

Identity Thieves Who Are Also Your Employees: What Can You Do and What Are the Risks?

A two-year investigation dubbed "Operation Swiper" conducted by New York authorities has indicted 111 people. The largest identity theft bust of its kind in U.S. history has busted up a \$13 million worldwide crime ring. "These crimes are getting more sophisticated and thieves have amazing knowledge of how to use technology," according to New York City Police Commissioner Raymond Kelly.

Here is how the operation worked: Bosses, or leaders, of the crime ring received blank credit cards from suppliers overseas. The ring leaders then hired "skimmers" to pose as waiters, cashiers, and retail salespeople to steal credit card information from their employers' customers using electronic devices. Once the identifying information of cardholders was obtained, the thieves sent the information to a "manufacturer" who programmed the stolen data into the magnetic strips of blank credit cards. The criminals also used card-printing machines to forge state drivers' licenses to match the fake credit cards.



Once the fraudulent credit cards were made, members of the crime ring went on huge shopping sprees to purchase computer products, designer shoes and other high-dollar merchandise to sell overseas.

Authorities said they confiscated \$650,000 in cash, Apple® computer products worth tens of thousands of dollars and \$850,000 worth of other computer equipment.

Encrypt Data on Portable Devices

A leading cause of data breaches comes from a simple human error: losing a laptop computer or other portable electronic device. For example, an untold number of computers are left at airport security stations each year. If such a device contains "personally identifiable data" (e.g., credit card numbers, social security numbers, driver's license numbers, state ID numbers, account numbers), the loss will usually trigger the customer notification requirements now mandated by law in most states. If the data is encrypted and password protected, however, these requirements are not typically triggered. Of course, encryption will also protect sensitive corporate data.

Therefore, one of the most important cyber risk control steps all businesses, large or small, should take is to



encrypt the data on these devices. This usually costs little or nothing and is not difficult to implement. Make certain your company and your clients require employees to use strong passwords and are encrypting data stored on portable electronic devices.

Cyber Crime

The need to prevent and stop identity theft has never been greater

Employers today do face the problem of outsiders attempting to steal their employees' personal information. However, in this case employers were subject to "an inside job."

"Skimmers" employed as salespeople and waitstaff used electronic devices to steal personal information from the employer's customers. Such criminal activity can lead to liability back to the employer as well as a public relations nightmare.

Performing thorough background checks on job applicants is the first line of defense against employee crimes. The type of background check tools used by the employer depends on the industry, organization and the job involved.

According to the U.S. Small Business Administration, pre-employment inquiries can include criminal record checks. Employers also should perform Internet searches and look at a job applicant's public social and professional media posts.

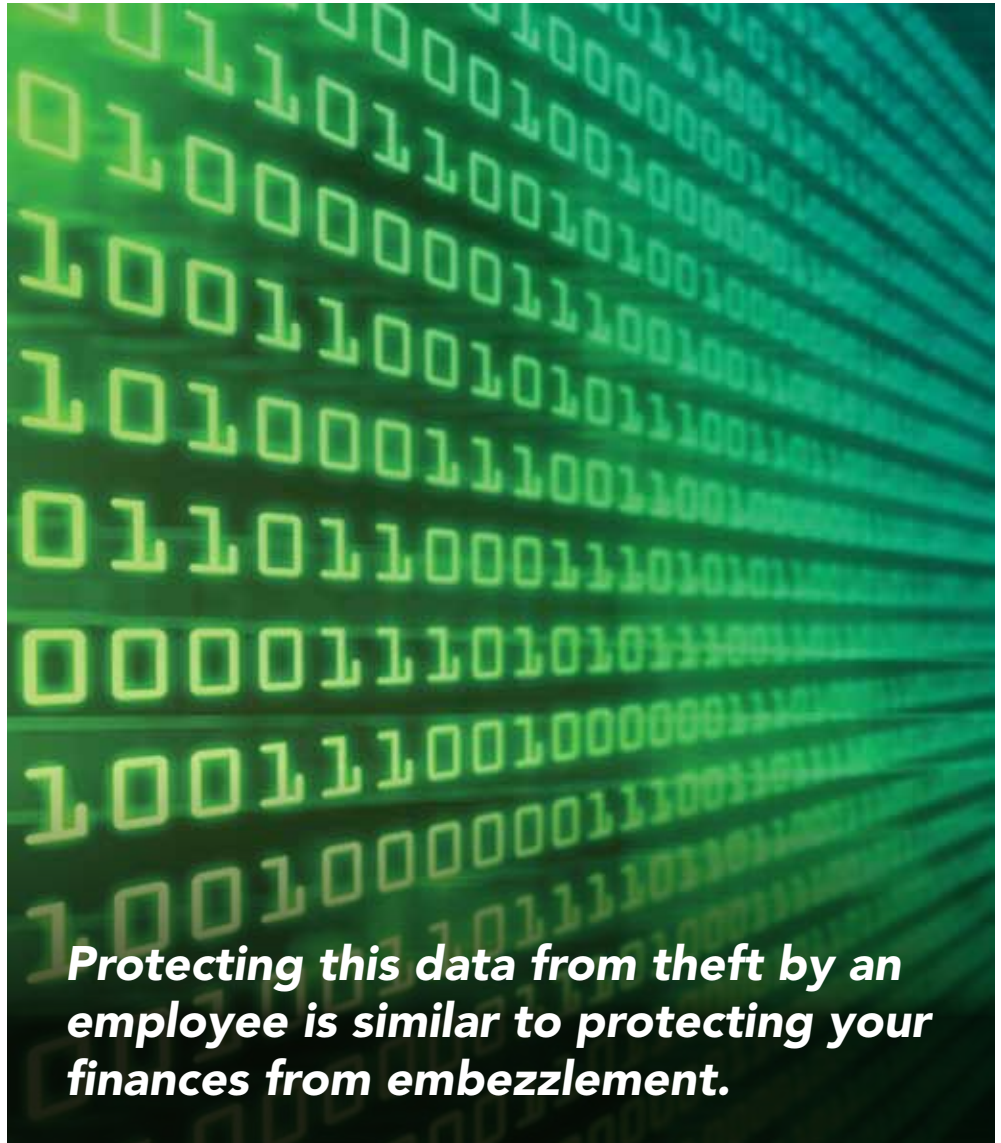
The scheme revealed in this case demonstrates the need for continuing risk control measures after hiring. Employers should continue to monitor their employees' behavior as well as their computer systems on a routine basis.

Frontline employees may intake from customers or other employees a plethora of personally-identifying information including social security numbers, dates of birth, addresses, work histories, and family member information.

Protecting this data from theft by an employee is similar to protecting your finances from embezzlement. Employers must set up checks and balances and other safeguards, including having more than one person in charge of data security. If possible, hire an outside party to audit your computer systems.

Employers should also establish and enforce a policy on computer usage and data management.

In addition to routine audits of your computer systems, consider these steps to ensure that personally-identifying information and all other employer data is not stolen or sabotaged:



Protecting this data from theft by an employee is similar to protecting your finances from embezzlement.

- Establish a clear and concise policy that employer data, including personally-identifying information, is valuable and protected.
- Define what is appropriate use and transfer of employer data, and provide examples of what is improper use of employer data.
- Communicate your knowledge that data thieves will go to extraordinary measures to capture sensitive data.
- List possible outcomes to an employee that steals or sabotages data including, but not limited to, termination and possible criminal prosecution.
- As part of employee orientation, make certain that employees acknowledge your data protection policy.
- Develop a procedure that locks down your data when an employee is terminated.
- Consider banning personal memory transfer devices, such as USB memory sticks, from employees.
- Consider limiting the sensitive information that employees can store on laptops.
- Consider regulating the information that employees can access from home and other remote entry places.

10 Tips for Safe Winter Driving

1. Get a grip. To have adequate snow traction, a tire requires at least 6/32-inch deep tread. (New passenger-car tires usually have 10/32-inch of tread.) Ultrahigh-performance “summer” tires have little or no grip in snow. Even “all-season” tires don’t necessarily have great snow traction: Some do, some don’t. If you live where the roads are regularly covered with snow, use snow tires (sometimes called “winter tires” by tire makers). They have a “snowflake on the mountain” symbol on the sidewall, meaning they meet a tire-industry standard for snow traction.

2. Make sure you can see. Replace windshield wiper blades. Clean the inside of your windows thoroughly. Apply a water-shedding material (such as Rain-X) to the outside of all windows, including the mirrors. Make sure your windshield washer system works and is full of an anti-icing fluid.

3. Run the air-conditioner. In order to remove condensation and frost from the interior of windows, engage your air-conditioner and select the fresh air option: It’s fine to set the temperature on “hot.” Many cars automatically do this when you choose the defrost setting.

4. Check your lights. Use your headlights so that others will see you and, we hope, not pull out in front of you. Make sure your headlights and taillights are clear of snow.

5. Give yourself a brake. Learn how to get maximum efficiency from your brakes before an emergency. It’s easy to properly use antilock brakes: Stomp, stay and steer. Stomp on the pedal, stay pressed hard on the pedal and steer around the obstacle. (A little bit of steering goes a very long way in an emergency.)

For vehicles without ABS, you’ll have to rely on the old-fashioned system: You. For non-ABS on a mixed-surface road, push the brake pedal hard until the wheels stop rolling, then immediately release the brake enough to allow the wheels to begin turning again. Repeat this sequence rapidly.

6. Watch carefully for “black ice.” If the road looks slick, it probably is. This is especially true with one of winter’s worst hazards: “black ice.” Also called “glare ice,” this is nearly transparent ice that often looks like a harmless puddle or is overlooked entirely. Test the traction with a smooth brake application.

7. Remember the tough spots, those trouble spots where icy roads tend to occur. Bridges and intersections are common places. Also: wherever water runs across the road.

8. Too much steering is bad. If a slick section in a turn causes your front tires to lose grip, the common — but incorrect — reaction is to continue turning the steering wheel. Sadly, there are situations where nothing will prevent a crash, but turning the steering too much never helps.

9. Avoid rear-tire slides. First, choose a car with electronic stability control. Fortunately, ESC will be mandatory on all 2012 models. Next, make sure your rear tires have at least as much tread as your front tires. Finally, if you buy winter tires, get four.

10. Technology offers no miracles. All-wheel drive and electronic stability control can get you into trouble by offering a false sense of security. AWD can only help a vehicle accelerate or keep moving: It can’t help you go around a snow-covered turn, much less stop at an icy intersection. ESC can prevent a spinout, but it can’t clear ice from the roads or give your tires more traction. Don’t let these lull you into overestimating the available traction.



Highway workers must comply with high-visibility clothing rule by Dec. 31

The Federal Register Final Rule and revised document of the 2009 Manual on Uniform Traffic Control Devices (MUTCD) was released on Dec. 16, 2009. The date for final phase-in for compliance on all public roads that are not federal-aid highways is Dec. 31, 2011. For federal-aid highways, the regulation has been in force since November 2008.

The Federal Highway Administration published the final rule regarding worker visibility as Part 634 of Title 23 Code of Federal Regulations to reduce the likelihood of worker fatalities and injuries caused by motor vehicles and construction equipment on federal-aid highways. The Rule states that all workers within the right-of-way of a federal-aid highway and public roads that are not federal-aid highways who are exposed either to traffic (vehicles using the highway for purposes of travel) or to construction equipment within the work area shall wear high-visibility safety apparel.



PREMIER
INSURANCE

We love insurance, so you don't have to.

1-800-A-POLICY
24-HOUR CLAIMS

CORPORATE OFFICE • P.O. BOX 6 • TWIN FALLS, IDAHO 83303
BOISE • BLACKFOOT • IDAHO FALLS • TWIN FALLS

visit premierinsur.com for more
information and helpful resources