

Online and e-mail fraud (“phishing”)

E-mail and Internet based fraudulent schemes, such as “phishing” are some of the fastest growing frauds today. Phishing involves the use of bogus e-mail that looks legitimate, possibly using a company’s logo and a fraudulent website in an attempt to obtain sensitive information such as bank account information, passwords, PINs (Personal Identification Numbers), etc. for fraudulent usage.

Many phishing schemes involve a fraudulent e-mail message that will request recipients to update or validate their financial or personal information in order to maintain their accounts. It will direct them to a fraudulent web site that may look very similar to the web site of the legitimate business. Often the message includes a warning regarding a problem related to the recipient's account and requests the recipient to respond by providing specific confidential information. The format of the email typically includes proprietary logos and branding, a "FROM" line disguised to appear as if the message came from a legitimate sender, and a link to a website or a link to an email address. All of these features are designed to assure the recipient that the email is from a legitimate business source when in fact, the information submitted will be sent to the perpetrator. Subsequently victims are lured into providing personal account information either by responding to the email or they may be directed to click on a legitimate looking web page link where they will be instructed to provide this sensitive information.

At Walden Federal, we do not send requests for confidential information via e-mail. **NEVER** disclose sensitive information such as your account number, debit or credit card number, passwords, PINs, Social Security numbers or any other information that would allow someone to gain access to your accounts or your identity. If you believe the security of your account has been compromised, contact us immediately at 1-800-458-8190.

If you feel that you may be a victim of a phishing scam or other form of identity theft, please take these immediate actions.

- * Change user passwords and login information on all online accounts;
- * Contact credit reporting services and have a "fraud alert" attached to your credit report file (see contact information below). Information stolen by a perpetrator could be used to establish accounts or obtain credit at other businesses; and
- * Monitor the activity in your accounts closely for a period of time and report suspicious activity immediately.

Additional information and publications are available through the Federal Trade Commission.

How Not to Get Hooked by the "Phishing" Scam, July 2003
www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm

ID Theft: When Bad Things Happen to Your Good Name
www.ftc.gov/bcp/online/pubs/credit/idtheft.htm

Three of the major credit bureaus can be contacted as follows:

- **Equifax** — To report fraud, call: 1-800-525-6285, and write: P.O. Box 740241, Atlanta, GA 30374-0241
- **Experian** — To report fraud, call: 1-888-EXPERIAN (397-3742), and write: P.O. Box 9532, Allen, TX 75013
- **TransUnion** — To report fraud, call: 1-800-680-7289, and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790