Lookout

Identity Theft in America

Shedding light on an evolving epidemic

Overview

It's highly likely that you or someone you know has had their identity stolen or been a victim of a large corporate data breach. Just in 2015, Javelin reported that 12.7M adults in the United States were victims of identity fraud.[1] Not to mention, as of October 19, the total number of U.S. breaches captured in the 2016 ITRC Breach Report totals 783, an increase of nearly 20 percent over last year's record pace for the same time period (656).[2] Regardless of whether it was a clicked phishing link, a stolen credit card number, or personal information that was leaked in one of the many corporate breaches clogging up the news headlines, identity theft could happen to anyone at anytime.

Identity theft can sometimes seem inevitable. In fact, according to a recent survey done by Lookout, 35 percent of respondents said that they have had their identity stolen in the past, and 41 percent of respondents think it's inevitable that their personal data or identity will be stolen at some point in the future.[3]

41%

of respondents think it's inevitable that their personal data or identity will be stolen at some point in the future

35%

of respondents said that they have had their identity stolen in the past

20%

year over year % increase of U.S. data breaches from October 2015 - October 2016

What is Identity Theft?

Identity theft is officially defined as the deliberate assumption of another person's identity. It is a crime where a criminal acquires and uses the victim's personal information, such as a Social Security or driver's license number, to take out loans, obtain new credit cards, rent an apartment, purchase a car, run up debt, file for bankruptcy and other criminal activities. Identity theft can not only damage someone's creditworthiness, it can also create unknown criminal records that can result in the identity theft victim being wrongly arrested or denied employment after a routine background check.

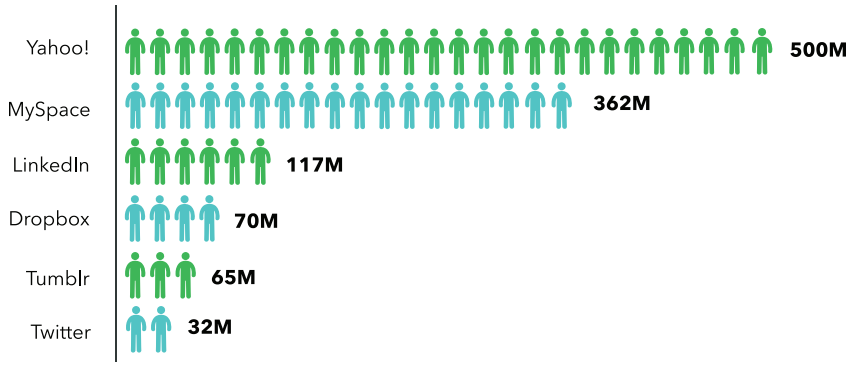
How Does it Happen?

Identity theft can happen a number of ways. For example, attackers may go through your garbage, or attempt to steal your mail in order to get personally identifiable information such as credit card or account numbers. Attackers have also kept up with technology, and are using new phishing techniques via email, websites or SMS, etc. to trick individuals into sharing personal information they can later leverage.

A common tactic for identity theft is using information leaked from corporate data breaches to log into existing user accounts. According to a recent Kroll Global Fraud Report, 22 percent of companies reported suffering from information theft in the past year.[4] How does this translate to identity theft? Think about the latest news headlines: "Yahoo! Breach leaked over 500M users data" and "LinkedIn Breach: 117 Million Emails and Passwords Leaked". Not to mention that Lookout's survey found that 60 percent of Americans reported that they have shopped or done business with a company that has been breached.

Major Corporate Breaches in 2016

Number of user credentials impacted



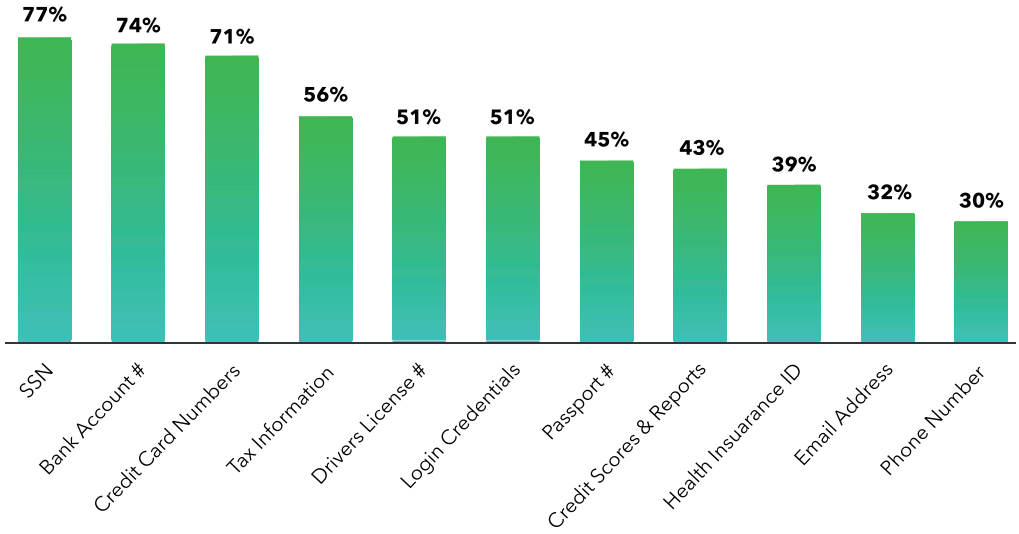
Credit card and financial info (like bank account numbers) and email addresses are the most typical types of private information impacted in a breach. Javelin reported that credit card and debit cards are among the most commonly stolen information, together representing 83 percent of the information breached for all consumers.[1]

How does this compare to what information people are most concerned about being stolen? Over 70 percent of Americans are worried about losing their Social Security number, bank account numbers and credit card numbers.

Personal Data Concerns

How concerned would you be if the following types of information were stolen?

% Very Concerned



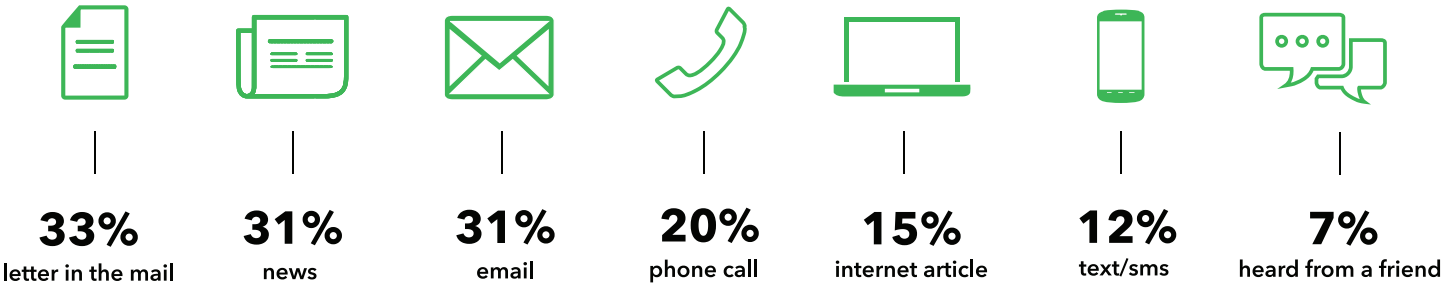
How Do You Find Out?

Unfortunately, finding out your identity has been stolen, or that your information has been involved in a larger company breach, isn't always a seamless action. You could notice something weird on your bank statement, hear from your credit card after multiple charges have been made, or even read about a massive breach in the news. People rarely hear about an incident quickly, or receive the notification via a means to ensure immediate action - for example, receiving a letter in the mail could take weeks.

In the case of your information being part of a corporate breach, the notification process is even more hazy. Turns out each state has a different law about disclosure timeliness, and when information actually needs to be shared with customers. According to Lookout's survey, mail, news and email are the most common mechanisms by which data breach victims are notified by companies/services. Interestingly, only 12 percent receive word of a breach by SMS/push notification.

Data Breach Awareness

How were you made aware of the breach?



So Your Identity Has Been Stolen. What Now?

As shown above, identity theft is something we should all be prepared to deal with. But according to our research, only a quarter of our survey respondents feel confident in knowing what to do if they are a victim of a data breach.

Timing is everything when it comes to protecting your identity. The sooner you can change your passwords, or thwart a thief who stole your identity, the better. Unfortunately our survey found that only 65 percent of victims of corporate data breaches are alerted within the first month, and even less find out about it within the first week. That means that 35 percent of victims don't get notified early enough to take precautionary measures.[3]

So what can you do? People can take a number of steps to help stay protected from identity theft, and tools to help you take action quickly if your identity is stolen.

How to protect yourself from identity theft:

- Use a password manager to generate and store random passwords. This makes sure no two accounts share the same password -- if one is hacked, the others stay safe. Secondly, even if one account shows up in a breach, the randomness of the password will make it almost impossible for attackers to crack.
- Enable multi-factor authentication for all your accounts, including email, banks, and your password manager. When logging in from a new device, and every 30 days, you'll need to enter a code from your smartphone. This way, even if an attacker knows your password they still can't get into your account so long as they don't have access to your phone as well.

75% of people aren't clear on what steps to take if their information is breached.

- Think before you click. Phishing is an old trick, yet still wildly effective. Attackers are using it over email, SMS messages, and even messaging apps. According to the Anti-Phishing Working Group, there were more phishing attacks in the first quarter of 2016 than any other time in history.
- Be careful when giving out personal information over the phone. Identity thieves may call, posing as banks or government agencies. To prevent identity theft, do not give out personal information over the phone unless you initiated the call.
- Use an app like Lookout to reduce the risk of identity theft:
    - Stay alerted about data breaches: Lookout's Breach Report will alert you if a company, app or service you use has been breached and give you straightforward tips on how to protect yourself.
    - Monitor your identity online: Lookout's Identity Theft Protection will monitor your personal and financial information and provide timely alerts whenever anything is found exposed online.
    - Take action if your identity is stolen: Lookout's certified Identity Restoration Experts are available 24/7 to assist with the time-consuming and overwhelming process of recovering and restoring your identity.

About the Data

(1) Javelin 2015 Identity Fraud Report
(2) Identity Theft Resource Center: Breach Report Hits Near Record High in 2015
(3) Lookout Survey
(4) Kroll Global Fraud Report, 2013/2014

Lookout Survey Methodology

- An online survey was conducted to a panel of potential respondents. The recruitment period was May 20, 2016 to May 25, 2016.
- A total of 2,000 panel respondents completed the survey (excluding terminates and abandonments). The goal was 1,000 respondents from each of the following categories:
  - United States Lookout customers: 1,000 respondents
  - United States market consumers (non-Lookout customers): 1,000 respondents
- Besides country, there were three screeners for the survey to determine eligibility:
  - All respondents were 18 years of age or older
  - Each respondent had to currently own a smartphone
  - The smartphone had to be an Android or an iPhone
  - Sample was provided by Market Cube, a research panel company. All were invited to take the survey via an email invitation.
  - Panel respondents were incented to participate via the panel's established points program.