



**Online Banking**

Ligon to:  Personal  Business

Access ID:

Submit

[Enroll Here](#)

Personal Banking Header



Rev. July 2010

Personal Banking Navigation



Business banking navigation



Mortgage banking navigation



Community Events Navigation



Online Bill Pay



Careers



FACTS	WHAT DOES CHOICE BANK DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: <ol style="list-style-type: none"> <li>1. Social Security number and income</li> <li>2. Account balances and payment history</li> <li>3. Credit history and credit scores</li> </ol> When you are <i>no longer</i> our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Choice Bank chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Choice Bank share?	Can you limit this sharing?
<b>For our everyday business purposes -</b> Such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	YES	NO
<b>For our marketing purposes -</b> to offer our products and services to you	YES	NO
<b>For joint marketing with other financial companies</b>	YES	NO
<b>For our affiliates' everyday business purposes</b> - information about your transactions and experiences	NO	We don't share.
<b>For our affiliates' everyday business purposes</b> - information about your credit worthiness	NO	We don't share.

Information about your credit worthiness		Share.
<b>For our nonaffiliates to market to you</b>	NO	We don't share.
Questions?	Call 920-230-1300 or go to <a href="http://www.choicebank.com">www.choicebank.com</a> .	

<b>Who we are</b>	
<b>Who is providing this notice?</b>	Choice Bank
<b>What we do</b>	
<b>How does Choice Bank protect my personal information?</b>	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.
<b>How does Choice Bank collect my personal information?</b>	We collect your personal information, for example, when you <ul style="list-style-type: none"> <li>1. Open an account or apply for a loan</li> <li>2. Pay your bills or make deposits or withdrawals from your account</li> <li>3. Give us your contract information</li> </ul> We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.
<b>Why can't I limit all sharing?</b>	Federal law gives you the right to limit only <ul style="list-style-type: none"> <li>1. Sharing for affiliates' everyday business purposes - information about your creditworthiness</li> <li>2. Affiliates from using your information to market to you</li> <li>3. Sharing for nonaffiliates to market to you</li> </ul> State laws and individual companies may give you additional rights to limit sharing. See below for more on your rights under state law.
<b>Definitions</b>	
<b>Affiliates</b>	Companies related by common ownership or control. They can be financial and non-financial companies. <i>Choice Bank does not share with our affiliates.</i>
<b>Nonaffiliates</b>	Companies not related by common ownership or control. They can be financial and non-financial companies. <i>Choice Bank does not share with nonaffiliates so they can market to you.</i>
<b>Joint marketing</b>	A formal agreement between nonaffiliated companies that together market financial products or services to you. <i>Our joint marketing partners may include credit card, insurance, investment, and financial product companies.</i>
<b>Other important Information</b>	
<b>Information for California and Vermont Residents Only:</b>	
<b>California Residents:</b> We will not disclose your personal information to non-affiliated third parties with whom we have joint marketing agreements.	
<b>Vermont Residents:</b> If we disclose personal information about you to nonaffiliated third parties with whom we have joint marketing agreements, we will only disclose your name,	

address, other contact information, and information about our transactions or experiences with you.

### **Website Privacy Policy Effective: August 2011**

Our Website Privacy Policy explains how we collect and use information when you visit this site. This policy is in addition to our Privacy Policy for collection and use of consumer information listed above.

#### **Information We Collect**

Visitors to our website remain anonymous. We do not collect personal information like names or addresses when you visit our website unless you choose to provide it to us through forms, surveys, emails, or submission of applications. If you choose to provide this information to us, we use it only for the purposes for which you gave it to us.

We do collect some technical information when you visit our website. This information never identifies who you are. The information we collect includes: date and time site was accessed, IP address, web browser used, and city, state and country. This information issued to help us make the site more useful for you. With this information, we learn about the number of visitors to our site, the types of technology visitor's use, ways to optimize the site's technical design, and system performance or problem areas. We do not share this information with others unless allowed or required by law.

#### **Cookies**

We may use a "cookie" on some pages of our website. A "cookie" is an electronic message used to provide you with information tailored to your needs. A "cookie" does not retrieve any data from your hard drive, does not contain computer viruses, and does not reveal anything about you. Our use of "cookie" technology is designed to customize and simplify use of our website.

#### **Linking to Other Sites**

We may provide links to sites not controlled by Choice Bank. We are not responsible for the privacy or security of these sites, including the accuracy, completeness, reliability, or suitability of their information. If you are asked to provide information on one of these websites, we strongly urge you to carefully review their privacy policies before sharing information. When leaving the Choice Bank website, you will be notified that you are leaving the site and that we are not responsible for the contents or practices of that site.

#### **Protecting Children's Privacy Online**

We do not knowingly solicit, collect, or use personal information from children under 13. Protecting children's identities and privacy online is important and we recommend that all minor children ask their parent's permission before sending any information about themselves to anyone over the internet. For more information about the Children's Online Privacy Protection Act, visit the FTC website: [www.ftc.gov](http://www.ftc.gov).

#### **Changes to Our Website Privacy Policy**

This policy is subject to change. If we make changes to our Website Privacy Policy, we will revise the effective date as of the date of the change. Please review this Policy periodically.

#### **Questions**

If you have questions about our privacy policies or information practices, you may send your questions to [info@choicebank.com](mailto:info@choicebank.com) or phone us at 920-230-1300.

#### **Personal Banking Header**



#### **Internet Safety Tips:**

Please ensure you have a firewall between you and the Internet. Microsoft Windows has had a firewall turned on by default since Windows XP SP 2, though having that version of Windows or later is no guarantee of its effectiveness. In addition, most home network equipment have basic firewall capabilities. There are various, free testing services on the Internet that can check your firewall for you without requiring you to install any software or make any other changes. As with everything on the Internet, be cautious if a site tries to install software on your computer or requests payment.

Please ensure your machine's operating system and applications are up-to-date with all security patches. "Patches" are software updates that address known security vulnerabilities, which can be exploited by viruses and other malware, as well as rogue websites. For Microsoft Windows users, Automatic Updates may or may not address all of your installed software, such as Microsoft Office products, which can also present a risk when surfing the Internet. Apple Mac software can be updated through the "Software Update" utility. Other software, such as Adobe Reader, Adobe Flash, Apple iTunes, Sun Java, and more should be updated as well.

Please ensure that you have anti-virus software installed and running, as well as ensuring that it is being updated regularly. Anti-virus companies issue updates on an almost-daily basis and sometimes more frequently than that. Given the prevalence and sophistication of viruses and other malware, it is critical that your anti-virus software be kept up-to-date.

Please be cautious when clicking links in unsolicited e-mails as e-mails are easily forged and can point your computer to malicious websites. Best practices when opening e-mail include asking the following

questions:

1. Did I expect this e-mail?
2. Is it from someone I know and trust?
3. Is the content reasonable and/or relevant?
4. Are there spelling mistakes or is there unusual grammar being used?

### February 2012 - FBI Warns of New Banking Scam

Some crafty criminals are aiming to steal one of the most valuable pieces of your personal property: your **banking** information.

In a new warning, the Federal Bureau of Investigation warns account holders of a new spam email scheme that involves a type of malware called "Gameover." The scheme involves fake emails from the National Automated Clearing House Association, the Federal Reserve or the FDIC. These messages attempt to trick recipients into clicking on a link to resolve some type of issue with their accounts or a recent ACH transaction. Once you click on the link, Gameover takes over your computer, and thieves can steal usernames, passwords and your money.

The FBI also warns the thieves' hacking capabilities can navigate around common user authentication methods **banks** use to verify your identity, which is certainly a cause for concern. Those additional authentication steps -- often personal questions, birth dates or other pieces of private information -- are meant to provide some extra security padding.

While phishing scams are nothing new to the world of online banking, this type of warning serves as a reminder of just how susceptible account holders can be to malicious attacks. As more account holders begin to jump on the mobile banking bandwagon, it's important to remember that a smartphone essentially acts as another computer. While this additional connection to the Internet is convenient, it also serves as another outlet where your information can be compromised.

Here are a few crucial steps to take to avoid falling victim to this type of Internet crime.

- Keep your computer and mobile device updated with the newest versions of anti-virus software.
- If you have any doubts about an email sender's authenticity, do not click on any embedded links.
- Remember, banks never request any personal information via email.
- Be vigilant about checking your account balances. The sooner you notice and report any type of fraudulent activity, the more likely you'll be able to be reimbursed for any missing funds.

### February 2012 - NACHA Email

Please be aware of fraudulent emails appearing to come from NACHA. These emails may state that an ACH file or entry has been rejected by the Electronic Payments Association and that the customer should click on the attachment to open the document which supposedly will tell them the nature of the reject. **DO NOT OPEN THE ATTACHMENT.**

Please see the below from the NACHA website:

#### **FRAUDULENT EMAILS...Be Aware That:**

- NACHA does not process nor otherwise touch the ACH transactions that flow via the **ACH Network** nor between financial institutions and their customers.
- NACHA does not send communications of any type to persons or organizations about individual ACH transactions that they originate or receive. If you or your customer has received a communication of this nature that purports to come from NACHA, it is fraudulent.
- NACHA is the industry trade association that manages the development, administration, and governance of the ACH Network, the backbone for the electronic movement of money and data.
- The ACH Network serves as a safe, secure, reliable network for direct consumer, business, and government payments, and annually facilitates billions of payments such as **Direct Deposit and Direct Payment**.
- These incidents are occurring with greater frequency and increased sophistication. Perpetrators are conducting similar phishing attacks in which they are sending fraudulent emails that claim to be from the Federal Reserve Bank, IRS, other federal agencies, as well as commercial financial institutions, other payment organizations, technology companies, and businesses.

### October 2011 - Scam Alert

The American Bankers Association has issued a new warning to highlight increases in phishing scams linked to consumer bank accounts.

According to the ABA, phishing schemes that aim to gather credit and debit details from consumers are on the rise. The crux of most scams: Misinforming consumers about closure of or trouble with their bank accounts, a lure to consumer replies from the socially engineered scam.

Last week's smishing attack, which targeted thousands of Wells Fargo customers by sending out a flood of phony text messages to mobile numbers in Oregon, is a prime example. The scam, feigning to come from Wells, attempted to get mobile recipients to respond with bank details related to their Wells accounts.

Earlier this month, Police in Pima County, Ariz., issued a similar warning about smishing, phishing attacks, targeting mobile users in the Tucson region.

Authorities say consumers were receiving phishy text message that asked account holder to call specified numbers to resolve possible compromises of their bank accounts. The smishing attacks included the last four digits of the user's debit card, which made the text messages appear legitimate.

The ABA says these types of schemes are common. In some cases, consumers are even asked to text or e-mail card expiration dates and CV security codes.

"Those who respond to these inquiries run the potential risk of having their information used to fraudulently purchase goods and services, or to obtain credit," the ABA says.

"Phishing is fairly cyclical," says Doug Johnson, vice president of risk management policy for the ABA. "Based on a recent uptick in activity, we decided to remind customers how to protect themselves from phishing, which is something we do periodically."

#### **Tips for Institutions and Consumers**

The ABA suggests financial institutions share tips and remind consumers that socially engineered schemes rely on methods financial institution would never employ.

To avoid fraud, banks and credit unions should remind consumers to:

- Never give out personal or financial information in response to an unsolicited phone call, fax, e-mail or text.
- Contact the bank to confirm the legitimacy of any e-mail that asks for the submission of personal or banking account information.
- Check credit card and bank account statements regularly for unauthorized transactions, even small ones.
- Make sure websites are secure when submitting financial information online. Check for padlocks or key icons at the bottoms of Internet browsers. Most secure Web addresses also use "https."
- Report suspicious activity to the Internet Crime Complaint Center, a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center.
- Contact your bank immediately if a phishy link may have been clicked or a suspicious communication responded to.
- For information about identity theft, visit the ABA's Consumer Connection.

#### **September 2010 - Labor Day Warning**

[Please click here to view warning](#)

#### **June 2010 - Security Alert**

We have learned that criminals have launched a major e-mail campaign to deploy the infamous ZeuS Trojan e-mail, which will send spam messages disguised as fraud alerts from the Internal Revenue Service (IRS), Twitter account hijack warnings, or salacious Youtube.com videos.

The fraudulent IRS e-mail uses the verbiage "Notice of Underreported Income" as the Subject Line and encourages the recipient to click a hyperlink to review their tax statement. All of the latest e-mails use a variety of URL shortening services.

To help protect against fraudulent activity, Choice Bank strongly recommends that you review Internet security procedures including, but not limited to:

- Ensure that up-to-date antivirus, antispam and antispyware programs are being used.
- Reminder, do not open attachments or download information from unexpected or spam e-mails.

#### **June 2010 - Telephone Scam**

Several clients and non-clients have reported receiving fraudulent calls that claim to be from Choice Bank. Such fraudulent calls may request confidential debit card or account information and claim such information is needed to confirm activation of the debit card or account.

Please note that Choice Bank will never contact clients or non-clients to request personal information in this manner. If you receive a call claiming to be from Choice Bank and asking for your personal information, such as listed above, do not reply or give out any of your personal information.

If you have received a call and have provided the requested information, please call the number on the back of your debit card to report the incident and have your card deactivated.

At [www.choicebank.com](http://www.choicebank.com) you can find more ways to protect your [identity](#) and learn what Choice Bank does to protect your confidential information by reading our [Privacy Statement](#).

Please note: The Oshkosh Northwestern recently reported that the Oshkosh Police Department is informing residents of a phone scam that may be related. The June 11, 2010 story can be found online at <http://bit.ly/9FdqbO>.

#### **February 2010 - Your Internet Safety**

The Bank is aware of various e-mail scams that purport to be from banks and may attempt to get you to install software, go to fake websites, or otherwise provide confidential information via other means to unauthorized parties.

confidential information via other means to unauthorized parties.

Please note that e-mail is very easy to forge and there is nothing the Bank can do to prevent it from reaching you. Also, there is nothing your e-mail provider can do to prevent forged e-mail, and many other technologies such as anti-virus or anti-spam cannot detect or stop it.







When you receive an e-mail that appears to be sent from the Bank and it is requesting an action on your part, please call us to double check that the e-mail is not fake.

We will never ask you to:

- Install software provided by e-mail.
- Go to a website to enter your personal information, including account numbers, social security numbers, driver's license numbers, date of birth, etc.
- Call a non-local or 800 number to provide personal information as noted above.

As always, if you have any questions or concerns about the updates please feel free to contact Choice Bank directly at (920) 230-1300 or [info@choicebank.com](mailto:info@choicebank.com).

[Back to Top](#)

Choice Bank Locations 	Facebook & Twitter 	Join Our Email List  email: <input data-bbox="1193 645 1385 678" type="text"/> <input data-bbox="1393 651 1433 678" type="button" value="GO"/>
 		
Inside Member Logo 	<input data-bbox="778 757 802 790" type="checkbox"/>	