Retail/Consumer Client

Internet Banking
Awareness and Education Program

1.855.678.7226 servicecenter@opusbank.com www.opusbank.com

Rev. 09/2015

Table of Contents

Retail/Consumer Client Internet Banking Awareness and Education Program

Securing Your Environment

Your identity is one of the most valuable things you own. It's important to keep your identity from being stolen by someone who can potentially harm your good name and financial well-being. Identity theft occurs when someone uses your name, address, Social Security Number, credit card or financial account numbers, passwords, and other personal information without your knowledge to commit fraud or other crimes. While the words may sound like a foreign language -- Phishing, Pharming, Vishing, Spyware, Dumpster Diving — they are the names of various techniques used by thieves to put your identity and finances at risk. These types of attacks grow more frequent and sophisticated every year. Identity theft is the fastest growing crime in the United States. According to U.S. Department of Justice statistics, identity theft exceeds drug trafficking as the number one crime in America.

Unsolicited Client Contact

Opus Bank will never contact its clients on an unsolicited basis to request their security logon credentials such as the combination of the client's username and password. If you receive a request of this type, do not respond to it. Please call us immediately at **(855) 860-5952** or e-mail us at fraudunit@opusbank.com to report any activity of this nature.

Opus Bank will only contact its clients regarding online banking activity on an unsolicited basis for the following reasons:

- Suspected fraudulent activity on your account;
- Inactive/dormant account;
- To notify you of a change or disruption in service; or
- To confirm changes submitted to your online banking profile.

If you receive an unsolicited contact from an Opus Bank team member for any reason not cited above, your identity will be confirmed through a series of security questions and you will always have the option of hanging up and calling Opus Bank to confirm that validity of our request. Remember, Opus Bank will NEVER ask for your logon security credentials.

Protecting Your Identity

The simple fact is you can protect yourself against most forms of identity theft. The first step is education. To make it easier to understand, we've divided identity theft into the 5 "Risks." Take a few moments to learn about each of the Risks and the steps you can take to avoid being a victim.

1) E-mail Risk

Phishing is an e-mail scam that is often used by cybercriminals to steal:

- Money via unauthorized wire transfers or ACH transactions
- Confidential personal information
- Online banking authentication credentials (User IDs and Passwords)

Retail/Consumer Client Internet Banking
Awareness and Education Program

A phishing e-mail may appear in your inbox, claiming to be from your financial institution, a family member, or any other trusted source. It may appear authentic but be careful as it can potentially be a scam. Do not respond to these types of e-mails and **do not** click on any attachments or links contained within these e-mails.

How to spot phishing e-mail scams:

- The sender's email address may not be accurate. Often, cybercriminals change or rearrange one letter in an e-mail address in an attempt to make it look legitimate:
    - Example: banker@opusbank.com vs. banker@opsubank.com (see the difference?)
- Any e-mail requesting personal information (user ID, password, social security number, tax ID, etc.), or asking you to verify an account, is usually a scam, even if it looks authentic.
- The e-mail may instruct you to click on a link, open an attachment, or call a phone number to update your account or even claim a prize, such as a sweepstake or lottery.
- The message will often threaten a dire consequence if you don't respond immediately.
- Sometimes you cannot spot a phishing e-mail because the sender's email account may have been hacked! Always be vigilant!

Follow these steps to avoid e-mail scams:

- Never reply to an e-mail asking for confidential information, even if it appears urgent. Chances are it is a phishing e-mail.
- Never click on a link from an unknown e-mail. Instead, if an e-mail link is claiming to navigate you to the Bank's website, instead type the known website address into your Internet browser. Fraudsters often setup fake websites made to look like your Bank's website.
- Never attempt to open an attachment from a suspicious e-mail. If you receive a suspicious attachment, call the sender and confirm that they sent you an attachment. Attachments, if opened, can contain malware (malicious software) and viruses that can infect your computer.
- Do not call any phone number provided in a suspicious e-mail. It could be a fake phone number. Instead, call a known phone number from a secure contact list of approved vendors, your business partner, and your financial institutions.
- Always use anti-virus and anti-spyware software on your computer, and keep them up-to-date. Refer to your Account Terms and Conditions for further security requirements.

Remember, **e-mail is not a secure form of communication.** If you follow the basic steps listed above, you can protect yourself from most phishing and other e-mail scams.

2) Internet Risks

The Internet is a great place to browse and do business, however it can also be a dangerous place for identity theft if you don't know what to watch for or how to protect yourself. There are

several types of malware – which means malicious software – that can infect your computer as you surf the web including:

- Viruses
- Spyware/Adware
- Trojan Horses
- Keystroke Loggers
- Ransomeware

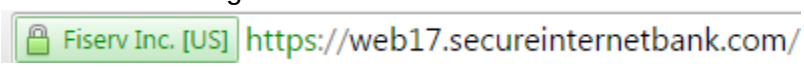
These programs are becoming more sophisticated and ingenious in their ability to infect your computer. Many are designed to steal your personal and/or business information. While "surfing" the Internet, follow these steps to protect your computer from the majority of Internet crime:

- Make sure you have anti-virus and anti-spyware software installed on your computer, keep them up-to-date, and run a full system scan at least weekly.
- Keep your computer operating system and application security patches current, and your firewall turned on.
- If you download anything from the Internet such as music, movies, or pictures, make sure you do so only from trusted websites. Downloads can be infected with spyware/adware attached to the file.
- Watch for signs of spyware—frequent pop-up ads, unexpected icons on your desktop, random error messages or sluggish computer performance are all signs of infection. The pop-up ads (adware) sometimes appear to offer free credit reports or credit scores as part of the scam. Opus Bank does not offer credit scores or credit reports. Run a full system anti-virus and anti-spyware scan to identify and safely remove spyware.
- Be careful when using public computers to perform any type of personal transactions. Just logging into a Website may give away passwords and other private information if spyware has been installed on that computer.
- Consideration should be given to designating a separate desktop for corporate online banking and visibly label the "online banking computer".
- When visiting the Bank's website and online banking website, ALWAYS ensure that it is the actual website. This can be done by visually verifying that the website is displaying an Extended Validation SSL Certificate (EV Certificate). The EV Certificate is a green bar to the left of the website address that validates that the website being visited is the true website. Example:

  For the Bank's website:

  For online banking:

Retail/Consumer Client Internet Banking
Awareness and Education Program

Following these steps will help protect you from the most common forms of identity theft while surfing the Internet.

3) Telephone Risk

The telephone is one of the most often used sources for criminal activity. Here's how it works. Your phone rings. The caller claims to be from your financial institution, or any other source. They begin asking questions about you and your account. This could be a telephone scam called Vishing. Someone is attempting to steal your identity, and it happens to millions of Americans every year.

Protect yourself from telephone scams by following these steps to protect yourself from most types of identity theft telephone scams:

- Never offer personal or account information over the phone without verifying the caller's identity.
- If you are uncertain of the identity of a caller, hang up and initiate the call yourself using a known phone number.
- Do not call any phone number received in a voice message or e-mail asking for personal information. It could lead you to a phony answering system.

As a general guideline, be highly suspicious anytime you are requested to provide personal information over the phone.

4) Payment Risk

Payment fraud happens when someone uses information from your checks, credit and debit cards, or any other form of payment without your knowledge to commit fraud or other crimes. Payment fraud can also occur when someone fraudulently accesses your online banking account to initiate unauthorized payments or money transfers. Payment fraud and other forms of identity theft can be avoided, if you know how to protect yourself.

Don't make it easy for criminals to steal your personal information by following some common sense tips to protect your identity:

- Protect your online banking access credentials. Never share your online banking User ID or password with anyone.
- Balance your checkbook and verify all account and credit card statements as soon as they arrive.
- Keep all checks, credit cards, and debit cards in a safe place.
- Don't leave outgoing checks or paid bills in your mailbox, and report lost or stolen items immediately.
- Don't write PIN numbers on your credit or debit cards, or leave them in your wallet for a thief to find.
- Use a paper shredder to securely dispose of any documents containing personal information.
- Make online purchases only from trusted Web sites. If you have questions about a company, you can check them out with the Better Business Bureau.

- Consider paying all your bills electronically with online bill pay. This method is considered more secure than mailing paper checks.

Reducing your risk of identity theft starts with protecting your personal information. Keep it from getting into the wrong hands. Always be diligent about protecting your identity.

5) Home Risks

The simple act of sending and receiving mail and putting your trash out at night can put your personal information at risk. Financial information, checks, account and credit card statements, and monthly bills can be stolen from your home, mailbox or even from your trash, and used to access your accounts and steal your identity.

Follow these steps to protect against identity theft in your home

- Invest in a personal shredder. This is your first line of defense. Shred checking and credit card statements, cancelled checks, pre-approved credit card offers, or anything with your personal information on it before disposal.
- Place your garbage out on the morning of pickup rather than the night before. This gives "dumpster divers" less opportunity to go through your trash.
- Install a mailbox with a locking mechanism, or pick up your mail immediately after it is delivered each day.
- Change that old habit of placing mail in your mailbox for the carrier to pick up. Always place out-going mail in an official, secure mailbox.
- It's good practice to store your mail, account statements, and other papers where they are out of sight and out of reach of anyone who might be in your home.

By following these steps you are on the right track to protecting your identity. Learning about all the identity theft danger zones and the simple steps you can take to avoid being a victim, is the best way to protect your good name.

Opus Bank Contacts

You are protected in a variety of ways when you use Internet Banking; however it is important to contact Opus Bank in the event you discover that you have lost your debit card or your online login information has been compromised. Also, report any unauthorized or unexpected transactions immediately.

Your account is protected against fraudulent transactions in a number of ways, so monitor your account balances and transactions frequently. If you want to report suspicious activity in your account, or if you have questions about the security of your account, you can call us at: **(855) 678-7226** or e-mail us at fraudunit@opusbank.com.

The security of your money and identity is as important to us as it is to you. Let's work together to protect it.

Retail/Consumer Client Internet Banking
Awareness and Education Program

Regulation E: Electronic Fund Transfers

This law is designed to protect consumers making electronic fund transfers. The term "electronic fund transfer" (EFT) generally refers to a transaction initiated through an electronic terminal, telephone, computer, or magnetic tape that instructs a financial institution either to credit or debit a consumer's asset account.

The Electronic Fund Transfer Act (also known as Regulation E), which was issued by the Board of Governors of the Federal Reserve System and adopted in 1978 as an add-on to the Consumer Credit Protection Act. The law and regulation establish the basic rights, liabilities and responsibilities of consumers who use electronic fund transfer services and of financial institutions that offer these services.

The following describes some examples of what is covered and not covered under Regulation E:

What is covered?	What is not covered?

Any transfer of funds that are 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;
• Electronic check conversion, whereby you may authorize a merchant or other payee to make a one-time electronic payment from your checking account using information from your check to pay for purchases or pay bills; and
• Electronic returned check charge, whereby you authorize a merchant or other payee to initiate an electronic fund transfer to collect a charge in the event a check is returned for insufficient funds.
	• Checks;
	• Check guarantee or authorization;
	• Wire or other similar transfers through Fedwire;
	• Securities and commodities transfers;
	• Automatic transfers by account-holding institutions;
	• Any preauthorized transfer to or from an account if the assets of the account-holding financial institution were $100 million or less on the preceding December 31.and
	• *Telephone-initiated transfers.* Any transfer of funds that:
	  o Is initiated by a telephone communication between a consumer and a financial institution making the transfer; and
	  o Does not take place under a telephone bill-payment or other written plan in which periodic or recurring transfers are contemplated.

Note: When a banking account is opened, all retail/consumer clients receive a Regulation E Disclosure, as required by the EFT Act, which will contain detailed information related to the regulation.

Retail/Consumer Client Internet Banking Awareness and Education Program

Purpose

On June 28, 2011, the FFIEC (Federal Financial Institutions Examination Council) issued a supplement to the *Authentication in an Internet Banking Environment* guidance released in October 2005. The purpose of the supplement is to reinforce the guidance's risk-management framework and update the FFIEC member agencies* expectations regarding customer authentication, layered security, or other controls in the increasingly hostile online banking environment.

The purpose of the Opus Bank Retail/Consumer Client Internet Banking Awareness and Education Program (the "Program") is to ensure that our Internet Banking clients are aware of the risks of using Internet Banking. The Program will remind clients about the importance of security measures that can protect them from being victims of fraud. Specifically the program will address the importance of password security, using unique user accounts, and ensuring their computer systems that are used for Internet Banking have security software, such as firewalls, and updated anti-virus protection. The Program will include education about security threats, provide information to help them increase and maintain password security by enforcing a strong password requirement and periodic password changes. At Opus Bank, we strongly believe that public awareness of Internet Banking risks and how to avoid them is the strongest weapon in the defense against monetary losses.

The following topics are intended to address the minimum elements that are part of Opus Bank's Retail/Consumer Client Internet Banking and Awareness and Education Program.

** The member agencies include the FRB, FDIC, NCUA, OCC and CFRB. For more information, please visit www.FFIEC.gov.*