HORIZON BANK

Fraud Protection and Response Guide

This guide was created to help make our customers aware of the potential risks and threats that are associated with Internet and electronic-based services, and to provide solutions and tools to help prevent fraud and scams.

OVERVIEW

The following sections are included in this Guide.

1. How to Report a Problem
2. Circumstances for Unsolicited Contact by Horizon Bank
3. Special Security Services
4. Alerts (Debit Cards, Internet Banking, e-Statements/e-Notices & Customer Service)
5. Phishing, Vishing, Smishing, Spoofing & Other Threats
6. Online, Email, Mobile, and Text Security Tips
7. Fraud Prevention Risk Self-Assessment Test
8. ID Theft Repair Kit – Steps to Take

1. HOW TO REPORT A PROBLEM

If you suspect your debit card has been compromised, please let us know right away. You can reach us by phone at (800) 264-4274, anytime, day or night, or by email at customer.service@horizon.bank.

For any other issues, please give us a call during any non-Holiday weekday using the (866) 914-2265 toll free number. Email can also be sent to customer.service@horizon.bank to report any banking problem, ask a question or request assistance. If you feel it is important to send confidential information, please use a secure method such as mail (P.O. Box 685133 – Austin, TX 78768), the message feature in our Online Banking system, or our free ***Secure Messaging*** service. (This free service is accessed from the drop-down list of our Online Systems on our website, www.horizon.bank.) Both the message feature in our Online Banking system or the Secure Messaging service will allow you to type any confidential information and attach any documents that may be related to your note.

When reporting a problem, please provide a description of your problem and the action you would like the bank to take. Of course, we will also need your name and information related to the account and transaction. We do provide specific reporting instructions on reporting errors or questions about electronic transactions in our Regulation E disclosure, included with your monthly statement.

2. CIRCUMSTANCES FOR UNSOLICITED CONTACT BY THE BANK

Our staff may contact you by telephone, email or text message if we observe any unusual activity or transactions that may be suspicious or processed through what we consider a high-risk channel. In these cases, we generally will want to confirm that the transactions were legitimate and approved. Our staff will identify themselves and explain the reason for the contact. We should never ask for your passwords or security codes. To assist you in verifying our identity, our staff should be able to provide you information such as your account numbers, transaction details or other personal information associated with the account related to the reason of the contact.

3. INTERNET/ELECTRONIC SPECIAL SECURITY SERVICES

Horizon Bank has incorporated layered security methods into our electronic security services to strengthen the effectiveness of our fraud prevention efforts. The following information outlines some of the services that are associated with our Debit Card and Online Banking systems.

Debit Cards

Debit cards are issued to customers to provide a convenient way to pay for goods and services and access cash at ATMs or merchants. Visa rules establish the primary security framework for these access devices that use the ATM networks or Visa credit card channels to complete the transaction. If selecting “debit” at the time of purchase, the systems will route the

transaction through the ATM network where a PIN is used as the primary security authorization. If "credit" is selected, the transaction is routed through the credit card network and relies on a signature or Visa rules for security requirements and the handling of disputes.

It is important to remember that there are a few differences between a debit card and a credit card. The biggest one that many customers are not aware of is the fact that with a debit card, you do not have the right to dispute a charge due to a disagreement with the service or product that was purchased from a merchant. Therefore, if you feel that you may need to retain that right, use a credit card instead of your debit card.

Here are some of the other security features that are incorporated into debit card transactions.

Visa Card & Security Code Requirements: The Visa system has specific card production requirements that include a magnetic data stripe and a security code on the backside of the card. The security code is often required when the card is used over a telephone and serves as a mini-PIN. Many pay-at-the-pump locations are now also requiring the cardholder's zip code as an identification requirement.

Real-Time Host Connection: Our bank is directly connected to the ATM and Visa networks so we can approve, deny, and mark-up transactions as they are received. This allows you the ability to see inter-day transactions and enables us to use the most up-to-date balance for making the pay/deny decision. If you make a deposit during the day, you will be able to make a purchase on your card the same day.

Real-Time Fraud Analytics: We have a very sophisticated software tool that is reviewing all transaction activity to help identify potential fraud threats. Although it is not foolproof, when we do suspect a problem we will initiate a call to the cardholder and/or suspend the card until we can confirm that it has not been compromised.

Optional Vacation Alerts: Since we look for unusual activity, this includes out-of-territory transactions. So, if you are going to travel, contact our staff so we can update the system for that time period with your general locations to avoid the automatic suspension of your debit card when the first transaction is attempted.

Default Daily Limits: The bank has established a daily maximum dollar amount that will be approved on a daily basis for both ATM and Point-of-Sale transactions. This security setting reduces the ability to take out all of your funds in the account during one day. If you feel that you will need to have a higher limit for a short time or specific transaction, contact the bank and we can adjust your setting to meet your needs. We can also lower your limit upon request. However, we strongly recommend that you do not leave the limit above our standard limits of $500 for ATMs and $5,000 for POS transactions.

PINs: When using the "debit" option, a PIN is required. (In some cases, the PIN will not be required if the purchase is under $25.00.) This PIN can be set to whatever 4-digit code you like, but you will need to contact our customer service department to complete the change on our systems. Do not write your code on the card or place it in your wallet. Also, do not share your PIN with others, including family members.

Transaction Confirmations (e-Commerce & International, in particular): As part of our daily review process, we will attempt to verify certain transactions that might be suspicious. You may receive an email, text or phone call from our staff just checking to make sure that you did authorize the transaction.

Online Banking Mark-ups: With our real-time connection, we are able to mark-up your approved transactions on our online system to help you keep track of every item as they are approved during the day.

Visa Zero Liability: Under Visa's rules, there is a zero liability clause that does provide consumers with an additional level of protection where they should not be charged the $50 maximum liability that is allowed under Regulation E for fraudulent or unauthorized transactions.

Optional Transaction Alerts (Text and/or Email): Horizon Bank offers a free service that we highly recommend for all our debit card users. With it, you can opt to receive a text or email alert within minutes for every attempted debit card transaction. This is a great fraud prevention and recordkeeping tool that will help identify potential fraud attempts immediately. You can set up these alerts by selecting "Create Alerts" under "Preferences" in online banking.

Online Banking Services

Banking services offered over the Internet represent a growing fraud threat due to the ability to transfer funds to other banks using some of the special banking services, such as External Exchange, ACH Origination and Wire Transfers. Online banking also poses a potential threat for the theft of confidential financial information since it contains account information and statements.

To combat this, we have incorporated multiple layers of security into our online banking services to provide secondary levels of authentication besides the initial Logon ID and Password. This section will explain some, but not all, of our security tools to help make sure your information and funds are safe and secure.

Multi-Channel Enabled: We have certain authentication, authorization and alert features that can be sent via the Internet (email), telephone (voice) and SMS (text) to provide alternative methods to prevent a single point of security compromise. Some of the special services, especially related to funds transfers to external institutions, will receive greater scrutiny. Additional authentication methods that use an out-of-band approval (not using an internet-based account or email) may be required or recommended to combat the man-in-the-middle or man-in-the-browser attack.

Computer Registration: Although we never rely only on computer identification as a primary control due to the possibility of compromised security cookies, it does offer a level of security for unsophisticated attacks. The system requires any computer that attempts to logon to the system and has not been previously registered (has the security cookie on the computer) to complete the registration process. The security code is sent to the user's registered email or phone (voice or text) for entry prior to allowing access. This code will be used to register the computer and create the security cookie. As noted below, the system can require the code be sent only to a phone (voice or text) to provide an out-of-band registration. Also, the system can be set to require the registration for every logon attempt to eliminate the threat of a compromised cookie.

IP Reputation Tools: When our security experts identify potentially dangerous/fraudulent Internet sites (as identified by their IP address), we will update our systems to block any access to or from those sites. This is just one of our extra security efforts we employ continuously to protect our customers from potential threats.

Automatic Logoffs (Time-Outs): After 30 minutes of inactivity or 60 minutes of total login time, your logon is automatically disabled and will require you to re-enter your password. The anti-phishing phrase (if you activated that tool) will usually first appear to let you know you are still connected to our servers and have not been re-directed to a fake site.

Login ID & Passwords: We do create unique Logon IDs and Passwords for every user. The password must be from 5 to 15 digits and include at least one number. We can also set your password to automatically expire upon your request as an optional security setting.

Enhanced User Rights & Limits: Our system creates customized rights and limits by user that can restrict activity and features to only what is desired or recommended by the bank. Limits on funds transfer rights and amounts will minimize the risk of unauthorized transactions.

External Funds Independent Pre-processing Confirmations: Prior to completing funds transfers to other institutions, our staff may send out confirmation requests or acknowledgments for certain transactions to make sure the user was aware of the request prior to its completion. A brief delay prior to final processing allows a limited amount of time for you to notify the bank if the transaction was not authorized. If no notice is received, the transaction will be sent unless there are additional security concerns identified by our staff or systems.

Risk & Fraud Software Analytics: Our bank has incorporated a sophisticated software application that will review user behavior and transaction risks to help identify unusual or suspicious activity. If identified, it will automatically alert you and the bank of a possible need for additional approvals or reviews. Although this is not foolproof, it does add yet another layer of risk mitigation against account take-overs**.**

Funds Transfer Back-Office Reviews: Our staff reviews every transaction as it is prepared for processing and does ongoing reviews for suspicious or unusual activity. When identified, we proactively contact our customers for approval prior to processing the transactions.

Optional Administrative New User/Recipient Alerts: For our Cash Management Administrative users, an alert (email, text or voice) can be automatically sent whenever a new sub-user or recipient is added to the company profile. This alert will let you know that a potential unauthorized user or recipient was entered on our system.

Optional One-Time Use Registrations: If desired, we can require you to register you computer every time you logon to prevent the possibility of your security cookie being compromised. Contact our customer service department to add this security setting to your Logon ID.

Optional Voice or Text-Only Computer Registration: As mentioned in the Computer Registration explanation, we can require that only out-of-band registration codes be allowed (no emails). This provides protection against the attacks where the user's computer and email account has been compromised. Contact our customer service department to add this security setting to your Logon ID.

Optional Anti-Phishing Phrase: This works with the Computer Registration cookie and will attempt to confirm that the user is properly connected to our servers and not a fake/redirected site that may look like our site. This phrase is added using the security options under the Preferences drop-down menu.

Password Expirations: Our system requires you to choose a new password at least every 365 days. You may also change your password at any time using the Security options under the Preferences drop-down menu.

Optional Dual-Authorization: For certain funds transfer transactions (funds transfers, ACH Originations, EFTPS and Wires) we can set your rights to where another user tied to your account must approve the transaction to provide a secondary authorization. Contact our customer service department if you would like this security feature added to your account.

Optional Out-of-Band Authorization: Similar to the Dual-Authorizations, we have another security feature that will require approval from an out-of-band source, like your cell phone. It will send a voice or text alert when a funds transfer has been created and needs a reply from the phone message to complete the transaction. Contact our customer service department if you would like to activate this tool.

Optional Physical or Soft Tokens: We have the ability to require a code generated by a secure token (either a physical fob or a mobile app) to be entered for any monetary transaction. The token will automatically generate a new secure code after a short period of time that will be confirmed by our system prior to allowing the transaction to be processed.

Optional PositivePAY: For customers that issue a large number of checks, we do offer a PositivePAY service that will require you to send a daily file of all the items you issue. We will create a list of approved payments that will be used to compare against every item we receive for payment. Call our customer service department for more information on this service.

User Customizable Alerts (Balance, Transaction and Calendar driven): Within our Internet Banking system we have created fully customizable alerts that you can set up to monitor transaction activity, balance changes and date/event driven reminders. Use the Create Alerts option under the Preference drop-down menu to set these alerts up. You may also need to set up your primary contact information under the Security Settings option in that same area.

Mobile Apps and Tablet/iPad Services

Advances in technology continue to make accessing your financial information more convenient. The tablets/iPads can view our Internet Banking system using a browser that will size the information to display better for the smaller-sized screen with these devices. We have a mobile app that is available on iPhones and Android devices. We do allow you to view balances, transaction activity/history, and cleared checks on your checking and savings accounts. You can also perform transfers between your linked accounts and make check deposits using the phone. Security codes and rights are required to connect to the systems and complete any monetary transaction.

Things You Can Do To Help

In addition to our best efforts to protect our systems and provide layered security, you also have an active role to play in helping prevent fraud. Here is a quick list of some tips to live by:

- Sign up for Alerts (for both debit cards and the Internet services)
- Pick good passwords and change every 90 days
- Request other optional security methods such as dual authorizations and tokens for your monetary transactions
- Secure your PC, laptop, tablet, iPad and/or cell phones by setting them to require a code/password after a limited amount of time with no activity. Guard against theft of these access devices.
- Keep virus detection, spyware, malware current
- Activate your personal firewall on your computer
- Keep operating system and browser patches current
- Do not click on links in emails unless your are sure they are from a trusted source
- Don’t install a plug-in or program on your computer unless you know it is legitimate
- Do not post personal information on your Internet profiles
- Shred your documents with confidential information before throwing out
- Review your account activity frequently and balance monthly statements
- Log out of your account when you are done
- Don’t use any public computer for accessing your accounts
- Activate as many of the optional security tools that seem appropriate for your needs
- Report any unusual activity immediately

We hope you found this information useful in explaining our security protection and optional services that you may want to consider. If you have any suggestions on how we can improve on our services or security protection, please let us know.

4. ALERTS (FREE SERVICES TO KEEP YOU INFORMED)

Horizon offers various tools designed to notify you when certain activity or changes occur to your accounts. We strongly recommend that you take advantage of as many of these free services as you feel will keep you up-to-date on your finances and warn you of potential unauthorized activity. Many of the alert services were described in the prior section, but we will highlight some of the most requested and important alerts. Remember that it is much easier to help protect against fraud losses than fill out paperwork and reports to get refunds on posted transactions.

Debit Cards

Debit card fraud continues to be a significant problem and early detection and reporting is the best way to block future transactions and reduce losses for everyone. Upon your request, we can link one or more email addresses and/or cell number(s) to any debit card so you automatically receive email and/or text alerts whenever a transaction is authorized, approved, and/or declined. This is an extremely useful fraud protection tool since these alerts are typically sent within minutes of the attempt/transaction and will tip you off right away if any unauthorized activity has occurred. It also is a great way to receive an electronic receipt that you can use to log in your records when you have an opportunity.

To set up these alerts, contact any of our offices or call (866) 914-2265 and be prepared to tell us which cards and types of alerts you would like enabled. For text alerts, be sure you have a text plan on your phone since the bank will not be responsible for any of the fees or charges assessed by your carrier for those messages. We do not charge any fees for this service.

Online Banking Service

Our Online Banking system has a “Create Alerts” feature located in the Preferences menu that allows you to set up your customized alerts. The system supports email, text and voice alerts. You will need to designate your email, cellphone and telephone numbers for these alerts in the Security section, located in the same menu.

There are three major types of alerts available: transaction-based, account balanced-based; and calendar-based. Some of the reminders you can set up include: when your balance drops below a certain level; when an ACH transaction was created; or when an anniversary, birthday or other special occasion occurs. These alerts are all available at no charge.

Online banking also has several security alerts that can be automatically generated based on account or transaction activity.

e-Statements & e-Notices

To request e-Statements and e-Notices, you must first have an Online Banking account. Once you are logged in to Online Banking, click on the “Statements” link under “Accounts,” which will take you to the enrollment page. Select the account for which you wish to receive e-Statements and e-Notices, approve the disclosure, and you will automatically be set up and able to immediately review your current and past statements.

If you are enrolled in our free e-Statements and/or e-Notices, you will receive an email when a new statement or notice is available. In the subject line, we will include the last 4 digits of the account number that the statement or notice is related to. To retrieve the notices, you simply need to logon into Online Banking and click on the Statements link located in the Account section.

Bank Initiated Alerts (Customer Service)

As part of our ongoing efforts to provide additional security reviews and respond to customer inquiries, our staff may send an alert in the form of an email, text or phone call about special activity or concerns on your accounts. These will include specific information to let you know it is legitimate and will help us ensure we are working to provide you high quality service.

5. PHISHING, VISHING, SMISHING, SPOOFING & OTHER THREATS

Criminals will use many schemes and tactics to try to get unsuspecting victims to drop their reluctance to provide confidential information or allow access to their computers. We have provided many tips and tools in this guide to help you better understand the risks and be prepared to avoid being placed at risk from fraud attacks. That said, new methods, schemes and malicious software arise everyday and we cannot include every threat or security precaution that will make you totally safe.

In this section we will describe some of the common frauds that are targeting victims to obtain access to their financial information or accounts.

Scam Prevention Tips

Let's start with providing some basic rules when dealing with scams and frauds. These simple rules can prevent you from opening yourself up to a fraud attempt that could result in the loss of money or confidential information.

- First and foremost, use common sense. If it sounds too good to be true, it probably is.
- Don't click on links or ads that are delivered without your specific request or efforts.
- Keep you anti-virus, malware, spyware and firewalls current and running.
- Keep your operating system and browsers up-to-date with security patches.
- Never give personal information to a stranger who contacts you, whether by telephone, email, or other means.
- You are responsible and liable for items you cash or deposit into your account, whether they are a check, money order, transfer, etc.
    - Don't accept payments for more than the amount of the service with the expectation that you send the buyer the difference.
    - Don't accept checks from individuals you've only met online.
    - Don't accept jobs in which you are paid or receive commission for facilitating money transfers through your account.
- Be wary of offers of mortgage modification, foreclosure rescue, or short sale scams involving money-back guarantees, title transfers, up-front fees, or high-pressure sales tactics.
- No matter how urgent someone claims a deal or job offer is, you should research and confirm its legitimacy.

Phishing (Email Scams)

This term is used to describe an email that attempts to claim it is from your financial institution (or other company you do business with) and uses language that is designed to have you click on a link in the email to respond to a problem or urgent request. These emails will include logos and can be very authentic looking, but they will always be relaying an urgent need to update your accounts, respond to a security threat or confirm or verify your identification.

What Should You Do If You Receive A Suspicious Email from Horizon Bank?

Our bank will send emails at times for various purposes in response to customer requests. If we are reporting that you have an e-Statement or e-Notice, we normally will include the last few numbers of the account it is related to for your reference. Some emails will also include your name and other account-specific information to help assure you that is from the bank. All email addresses sent from our staff should end in …@horizon.bank. Some of our alerts and automated notifications may have something different, but there should be data in the email that would describe your account or transaction in sufficient detail to make you confident it is legitimate.

However, if you have any questions, do not click on any link in the email. Contact us at (866) 914-2265 or send an email to customer.service@horizon.bank to report the email. We will confirm if it was legitimate and answer any questions you may have.

How Do You Recognize a Fraudulent Email?

The adage, "You can't tell a good book by its cover," is true with emails too. Technology allows criminals to easily copy the look and feel of legitimate emails from financial institutions and change the language and include links. These scams also use pop-up window advertisements and other tricks like surveys and logos of trusted companies (ex. FDIC or Verisign) to add to the credibility of their appearance. Scammers can even impersonate the sender's email address so the communication looks like it is from the financial institution. Since many of the fraudsters may not be located in the U.S., they often make simple mistakes that may tip their hand as a fraud.

The list below has some of the most common things to look for:

- **General Appearance:** The email and graphics just do not look professional or similar to prior emails you have received from the bank.
- **Sender or Reply Email Address**: If you receive an email from Horizon Bank, all your responses should go to an address ending with …@horizon.bank.
- **Anonymous Greeting:** If your name is not in the greeting and it says something like, "Valued Customer" or a similar phase that would work for anyone, that is the first tip. Although our emails may also use the term of "Dear Customer" on the automated emails, there should be some other account/transaction identifying information that would let you know it is from the bank.
- **Weirdly Worded Sentences and Typo's:** Some of these are due to a lack of familiarity of English, but some are intentional to avoid the email being blocked by spam filters. (We hope we do not miss-spell any words in our emails, but it can happen.)
- **Strange or Unfamiliar Links:** When you scroll over a link included in an email, the URL should be that of the sender. If it is something unfamiliar, that is a tip not to click it. Remember, you can always type the URL instead of clicking, since the fraudster can tie another URL to the one that may be listed in the email.
- **Urgent or Compelling Language:** There will always appear to be an urgent need or problem that can only be solved by you clicking on a link or going to a website to provide information. In some cases, they may ask you to call and provide the number. Only use numbers or websites that you have obtained directly from the bank or a company's website. (such as: www.horizon.bank).
- **Misspelled Bank/Company Name:** This is done to attempt to by-pass spam filters. Horizon Bank will sometimes include our official suffix and use Horizon Bank, SSB.

Vishing (Voice/Phone Scams)

Known as **vishing**, or voice phishing, this tactic is a phishing attempt made through a telephone call or voice message. Fraudsters may have the ability to spoof their caller ID so it could appear that the telephone call is coming from a legitimate company. Fraudsters may also have identifying customer information, such as your name, which they may use to make the call appear more authentic. With cell phones and IP communications, you can no longer rely that a call from any area code means the caller is actually in the area of the country that the are code represents, or even that the call is even originating in the U.S.

If you are uncomfortable with a phone call that was not initiated by you, hang up or ask for the purpose of the call. Then, contact the company using legitimate sources such as contact phone numbers found on the company's website, your bank statements, and those listed on your ATM, debit or credit card.

Smishing (Text Scams)

A phishing attempt that is sent via SMS (Short Message Service) or text message to a mobile phone or device is referred to as **smishing**. The purpose of text message phishing is the same as traditional email phishing: to convince recipients to share their sensitive or personal information.

Never take action on a request for your personal or financial information, including account numbers, passwords, Social Security number or birth date. Use caution if you receive a text message expressing an urgent need for you to update your information, activate an account, or verify your identity by calling a phone number or submitting information on a website. These messages may be part of a phishing scam conducted by fraudsters in an attempt to capture your confidential account information and may be used to commit fraud.

Spoofing (Fake Site Scams)

Fraudsters may attempt to direct you to spoof websites via emails, pop-up windows or text messages. Because it is very easy to copy a website's appearance including all the graphics, be wary when you receive a link for any bank or company that you did not intentionally seek. Sometimes fraudsters will register URLs for sites that are close the spelling of a legitimate site, realizing that people may miss-type the address. They will copy the true site and add some text that will announce some problem where the customer is asked to verify their information. These websites are used to try to obtain your personal information. One way to detect a phony website is to consider how you got to the site. Use caution if you may have followed a link in a suspicious email, text message, online chat or other pop-up window requesting your personal or account information. We recommend that you type in the URL instead of clicking any link since they may not actually go where the listing said it would.

Other Scams

Scams seem to be growing as fast as new technology or services are introduced or developed. Some other ways that the scam is promoted is through the use of pop-up windows – small windows or ads – to obtain personal information. These windows

may be generated by programs hidden in free downloads such as screen savers or music-sharing software. To protect yourself from harmful pop-up windows, avoid downloading programs from unknown sources on the Internet and always run anti-virus software on your computer.

Some fraudsters still use low-tech methods to obtain your personal and financial information. Phishing attempts can be made through regular mail or fax machines. If you are suspicious about a piece of mail or fax you have received that requests personal or financial information, you should discard it. If you've responded to a mail or fax phish and provided personal or financial information, contact the company the mail or fax appears to be from. Use a legitimate source such as the phone number listed on the company's website, billing statement, or on the back of your ATM, debit or credit card to let the company know that your information was compromised.

6. ONLINE, EMAIL, MOBILE AND TEXT SECURITY TIPS

In this section we have summarized some general tips that may help you keep your information and money safe from a fraud attack. Some of them have been mentioned in other areas of the guide, but it never hurts to be reminded. Feel free to share this information with your friends and family

Online Security Tips

- Do not use your Social Security number as a username or password. Change your usernames and passwords regularly and use combinations of letters, numbers, and special characters such as # and @. Do not use your online banking username and passwords as credentials for other online accounts.
- Protect your online passwords. Don't write them down or share them with anyone.
- If used, protect your answers to security questions. Select questions and provide answers that are easy for you to remember, but hard for others to guess. Do not write down your security questions or answers or share them with anyone. If you have selected security questions on other websites, avoid using the same questions to protect your Horizon Bank Online Banking account. Please note that we will never ask you to provide answers to your security questions via email.
- Use secure websites for transactions and shopping. Shop with merchants you know and trust. Make sure Internet purchases are secured with encryption to protect your account information. Look for "secure transaction" symbols like a lock symbol in the lower right-hand corner of your web browser window, or "https://…" in the address bar of the website. The "s" indicates "secured" and means the web page uses encryption.
- Always log off from online banking and any website after using your credit or debit card, or other sensitive information. If you cannot log off, quit your browser to prevent any potential unauthorized access to your account information.
- Quit your browser when you're not using the Internet.
- Be cautious when using public hotspots because they may have little security. Consider setting your Wi-Fi auto-connect settings to use the highest security settings.

Email Security Tips

- Be wary of suspicious emails. Never open attachments, click on links, or respond to emails from suspicious or unknown senders.
- If you receive a suspicious email that you think is a phish, do not respond or provide any information. Send the email to customer.service@horizon.bank
- If you respond to a phish email with personal or account information, contact our staff at (866) 914-2265.

Mobile Banking Security Tips

When you use a mobile device for browser or text-based account access, keep these tips in mind:

- Use the keypad lock or phone lock function on your mobile device when it is not in use. These functions password-protect your device to make it more difficult for someone else to view your information. Also be sure to store your device in a secure location.
- Frequently delete text messages from your financial institution, especially before loaning out, discarding, or selling your mobile device.

- Never disclose via text message, phone call or email your personal or financial information, including account numbers, passwords, and Social Security number or birth date.
- If you lose your mobile device or change your mobile phone number, remove the old number from your mobile banking profile under the "Mobile Banking Options" link under the Preferences drop-down menu in Online Banking

Applications are programs you can download to your mobile device. Applications or "apps" that let you monitor your finances and conduct certain transactions are increasing in popularity.

- Download mobile apps from reputable sources only to ensure the safety of your personal and account information. We encourage users to download the most recent versions of our apps and keep them updated. Our apps are supported by Android and iPhone devices.
- For your security, sign off when you finish using an app rather than just closing it.

Computer Security Tips

- Avoid downloading programs from unknown sources.
- Keep your computer operating system up-to-date to ensure the highest level of protection.
- Install a personal firewall on your computer.
- Install, run and keep anti-virus and other software updated.
- Turn your computer off completely when you are finished using it – don't leave it in sleep mode.
- Conduct online banking activities on secure computers only. Public computers (computers at internet cafes, copy centers, etc.) should be used with caution, due to shared use and possible tampering. Online banking activities and viewing or downloading documents (statements, etc.) should only be conducted on a computer you know to be safe and secure.
- Ensure your computer software and plug-ins are current. Before downloading an update to your computer program, first go to the company's website to confirm the update is legitimate

7. FRAUD AWARENESS CUSTOMER SELF AUDIT WORKSHEET

Horizon Bank is concerned about your privacy and security regarding your confidential financial information. This worksheet is provided as a tool to evaluate the risks and security issues related to certain activities or behaviors in your daily life.

All the answers should be "Yes," and any "No" answers indicate that you may be at a greater risk for an attempted or successful fraud attack. If you have any questions about the security of your accounts at the bank, please contact any of our customer service representatives.

Self-Audit Questionnaire for Fraud Awareness:

Yes	No	
□	□	Your computers have anti-virus, spyware and malware protection software that is updated regularly with scheduled scans performed at least on a weekly basis. Your operating systems and web-browsers are also updated with the latest patches, and you have activated your personal firewall. [*If No, install and update these critical software tools regularly from legitimate sources.]*
□	□	When using social media, you do not include personal information such as your physical address, phone number or date of birth including the year. Additionally, you do not list any additional confidential information such as the city where you were born, your mother's maiden name, or Social Security Number on websites or comments. [If No, remove this information from your profiles or comments.]
□	□	You use different passwords for your various banking sites which do not include easily guessable words or identifiable traits such as your birthday, name of a family member, or pet. Your passwords are not less than 5 characters and at least 2 of the characters are a number, special symbol and/or Capital letter. *[If No, change your passwords. We recommend that you change them every 90 days.]*
□	□	When using email, you never include confidential information about your financial

accounts or other information that could provide access to your banking accounts. This would include your account numbers, bank name, login IDs, passwords and other confidential information. You do not click on links in emails unless you are sure they are from a legitimate or trusted source.
[If No, stop including this information – email is insecure and can be intercepted.]

□ □ When discarding statements or other documents that contain confidential information, you always shred the document or obliterate the information that is confidential. This information typically is the account number, name, address, bank or other identifying data that could be used to allow unauthorized access or an account takeover.
[If No, start shredding or masking data – dumpster diving is a big ID theft threat.]

□ □ You reconcile your monthly statements and report any discrepancy or suspicious activity immediately. You receive e-Statements to reduce the risk of mail theft.
[If No, review transactions and balance statements monthly; request e-Statements.]

□ □ You have set up transaction and balance alerts on your debit cards or deposit accounts to warn you when transactions are completed or if the balance changes significantly.
[If No, contact us to set up alerts as necessary to monitor activity.]

Answering "Yes" to all these questions will not guarantee that you will not be a victim of fraud, but it should lower your exposure to many of the common threats and risks in the marketplace.

8. IDENTITY THEFT REPAIR KIT – STEPS TO TAKE

This checklist will help you get started on the tasks to deal with an Identity Theft attack. We also have ID Theft Consumer Guides that have much more information on our website that were developed by the Federal Trade Commission. (This is the federal agency that is responsible for tracking and assisting victims of ID Theft.)

1. Contact Horizon Bank.
- ☐ Report any fraudulent activity on your Horizon Bank accounts by calling us at (866) 914-2265.
- ☐ Review activity on all accounts, including your checking, savings, credit card, debit card, loans, or online banking accounts, and look for changed addresses, changed Personal Identification Numbers (PINs), or new cards ordered.
- ☐ Close accounts that have been breached and reopen them with new account numbers, passwords, and PINs.
- ☐ Change your online banking username and password.

2. Contact the major credit bureaus.
- Equifax: 1-800-525-6285 or www.equifax.com
- Experian: 1-888-397-3742 or www.experian.com
- TransUnion: 1-800-680-7289 or www.transunion.com
  - ☐ Place a "fraud alert" on your credit file.
  - ☐ Request a free copy of your credit report.

3. Contact other creditors.
- ☐ Contact credit card companies, utility providers, banks, lenders and financial institutions.
- ☐ Follow up phone conversations with a letter or email.
- ☐ Close accounts that have been breached and reopen them with new account numbers, passwords, and PINs.

4. File a report with local police.
- ☐ A police report will lend credibility to your case when dealing with creditors who may require proof of criminal activity.

5. Report the criminal activity to the Federal Trade Commission (FTC).
- ☐ Call 1-877-ID THEFT (1-877-438-4338) to speak with a trained identity theft counselor.
- ☐ You can also file your complaint online at www.consumer.gov/idtheft.

6. Contact other agencies as appropriate.
- ☐ Notify the **Postal Inspection Service** if you believe your mail was stolen or redirected: www.usps.com.

- ☐ Call the **Social Security Fraud Hotline** if you suspect someone is using your Social Security number for fraudulent purposes: 1-800-269-0271.
- ☐ Contact your local **Department of Motor Vehicles** office if you believe someone is trying to get a driver's license or identification card using your name and information: www.dmv.org.

7. Continue to carefully review all your accounts.

- ☐ Since identity theft can take time to completely resolve, carefully review all charges and transactions appearing on account statements and online.
- ☐ Report any discrepancies immediately.

8. Keep track of the organizations you contact.