

Identity Theft is a Major Problem: Whose Responsibility is It to Protect the Consumer?

Article by: Cindy Schroeter Graham

We have heard a lot about consumers' personal information getting into the hands of identity thieves. More and more people are taking steps to minimize their exposure to such theft by reducing information on personal checks, refusing to share social security numbers with just anyone who asks, being prudent in their use of credit cards, and shredding "junk" mail that might allow another person to pose as them. However, we can do little to protect ourselves against lackadaisical security methods or unscrupulous business practices.

Because recent reports confirm that personal information continues to fall into the wrong hands, consumers have become increasingly concerned about how companies handle their personal information. But consumers can only do so much; then it's up to businesses to provide their customers with privacy policies that will ensure their information is handled appropriately and secured from the hands of would-be opportunists, as well as outright crooks.

How can this be accomplished? As business owners, managers, or supervisors, we need to establish and enforce effective company privacy policies. These policies should outline the handling, reviewing, storage, and destruction of customers' personal information, as well as that of employees. Once privacy policies are drawn up, they must be carried out. All employees should be trained in the handling of sensitive information. When employees obtain personal information from customers, several questions need to be asked. Who is allowed to handle it? How long will the information be unsecured? Can information viewed on computer screens be seen by others? How will the information be secured? Who will have access to it? How long will it be kept, and when will it be destroyed?

Establishing strict information handling procedures may be cumbersome. However, they are necessary if we are to gain and keep the confidence of our customers and our employees. Review the following privacy policies that should be established and practiced by every business.

- Adjust computer screens so customer information is not visible by anyone standing in close proximity. If the screen cannot be moved, place something in the line of sight to block unwanted viewers. Hanging plants, room dividers or frosted glass can block the view.
- Computers should be password protected. When an employee leaves his/her computer, it should always be secured and protected by a password. Even if you leave your computer for just a few minutes, unsecured information could be accessed by anyone passing by.
- Customer files should never remain unattended on a desk that can be accessed by customers or unauthorized employees (including cleaning or maintenance staff). Files left unattended can be quickly viewed and documents stolen or copied. Files should always be in a secured drawer or locked room when not in use.
- Customer information should be secured as quickly as possible. Once information is obtained from a customer, the document or program should not be left unattended. Secure all information before servicing another customer.
- When customer information is secured, assign specific employees who will have access to the information. The more employees who have access to the information, the more chances exist for misappropriation. Don't tempt employees with the access if they don't really need it.
- Don't discuss customer information when other customers or employees are able to hear. When requesting information from the customer, have the customers write it down for you. Once you are finished with the written information, it is very important that you hand it back to the customer. This way the customer can dispose of it, and there are no concerns that the written information is intentionally or inadvertently passed on to someone else.
- Don't leave outgoing mail out over night or over the weekend. Mail or any other documents that are waiting in an "out box" can be easily accessed by cleaning, maintenance, or service staff, as well as by children or friends of employees. Keep outgoing items secured until pick up time. A central location should be designated for such items during the week. Often items placed with other outgoing mail or documents are quickly forgotten, that is, until the recipient notifies you that the document has not been received. The more time that has lapsed between sending and receiving the mail or documents, the less likely you will be to locate them.
- Documents waiting to be shredded should be in a secure place. Many offices use a box under each desk, where documents are thrown until the end of the week. This system provides easy access to documents that are seldom noticed if they go missing. Shred bins should be locked or kept in a locked room. Larger bins are often used to store documents until a document disposal company takes them. These bins should also be locked or kept in a secured area.

As employers, we often obtain information from Consumer Reporting Agencies (CRAs), to help with our hiring decisions. The Fair and Accurate Credit Transaction Act (FACTA) places emphasis on the accuracy of information,

and under new FACTA provisions, any business that uses consumer reporting agencies must adopt proper disposal procedures for the information obtained.

Consumer Reporting Agencies are not just "credit" reports issued by one of the three major credit bureaus. Consumer reports include medical records or payments, insurance claims, employment history, check writing history, and residential or tenant rental history. There are several companies that specialize in providing reports for specific purposes. FACTA defines companies that issue non-credit reports as "nationwide specialty consumer reporting agencies." Consumers may request a free annual report from any of the specialty CRAs.

FACTA also says that receipts for credit and debit card transactions can include no more than the last five digits of the credit card number and expiration date. If you are using a merchant processing machine check to make sure the program is not printing the entire number. If it is, call your provider and request the program be updated to comply with FACTA. Noncompliance could result in fines.

Take steps now to ensure that your merchant processing program will not print the entire credit/debit card number. This does not apply to merchants who only accept handwritten or imprinted card information. This method creates its own problem of securing the consumers card information at all times.

What all this boils down to is that we, as employers, business owners, managers, and supervisors need to make a greater effort to provide our customers with the peace of mind that their identities and their information are safe with us. All of our employees need to handle customer information with care and respect that is apparent to all customers. Without our help in the secure handling of the personal information of our customers and employees, the fight to stop identity theft and fraud will continue to rage. We need to be smarter than the crooks by eliminating their means of obtaining information.

Who knows, the next customer to have information stolen might just be you.

Cindy Schroeter Graham
Identity Theft Prevention Coach
WhoElselsYou@easyas123.biz
<http://www.WhoElselsYou.com>

Cindy is the author of the book, "Who Else is You?" In it, she outlines strategies on how to reduce the risk of becoming an identity theft victim. An expert who has studied current identity theft trends and has been presenting Identity Theft Prevention seminars since 2002, Cindy understands the risks of business owners and consumers when it comes to the exposure of personal information. For more information on her speaking, consulting or book, please visit: <http://www.whoelseisyou.com> or call 970-285-1581 or email Cindy@easyas123.biz.