



# INFORMANT

EDUCATIONAL INFORMATION ABOUT SAFE USE OF THE INTERNET

## IDENTITY THEFT

PROTECTING YOUR BUSINESS & YOUR CUSTOMER INFORMATION

Law enforcement agencies describe identity theft as the fastest growing crime that business, consumers and governments face.

### What is identity theft?

Identity theft refers to crimes in which someone wrongfully obtains and uses another person's personal data, including name, date of birth, social security number, driver's license number, and your financial information from credit cards, bank account and phone-card numbers.

### How identity thieves get your information:

- **Business record theft:** by stealing files out of offices where you are a customer, employee, patient or student.
- **Shoulder Surfing:** by standing behind you in line and memorizing your information while you write a check, or punch in your phone or credit card numbers.
- **Dumpster Diving:** by rummaging through your trash or landfills.
- **Skimming:** by stealing your credit card number as your card is being processed at a restaurant, store or other business.
- **Inside job:** company employees who have access to sensitive company information and steal it for their own personal gain.

### How does your company keep client information?

Most companies collect and retain client information:

- A single computer can hold thousands of client records.
- A filing cabinet may contain access codes, passwords and license numbers that are shared with partners, suppliers or vendors.
- Outside contractors manage company IT functions and databases and have access to sensitive company information.

### For More Information

- [www.ftc.gov/bcp/edu/microsites/idtheft](http://www.ftc.gov/bcp/edu/microsites/idtheft)
- [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com)
- [www.equifax.com](http://www.equifax.com)
- [www.experian.com](http://www.experian.com)
- [www.transunion.com](http://www.transunion.com)
- [www.privacyrights.org/identity.htm](http://www.privacyrights.org/identity.htm)
- [www.consumeraction.gov](http://www.consumeraction.gov)

### Securing company data and storage:

- Paper records with personal information should be locked, and computer terminals password-protected.
- Place your computer server(s) in a secure, controlled location, and keep other devices such as back-up CDs or tape drives, locked away.
- Physically lock up all laptops to prevent thieves from walking away with one.
- Keep customers and other non-authorized personnel out of private and secure areas.
- Instruct employees to save data, including databases, to network drives where these are available and not to "C" hard drives on computers.
- Prevent unauthorized photocopying of company records.
- Instruct employees to be discrete when discussing sensitive information over the phone, so that others around them won't be able to hear what they are saying.
- Properly screen and do background checks on all new and potential employees.
- Establish a company policy for handling sensitive customer information and educate all employees on the proper procedures for collecting and storing the information. Appoint one person to be in charge of implementing the procedure.

### PROTECT YOURSELF & YOUR CUSTOMERS!

#### WHAT IDENTITY THIEVES LOOK FOR

- Name
- Address
- Date of Birth
- Social Security No.
- Driver's License No.
- Mother's maiden name
- Account numbers
- Card expiration dates
- Internet passwords
- Personal Identification No's
- User IDs for online account access
- Security codes from the back of credit and debit cards

Be sure to use a cross-cut shredder to dispose of documents containing any of the information listed at left.