CUSTOMER SECURITY AWARENESS PROGRAM

Customer Awareness Program
Audubon Savings Bank's Commitment to Security

Each year more and more people have their identity stolen and the staff and management of The Audubon Savings Bank want to give you the information you need to help protect yourself against ID theft.

While we cannot guarantee that your ID will never be stolen we will NEVER request personal information by email or text messaging including account numbers, passwords, personal identification information or any other confidential customer information.

Fraudulent emails may be designed to appear as though they are originated by Audubon Savings Bank. Do not respond to any email communications which request any type of personal or confidential information and do not go to any links listed on that email. These communications are not originated by Audubon Savings Bank!
Never give out any information that the Bank already has to a caller, texter, or email sender. If you contact us we may verify the last 4 digits of your SSN, or the date of your last deposit to confirm your identity but we will never contact you and ask for your debit/credit card number or your full SSN. If we need to contact you, it will always be done in a manner that protects your personal, confidential information and we will clearly identify ourselves.
One of Audubon Savings Bank's top priorities is to safeguard YOUR confidential information and we work diligently to do so.

We always work with the local regulatory and law enforcement departments to be certain any type of illegal activity is stopped as soon as possible. We have multi-layer security to protect your confidential information and will continue to be vigilant in protecting it.

Immediately report any suspicious emails or websites to Audubon Savings Bank by forwarding the message to info@audubonsavings.com
If you suspect identity theft or have any questions regarding this notice, please contact Audubon Savings Bank at 856-656-2202.

June 2017

Unsolicited Customer Contact

Audubon Savings Bank will never contact its customers on an unsolicited basis to request their security logon credentials such as the combination of the customer's username and password. If you receive a request of this type, do not respond to it. Please call us immediately at 856-656-2202 or e-mail us at info@audubonsavings.com to report any activity of this nature.

Audubon Savings Bank will only contact its customers 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 Audubon Savings Bank 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 Audubon Savings Bank to confirm that validity of our request.

Remember, Audubon Savings Bank will NEVER ask for your logon security credentials.

Online Banking Security

Audubon Savings Bank is committed to protecting your personal information. Our Online Banking uses several different methods to protect your information. All information within our Online Banking uses the SecureSocket Layer (SSL) protocol for transferring data. SSL is a cryptosystem that creates a secure environment for the information being transferred between your browser and Audubon Savings Bank. All information transferred through Online Banking has a 128-bit encryption which is the highest level of encryption. In addition to the security features put in place by Audubon Savings Bank here are some tips on keeping your information secure.

- Never give out any personal information including User Names, Passwords, SSN or Date of Birth
- Create difficult passwords which include letters, numbers, & symbols when possible
- Don't use personal information for your user names or passwords like Birth Dates & SSN
- Avoid using public computers to access your Online Banking
- Don't give any of your personal information to any web sites that does not use encryption or other secure methods to protect it

What is Identity Theft?

Identity theft involves the unlawful acquisition and use of someone's identifying information, such as:

- Name
- Address
- Date of Birth
- Social Security Number
- Mother's Maiden Name
- Driver's License
- Bank or Credit Card Account Number

Thieves then use the information to repeatedly commit fraud in an attempt to duplicate your identity which may include opening new accounts, purchasing automobiles, applying for loans, credit cards, and social security benefits, renting apartments and establishing services with utility and telephone companies. It can have a negative effect on your credit and create a serious financial hassle for you.

How do I protect myself?

- Report lost or stolen checks or credit cards immediately
- Never give out any personal information including birth date, SSN or Passwords
- Shred all documents containing personal information, like bank statements, unused checks, deposit slips, credit card statements, pay stubs, medical billings, and invoices
- Don't give any of your personal information to any web sites that do not use encryption or other secure methods to protect it

For more information about identity theft and other tips on how to protect yourself and your information please visit the following websites.
Caution-By clicking on the links below you will be leaving Audubon Savings Bank's secure website.

Computer Security
www.onguardonline.gov
Federal Trade Commission:
www.ftc.gov/bcp/edu/microsites/idtheft
FDIC Consumer Alerts:
www.fdic.gov/consumers/consumer/alerts
United States Department of Justice:
www.usdoj.gov/criminal/fraud
Equifax
P O Box 105069

Atlanta, GA 30349-5069
www.equifax.com
To order a report: (800) 685-1111
To report fraud: (800) 525-6285
Experian
P O Box 2002
Allen, TX 75013-0949
www.experian.com
To order a report: (888) 397-3742
To report fraud: (888) 397-3742
Trans Union
P O Box 1000
Chester, PA 19022
www.transunion.com
To order a report: (800) 916-8800
To report fraud: (800) 680-7289

Debit Card Protection

Debit card usage has increased dramatically in recent years and fraudulent use of debit cards has also increased.
We at Audubon Savings Bank have some suggestions for you for the care and usage of debit cards.

- NEVER give your debit card information when requested by phone, email, or texting. We at neither Audubon Savings Bank nor any other bank we know of will ever request information from you in this manner. Please contact us if you receive any such request.
- If available, use the EMV Chip card.
- It is a good idea to pay by credit card if your card leaves your sight. An example might be when a waiter takes your card from your table in a restaurant or when ordering online. Debit cards are easier to process illegally vs. credit cards.

Regulation E: Electronic Fund Transfers

Regulation E protects individual customers using electronic funds transfers (EFT). Non-consumer accounts are not protected by Regulation E.

What is an EFT?
An EFT is any transfer of funds that is 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
- Transfers initiated through internet banking and bill pay.

How does Regulation E apply to a consumer using Online Banking and/or Bill Pay?

Regulation E is a consumer protection law for accounts such as checking or savings, established primarily for personal, family, or household purposes. Regulation E provides consumers a means to notify their financial institution that an EFT has been made to their account without their permission. If you are unsure if your account is protected by Regulation E contact us.

Refer to the Banks Electronic Funds Disclosure for more information regarding your rights under the regulation. You may find the Electronic Funds Disclosure in your new account packet, or may access the disclosure online.

Business/Commercial customers are not covered by Regulation E.

As a result, it is critical that business/commercial customers implement sound security practices within their places of business as outlined in this Program to reduce the risk of fraud and unauthorized transactions from occurring.

Good practices can keep business/commercial customer's information secure.

Corporate Account Takeover

Corporate Account Takeover is a form of identity theft in which criminals steal your valid online banking credentials. The attacks are usually stealthy and quiet. Malware introduced onto your systems may go undetected for weeks or months. Account-draining transfers using stolen credentials may happen at any time and may go unnoticed depending on the frequency of your account monitoring efforts.

The good news is, if you follow sound business practices, you can protect your company:

- Use layered system security measures: Create layers of firewalls, anti-malware software and encryption. One layer of security might not be enough. Install robust anti-malware programs on every workstation and laptop. Keep the programs updated.
- Manage the security of online banking with a single, dedicated computer used exclusively for online banking and cash management. This computer should not be connected to your business network, should not retrieve any e-mail messages, and should not be used for any online purpose except banking.
- Educate your employees about cybercrimes. Make sure your employees understand that just one infected computer can lead to an account takeover.

Make them very conscious of the risk, and teach them to ask the question: "Does this e-mail or phone call make sense?" before they open attachments or provide information.

- Block access to unnecessary or high-risk websites. Prevent access to any website that features adult entertainment, online gaming, social networking and personal e-mail. Such sites could inject malware into your network.
- Establish separate user accounts for every employee accessing financial information and limit administrative rights. Many malware programs require administrative rights to the workstation and network in order to steal credentials. If your user permissions for online banking include administrative rights, don't use those credentials for day-to-day processing.
- Use approval tools in cash management to create dual control on payments. Requiring two people to issue a payment – one to set up the transaction and a second to approve the transaction – doubles the chances of stopping a criminal from draining your account.
- Review or reconcile accounts online daily. The sooner you find suspicious transactions, the sooner the theft can be investigated.

Self-Assessment

Online Banking Business/Commercial customers are strongly encouraged to perform an annual Self-Assessment focusing on their online banking practices and network security. A Self- Assessment will evaluate whether the customer has implemented sound business practices to address the five key principles outlined in the "Securing Your Business" section within this document.

Securing Your Business

Is your company keeping information secure?
Are you taking steps to protect sensitive information? Safeguarding sensitive data in your files and on your computers is just plain good business. After all, if that information falls into the wrong hands, it can lead to fraud or identity theft. A sound data security plan is built on five key principles:

- **Take stock**. Know the nature and scope of the sensitive information contained in your files and on your computers.
- **Scale down**. Keep only what you need for your business.
- **Lock it.** Protect the information in your care.
- **Pitch it**. Properly dispose of what you no longer need.
- **Plan ahead**. Create a plan to respond to security incidents.

The following information is provided by the Federal Trade Commission, Bureau of Consumer Protection.

Take Stock

Know the nature and scope of the sensitive information contained in your files and on your computers.

- Take inventory of all file storage and electronic equipment. Where does your company store sensitive data?
- Talk with your employees and outside service providers to determine who sends sensitive information to your business, and how it is sent.
- Consider all of the methods with which you collect sensitive information from customers, and what kind of information you collect.
- Review where you keep the information you collect, and who has access to it.

Scale Down

Keep only what you need for your business.

- Use Social Security numbers only for required and lawful purposes. Don't use SSNs as employee identifiers or customer locators.
- Keep customer credit card information only if you have a business need for it.
- Review the forms you use to gather data — like credit applications and fill-in-the-blank web screens for potential customers — and revise them to eliminate requests for information you don't need.
- Change the default settings on your software that reads customers' credit cards. Don't keep information you don't need.
- Truncate the account information on any electronically printed credit and debit card receipts that you give your customers. You may include no more than the last five digits of the card number, and you must delete the card's expiration date.
- Develop a written records retention policy, especially if you must keep information for business reasons or to comply with the law.

Lock It

Protect the information that you keep.

- Put documents and other materials containing sensitive information in a locked room or file cabinet.
- Remind employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.
- Implement appropriate access controls for your building.
- Encrypt sensitive information if you must send it over public networks.
- Regularly run up-to-date anti-virus and anti-spyware programs on individual computers.
- Require employees to use strong passwords.
- Caution employees against transmitting personal information via e-mail.
- Create security policies for laptops used both within your office, and while traveling.
- Use a firewall to protect your computers and your network.
- Set "access controls" to allow only trusted employees with a legitimate business need to access the network.
- Monitor incoming Internet traffic for signs of security breaches.
- Check references and do background checks before hiring employees who will have access to sensitive data.
- Create procedures to ensure workers who leave your organization no longer have access to sensitive information.

- Educate employees about how to avoid Phishing and phone pretexting scams.

Pitch It

Properly dispose of what you no longer need.

- Create and implement information disposal practices.
- Dispose of paper records by shredding, burning, or pulverizing them.
- Defeat "dumpster divers" by encouraging your staff to separate the information that is safe to trash from sensitive data that needs to be discarded with care.
- Make shredders available throughout the workplace, including next to the photocopier.
- Use a "wipe" utility programs when disposing of old computers and portable storage devices.
- Give business travelers and employees who work from home a list of procedures for disposing of sensitive documents, old computers, and portable devices.

Plan Ahead

Create a plan for responding to security incidents.

- Create a plan to respond to security incidents, and designate a response team led by a senior staff person(s).
- Draft contingency plans for how your business will respond to different kinds of security incidents. Some threats may come out of left field; others — a lost laptop or a hack attack, to name just two — are unfortunate, but foreseeable.
- Investigate security incidents immediately.
- Create a list of who to notify — inside or outside your organization — in the event of a security breach.
- Immediately disconnect a compromised computer from the Internet.

Audubon Savings Bank Contacts

You are protected in a variety of ways when you use Internet Banking; however it is important to contact Audubon Savings Bank in the event you that your company's online access 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(s), or if you have questions about the security of your account(s), you can call us at: 856-656-2202 or e-mail us at info@audubonsavings.com.

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

Additional Resources

The following links are provided solely as a convenience to our Business/Commercial Online Banking customers. Audubon Savings Bank neither endorses nor guarantees in any way the organizations, services, or advice associated with these links. Audubon Savings Bank is not responsible for the accuracy of the content found on these sites.

- Avoiding Online Scams:
  http://onguardonline.gov/articles/0001-avoiding-online-scams
- Avoiding Social Engineering and Phishing Attacks:
  http://www.us-cert.gov/cas/tips/ST04-014.html

- Computer Security:
  http://onguardonline.gov/articles/0009-computer-security
- Phishing:
  http://onguardonline.gov/articles/0003-phishing
- Phishing – Avoid the Bait:
  http://onguardonline.gov/flash/phishing_loader.swf?fileToLoad=http://www.onguardonline.gov/flash/phishing.swf
- Consumer Advisories:
  http://www.ic3.gov/media/2010/WorkAtHome.pdf
- Consumer Threat Alerts:
  http://home.mcafee.com/consumer-threats-signup
- OCC Consumer Advisories:
  http://www.occ.treas.gov/news-issuances/consumeradvisories/2011/index-2011-consumer-advisories.html
- US Cert:
  http://www.us-cert.gov/nav/nt01/
- StaySafeOnline:
  http://www.staysafeonline.org/tools-resources/tip-sheets