FTC FACTS for Business

Information Compromise and the Risk of Identity Theft: Guidance for Your Business

These days, it is almost impossible to be in business and not collect or hold personally identifying information — names and addresses, Social Security numbers, credit card numbers, or other account numbers — about your customers, employees, business partners, students, or patients. If this information falls into the wrong hands, it could put these individuals at risk for identity theft.

Still, not all personal information compromises result in identity theft, and the type of personal information compromised can significantly affect the degree of potential damage. What steps should you take and whom should you contact if personal information is compromised? Although the answers vary from case to case, the following guidance from the Federal Trade Commission (FTC), the nation's consumer protection agency, can help you make smart, sound decisions.

Check federal and state laws or regulations for any specific requirements for your business.

Notifying Law Enforcement

When the compromise could result in harm to a person or business, call your local police department immediately. Report your situation and the potential risk for identity theft. The sooner law enforcement learns about the theft, the more effective they can be. If your local police are not familiar with investigating information compromises, contact the local office of the FBI or the U.S. Secret Service. For incidents involving mail theft, contact the U.S. Postal Inspection Service. Check the blue pages of your telephone directory or an online search engine for the number of the nearest field office.

Exhibit M

Notifying Affected Businesses

Information compromises can have an impact on businesses other than yours, such as banks or credit issuers. If account access information — say, credit card or bank account numbers — has been stolen from you, but you do not maintain the accounts, notify the institution that does so that it can monitor the accounts for fraudulent activity. If you collect or store personal information on behalf of other businesses, notify them of any information compromise, as well.

If names and Social Security numbers have been stolen, you can contact the major credit bureaus for additional information or advice. If the compromise may involve a large group of people, advise the credit bureaus if you are recommending that people request fraud alerts for their files. Your notice to the credit bureaus can facilitate customer assistance.

Equifax
U.S. Customer Services
Equifax Information Services, LLC
Phone: 1-800-685-1111
Email:
businessrecordsecurity@equifax.com

Experian
Experian Security Assistance
P.O. Box 72
Allen, TX 75013
Email:
BusinessRecordsVictimAssistance@experian.com

TransUnion
Phone: 1-800-372-8391

If the information compromise resulted from the improper posting of personal information on your website, immediately remove the information from your site. Be aware that Internet search engines store, or "cache," information for a period of time. You can contact the search engines to ensure that they do not archive personal information that was posted in error.

Notifying Individuals

Generally, early notification to individuals whose personal information has been compromised allows them to take steps to mitigate the misuse of their information. In deciding if notification is warranted, consider the nature of the compromise, the type of information taken, the likelihood of misuse, and the potential damage arising from misuse. For example, thieves who have stolen names and Social Security numbers can use this information to cause significant damage to a victim's credit record. Individuals who are notified early can take some steps to prevent or limit any harm.

When notifying individuals, the FTC recommends that you:

- consult with your law enforcement contact about the timing of the notification so it does not impede the investigation.
- designate a contact person within your organization for releasing information. Give the contact person the latest information about the breach, your response, and how individuals should respond. Consider using letters (see sample on page 4), websites, and toll-free numbers as methods of communication with those whose information may have been compromised.

It is important that your notice:

- describes clearly what you know about the compromise. Include how it happened; what information was taken, and, if you know, how the thieves have used the information; and what actions you have taken already to remedy the situation. Explain how to reach the contact person in your organization. Consult with your law enforcement contact on exactly what information to include so your notice does not hamper the investigation.
- explains what responses may be appropriate for the type of information taken. For example, people whose Social Security numbers have been stolen should contact the credit bureaus to ask that fraud alerts be placed on their credit reports.

See www.ftc.gov/idtheft for more complete information on appropriate follow-up after a compromise.

- includes current information about identity theft. The FTC's website at www.ftc.gov/idtheft has information to help individuals guard against and deal with identity theft.
- provides contact information for the law enforcement officer working on the case (as well as your case report number, if applicable) for victims to use. Be sure to alert the law enforcement officer working your case that you are sharing this contact information. Identity theft victims often can provide important information to law enforcement. Victims should request a copy of the police report and make copies for creditors who have accepted unauthorized charges. The police report is important evidence that can help absolve a victim of fraudulent debts.
- encourages those who discover that their information has been misused to file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Information entered into the Identity Theft Data Clearinghouse, the FTC's database, is made available to law enforcement.

Model Letter

The letter on page 4 is a model for notifying people whose names and Social Security numbers have been stolen. In cases of stolen Social Security numbers, it is important that people place a fraud alert on their credit reports. A fraud alert may hinder identity thieves from getting credit with stolen information because it is a signal to creditors to contact the consumer before opening new accounts or changing existing accounts. Potential victims of a theft also should review their credit reports periodically to keep track of whether their information is being misused. For some victims, weeks or months may pass between the time the information is stolen and the time it is misused.

For More Information

This publication provides general guidance for an organization that has experienced an information compromise. If you would like more individualized guidance, you may contact the FTC at idt-brt@ftc.gov. Please provide information regarding what has occurred, including the type of information taken, the number of people potentially affected, your contact information, and contact information for the law enforcement agent with whom you are working. The FTC can prepare its Consumer Response Center for calls from the people affected, help law enforcement with information from its national victim complaint database, and provide you with additional guidance as necessary. Because the FTC has a law enforcement role with respect to information privacy, if you prefer to seek guidance anonymously, you may do so.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to www.sba.gov/ombudsman.

MODEL LETTER FOR THE COMPROMISE OF SOCIAL SECURITY NUMBERS

Dear _____:

We are contacting you about a potential problem involving identity theft. [Describe the information compromise and how you are responding to it.]

We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

Equifax	Experian	TransUnionCorp
800-685-1111	888-397-3742	800-680-7289

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call [insert contact information for law enforcement] and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

We have enclosed a copy of *Take Charge: Fighting Back Against Identity Theft*, a comprehensive guide from the FTC to help you guard against and deal with identity theft.

[Insert closing]

Your Name

FEDERAL TRADE COMMISSION	ftc.gov
1-877-FTC-HELP	FOR THE CONSUMER

Federal Trade Commission
Bureau of Consumer Protection
Division of Consumer and Business Education

June 2004