How to Deal With a Security Breach

This guide is adapted with permission from the Privacy Rights Clearinghouse publication "How to Deal with a Security Breach, www.privacyrights.org/fs/fs17b-SecurityBreach.htm

Security breaches involving your personal information – also referred to as data breaches – can create a significant risk of fraud or identity theft if the information is acquired by the wrong person. This guide informs you of the risks involved and the measures you can take if you're affected by a security breach.

If you received a letter informing you that your personal information may have been compromised due to a security breach, do not panic. A security breach does not necessarily mean that you will become a victim of identity theft. However, you are encouraged to follow the steps outlined below to reduce your risk of becoming an identity theft victim.

1. Determine what type of breach has occurred. Carefully read the notification letter you receive to figure out what type of personal information was impacted by the breach, when it was likely acquired or subject to acquisition, and who may have been able to acquire it. You will need to know if the breach could affect your existing accounts, could result in the creation of new accounts, could compromise your personal identifying documents (like your Social Security number), or could potentially result in all of these categories of fraud.

If the notification you receive does not provide sufficient detail for you to fully understand how the breach may affect you, contact the business or organization and request more information. Many businesses will set up a toll-free hotline for questions about the breach. Or you can go to the business website to see if it had issued a press release or posted additional information. The business may legitimately need to maintain certain information for security or proprietary reasons, but it should be able to give enough descriptive details to help you determine what you need to do to protect yourself from fraud.

- **Existing accounts**: If the breach involved your *existing* credit or debit card account, you will want to monitor your accounts online, by phone, or in person to see if any suspicious charges have been made. Inform your bank or creditor about the breach. You may want to request a new card or account number, and many banks and creditors will automatically provide a new account in this situation.

  You may also want to ask that a password or security question be added to your accounts to provide another layer of protection. Contact the creditor if your statement does not arrive on time. A missing bill could mean that an identity thief has changed your address.

  If you discover that someone has made fraudulent charges or debits in your name, file a police report and make sure you obtain a copy. Use the report to dispute the charges or debits so you can obtain a refund or reversal of the charges.

- **ID documents:** If the breach could compromise your identifying cards or documents or result in the creation of new identifying documents in your name, you will need to contact the entity that issued the card or document and request a replacement or fraud alert be placed on your account.

  Some breaches compromise driver's license numbers, ID card numbers, passports, or other identifying documents. In most instances, you will need to contact the agency or

organization that created or issued the document to notify them of the breach. You may want to ask that a fraud alert, password or security question be added to your file. Or depending on the level of vulnerability you could request a new document or card. For more information about situation-specific responses, including contact information for the Bureau of Motor Vehicles, IRS, Social Security Administration, and Passport Office, consult our Identity Theft Victim Kit located online at www.IndianaConsumer.com/IDTheft.

- **The potential for new accounts to be opened**: If the breach involved disclosure of your Social Security number (SSN), a fraudster could use that information to open *new accounts* in your name. You will not immediately know of the new accounts because criminals usually use an address other than your own for the account. Since you will not be receiving the monthly account statements, you are likely to be unaware of the account(s).

  That is why it is important to place a fraud alert with the three major credit reporting agencies immediately when you learn that your SSN has been compromised, and then to monitor your credit reports on an ongoing basis.

  Other evidence of new account fraud include receiving credit cards in the mail that you did not apply for, being denied credit when you know you've had a good credit score, and being contacted by debt collectors for payments that you do not owe.

The remainder of this guide provides instructions on how to establish fraud alerts, place a freeze on your credit reports, and keep track of your credit reports for **security breach situations involving your SSN** -- in other words, breaches in which there is an opportunity for *new* accounts to be opened in your name.

2. Notify the credit bureaus and establish a fraud alert. Immediately call the fraud department of one of the three credit reporting agencies -- Experian, Equifax, or Trans Union. When you request a fraud alert from one bureau, it will notify the other two for you. Your credit file will be flagged with a statement that says you may be a victim of fraud and that creditors should phone you before extending credit.

- Equifax fraud department: (888) 766-0008
  Web: www.equifax.com

- Experian fraud department: (888) EXPERIAN (888-397-3742)
  Web: www.experian.com/fraud

- Trans Union fraud department (800) 680-7289
  Web: www.transunion.com

Under new provisions of the Fair Credit Reporting Act (FCRA), you can place an initial fraud alert for only 90 days. You can renew the fraud alerts after 90 days if you wish. You may cancel the fraud alerts at any time.

If your SSN was improperly obtained, there may be additional steps you will want to take to protect yourself. Read our Identity Theft Victim Kit online at www.IndianaConsumer.com/IDTheft for more information about situation-specific actions and responses.

3. Order your credit reports and review carefully Disclosure of your Social Security number and other personal information could lead to the creation of new accounts in your name, so you will need

to obtain a copy of your credit report and review it for unfamiliar accounts and inquiries. You are entitled to one free credit report per year from each major consumer reporting agency – Experian, Trans Union, and Equifax – under the federal Fair Credit Reporting Act. To order your free reports, go to www.annualcreditreport.com or call (877) 322-8228. Additionally, many businesses that experience breaches will offer free credit monitoring services to affected individuals.

When you receive your report, review it carefully to make sure the information is accurate. If you notice any unfamiliar accounts, loans, inquiries, or contact information, follow the agency dispute procedures to request that the information be corrected. You will also need to file a police report and dispute the fraudulent charges.

4. Consider a security freeze. A security freeze offers an extra layer of protection by preventing third parties, with limited exception, from obtaining your credit report without your permission. Security freezes, which have been available under Indiana state law since September 1, 2007, are designed to prevent identity thieves from opening accounts in your name.

5. Consider filing a consumer complaint with the Attorney General's Identity Theft Unit. If you believe the company or organization that experienced the security breach failed to comply with the disclosure law, or if you have become an identity theft victim because of the breach, you can contact the Identity Theft Unit to file a consumer complaint. The Unit will assist you in responding to the effects of identity theft, and it will investigate the matter to track down the thief and work with law enforcement and prosecutors to hold him or her accountable. The Unit will also investigate the breach for compliance with the disclosure law and may take enforcement action if a violation is discovered.

To file a complaint with the Identity Theft Unit, visit www.IndianaConsumer.com/IDTheft.

6. Continue to monitor your accounts, mail, and credit reports. Since you may never know how many persons obtained your personal information as a result of a security breach, where they're located, and what they did with the information, you will need to continue monitoring your accounts and credit reports for a period of time after the breach to watch for fraudulent activity. Keep checking your bank and credit accounts for unfamiliar charges. Continue ordering your credit reports and review them carefully for errors or fraudulent accounts. And watch your mail for suspicious or unexpected bills or account correspondence. Fraud or identity theft attempts may not occur right after the breach or even for months or years following the breach, so it is important to make a habit of closely monitoring your financial data and personal information.

FAQ on Security Breaches

1. What causes a security breach to occur?

Security breaches can be caused by the theft of a laptop computer or electronic device, a hacker who gains access to confidential records or systems, an employee that fails to follow security procedures, or a business that fails to use appropriate security measures to protect sensitive data, among other causes. A few common methods include:

- Computer files containing university student information, including Social Security numbers (SSNs), are hacked.
- A bank's computer back-up tape with customer account data has been lost while being shipped to a storage facility.

- A dishonest healthcare employee has obtained computer files containing patients' records, including SSNs and dates of birth, and may have sold the records to criminals.
- Imposters have established accounts with a large information broker enabling members of an international crime ring to obtain thousands of comprehensive consumer profiles, including SSNs and dates of birth.
- A company laptop has been stolen from the back seat of an employee's car. It contains account data and SSNs on hundreds of thousands of customers.
- For more examples of security breaches, read the Privacy Rights Clearinghouse's chronology of breaches at www.privacyrights.org/ar/ChronDataBreaches.htm.

2. How will I know if a security breach has occurred involving my personal information?

Indiana's disclosure law requires data base owners, state agencies, businesses, and organizations that collect and maintain personal information to notify you in the event of a security breach. Upon discovering that a breach has occurred, a business or organization must disclose the breach to each Indiana resident whose personal information was affected.

Under the law, this disclosure must occur "without unreasonable delay." The notification should provide enough detail so that you can be prepared to protect yourself against identity theft or fraud. Failure to comply with the notification requirement can result in a lawsuit by the Attorney General and an order to pay civil penalties of up to $150,000.00.

Notification can occur by mail, phone, fax, or email. Substitute notice – disclosing the breach on the business website and to major news reporting media in the relevant geographic areas – is permitted if more than 500,000 persons are affected or if the cost of notification would exceed $250,000.00.

3. How is personal information defined?

"Personal information" is defined by statute to include either your (1) Social Security number; or (2) your name and address, *plus* any one of the following: driver's license number; state ID card number, credit card number, or debit card or financial account number in combination with the security code or password that would permit access to the account. SSNs or account numbers that are redacted to show only the last 4 digits do not constitute personal information. Neither does data that is encrypted to render it unreadable.

4. What are the risks involved in a security breach?

If your personal information falls into the wrong hands, it could be used to open new accounts in your name, drain your existing accounts, or commit some other form of identity theft or fraud against you. A Social Security Number by itself can be used to create a new account in your name, which could result in collection actions and harassment, lawsuits to collect the erroneous debt, inaccurate credit reports that may keep you from getting a car loan or mortgage re-finance, and many other types of monetary damage and frustration.

Identity theft continues to be one of the top consumer complaint categories at the state and federal levels, and the increasing number of persons affected by security breaches is likely a factor in that trend. It's important that you have timely and accurate information about security breaches that may impact you so that you can act quickly to protect yourself. Delayed notification may lead to further instances of fraud, higher monetary damage amounts, and even the passing of important deadlines that affect your legal rights to recover your money or restore your identity.