Identity Theft
A Growing Problem for Business

With identity thieves typically netting more per heist than the average bank robber, and with less risk of prosecution, ID theft has quickly become one of the nation's fastest growing white-collar crimes and a major problem for businesses. It's such a problem in fact, that a recent study released by Javelin Research and the Better Business Bureau estimates identity theft accounts for roughly $50 billion in losses each year for U.S. companies.

Whether it's a large, multi-national corporation or small neighborhood store, your business is the custodian of your customer's personal information and the keeper of sensitive information about your employees. Large or small, your business can be the target of identity thieves who would like to steal that personal information or the identity of your company itself.

How it Happens

Although identity theft crime has exploded with the growth of networked computers and high speed, "always on" Internet access, it cannot be blamed on technology alone. Many identity thieves steal sensitive information the old-fashioned way; by entering unlocked areas inside a business, rummaging through outgoing mail or digging through dumpsters. While most companies think of identity thieves as an external threat, keep in mind that employees with access to sensitive customer or company records also can steal information for personal financial gain. Roughly eight percent of businesses victimized by identity thieves cite corrupt employees as the perpetrator.

In addition to outright theft of records or data, identity thieves also use scams to trick businesses into volunteering sensitive information. This type of fraud, know as phishing, attempts to gain access to information by impersonating a legitimate company. The scam artist sends an e-mail instructing recipients to click on a convenient link to receive or provide information that can be used by phishers to access the company's sensitive internal or business information, giving them logins, passwords and/or other sensitive information.

Hostile Takeover

While business records and personal information are usually the target, some identity thieves don't just stop with your data. In certain instances, these thieves have even been known to impersonate companies, using fake documents to order expensive merchandise, arrange business deals or divert mail deliveries.

Sometimes a business will become aware that its name is being used for fraudulent purposes when a customer calls to complain about a rude sales representative or non-delivery of a product. Or the stolen identity may be revealed when a business receives bills for goods and services that it never ordered and that were delivered to another address. Other times the tip-off comes when people call to ask about a non-existent job listing; when a stranger calls to ask about a paycheck they never received; or when the receptionist receives phone calls for an "employee" who does not work there. Any of these could signify that someone is using your business's good name for fraudulent purposes.

Companies can guard against the unauthorized use of their name by treating unsolicited e-mail or fax requests for financial information or personal data with

suspicion, never replying to unsolicited e-mails concerning company bank accounts, and contacting the actual business or government agency that is requesting financial information from your business to verify its legitimacy.

Safeguarding Information

If your business maintains personal information on customers, it is your responsibility to protect that information from theft or misuse. Though identity theft will continue to be a problem both for consumers and for companies, there are steps business owners can take to minimize their risk.

If customer information is stored on portable devices or laptops, make sure office protocol clearly defines which employees are allowed to check out these devices. Ensure that any device containing business or consumer data is password protected and encrypted if possible. The loss of just one laptop with sensitive information can cost a company as much as $90,000 or more in fines, credit monitoring for victims, public relations damage control and class action litigation.

For physical records, one of the best self-defense measures businesses can implement is to shred information before it is discarded. Even the smallest business can afford an inexpensive paper shredder, and employees should be instructed to use a shredder to destroy unneeded customer or employee records. In fact, under the Fair and Accurate Credit Transactions Act (FACTA) signed into law in 2003, any business that collects personal information on its customers is required to properly dispose of certain consumer information and records. The rule requires the destruction of all papers or electronic records containing names, addresses, ID numbers, income, employment and health records so that the information cannot practically be read or reconstructed. In non-technical language, this means "destroying or erasing electronic media" and "burning, pulverizing or shredding" paper documents.

Off the Clock

When reviewing policies and procedures for safeguarding personal information your company collects, remember to include training for your employees. Make sure all employees know how to spot phishing attempts, and what to do in case of a security breach or loss of customer information. Taking the time to educate employees will not only help protect the business, but its employees as well. In 2004, individual ID theft victims spent an average of 330 hours recovering from this crime, often over a period of years. Employees trying to clear their good name can suffer from lower productivity caused by stress or miss work as they attempt to correct their credit records.

Identity theft can alienate customers and damage your company's reputation, but taking preventative measures like securing access to sensitive information, educating employees and properly disposing of records can help stop ID theft and prevent bad things happening to your company's good name.

More information and tips for protecting your company from identity theft are available from the BBB at www.bbb.org/idtheft or the Federal Trade Commission at www.ftc.gov.