



How small business can help in the fight against ID theft

Identity theft is not just a consumer's problem. It takes businesses and consumers working together to provide the greatest protection against identity theft. When their customers' personal information is stolen, businesses may not only have legal obligations to help correct the problem, but also may be subject to financial losses themselves.

According to the Better Business Bureau, small businesses typically are not as focused on data security as are larger corporations. Some small business owners believe that locking up their storefront is sufficient protection against theft of important data. Others assume they are better protected than they really are while others may suspect they should be doing more, but do not know how.

The Federal Trade Commission cautions businesses that under the 2003 amendments to the Fair Credit Reporting Act identity theft victims are entitled to get from businesses a copy of the application or other business transaction records relating to their identity theft free of charge. Businesses must also provide these records to an investigating law enforcement agency.

Finally, businesses that lose their customers' information, no matter how that loss occurs, may lose their most valuable asset, the customers themselves. As more and more consumers become victims of identity theft, they make their choice of where to do business dependent on what privacy protection assurances the business can offer. For all these reasons, businesses can no longer afford to be lax about protecting their customers' personal information – and their own.

If you do not need it, do not collect it

Many businesses collect more information than they need, particularly when asking customers to fill out forms. Consider excluding the address, email and phone number if you need only a name. The social security number is a confidential number that is required only if a customer is earning income (either employment or investment) for tax reporting – it should not be collected otherwise. When you order your next set of forms, eliminate all the information that you do not really need.

Personal information is not for broadcast

Can people standing in line at your office or store overhear others give your staff telephone numbers or account details? Instruct employees who need to collect personal information to talk in a discreet and quiet manner. Turn computer screens so they cannot be viewed by anyone other than the operator.

Protect customer cards

When customers are making purchases, ensure that they have sufficient privacy to securely enter their PINs. Place shields on point-of-service terminals and check the terminals regularly to verify that equipment has not been tampered with. Locate security video cameras so that they cannot record the entry of customer PINs.

Be card smart

Staff should verify that customers are who they say they are by checking signatures on cards, and, as appropriate, photo IDs. The Fair and Accurate Credit Transaction Act, requires that debit/credit card numbers are truncated when electronically printing receipts (i.e. does not print more than the last five numbers on the card) and that the card's expiration date is deleted, to better protect consumers. Do not copy down any card number that you do not need.

If you keep it, secure it

Paper records with personal information should be locked, and computer terminals password protected with strong passwords. Place the computer server(s) in a secure, controlled location, and keep other devices (e.g. back-up CDs or tape drives) locked away. Physically lock up all laptops to prevent thieves from walking away with one. Develop and implement policies about who can take laptops home, what security precautions should be taken when the laptop is away from the business (example – not keeping a laptop in a car whether locked or unlocked), and what access employees have to information while they are offsite. Also develop this same kind of a plan for mobile devices which may store personal or confidential information.

Keep customers and other non-authorized personnel out of private and secure areas.

Instruct employees to save data to network drives where these are available and not to "C:" hard drives, which are much less secure. Should someone steal the hard drive, information stored on network drives will remain protected. Make sure your network and computers have the latest firewall, virus and malware protection and operating system updates. This helps plug vulnerability gaps that develop as hackers work at new ways to gain access. Secure Wi-Fi networks by making sure they are encrypted and the SSID (Service Set Identifier) is hidden from broadcast by the router or access point.

Consider an alarm system, preferably one monitored by a security company. Your business insurer may be able to assist you with a security assessment of your operations.

Prevent unauthorized photocopying and put photocopiers that are used to copy sensitive information in a secure environment, away from public access. Since a large number of the more current model photocopiers store copied pages on a hard drive, make sure the data is secured or wiped when the copier is traded in or sold to another user.

Screen and train employees

A significant number of identity thefts start with a dishonest employee who gives personal information to an identity thief. To protect your business against internal fraud, consider background checks for employees who have access to personal information. There are companies who can complete these checks (including criminal background, references and education credentials) on your behalf. Consider conducting regular clearance checks for employees in high-risk areas (e.g. with employees' annual performance review) to ensure staff remain free of criminal records.

Make sure staff understands privacy information policies and how to ask customers for personal information, such as not asking for customer personal data in front of others, checking signatures, and keeping customer data under lock and key and in password-protected computer files. All confidential waste,

including credit card information and photocopied ID documents must be shredded, preferably with a cross-cut shredder, to prevent dumpster diving.

If information is compromised

Create an action plan now for how to respond to a data breach. If identity thieves strike, or if information goes missing, an action plan will be invaluable in responding quickly to the breach. Fast action can help reduce potential damage, and it may help your business or organization to maintain its good reputation and avoid liability in a civil action.

To respond to a data breach or loss of information, you need to follow two tracks at the same time: investigate the problem internally, and devise a plan for notifying people that a problem has occurred. Determine what information was stolen, when and how it occurred, and what you need to do to ensure that no other data is stolen or lost.

Timing is critical since prompt notification might help prevent identity theft or at least mitigate the damage. If a small number of customers are affected, inform them in writing immediately. If a larger number are affected, you may want to determine a more efficient method for advising potential victims quickly.

You should also notify law enforcement agencies as soon as you are aware that information may have gone missing or has potentially been compromised.

Wisconsin law requires businesses to notify individuals in certain circumstances if their personal information has been lost, stolen or otherwise compromised. For more information on this topic, see our fact sheet entitled "Wisconsin's Data Breach Notification Law."

For more information or to file a complaint, visit our website or contact the Office of Privacy Protection.

**Bureau of Consumer Protection
Office of Privacy Protection
2811 Agriculture Drive
PO Box 8911
Madison WI 53708-8911**

E-MAIL: DATCPWisconsinPrivacy@wi.gov

WEBSITE: privacy.wi.gov

Toll-free in WI: (800) 422-7128

(608) 224-5163

FAX: (608) 224-4677

TTY: (608) 224-5058