Security

How We Protect Your Information

It is important to Axos Bank to provide a safe and sound Online Banking experience for our customers. In light of emerging threats and an increasingly hostile environment, we have enhanced our customer education and awareness program.

To protect our customers, only those employees, agents, and contractors who need your information to service your accounts have access to the information you provide us. We also give you information that can help you keep your personal information safe.

Here are some of the ways we protect you:

- We use anti-virus protection to help us detect and prevent viruses.
- Our Firewalls help block unauthorized access by individuals or networks.
- The Secure Socket Layer encryption creates a secure connection with your browser when you login, or fill out an application, or register in online services.
- We don't and will not share your usernames and passwords with anyone.
- We automatically log you out of your secure session after a period of inactivity to help protect against others seeing or using your online accounts.
- We monitor activities for potential fraud.

How to Report Identify Theft, Fraud, or Suspected Lost Stolen Cards

For information regarding identity theft and fraud, how to protect yourself, and what to do if you believe you are the victim of identity theft or fraud, please refer to Protect Your Identity below for more information.

Online Security: Steps You Can Take

While we invest in the technology and processes to ensure we provide a secure environment for all of your financial transactions, data transmissions, and communications, we believe protecting your identity and personal information is a team effort. We recommend you also take steps to shield yourself and computer from fraudsters who may try to obtain your personal information electronically.

Here are some steps you can take to protect yourself.

Effective Passwords

Your identity is one of your most valuable resources. That is one reason why we want to help you take extra precautions to protect it. We recommend you help safeguard your identity and personal information by using effective password protection. Here are some suggestions for creating safer passwords and some cautions against weaker ones.

Tips for choosing more-secure passwords:

- Create original passwords that contain a combination of letters, numbers, and even special characters (#, &, %) if allowed.
- Use both capital and lowercase letters (if your password can be case sensitive).

- Ensure your passwords are at least eight characters.

Avoid using:

- Your Social Security number
- Account numbers
- Phone numbers or addresses
- Birth dates or anniversaries
- Obvious or common nicknames
- Names of relatives or pets
- Common words from the dictionary

Additional precautions:

- Use a unique password for each service or website.
- Choose a password you can easily remember, so you don't have to write it down.
- Avoid using software that saves or remembers your passwords.
- Change your passwords at least twice a year.

Phishing

"Phishing" refers to fraudulent processes in which fraudsters attempt to obtain your personal information through electronic communications, such as emails, text messages, or instant messages. These messages appear to be from a trustworthy entity, such as a bank, insurance company, retailer, or regulatory agency. However, the messages are not legitimate. The fraudsters typically ask you to send your personal information to a website and then use that information to commit identity theft.

Remember, Axos Bank does not request personal information by email, text messaging, or instant messaging. Beware of any unsolicited emails that request personal information of any kind. Do not respond to any such emails, texts, instant messages, pop-ups, or links.

The following tips will help you spot fraudulent messages

- The message title generally concerns an "urgent matter" that requires your immediate attention, such as "verifying" certain information to prevent the company from suspending or closing your account.
- The sender may ask for ATM or credit card numbers, personal identification numbers (PINs), sign-on IDs, and other personal information, such as your Social Security number, date of birth, or mother's maiden name — all of which thieves can use to take over an account or commit identity theft.
- The sender's name is usually generic, such as "Customer Service Department," or is just the company's name, such as "ABC Bank."
- The message may look professional and official, often displaying the look and feel of a website that you know. It may even contain links or pop-up windows that have the appearance of legitimacy.
- The message may point you to a domain name that is spelled very close to or appears to be related to the legitimate domain name.
- The message may point you to a web page that is protected by Secure Socket Layer (SSL), better known as https.

Spyware

Spyware, which includes keystroke loggers, screen and mouse recorders, and other types of malware,

allows distant hackers to extract sensitive data from your computer. These programs often slow down your computer and send harvested information to criminals.

Follow the tips below to protect your computer and private information from these dangerous programs

- Never open any email attachments, web links, or files if the sender or source is not trustworthy or cannot be confirmed. This will help prevent spyware (which is designed to secretly access information) from being installed on your computer.
- Use the automated update wizards in your operating system to download and install the latest security patches.
- Install a firewall and anti-virus software with spyware protection on your computer. Use the automatic update options, and keep your subscriptions current, as fraudsters continue to develop new malware and viruses.
- Use email spam-filtering software.
- Avoid using public computers shared by many individuals to pay your bills, check your account balance, or transact business. If you do have to use a public computer, remember to log out of any websites completely and log off the computer.
- Always use encryption for wireless access.

Mobile Device Security

Configure your mobile device to require a passcode to gain access and with auto-lock features. Avoid storing sensitive information. Mobile devices have a high likelihood of being lost or stolen so you should avoid using them to store sensitive information such as passwords, and bank account numbers. If sensitive data is stored then encryption should be used to secure it. To prevent unauthorized access to your mobile device, configure your settings to have the device automatically wiped after 10 failed passcode attempts. Install security software to prevent malware from infecting your mobile device. There are a number of vendors who provide this service through apps found in your vendor's app store.

Social Engineering

In a social engineering attack, an attacker uses human interaction to manipulate a person into providing them information. People have a natural tendency to trust. Social engineering attacks attempt to exploit this tendency in order to steal your information. Once the information has been stolen it can be used to commit fraud or identify theft.

Criminals use a variety of social engineering attacks to attempt to steal information, including:

Website Spoofing

Pay attention to the web address (URL) of websites. A website may look legitimate, but the URL may have a variation in spelling or use a different address. If you are suspicious of a website, close your browser and contact the company directly by phone Do not click links on social networking sites, pop-up windows, or non-trusted websites. Links can take you to a different website than their labels indicate. Typing an address in your browser is a safer alternative. Only give sensitive information to websites using a secure connection. Verify the web address begins with https:// (the "s" is for secure) rather than just HTTP:// with no "s".

For Commercial Banking Customers:

We recommend you perform regular risk assessments to determine any potential exposure you may have related to Internet banking activities with an enhanced focus on "high risk" transactions. A sample

risk assessment form is available below. Please adopt your risk assessment/management program in light of your own operating environment, business type, market conditions, legal and compliance risk, control environment, and any other potential threats and risks application to your situation.

Sample Risk Assessment Form

The problem of identity theft

According to government and private sector estimates, some 9 million Americans a year are at risk of having their identities stolen. Identity theft occurs when someone steals personal information and uses it to establish credit, borrow money, charge items or even commit crimes in your name.

While the incidence of Internet identity theft is growing, fraud experts agree individuals are more likely to become a victim of this federal crime by more traditional means, such as improperly discarding credit cards or other financial data. Here are some tips on how to avoid becoming an ID theft victim and what to do should you become a victim of identity theft.

Protect your identity

- Never respond to unsolicited requests for your social security number (SSN) or financial data.
- Before discarding, shred credit cards, ATM receipts and any pre-approved credit offers you have received, but don't plan to use.
- View your online account statements to detect fraud earlier and contact your financial institution immediately if you see anything suspicious.
- Check your account activity frequently looking for anything unusual.
- Avoid personal ID (PIN) codes that provide access easy to identify.
- Use only secure sites when making online purchases. Secure pages begin with "https."
- Pay for online purchases by credit cards to assure you get what you paid for and limit your liability.
- Consider signing up for a credit monitoring service that notifies you when changes are posted to your credit report. This is one of the fastest ways to identify if others open accounts in your name.
- Safeguard your SSN, and check Earnings and Benefit statements annually for fraudulent use.

Watch out for signs of fraud

- You see unexpected charges on your account.
- Your credit report shows accounts that are not yours or contains inaccurate information.
- Bills or statements you still receive by US mail stop arriving. This could mean an identity thief has taken over your account and changed your billing address.
- Your banking statement shows checks are significantly out of order.
- You receive credit cards without applying for them.
- You are denied credit for no apparent reason.
- You receive notice that you have been denied credit but did not apply for credit.
- You receive calls or letters from debt collectors & businesses about merchandise you didn't buy.

Know the scams

If it sounds too good to be true, it probably is. Scams are not only limited to the internet. Criminals also use phone and email scams to gain personal information and commit fraud and identity theft. Here are

a few typical identity theft scams:

- You are notified by phone, email, or letter that you won a prize or lottery, but you don't remember entering it.
- You are asked to pay money in advance for "administration fees" or "taxes" prior to receiving a prize or winnings.
- You are promised to receive a huge sum of money in return for using your bank account to send or receive money.
- You are promised to make extra money working at home in return for using your bank account to send or receive money.
- You are required to pay a fee in advance to stop foreclosure, modify a loan, or receive advice from a company or individual to stop paying your mortgage. The FTC provides an informative video on this subject at http://www.consumer.ftc.gov

The best way to verify calls or emails received regarding your finances is to contact your financial institution directly. Locate the contact information on one of your statements or other materials from the company.

For more information on Internet safety visit Onguard Online (http://www.onguardonline.gov). This is a Federal Trade Commission (FTC) maintained site that provides practical tips on how to guard against Internet fraud, secure your computer, and protect your personal information.

If you have become a victim of identity theft, immediately take the following actions

- File a police report.
- Contact your banker.
- Notify anyone with whom you have a financial relationship.
- Tag accounts closed due to fraud, "Closed at the consumer's request."
- Notify credit bureau fraud units.
- Establish a password for telephone inquiries on credit card accounts.
- Place a fraud alert statement on your credit report.
- Request bi-monthly copies of your credit report until your case is resolved (free to fraud victims).
- Report check theft to check verification companies.
- Check the post office for unauthorized change of address requests.
- Follow-up contacts with letters and keep copies of all correspondence.

Where to get help

Credit Reporting Bureaus

Equifax

www.equifax.com

To order your report:
Call: 1-800-685-1111
Write: P.O. Box 740241, Atlanta, GA 30374-0241

To report fraud:
Call: 800-525-6285
TDD (For the hearing impaired): 800-255-0056 (ask the operator to call Auto Disclosure Line (800-

685- 1111) to request a copy of report)
Write: P.O. Box 740250, Atlanta, GA 30374-0241

Experian

www.experian.com

To order your report:
Call: 888-397-3742
Write: P.O. Box 2104, Allen TX 75013

To report fraud:
Call: 888-397-3742
TDD (For the hearing impaired): 800-972-
0322 Write: P.O. Box 1017, Allen TX 75013

Trans Union

www.transunion.com

To order your report:
Call: 800-916-8800
Write: P.O. Box 1000, Chester, PA 19022

To report fraud:
Call: 800-680-7289
TDD (For the hearing impaired): 877-553-7803
Write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634

Social Security Administration

Report Fraud 800-269-0271
Order Benefits and Earning Statement 800-772-1213

Reporting Fraudulent Check Use

Check Rite 800-766-2748
Chexsystems 800-428-9623
CrossCheck 707-586-0551
Equifax 800-525-6285
National Processing Co 800-526-5380

SCAN 800-526-5380
TeleCheck 800-710-9898

More information about identity theft and how to avoid it can be found at:

- Federal Trade Commission
- The Privacy Council

Protect yourself offline

You can reduce your chances of falling victim to fraud and identity theft with the help of these everyday safety tips.

- **Secure your personal information**

  Only carry the identification you need on a daily basis in your wallet, purse, or briefcase. Don't carry your Social Security card with you. It's a good idea to make copies of all of the information that you carry (credit cards, driver's license, and insurance cards) and keep the copies in a secure place such as a safe, locked drawer, or safe deposit box. If they are stolen or you lose them, you'll have a record of who to call.

- **Protect your Social Security number**

  Be cautious when asked for your Social Security number. Always verify the reason it is required. Never write your Social Security number on your checks. Keep documents that contain your Social Security number in a secure place such as a locked drawer.

- **Manage your mail carefully**

  Always shred documents that contain personal information instead of placing them in your trash can or recycling bin. This includes pre-approved credit card offers. Criminals look for personal information in trashcans and use it to access your accounts or open new accounts using your identity.

- **Check your checks**

  Store blank and canceled checks securely. Report lost or stolen checks immediately. Use your checks in order and look for check numbers out of order on your statements. A check number out of order could indicate fraud. Use online bill payment or electronic funds transfers instead of writing checks to reduce check fraud.

- **Take advantage of direct deposit**

  Use direct deposit to have paychecks and other recurring deposits placed directly into your accounts. This reduces the risk of a criminal obtaining your account number from a paper check.

- **Keep an eye on your credit**

  Check your credit report annually. As a consumer, you are entitled to one free credit report from each of the three reporting agencies once a year.

  Always keep your credit and debit cards in a safe place. If your card is lost or stolen, contact the issuing company immediately. Memorize your PIN code. Do not write it down or share it with anyone including bank employees or police agencies.

- **Use caution at the ATM**

  Be aware of your surroundings at the ATM. Make sure others cannot see the keypad while you're entering your PIN. If you do print a receipt, take it with you and keep it in a safe place. The receipt may contain information about your account balance and a partial account number, which may be used for fraud. When you're done with your receipts, shred them.

The Safety of Your Identity Is Our Top Priority

In addition to our state-of-the-art encryption technologies, Axos Bank uses industry-leading practices to guard your personal information.

- **Electronic Documents**

  All Axos Bank documents are encrypted and stored in our Secure Message Center where they can only be accessed by the account holder.

- **Fraud Alerts**

  Axos Bank proactively monitors your account for any unusual activity, and if we see anything suspicious, we will contact you to let you know about it right away.

- **Dedicated Fraud Specialists**

  Just let us know in the event of any fraudulent activity, and we will assign a specialist until all your issues have been resolved.

  We also recognize how important it is to protect your identity from unlawful use, and shield your accounts from fraud and unauthorized access. With that in mind, we want you to know **it is not our practice to ask for your Axos Bank Online User ID or password in an email**.

  Further, you can be assured that it is not our practice to:

  - Send an email that requires you to enter personal information directly into the email.
  - Send email threatening to close your account if you do not take the immediate action of providing personal information.
  - Send an email asking you to reply by sending personal information.
  - Share your name with any contacts outside our firm in a manner inconsistent with our Privacy Policy.
  - Our bank, other financial institutions and regulatory agencies (i.e. FDIC, OCC, etc.) will never request sensitive information via SMS.

With those things in mind, please exercise caution when reading an email that may appear to have been sent by us.

How to report fraud

If you might have inadvertently compromised your Axos Bank account, it's important you speak with us immediately. The sooner we know what has happened, the sooner we can begin helping you. Please call us now at 1-877-247-8002**.**

Report fraud by email:

We strongly encourage you to call us immediately if you think your Axos Bank account has been put in jeopardy. If, for some reason you prefer to contact us electronically, please forward the suspicious email to customerservice@axosbank.com. Please include the account holder's name, zip code and phone number so we can easily identify you.

Children's Online Privacy

Axos Bank does not knowingly collect, use or disclose personal information from children under age 13 without obtaining verifiable parental consent. Our website is directed to a general audience and may be accessed by the public. Should a child whom we know to be under 13 send personal information to us, we will only use that information to respond to a one-time request from the child, provide notice to the child's parents, or ensure the safety of the child. Parents can be proactive and limit web site access to their children by installing filtering software.

Children's access to the Internet can permit them to visit inappropriate web sites and be exposed to unnecessary risks. The Children's Online Privacy Protection Act (COPPA) protects children under the age of 13 from the online collection of personal information. For more information about COPPA, visit the Federal Trade Commission website: www.ftc.gov.

Additional Privacy and Security Resources

Here is a list of websites that provide additional information related to privacy and security. These are not associated with Axos Bank but are helpful consumer resources.

Federal Trade Commission (FTC) Identity Theft Home - http://www.ftc.gov/idtheft

The FTC hosts this site as a one-stop national resource to learn about the crime of identity theft. It provides detailed information to help you deter, detect, and defend against identity theft.

Free Credit Report Information - http://www.ftc.gov/freereports

The federal Fair Credit Reporting Act (FCRA) requires each of the nationwide consumer reporting companies to provide you with a free copy of your credit report, at your request, once every 12 months.

FDIC Consumer Protection - http://www.fdic.gov/consumers/index.html

The Federal Deposit Insurance Corporation's (FDIC) online presentation titled "Don't Be an Online Victim: How to Guard Against Internet Thieves and Electronic Scams" provides steps you can take to prevent becoming a victim of financial fraud.

National Cyber Security Alliance - http://www.staysafeonline.org

The National Cyber Security Alliance (NCSA) is a public-private partnership focused on promoting internet security and safe behavior online.

Anti-Phishing Working Group - http://www.antiphishing.org

The Anti-Phishing Working Group (APWG) is a global association of companies and law enforcement agencies focused on eliminating fraud and identity theft that result from all types of phishing scams.