Published on *Privacy Rights Clearinghouse* (https://www.privacyrights.org)

What to Do When You Receive a Data Breach Notice [1]

Posted Feb 01 2006
Revised Feb 07 2019

1. What is a data breach?

A data breach is a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual. A data breach may occur as a result of:

- Hacking (unauthorized intrusion into a computer or a network)
- Theft of credit or debit card numbers (for example, at a compromised point of sale terminal)
- Lost, discarded or stolen documents or connected devices
- Mishandled sensitive information
- For many more examples of data breaches, see PRC's Chronology of Data Breaches [2]

It's important to understand that a data breach does not necessarily mean that you will become a victim of identity theft. If you are a victim of a data breach, you are at greater risk of identity theft, but until your information is misused, you are not considered to be an identity theft victim.

- An identity theft victim is a person whose personal information not only has been exposed, but also has been misused.
- If you have already become a victim of identity theft, please see our Consumer Guide Identity Theft: What to Do if It Happens to You [3].

2. What kind of personal information has been exposed by the data breach?

Once you determine the kind of information that was exposed by a breach, you can determine the action that you need to take. Five major kinds of data breaches are:

- A breach involving your credit or debit card information
- A breach involving another existing financial account
- A breach involving your driver's license number or another government-issued ID document
- A breach involving your Social Security number
- A breach exposing your password

The sections below describe the action that you should take to protect yourself for each of the above types of breaches.

3. Breach involving your credit or debit card information

Breaches of your credit or debit card information may occur in retail stores at point-of-sale (POS) terminals or as part of an online transaction. These breaches can be massive in size, sometimes affecting millions of cardholders.

You might become aware of a breach affecting your credit or debit card because your financial institution has reissued your payment card with a new account number. However, many financial institutions do not automatically reissue cards that may have

been compromised.

If you become aware (through news media coverage or otherwise) that there has been a payment card breach at a retailer at which you have shopped, what should you do?

First, determine whether you have used a debit or credit card at the merchant. There is far greater risk to you from a compromised debit card. If your debit card is used fraudulently, funds can quickly be withdrawn from your bank account without your knowledge. Your bank account can be emptied. On the other hand, if you used a credit card, you will have an opportunity to dispute any fraudulent transactions before you have to pay the bill, so you will still retain access to the funds in your bank account.

After you determine the type of payment card that you may have used, take these steps to reduce the risk of fraud:

- Ask your card issuer to cancel your current card and reissue the card with a new account number. They are not required to do so, and there may be a charge for the replacement card. However, this is especially important if you have used a debit card at the breached entity.
- Carefully monitor all your account transactions.
- If your card issuer offers it, set up text or email alerts of any activity.
- Make sure that your account statements arrive in your mailbox at their normal time. Consider setting up access to online statements, with email notification from the card issuer when your statement is ready for viewing.
- If you become aware of any fraudulent transactions, immediately call your financial institution and follow up by formally disputing the transaction in writing.
- Be suspicious of any email or phone call that you might receive about the breach that requests personal information.

4. Breach involving your existing financial accounts

If the breach involves an existing financial account, such as a checking, savings, money market, or brokerage account, here are some steps that you can take to reduce the risk of fraudulent activity:

- Ask your financial institution to cancel your account and issue a new account number.
- Carefully monitor all your account transactions online.
- If your financial institution offers it, set up text or email alerts of any activity.
- Make sure that your account statements arrive in your mailbox at their normal time. Consider setting up access to online statements, with email notification from the card issuer when your statement is ready for viewing.
- If you become aware of any fraudulent transactions, immediately call your financial institution and follow up by formally disputing the transaction in writing.
- Be suspicious of any email or phone call that you might receive about the breach that requests personal information.

5. Breach involving your driver's license or other government identification documents

If you are notified of a breach involving your driver's license or another government identification document (such as a passport or non-driver ID), contact the agency that issued the document and find out what it recommends in such situations. You might be instructed to cancel the document and obtain a replacement. Or the agency might instead "flag" your file to help prevent fraud.

6. Breach involving your Social Security number (SSN)

If the breach includes your Social Security number (SSN), the information could be used to open new accounts in your name. This is called new account fraud**.** You will not immediately know about these new accounts because criminals usually use an address other than your own for the account. That is why it is so important to immediately place a security freeze on your credit reports when you learn that your SSN has been compromised.

Consumers can place a security freeze on their credit files at the credit reporting agencies (Equifax, Experian, and TransUnion) at no cost. With a freeze in place, you can prevent *new creditors* (such as a credit card company or lender) from seeing your credit reports. The freeze prevents fraudulent new accounts because new creditors are not able to check your credit report. Requests for access to your credit file will be denied. Most creditors will not issue new credit if they cannot see the consumer's credit report. You must separately request a freeze from *each* of the three major credit reporting agencies in order to be fully effective. The websites of each of the credit reporting agencies provide instructions for placing a security freeze:

- Equifax [4]
- Experian [5]
- TransUnion [6]

If you want to apply for new credit, you can remove a security freeze temporarily. You can also permanently remove a freeze.

A security freeze does not apply to credit checks for:

- Employment or background screening purposes
- Tenant screening
- Insurance underwriting
- Identity verification purposes

Security freezes will not impact your credit score or your relationship with your *existing creditors*. Any existing creditor can continue to see your credit reports in order to periodically review your account.

A security freeze cannot stop misuse of your existing bank or credit accounts. You still must check your accounts for any errors or fraudulent activity.

Security freezes should not be confused with credit locks. Credit bureaus often encourage consumers to use a credit lock rather than a security freeze. While a security freeze provides protection that is governed by law, locks are governed by your contractual agreement [7] for each credit bureau. Having a contractual agreement is not as good as having protections under law. For example, the contract may include provisions that you may be better off not agreeing to, such as an arbitration agreement.

In addition to placing a security freeze on your credit reports, you will want to order copies of your credit reports from each credit bureau. You have the right to one free credit report each year from the three credit bureaus: Equifax, Experian, and TransUnion. When you receive your credit reports, look for signs of fraud such as credit accounts that are not yours. Check if there are numerous credit inquiries on your credit report. If a thief is attempting to open up several accounts, an inquiry will be listed on your credit report for each of those attempts. Also, check that your SSN, address(es), phone number(s), and employment information are correct.

You can order your free credit reports:

- By telephone: (877) 322-8228
- Online: www.annualcreditreport.com [8]
- By mail. Print out the order form here [9].

7. Breach exposing your password

If your password is exposed by a data breach:

- Change it immediately. Do not use a password that is similar to your old password.
- If you have used the same or a similar password elsewhere, change it immediately.
- Be suspicious of any email that you may receive asking you for personal information or containing any links. Independently verify the authenticity of the email.

Source URL (modified on February 7, 2019): https://www.privacyrights.org/consumer-guides/what-do-when-you-receive-data-breach-notice

Links
[1] https://www.privacyrights.org/consumer-guides/what-do-when-you-receive-data-breach-notice
[2] https://www.privacyrights.org/data-breach
[3] https://www.privacyrights.org/consumer-guides/identity-theft-what-do-if-it-happens-you
[4] https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
[5] https://www.experian.com/freeze/center.html
[6] https://www.transunion.com/credit-freeze/place-credit-freeze
[7] https://www.consumerreports.org/credit-bureaus/why-credit-freeze-is-better-than-credit-lock/
[8] http://www.annualcreditreport.com/
[9] http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf