

Managing Identity Theft - Guidance for Your Business

It is almost impossible to be in business and not collect or hold personally identifying information - such as Social Security numbers, credit card numbers, bank account numbers, etc. - about customers, employees and business partners. If this information falls into the wrong hands, it could put these individuals at risk for identity theft. The following guidance, provided by the Federal Trade Commission (FTC), outlines how you should proceed if personal information has been compromised at your organization. Check federal and state laws or regulations for any specific requirements for your business.

Notify Law Enforcement

If personal information is comprised and could result in harm to a person or business, call your local police department immediately.

If your local police department is not familiar with investigating information compromises, contact the local office of the Federal Bureau of Investigation (FBI) or the U.S. Secret Service. For incidents involving mail theft, contact the U.S. Postal Inspection Service.

Notify Affected Businesses

If account access information (credit card or bank account numbers) have been stolen and you do not maintain the accounts, notify the institutions that do so that they can monitor these accounts for fraudulent activity.

If you collect or store personal information for other

businesses, notify them of any information compromises immediately.

If the information involved the improper posting of personal information on your website, immediately remove the information and contact the appropriate search engines to ensure that they do not archive personal information that was posted in error.

If names and Social Security numbers have been stolen,

If your business collects or holds personally identifying information, you need to be prepared to manage potential security breaches.

contact the three major credit bureaus for additional information and advice. When calling, advise the credit bureau that you will also be alerting the affected parties to place a fraud alert on their files.

- **Equifax**

Equifax Credit Information Services

P.O. Box 740241

Atlanta, GA 30374

800-685-5000

Email: cust.serv@equifax.com

Provided by TPG Insurance Services

Managing Identity Theft - Guidance for Your Business

- **Experian**

Data Breach Support

P.O. Box 9556

Allen, TX 75013

888-243-6951

Email: databreachhelp@experiandirect.com

- **TransUnion**

TransUnion Fraud Victim Assistance Department

P.O. Box 2000

Chester, PA 19016-2000

800-680-7289

Email: fvad@transunion.com

Notifying Individuals

When information is stolen, consider the following before notifying any individuals affected: nature of the compromise, type of information taken, likelihood of misuse and the potential damage arising from misuse. If the information could lead to ID theft, contact the affected individuals immediately.

When notifying individuals that their identity has potentially been stolen, the FTC offers the following suggestions:

- Consult with your law enforcement officer about the timing of the notification so it does not impede on the investigation.
- Designate a contact person within your organization to release information. Give this person the latest information about the breach, your responses and how individuals should respond. Consider using letters, websites and toll-free numbers as methods of communication with those whose information

may have been compromised.

- When contacting potentially affected individuals, describe clearly what you know about the compromise. Alert the individual of how it happened, what information was taken, how the thieves have used the information (if known) and what actions have already been taken to remedy the situation. Also explain how to reach the contact person at your organization.
- Explain how potential ID theft victims should respond to the theft based on the type of information stolen.
- Provide contact information and the case report number for the law enforcement officer working on your case. Also advise potential victims to obtain a copy of the police report to make copies for creditors who have accepted unauthorized charges.
- Encourage potential ID theft victims to file a complaint with the FTC at www.identitytheft.gov or 877-438-4338.

For more information on how to protect your business from potential security breaches, contact the FTC at idt-brt@ftc.gov and TPG Insurance Services. We have additional risk management tools to assist you in handling identity theft.

**RISK
INSIGHTS**