Safeguarding the privacy of your customers' information

Your legal obligations

The Federal Trade Commission's "standards for safeguarding information" rule ("safeguards rule") requires you to take steps to ensure the security of customer data.

The FTC requires businesses to have a written program in place documenting the steps taken to safeguard your customer's personal information.

Have you completed your information security plan?

Background

President Clinton signed the Gramm-Leach-Bliley Act into law on November 12, 1999.

The GLBA's Title V dealt with privacy, and, in particular, the disclosure of so-called non-public personal information.

No later than July 1, 2001, under GLBA and under the FTC's final "privacy of customer information" rule ("privacy rule"), auto dealers and (according to regulations issued by other federal regulatory agencies) other "financial institutions" were required to provide "customers" and, in some cases, "consumers," initial privacy notices and then follow up with annual privacy notices to continuing "customers."

The GLBA also mandated that each federal regulatory agency (including the FTC) issue an appropriate rule governing the way "financial institutions" subject to that agency's jurisdiction would be required to "safeguard customer records and information." The safeguards rule was published in the Federal Register on May 23, 2002 (16 CFR 314). Compliance is mandatory. **(www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule.)**

Perhaps more relevant to your needs is the FTC's "financial institutions and consumer data:

Complying with the safeguards rule" which may be found on the internet at **https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying**. This bulletin is being sent to you now as a sort of checklist for you, against which you can measure the steps we presume you have already taken in order to be in compliance with the safeguards rule.

Objectives of the FTC's safeguards rule

It is important that you understand why the GLBA required the federal agencies, including the FTC, to publish "safeguards rules." Browsing through your local newspaper or watching the evening news may offer some answers. "Identity theft" is in the news quite often these days and is a significant national problem.

In a recent high-profile case, an employee of a software vendor, who provided services to the three national credit agencies, sold customer information to identity thieves. At last report, authorities knew of at least 30,000 victims and an estimated $2.7 million in losses.

Consider the number of consumer customers your business currently has and the much larger number of "customer files" that your business has established over the years and still maintains, whether in paper, digital or other data-preservation formats, or multiple formats. In particular, think about the active files now kept in various physical locations in your offices or in your computer's active files database. Now consider how safe and well-protected that information is. Whatever your answer might be, the stated objectives of the safeguards rule are:

1. Ensure the security and confidentiality of customer information.
2. Protect against any anticipated threats or hazards to the security or integrity of such information.
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Let's review your security plan.

- You must have a written information security plan. This plan should describe your program to protect customer information. Depending upon your organization, the plan could be as short as one or two pages or much, much longer. That is because the safeguards rule specifies that your program should be appropriate to your organization's "size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue."
- You must have designated the employee or employees who will coordinate your safeguards program. Ideally, the employee(s) should be identified in the plan, and, as personnel changes, you

must be certain to always have one or more employees who are designated as the "safeguards" point person(s), and the employee(s) should know that he, she or they have been so designated.

- You must have identified and assessed the risks that must be addressed in safeguarding customer information in each relevant area of your organization's operation and evaluate–and at reasonable intervals re-evaluate–the effectiveness of current safeguards for controlling these risks.
- You must have a program for monitoring the plan and the safeguards in place.
- You must have procedures for regularly checking the adequacy of the security you have established with respect to maintaining customer information.
- You must evaluate all aspects of your program from time to time, to make appropriate adjustments and explain why you believed the adjustments were appropriate.
- You must always select appropriate service providers and require them (by contract) to implement safeguards that are appropriate to their organization in protecting consumer information.

In addition, the safeguards rule requires that you consider all areas of your operation, with special emphasis on three critical areas: employee management and training; information systems; and managing system failures.

The FTC suggests the following practices be implemented. (Please refer to the actual FTC document on their website for complete content):

- Employee management and training - The success or failure of your information security plan depends largely on the employees who implement it.
- Check references prior to hiring employees who will have access to customer information.
- Ask every new employee to sign an agreement to follow your organization's confidentiality and security standards for handling customer information.
- Train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, such as:
  - Locking rooms and file cabinets where paper records are kept
  - Using strong passwords (at least eight characters long)
  - Encrypting sensitive customer information when it is transmitted electronically over networks or stored online
  - Referring calls or other requests for customer information to designated individuals who have had safeguards training
- Instruct and regularly remind all employees of your organization's policy and the legal requirement to keep customer information secure and confidential. You may want to provide employees with a detailed description of the kind of customer information you handle (name, address, account number, and any other relevant information) and post reminders about their responsibility for security in areas where such information is stored – in file rooms, for example.
- Limit access to customer information to employees who have a business reason for seeing it. For example, grant access to customer information files to employees who respond to customer inquiries, but only to the extent they need it to do their job.
- Maintain security of information systems including network and software design; information processing, storage, transmission, retrieval, and disposal. Here are some suggestions on how to maintain security throughout the life cycle of customer information – that is, from data entry to data disposal:
  - Store records in a secure area. Make sure only authorized employees have access to the area. For example:
    - Store paper records in a room, cabinet, or other container that is locked when unattended.
    - Store electronic customer information on a secure server that is accessible only with a password–or has other security protections–and is kept in a physically-secure area.
    - Don't store sensitive customer data on a machine with an internet connection.
    - Maintain secure backup media and keep archived data secure, for example, by storing offline or in a physically secure area.
  - Provide for secure data transmission (with clear instructions and simple security tools) when you collect or transmit customer information. Specifically:
    - If you collect information directly from consumers, make secure transmission automatic. Caution consumers against transmitting sensitive data, like account numbers, via electronic mail.
    - If you must transmit sensitive data by electronic mail, ensure that such messages are password-protected so that only authorized employees have access.
  - Dispose of customer information in a secure manner. For example:
    - Hire or designate a records-retention manager to supervise the disposal of records containing non-public personal information.
    - Shred or recycle customer information recorded on paper and store it in a secure area until a recycling service picks it up, and promptly dispose of outdated customer information.
  - Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information.
- Managing system failures – Effective security management includes the prevention, detection and response to attacks, intrusions or other system failures. Consider the following suggestions:
  - Maintain up-to-date and appropriate programs and controls:
    - Follow a written contingency plan to address any breaches of your physical, administrative or technical safeguards.
    - Check with software vendors regularly to obtain and install patches that resolve software vulnerabilities.
    - Use anti-virus software that updates automatically.
    - Maintain up-to-date firewalls, particularly if you use broadband internet access or allow employees to connect to your network from home or other off-site locations.
    - Provide central management of security tools for your employees and pass along updates about any security risks or breaches.
  - Take steps to preserve the security, confidentiality and integrity of customer information in the event of a computer or other technological failure. For example, back up all customer data regularly.
  - Maintain systems and procedures to ensure that access to non-public consumer information is granted only to legitimate and valid users.
  - Notify customers promptly if their non-public personal information is subject to loss, damage or unauthorized access.

The Zurich Services Corporation
1299 Zurich Way, Schaumburg, IL 60196-1056
800 382 2150 www.zurichna.com

BBB ACCREDITED BUSINESS

ZURICH®