDENTIFIABLE INFORMATION?

Personally identifiable information is any data that can be used to identify, contact or locate a person, such as but not limited to: name, address, e-mail address, phone number, date of birth, Social Security number, bank account information, PIN number, and credit card number.

TYPES OF IDENTITY THEFT:

- **Account takeover** occurs when an identity thief acquires your existing credit card information or bank account information and uses this information to purchase products and services on credit or to make withdrawals, transfers and other transactions from your bank account. They may even file for government benefits and tax refunds using your personal information.
- **Application fraud** is when the thief uses your Social Security number and other personally identifying information to open new accounts (telephone or utility service, credit cards, loans or mortgages) in your name.

COMMON HIGH-TECH METHODS OF IDENTITY THEFT:

Phishing is a fraudulent attempt, usually made through email, which appears to originate from a financial institution, government agency or other well-known or reputable company, used to gain access to your personal information such as your social security number, a credit card number, the 3-digit security code on the back of your credit or debit card, an account number, or login password.

SMShing is a form of *phishing* that uses mobile phone SMS (Short Message Service) text messages to lure victims into visiting fraudulent websites or calling fraudsters.

Examples of Phishing or SMShing messages received via email or text:

- "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

Avoid phishing and SMShing scams by being alert for emails that:

- contain unfamiliar or suspicious links or attachments;
- are unsolicited and/or from an unknown sender;
- are sent multiple times from different senders; or
- contain poor grammar or incorrectly spelled words.

If you receive an email or text message that contains any of these elements or any combination of these elements, you should delete it immediately. Do not open it, click on the links or open any attachment even if the message seems to be from an organization you trust. Do not reply to the email or forward it to anyone.

Remember, legitimate businesses don't ask you to provide sensitive or personal information through insecure channels.

Website spoofing involves a site that has been designed to look like that of a legitimate site like a credit card or bank, but really, it has been created by a scammer in an effort to collect personal information from the visitors that come to the site. Once the scammer collects the information it can be used for identity theft fraud.

COMMON LOW-TECH METHODS OF IDENTITY THEFT:

***Purse/Wallet Stealing*.** Identity thieves will steal purses and wallets to obtain personal information.

Dumpster Diving. Identity thieves rummage through personal or business trash or dumpsters to obtain personal information that may have been carelessly discarded. **Always shred unwanted documents containing personal information.**

***Skimming*.** Thieves insert small devices ("ATM skimmers") into the ATM slot to steal bank card information. They may also install tiny cameras to record PIN numbers entered. Armed with this information, thieves can take over your account.

***Shoulder Surfing*.** Thieves can obtain personal information through eavesdropping. They may be listening when you provide your account number or Social Security Number to a bank teller, for example. They may position themselves so that they can observe a computer screen or keyboard. Be aware!

Mail Theft. Thieves steal mail from unlocked mailboxes in order to take over that person's account(s) or to use that information to obtain newly issued debit cards, bank or insurance statements, investment reports, benefits documents or tax information.

Re-routing of Mail. Identity thieves will divert your mail to another location by completing a Change of Address form in order to takeover your existing account(s). Remember, address changes should not be done over the phone. A change of address should require your written authorization or be done in person. Online address changes should require a PIN or other method of identification.

William Penn Bank does not permit address changes by phone. Change of address requests must be in writing and signed by the account holder or requested in person with proof of identification.

OTHER IDENTITY THEFT SCAMS:

Telephone scams involve an identity thief, posing as a bank official, governmental official, merchant, lottery or charitable organization representative, or many other types of individuals, who will telephone and make a compelling pitch and obtain your personal or financial information in the process. This is a common method used to obtain credit card information and other personal information in order to takeover your account. An identity thief can easily change a caller ID. **Remember, just because you recognize the name or company on the caller ID, it doesn't mean it is legitimate.**

Pretext Calling is a fraudulent means of obtaining an individual's personal information through the use of some form of pretext to obtain customer information.

- ***Example***: Armed with limited information, such as a customer's name, address and/or social security number, a pretext caller may pose as a customer or an employee in an attempt to convince another employee to divulge confidential information. In some instances, pretext callers may call an institution repeatedly until the caller finds an employee willing to provide the information. Identity thieves may engage in pretext calling to obtain personal information for use in accessing current accounts (account takeover) or in creating fraudulent accounts.

Deceptive prize promotion scams (i.e. sweepstakes or lotteries). These scams often target the elderly using a series of letters, emails or phone calls notifying the victim they are a "winner". In exchange for the winnings, the victim is usually required to pay processing fees or expenses and provide personal information. Payment of fees or expenses is often required to be wired or sent overnight in the form of check or money order.

- If you didn't enter a contest, sweepstakes, or play the lottery, you didn't win!
- You never have to pay anything upfront to redeem a legitimate prize.
- If you receive a partial-payment check for winning, it's a scam.
- Foreign lotteries are not open to U.S. residents.

Grandparent Scam (targets Senior Citizens). Scammers call or email elderly victims and pretend to be a relative in distress – such as a grandchild in the hospital, arrested or lost in a foreign country – and needing money fast. The scammer usually requests the funds be wired and also instructs the victim not to contact anyone in the family. No matter how dramatic the story sounds, **don't wire money**. Don't send a check or money order by overnight delivery either. Con artists recommend these services so they can get your money before you realize you've been cheated.

IF ANYONE EVER ASKS YOU TO WIRE MONEY, HERE ARE KEY POINTS TO REMEMBER:

- If you don't know them, don't wire. Period.
- If you think you do know them or know on whose behalf they're calling, check their story thoroughly.
- If you get a check, with a request to wire back part of the payment, don't deposit it. Report it to the police and the FTC.
- Know that you alone are responsible for verifying the authenticity of the person with whom you're dealing, not the wiring company.
- Understand that if you're scammed, it's highly unlikely you'll ever get your money back.

Explain these types of scams to elderly friends and family members. Tell them to hang up if they receive a call like this and verify with the supposedly distressed family members before wiring any money.

Fake Check Scams. If someone you don't know wants to pay you by check but wants you to wire some of the money back, beware! It's a scam that could cost you thousands of dollars.

There are many variations of the fake check scam. It usually starts with someone offering to:

- Buy something you advertised for sale;
- Pay you to work at home;
- Give you an "advance" on a sweepstake you've won; or
- Give you the first installment on the millions you'll receive for agreeing to transfer money in a foreign country to your bank account for safekeeping.

The scammers often claim to be in other countries and say it's too difficult to pay you directly, so they'll have someone in the U.S. who owes them money send you a check. The amount of the check may be more than you're owed, so you're instructed to deposit it and wire the rest to the scammer. Or you're told to wire some of the money

back to pay a fee to claim your "winnings". Whatever the set-up, the result is the same--after you've wired the money, you find out that the check has bounced.

- ***Can my bank tell if the check is good or not when I deposit it?***

These checks look so real that even bank tellers may be fooled. Some are phony cashier's checks; others look like they're from legitimate business accounts. The companies whose names appear may be real, but someone has dummied up the checks without their knowledge.

Under federal law, banks must make the funds you deposit available quickly--usually within one to five days. But just because you can withdraw the money doesn't mean the check is good, even if it's a cashier's check. Forgeries can take weeks to be discovered.

- ***If the check turns out to be fake, isn't that the bank's problem?***

You are responsible for the checks you deposit. That's because you're in the best position to determine how risky the transaction is--you're the one dealing directly with the person who is arranging for the check to be sent to you. If it bounces, you owe your bank the money you withdrew. The bank may be able to take it from your accounts or sue you to recover it. 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.

- ***How do these scammers find their victims?***

Fake check scammers 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.

- ***How can I protect myself from fake check scams?***

There is no legitimate reason for someone who is giving you money to ask you to wire money back—that's a clear sign that it's a scam. If a stranger wants to send you a check, insist on a cashiers check for the exact amount, preferably from a local bank or one with a branch in your area.

If you think someone is trying to pull a fake check scam, don't deposit it – report it! Contact the National Consumers League's National Fraud Information Center, fraud.org or toll-free 800-876-7060. There are also more detailed tips about fake check scams in the telemarketing and Internet fraud sections of the website.

HOW YOU CAN HELP PROTECT YOUR INFORMATION:

- Review account statements on a regular basis to verify all activity and charges. Report any unauthorized transactions to your financial institution right away.
- Keep your information secure and never share it with any source of which you are unsure.
- Never give personal information on the phone, in a text message or over the internet unless you know exactly with whom you are dealing. **If you did not initiate the communication, you should not provide any information.**
- Never call the phone number OR click a link provided in an email or text message (phishing scams).
- Protect your cell phone and computer with anti-malware (programs used to remove viruses, spyware, Trojan and other computer threats) products.
- To further protect yourself, please read and follow the "Online Banking Security" tips on our website.

Remember, William Penn Bank will never request personal information from you on the phone or over the computer.

IF YOU SUSPECT THAT YOU HAVE BEEN A VICTIM OF IDENTITY THEFT:

- Contact your financial institution and report suspicious activity. Close existing accounts that you believe may have been compromised and open new ones.
- Change any passwords. If you use the same password for other accounts, change those passwords, too.
- Contact the local police and file a police report.
- Report suspicious e-mails or calls to the FTC (Federal Trade Commission) by calling 1-877-IDTHEFT.
- Call the three major credit bureaus to request that a fraud alert be placed on your credit report:

  Equifax: 1-800-525-6285

  Experian: 1-888-397-3742

  TransUnion: 1-800-680-7289