

ORCA TALES

October 2009

“We can tell you more about them than their mother”

Volume 16 Issue 10

Protecting Personal Information — For Businesses

Thousands of corporate executives have read the Federal Trade Commission's new publication, *Protecting Personal Information: A Guide for Business*, available at ftc.gov/infosecurity. They've picked up practical tips on how their company can secure and protect the personal information it keeps. But some business owners may still be wondering why data security should be at the top of their agenda. Two reasons show why your company should strive to safeguard personal information.

First, good security is just plain good business. Aware of the risk of identity theft, today's customers are concerned about their privacy. As any business that has experienced a breach has learned, customers prefer companies that demonstrate a commitment to security. For the same reasons, customers will think twice before doing business with a company that has experienced a privacy glitch. Given this choice, many businesses find it more cost-effective to secure the information they have rather than try to repair the damage and rebuild consumer confidence after a data loss or breach.

The second reason to take proactive steps to secure data is that federal and state laws may require companies to implement reasonable information security practices. Depending on your business and the type of information you keep, these laws may apply to you, including:

Fair Credit Reporting Act — Also known as the FCRA, this law is designed primarily to protect the privacy of what it calls “consumer report” information — the details in a consumer's credit report — and to guarantee that the information supplied by consumer reporting agencies is as accurate as possible. A consumer report contains information about individuals' personal and credit characteristics, character, and general reputation. To be covered by the FCRA, a report must be prepared by a “consumer reporting agency,” a business that assembles reports for other companies. In your files right now you may have consumer reports on your employees if you've done background checks, perhaps as part of hiring. Or you may have consumer reports if you've needed to look into customers' credit histories. You have a legal obligation to keep this information secure when it's in your possession. But what about when you no longer have a legitimate business need to keep it? Scaling back on what's in your files is a great idea as long as you show care in how you get rid of sensitive information like consumer reports. Under the FCRA, the FTC has issued a rule requiring companies to exercise care when pitching out consumer reports or information derived from them. Called the Disposal Rule, it requires businesses who have information covered by the FCRA to take reasonable measures when they dispose of it. Businesses that collect consumer credit information, credit reports, or employee background histories should be familiar with this rule and make sure they're in compliance. (By the way, the FCRA was amended in 2005 by another law called the Fair and Accurate Credit Transactions Act, or FACTA. You may hear about FCRA or FACTA, but they both refer to the same law.)

Gramm-Leach-Bliley Act — Also known as GLB, this law applies to “financial institutions.” Companies need to know that as the law defines it, the term “financial institutions” is broad and includes more than just banks. It applies to businesses engaged in a wide range of financial activities, including, for example, car dealers, tax preparers, and even (in some cases) courier services. Businesses that are financial institutions and that are not regulated by other agencies may fall within the FTC's Safeguards Rule. Among other things, this rule requires businesses to have reasonable

What People Are Saying About Orca...

“Rebekah,

Many, many heartfelt thanks for your generous support and participation in WA State CARH (affordable housing). You and Orca Information have stepped up to the line and DELIVERED a great service and you've donated your sharp minds (and awesome whales) to the cause. You guys “ROCK” - and you're loved and appreciated!”

- Joe Diehl / Executive Director

What is AnnualCreditReport.com?

AnnualCreditReport.com is the **ONLY** authorized source to get your free annual credit report under federal law. The Fair Credit Reporting Act guarantees you access to a free credit report from each of the three nationwide reporting agencies — Experian, Equifax, and TransUnion — every twelve months. The Federal Trade Commission has received complaints from consumers who thought they were ordering their free annual credit report, but instead paid hidden fees or agreed to unwanted services. **Don't be fooled** by TV ads, email offers, or online search results. Go to the authorized source when you request your free report.

How do I request my free credit report?

You can request your free report online, by phone or by mail. Visit AnnualCreditReport.com, call 1-877-322-8228, or fill out the Annual Credit Report Request form and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. No matter how you request your report, you have the option to request all three reports at once or to order one report at a time. By requesting the reports separately, you can monitor your credit more frequently throughout the year.

Why should I request my credit report?

Because the information in your credit report is used to evaluate your applications for credit, insurance, employment, and renting a home, you should be sure the information is accurate and up-to-date. In addition, monitoring your credit is one of the best ways to spot identity theft. Check your credit report at least once a year to correct errors and detect unauthorized activity.

What should I look for when I review my credit report?

If you see accounts you don't recognize or information that is inaccurate, contact the credit reporting agency and the information provider. For more information, read the FTC's tips on how to dispute credit errors (www.ftc.com).

FOR SALE

Real Estate—Land and Homes

Lake Chelan, Washington

Dan Folsom

Real Estate Broker (& Rebekah's Brother)

509-682-2371

Employment Screening ~ Eviction Support ~ Tenant Screening

~ 800-341-0022 / 360-588-1633 ~ www.orcainformation.com ~ orca@orcainfo-com.com

policies and procedures to ensure the security and confidentiality of customer information.

Federal Trade Commission Act — The FTC Act prohibits deceptive or unfair trade practices. Under the FTC Act, businesses must handle consumer information in a way that is consistent with their promises to their customers (for example, what they say in their online privacy policy), and avoid data security practices that create an unreasonable risk of harm to consumer data.

Other federal laws — Other federal laws may affect a company's data security requirements, including the Health Insurance Portability and Accountability Act (HIPAA), which applies to health data; the Family Educational Rights and Privacy Act (FERPA), which applies to student records; and the Driver's Privacy Protection Act (DPPA), which applies to information maintained by state departments of motor vehicles.

State laws — As concerns over identity theft and data security have increased, many states have passed laws or regulations to protect their citizens. In addition to complying with federal laws, businesses should look to state laws to make sure they are in compliance.

If this seems complicated, don't worry. Despite these different rules, the FTC has tried to develop a single basic standard for data security that strikes the balance between providing concrete guidance, and allowing flexibility for different businesses' needs. The standard is straightforward: **Companies must maintain reasonable procedures to protect sensitive information.** Whether your security practices are reasonable will depend on the nature and size of your business, the types of information you have, the security tools available to you based on your resources, and the risks you are likely to face.

If you have questions about how these laws affect your business, consider consulting with your attorney. Visit ftc.gov to learn more about the laws enforced by the FTC. Finally, be sure to get your copy of *Protecting Personal Information: A Guide for Business* at ftc.gov/infosecurity.

**Article by, Burke Kappler, whom is an attorney in the FTC s Bureau of Consumer Protection who specializes in data security investigations and enforcement.*

The Orca
pod
wants to
wish all



of you a Safe and Fun
Happy Halloween!!!

A Safe Workplace

Whether you are at home or at work, crime prevention is everybody's business. When you go to work, don't leave your crime prevention sense at home. Almost any crime that can happen at home or in your neighborhood can happen in the workplace.

Preventing Office Crime

- Keep your purse, wallet, keys, or other valuable items with you at all times or locked in a drawer or closet.
- Check the identity of any strangers who are in your office-ask whom they are visiting and if you help them find that person. Don't forget to request identification from service or utility workers as well. If this makes you uncomfortable, inform security or management about your suspicions.
- Do not allow visitors to be alone in your office space. Be sure to provide an escort at all times.
- Be discreet. Don't advertise your social life or vacation plans and those of your co-workers to people visiting or calling your place of work.

Check the Locks and Doors

Good locks are the first line of defense. Volunteer to lead a team of employees to work with management to ensure the physical security of your workplace.

- Check for high security locks, such as Medeco or electronic access control units on all doors-closets that have private information or hazardous materials, outside doors, basements, are a few to consider.
- Verify that the electronic access control unit in use has secure key bypass utilizing patented control of duplication of keys. Any access control unit is only as good as its mechanical override devices.
- Make sure all doors are solid. Look for sheet steel on both sides of back and basement doors.
- Make sure doorframes and hinges are strong enough that they cannot be pried open.
- Lock steel bars or door barriers with high security padlocks that have a hardened steel body and shackle to resist drills, hammers, blowtorches, and bolt cutters.
- Be certain all windows are secure.
- If doors only have a locking knob or lever, install or have installed, a deadbolt for additional security.
- Have management change locks before you move into a new office unless they can account for all keys and provide assurance that keys have not been made without their knowledge.
- Don't assume someone else has report a door, window, or lock that is broken or not working properly. Report these problems immediately.

Check the Lights

Your workplace should be protected with proper lighting.

- Install motion sensitive as well as constant outside lights.
- Illuminate dark places around the building by trimming shrubs, adding lighting, etc.
- Leave some interior lights on even when the business is closed.

To be continued....