

Bank of Commerce will never request your personal information via an unsolicited email or phone call. We will never call you requesting your card number, PIN, expiration date, or 3-digit number. Please report any suspicious requests to: idtheftinfo@reddingbankofcommerce.com

Detecting Scams



Here are some basic things to look out for when trying to determine if something is a scam or not.

UNIVERSAL RULES

- If it's too good to be true, it probably is.
- When in doubt, check it out.
- A bank, credit card company, or utility company will **never** ask for your personal information by email, whether you have an account or not, period.

Companies you may already be doing business with –

- Banks will always conduct all business conversations with you either in writing via postal mail or over the phone. In both instances they will identify you by name and already have your account information in hand. They have no need to request your account information!
- Companies that do business strictly online (such as PayPal or Amazon) will address you by name. Never by "Dear Customer" or "Dear your@email.com"
- When in doubt, access your account directly with the company. Do not click on any links in any emails. Always go directly to that company's homepage and access your account. If there is a legitimate problem, the company will tell you when you access your account.

Credit Reporting Agencies (CRA's) Contact Information



Equifax

www.equifax.com

To place a Fraud Alert call: (800) 525-6285

Or write to:

Equifax

P.O. Box 740241

Atlanta, GA 30374-0241

Experian

www.experian.com

To place a Fraud Alert call: (888) 397-3742

Or write to:

Experian

P.O. Box 9554

Allen, TX 75013-0949

TransUnion

www.transunion.com

To place a Fraud Alert call: (800) 680-7289

Or write to:

TransUnion

P.O. Box 6790

Fullerton, Ca 92834

Free Annual Credit Report call: (877) 322-8228

www.annualcreditreport.com

Protecting Your Online Identity



The need to protect your identity online has become increasingly important with the growing number of social networking and blogging sites available. Personality profiles and blogging about personal experiences creates a public record of your personal information. Once it is posted – it's nearly impossible to pull back.

- Use the highest level privacy settings that the site allows. Do not accept default settings.
- Be careful when picking a screen name – make sure it doesn't provide clues to your "identity".
- Create a strong password and change it often. (See Volume 3)
- Be wise about what you post. Never post personal information such as your address, phone numbers, e-mail address, driver's license number, Social Security Number (SSN), birth date, birth place, school's name, or student ID number.
- Be careful when posting photos. Make sure they do not depict negative behaviors – including drinking, provocative poses or illegal activities. While you may attempt to delete the photo at a later time, it will continue to exist in the cyber world.
- Only connect to people you already know and trust. Don't put too much out there – even those you know could use your information in a way you didn't intend.
- Verify emails and links in emails you supposedly get from your social networking site (e.g. the recent Facebook scam emails that asked customers to re-set their passwords). These are often designed to gain access to your user name, password, and ultimately your personal information.