Protect Yourself After a Data Breach

You wake up, take a sip of your morning coffee, and turn on the TV. The news anchors report that another data breach occurred. Your stomach drops. Once again, your most personal information may be compromised.

Unfortunately, the financial ramifications can resonate for years if hackers take action on the information they’ve stolen or sell it on the dark web.

**Taking precautions**
While Americans saw an increasing number of data breaches in recent years, the breach of insurance giant First American Financial in May 2019 topped them all with 885 million records exposed.\(^1\) These records, dating back to 2003, were left vulnerable to hackers due to poor security put in place by First American Financial.\(^1\) Worldwide, the public was hit even harder in 2019 by the Elasticsearch data breach. The breach of this search and analytics engine exposed the social media profile records of 1.2 billion people.\(^2\)

### Recent Data Breaches

<table>
<thead>
<tr>
<th>Year</th>
<th>Company</th>
<th>Number of Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td>First American Financial</td>
<td>885 million</td>
</tr>
<tr>
<td>2018</td>
<td>Marriott Starwood</td>
<td>500 million</td>
</tr>
<tr>
<td>2017</td>
<td>Equifax</td>
<td>143 million</td>
</tr>
<tr>
<td>2016</td>
<td>Adult Friend Finder</td>
<td>412 million</td>
</tr>
<tr>
<td>2015</td>
<td>Anthem</td>
<td>78 million</td>
</tr>
<tr>
<td>2014</td>
<td>eBay</td>
<td>145 million</td>
</tr>
<tr>
<td>2014</td>
<td>JP Morgan Chase</td>
<td>76 million</td>
</tr>
<tr>
<td></td>
<td>Home Depot</td>
<td>56 million</td>
</tr>
<tr>
<td>2013</td>
<td>Yahoo</td>
<td>3 billion</td>
</tr>
<tr>
<td></td>
<td>Target Stores</td>
<td>110 million</td>
</tr>
<tr>
<td></td>
<td>Adobe</td>
<td>38 million</td>
</tr>
<tr>
<td>2012</td>
<td>US Office of Personal Management (OPM)</td>
<td>22 million</td>
</tr>
<tr>
<td>2011</td>
<td>Sony’s PlayStation Network</td>
<td>77 million</td>
</tr>
<tr>
<td></td>
<td>RSA Security</td>
<td>40 million</td>
</tr>
<tr>
<td>2008</td>
<td>Heartland Payment Systems</td>
<td>134 million</td>
</tr>
</tbody>
</table>

Sources: CSO from IDG, 2018; Forbes, 2019

---

\(^1\) Source: "Understanding The First American Financial Data Leak: How Did It Happen And What Does It Mean?," Forbes, 5/26/19

\(^2\) Source: “Biggest data breaches of 2019: Same mistakes, different year,” CNET, 12/17/19
Sadly, no matter what precautions you might take, the chance your personal information—Social Security number, driver's license number, birthday, etc.—was or will be part of a data breach is high. If you're feeling anxious because your personal information has been compromised, the first step is to remain calm. You're not alone—many others were affected, too.

Here are the next three steps you can take ranked by effort and cost:

1. **Minor: Keep an eye on your bank and credit accounts**
   Don't throw that paper statement in the recycling bin or erase that email before you take a closer look at it each month. Regularly log in to review your activities online, too. You could even enable notifications on your phone's credit card app to see when a purchase is made in real time.

2. **Medium: Sign up for credit monitoring services**
   Would you rather have someone else take the time to review your finances? Fraud-protection specialists can watch for any out-of-the-ordinary behavior on your accounts and ensure you're notified if new ones are opened in your name without your knowledge. They'll alert you of any suspicious activity. Some are free, including Credit Karma, while others may require ongoing payment. Some companies, such as LifeLock, offer consumers their monitoring services for between $9.99 and $29.99 depending on what level of protection is sought. The four—yes, four—national credit reporting companies, Equifax, Experian, TransUnion, and Innovis, also offer their own versions of these paid memberships.

3. **Major: Freeze your credit**
   Pay a fee, and you can essentially shut down all access to your credit report. This requires reaching out to each of the four national credit reporting companies:
   - **Equifax**
     https://www.equifax.com
     866-640-2273
   - **Experian**
     https://www.experian.com
     888-397-3742
   - **TransUnion**
     https://www.transunion.com
     888-909-8872
   - **Innovis**
     https://www.innovis.com
     800-540-2505
Once this occurs, lenders will not have access to your credit. This prevents anyone from opening fraudulent accounts or applying for loans in your name. Depending where you live, freezing your account can cost anywhere from free to $10 at each agency. It will have no impact on current accounts.

Just make sure you’re not in the market for a home or car loan, applying for a credit card, or even looking for a new cell phone plan. As long as your accounts are frozen, no new accounts can be created—even if it’s you requesting them. To lift the freeze from your credit, simply reach back out to the four companies and pay an additional charge to turn things back on again. Four states—Kentucky, Nebraska, Pennsylvania, and South Dakota—automatically remove your credit freeze after seven years.

**Seeking additional guidance**
You may not be able to prevent every cyber attack, but your options to fight back are fairly straightforward. Be vigilant. Get help if you can. If all else fails, freeze your credit until you need to access it.

If you still have questions on what to do next, set up time to talk with your financial advisor. He or she can potentially be a great source of information if you’re debating what steps to take the next time your morning coffee is ruined with more bad news about data breaches.

**Ongoing Safeguards**

1. Only share personal data with trusted sources. Make sure you’re on a secure connection while sharing information online.

2. Use services such as PayPal, Apple Pay, or Android Pay to make purchases online more secure. Instead of passing along bank, credit, or debit card numbers and your contact information, these services maintain control of that data.

3. Check your credit with the major credit reporting companies regularly through the free Annual Credit Report program (AnnualCreditReport.com). Under federal law, you’re entitled to a free check every 12 months.

This material is provided for educational purposes only. Hartford Funds may or may not be invested in the companies referenced herein; however, no particular endorsement of any product or service is being made.

This information has been prepared from sources believed reliable but the accuracy and completeness of the information cannot be guaranteed. This material and/or its contents are current at the time of writing and are subject to change without notice. This material may not be copied, photocopied or duplicated in any form or distributed in whole or in part, for any purpose, without the express written consent of Hartford Funds.

Links from this paper to a non-Hartford Funds site are provided for users’ convenience only. Hartford Funds does not control or review these sites nor does the provision of any link imply an endorsement or association of such non-Hartford Fund sites. Hartford Funds is not responsible for and makes no representation or warranty regarding the contents, completeness or accuracy or security of any materials on such sites. If you decide to access such non-Hartford Funds sites, you do so at your own risk.

Hartford Funds Distributors, LLC, Member FINRA.

CCWP015_1219  215157