



Safeguarding Your Information

At Bank of Commerce, the security of customer information is a priority. We are strongly committed to the safety and confidentiality of your records. Every day, unscrupulous individuals are busy developing new scams targeting the unsuspecting public. One of the best ways to avoid fraud is to become an educated consumer.

- Enroll in our free Online Banking service and monitor your account frequently through our website www.bocokonline.com.
- Immediately open and carefully examine your monthly account statement when received.
- Report any unauthorized charges on your account to the bank immediately.
- Sign up for free electronic statements to avoid having your paper statement sitting in an unsecure mailbox where it could be compromised.
- Request our free Debit Card Alerts that notify you any time your debit card is used.
- Set up free instant alerts through Online Banking to be notified via phone, e-mail and/or SMS text message when there is login activity or changes in your expected balance.
- Be alert for copycat Web sites that deliberately use a name or Web address very similar to, but not the same as the real one. The intent is to lure you into clicking on the link and providing your personal information, such as a bank account number, credit card number or Online Banking login information.
- Always use your pre-established links to access Web sites and avoid clicking on links in unsolicited e-mails. If you ever receive a suspicious e-mail representing itself as Bank of Commerce, please forward the message in its entirety to customerservice@bocokonline.com.
- Ensure that your personal and business computers have updated anti-virus and firewall protections. Apply security patches for all programs and operating systems regularly.
- Passwords should be unique to you and changed regularly. Do not use birthdays or other numbers or words that may be easy for others to guess. Never write down your password or give it to another person.

Please keep in mind that Bank of Commerce will **NEVER ASK FOR YOUR ONLINE BANKING PASSWORD BY PHONE OR EMAIL!**

For personal accounts, limitations on your liability for unauthorized electronic funds transfers and other electronic errors that are covered by Regulation E are explained in the EFT Disclosure Statement in our Consumer Terms and Conditions brochure. Business account holders should establish internal security procedures for employees authorized as users to prevent unauthorized use by other employees or persons.

If at any time you have questions regarding security or possible fraud, please call our Customer Service Department at any of our locations or e-mail customerservice@bocokonline.com.



Identity Theft

Identity theft occurs when a fraudster obtains your personal information to steal money from your accounts, open new credit cards, apply for loans, rent apartments and commit other crimes — all using your identity. These acts can damage your credit, leave you with unwanted bills and cause you countless hours of frustration to clear your good name.

Victims of identity theft often aren't aware they've been targeted until unknown charges appear on their bank or credit card statements, are contacted by a collection agency, or are denied credit.

How Identity Theft Happens

Listed below are a few common tactics identity thieves use to gain access to your information:

- Stealing wallets and purses containing your identification, credit, and bank cards.
- Stealing mail including bank and credit card statements, phone bills, and tax information.
- Completing a "change of address form" to divert your mail to another location.
- Stealing or illegally purchasing personal information you share on the Internet.
- Call you claiming to be a reputable company asking for personal information.
- Send you an email, appearing to be from a reputable company, requesting you to respond or go to a web site and provide your personal information. This practice is known as "Phishing".
- Set up bogus web sites that look like familiar legitimate sites and ask you to provide personal information. This practice is known as "spoofing".

What to do if You've Become a Victim of Identity Theft

If you're a victim of account fraud, you should notify your bank(s) immediately. If your account(s) is with Bank of Commerce, you should call our Customer Service Department at any of our locations or email customerservice@bocokonline.com. Our Customer Service Representatives will work with you in an effort to make appropriate corrections of unauthorized transactions in your Bank of Commerce accounts. We will also correct any erroneous reports submitted by us to credit bureaus and will attempt to help protect you from future identity theft or account fraud. We suggest that you immediately:

- Contact the fraud department of one of the three credit bureaus. Ask them to place a "fraud alert" on your file. This notifies creditors to contact you prior to any additional accounts being opened in your name.

Equifax

1-800-525-6285

P.O. Box 740241

Atlanta, GA 30374-0241

Experian

1-888-397-3742

P.O. Box 9532

Allen, TX 75013

TransUnion

1-800-680-7289

P.O. Box 6790

Fullerton, CA 92834

- Contact your local police department and ask to file a report. Even if the police can't catch the identity thief, a police report may help you in clearing up your credit records.
- Notify the issuers of the credit cards you carry. If unauthorized charges appear on your legitimate credit cards or, if unauthorized cards have been issued in your name, request replacement cards with new account numbers. Also, monitor credit card bills for any new fraudulent activity. If found, report it immediately to the credit card issuers and credit reporting agencies.



- File a complaint with the Federal Trade Commission (FTC). Call the FTC's identity theft hotline toll-free at 1 (877) IDTHEFT (438-4338). The hotline is staffed by counselors trained to help victims of identity theft. You may also file a complaint online at www.consumer.gov/idtheft.
- Check online accounts, merchants or payment services that you use for any fraudulent activity on your account.
- Contact the Social Security Administration Fraud Hotline (800) 269-0271 to report the unauthorized use of your personal identification information.
- Notify the Department of Motor Vehicles of your identity theft. Check to see whether an unauthorized license number has been issued in your name.
- Contact the local office of the U.S. Postal Service or go to www.usps.com to file an "Identity Theft via United States Mail" complaint form with the Postal Inspector.
- Document the names and phone numbers of everyone you speak to regarding the incident. Follow up your phone calls with letters. Keep copies of all correspondence.

Additional Ways to Protect Your Identity

There are some simple precautions you can take to minimize the chance that you will be a victim of identity theft:

- Check your credit report regularly. Consumers are entitled under federal law to get one free comprehensive disclosure of all the information in their credit file from each of the national credit bureaus once every 12 months. You may request your free annual credit report by visiting www.AnnualCreditReport.com or by calling (877) FACTACT.
- Shred your confidential mail.
- Keep account numbers, Personal Identification Numbers (PIN's), credit cards, debit cards, and checks in a secure location.
- Don't select a PIN that has personal significance, such as birthday or address. Change your PIN frequently.
- Memorize your PIN. Do not share your account numbers or PINs with friends or family.
- When conducting transactions on the Internet, make sure the web sites you visit are secure and reputable. Utilize anti-virus software to detect malicious messages and firewalls to prevent hackers attempting to take control of your computer.
- Always take your receipts with you when using your debit card at a merchant or ATM.
- Never give your confidential information, including your account number and social security number, to a phone caller regardless of whom they claim they are representing. Reputable companies and organizations will never request this information via phone.
- Delete unsolicited or unknown email.

We're Here to Help!

The unauthorized use of someone's identity is a serious matter to **Bank of Commerce**. If you suspect you may be a victim of identity theft or account fraud, please call our Customer Service Department immediately at any of our six locations or email customerservice@boconline.com.