New Account Fraud—A Growing Trend in Identity Theft

November 2016

Original data analyzed by: Identity Theft Resource Center® (ITRC)
Sponsored by: LifeLock
# Table of Contents

**Introduction and Methodology**.................................................................................. 3  
**Executive Summary**................................................................................................. 5  
**Key Findings**  
  - How information was compromised ...................................................................... 6  
  - Awareness of “New Account Fraud” and Level of Concern ............................... 7  
  - Personal information and New Accounts ............................................................ 8  
  - Personal Information Compromised ...................................................................... 9  
  - Finding Out about a New Account ....................................................................... 10  
  - Finding Out about a stolen credit card ................................................................ 11  
  - Responsibility for protecting personally identifiable information .................. 12  
  - Trust in Financial Institutions ............................................................................. 13  
**Conclusion**.................................................................................................................. 14
Introduction and Methodology

Looking back at the types of information compromised during 2015, the Identity Theft Resource Center (ITRC) saw an astronomical rise in the number of Social Security numbers (SSNs) exposed as a result of many high profile breaches. According to the ITRC’s 2015 Breach Report, there were more than 165 million SSN’s exposed, more than 10 times the number compromised in 2014. What makes this statistic even more staggering is the fact that there were two fewer data breaches in 2015 than were reported in 2014. Javelin Strategy & Research’s 2016 Identity Fraud: Fraud Hits an Inflection Point¹, revealed that one in five data breach victims suffered fraud in 2015, rising notably from one in seven in 2014.

With this tremendous influx of SSNs on the black market, which are now quite likely in the hands of identity thieves, it may come as no surprise that new account fraud (NAF) is on the rise in the U.S. According to Javelin, SSN breach victims suffered a substantially higher rate of new account fraud than all consumers – more than 6 times higher. In fact, new account fraud surged to more than double its 2014 incidence for all consumers².

There are several factors which may have contributed to the rise in new account fraud among 2015 survey respondents and they include the introduction of EMV-chip-enabled cards in the U.S. and the vast number of SSNs which were breached during 2015. EMV cards make it much more difficult for identity thieves to commit counterfeit card fraud (a form of existing credit card fraud) making new account fraud much more appealing as the lowest hanging fruit. Combine that with 165 million compromised Social SSNs during 2015 and you have a perfect storm for the growth of new account fraud.

With this trend in mind, the ITRC recently conducted an online survey seeking answers about consumers’ awareness of new account fraud, a term often used to define one type of identity theft. For the purpose of this survey, new account fraud was defined as “the opening of a new financial account using another’s personal identifying information —with the primary intent to commit fraud.”

¹ 2016 Identity Fraud: Fraud Hits an Inflection Point February 2, 2016
² 2016 Identity Fraud: Fraud Hits an Inflection Point February 2, 2016
The ITRC fielded this online survey with individuals who had their personal information compromised to measure their awareness and knowledge of the issues involved in new account fraud. ITRC also sought answers to a series of questions regarding these consumers’ understanding of what pieces of information makes them more vulnerable to NAF.

Specifically, the survey was designed to test existing knowledge that includes the following:

- The definition and characteristics of new account fraud
- If they know what it is, and whether they are concerned about it
- How respondents think they might find out about it happening to them

“There are many forms of identity theft and this survey provided insight into the participant’s awareness and understanding of new account fraud and related issues,” said Karen Barney, Director of Research and Publications. “These survey responses will enable the ITRC to create focused educational materials and documents to provide enhanced levels of assistance to victims when these types of identity theft cases occur.”

**Methodology**

The respondents were website visitors who clicked on an image posing the question “To the best of your knowledge, has your personal information ever been compromised? If yes, click here.”

The website-based survey received 332 responses. This question-based entry into the survey allowed for a filtering process by which participation was limited to those who had already experienced some kind of personal information exposure. As such, those who responded may have already had an identity theft experience which led to them to the ITRC website. These are important elements to remember when analyzing the data.

The survey was designed to help the ITRC and partner organizations identify and understand consumer perceptions on this issue in order to better develop educational materials and informational campaigns.
Executive Summary

The information presented in this survey speaks to the need for greater public awareness, better means of educating consumers on personal security, and an increased understanding of the role that consumers play in their own protection.

Consumers whose data has been compromised in the past were asked to indicate the method by which a criminal accessed their personal information. The results are somewhat surprising. The survey responses reflect that there continues to be a wide array of methods by which criminals are able to obtain personal information.

The responses to the ITRC’s questions also demonstrated some intriguing results, especially when taking into consideration the fact that all of the survey respondents had already had their data compromised. Statistics include the following:

- 30 percent of the respondents did not know that their Social Security numbers are critical pieces of the identity theft puzzle.
- 80 percent believe that the responsibility for preventing new account fraud (a specific form of identity theft) rests with the individual consumer.
- More than 86 percent of the respondents were very or extremely concerned about new account fraud happening to them.
- 55 percent believe they will never be informed if their credit card numbers are stolen in a data breach.

“Responses to many of the survey questions emphasize the need for increased education around the topics of data breaches, new and existing account fraud, and the vulnerabilities victims face when their sensitive personal information becomes exposed”

Eva Velasquez
ITRC President/CEO
Key Findings

How information was compromised

One of the most concerning issues reflected in this survey is how scammers obtained the personal information from the respondents.

Of the 332 people who responded, 77.7 percent of them indicated that their data had been directly compromised through either the loss or theft of their wallets, smartphones, mail, or other items that contained their information. Those individuals were targeted in a one-on-one crime, as opposed to the 47.4 percent of respondents who stated that they were the victims of a more sophisticated, widespread approach like hacking, phishing emails, or data breaches. Keep in mind there is some duplicity in those numbers, as some respondents were the victims of multiple means of having their data accessed.

Perhaps the most interesting highlight from the survey was this: of the survey respondents—again, all of whom have had their information compromised in the past—the most common method by which scammers got ahold of their information was because the victim willingly handed it over. In almost 20 percent of the cases, the survey participants gave out their personal identifiable information to someone who contacted them over the phone. (Figure 1).

It becomes readily apparent, in the survey responses provided, that there are just as many low-tech ways of stealing information as there are high-tech ways.
These findings are notable as many interested parties, including media, law makers and industry businesses, frequently inquire about the most common way personal information is compromised. It becomes readily apparent, in the survey responses provided, that there are just as many low-tech ways of stealing information as there are high-tech ways.

**Awareness of “New Account Fraud” and Level of Concern**

Nearly 84 percent of the survey respondents indicated they had never heard the phrase “new account fraud.” Despite this, most of those who participated in the survey were able to identify commonly accepted examples of new account fraud. However, there was some difficulty in recognizing whether or not a new Facebook account being opened was considered NAF, with 54 percent indicating they thought it was.

Even though a large majority indicated they were unfamiliar with the term NAF, more than 86 percent of the respondents were very or extremely concerned about this type of fraud happening to them. (Figure 2)
When asked why they felt concern, more than 65 percent of the survey respondents indicated they were worried about the time it would take to correct problems. This was followed by fear of damage to credit score (63.3 percent), fear of not being able to recover out-of-pocket expenses (48.5 percent), and fear of an existing account being taken over (44 percent). (Figure 3)

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fear of my existing account being taken over</td>
<td>43.9%</td>
</tr>
<tr>
<td>Fear that I won’t be able to have access to funds in my account</td>
<td>38.4%</td>
</tr>
<tr>
<td>Fear of damage to my credit score</td>
<td>63.3%</td>
</tr>
<tr>
<td>Fear of being charged bank fees</td>
<td>35.4%</td>
</tr>
<tr>
<td>Fear of not being able to recover out-of-pocket expenses</td>
<td>48.5%</td>
</tr>
<tr>
<td>Because it’s happened to me before</td>
<td>26.6%</td>
</tr>
<tr>
<td>Because it happened to people I know</td>
<td>12.7%</td>
</tr>
<tr>
<td>Because my purse was stolen</td>
<td>13.1%</td>
</tr>
<tr>
<td>Worried about time it will take to correct problems</td>
<td>65.4%</td>
</tr>
</tbody>
</table>

**Personal Information and New Accounts**

Survey participants were also asked about what they believe to be the single most important piece of personal information necessary to open a financial account. Seventy percent of the respondents indicated a Social Security number is the key piece of information needed by fraudsters to open a new account, which is indeed the case. (Figure 4)
While this could be seen as a strong positive percentage, it still begs the question, “What about the other 30 percent who believe their driver’s license/state ID, a credit card, passport, or just your name and address are the most important piece of information?” Other responses also included birth certificate, mother’s maiden name, current pay stub, and birthdate.

**Personal Information Compromised**

The type of personal information compromised is often a determining factor in whether or not the compromise might result in a case of identity theft.

More than 76 percent of the respondents indicated their Social Security numbers had been compromised, followed by 48 percent indicating their driver’s license/state ID had been exposed. Nearly 32 percent of the survey respondents indicated their debit card number had been compromised, slightly higher than the 28 percent who reported the compromise of their credit card number. (Figure 5) It is important to recognize here that the SSN is the golden ticket for thieves for opening new accounts.
Finding out about a New Account

When asked, “How do you think you would find out about a fraudulently opened account?” respondents were allowed to select multiple responses. Nearly half of the survey participants responded, “I don’t know.” This response was followed by 48 percent of the respondents who indicated they would see it on a credit report, and 13 percent who believed they would be notified by law enforcement. (Figure 6)
Many of the respondents also believed they would be notified by their bank – either by mail, email, text message, or by phone. Education efforts on this issue could focus on proactive steps consumers can take to monitor their credit reports on a regular basis.

“Responses to many of the survey questions emphasize the need for increased education around the topics of data breaches, new and existing account fraud, and the vulnerabilities victims face when their sensitive personal information becomes exposed”, said. Eva Velasquez, President/CEO Identity Theft Resource Center.

“This is particularly true in terms of raising awareness on safeguarding your personal identifiable information, and taking action following a data breach or notification of compromised data. Tailored programs that address these issues will narrow the knowledge gap considerably,” Velasquez added.

Finding out about a stolen credit card number

For contrast in finding out about new account fraud, we also asked about stolen existing credit card numbers. When asked, “Which of the following do you think would happen if your credit card number was exposed in a breach?” nearly 55 percent of the participants felt they would never know. Just over 38 percent thought they would be notified by their financial institution, with nearly 29 percent responding that they would be notified by the retailer/online site. Nearly 13 percent indicated they thought they’d be notified by law enforcement.

It is disturbing that the majority of survey participants felt like they would never know. The ITRC, which has been tracking breaches since 2005, has long recognized that data breaches have been underreported over the years. As such, many consumers whose information has been compromised are not made aware of the exposure of their information. Oftentimes the notification from a financial institution is in the form of a new credit card. As to retailers/online sites, their compliance to state breach notification laws is often contingent upon whether or not the incident is reported in the media first. Law enforcement is seldom, if ever, responsible for notifying consumers.
Responsibility for protecting personally identifiable information

Regarding the protection of personal information, survey participants were asked how much responsibility they believe each of the following have: the individual; their financial institutions; companies or retailers that they do business with online; brick and mortar companies or retailers you do business with in person; their internet browser; and the government.

Ranking first was the individual, with nearly 80 percent of the respondents indicating they have “a lot” or “tremendous” amount of responsibility. Financial institutions ranked second with approximately 65 percent of the respondents placing high levels of responsibility on them, followed by the government with 54 percent indicating “a lot” or “tremendous” amount of responsibility. These were followed by online companies at 50 percent, brick and mortar stores/retailers at 43 percent, and internet browsers with 42 percent of the respondents indicating a high level of responsibility for these entities. These results are encouraging as they reflect the growing need for personal responsibility in protecting one’s own personal information and not putting that responsibility on other entities.

Trust in financial institutions

In addition, participants were asked how much they trusted their financial situation (FI) in a number of areas using a scale from 1 to 5 where “1” meant they do not trust them at all and “5” indicated they trusted them completely. Less than 24 percent of the respondents fully trusted their FI to keep them informed about changes to their account while 23 percent did not trust them at all.

The same lack of trust was expressed when asked about their FI educating them on matters relevant to the privacy of their account. While 23 percent trusted the FI fully, 24 percent had no trust at all. Responding to the question about the FI keeping personal information safe, secure and protected, 27 percent had full trust in the FI while 23 percent had no trust at all. Lastly, when asked to respond to whether the FI would notify them if there’s been a breach or compromise of their information, 27 percent of the respondents trusted the FI while 24 percent did not trust the FI at all.
Conclusion

Notable, and alarming, is the response that in almost 20 percent of the cases the victim gave out their personal identifiable information to someone who contacted them over the phone...

Overall, the survey findings speak to the need for greater public awareness, better means of educating consumers about personal security, and an increased understanding of the role that consumers play in their own protection. It should be noted that all survey respondents came to the survey by visiting the ITRC website for reasons independent of the survey. This would seem to indicate that the participants already had something occurring in their life which led them to seeking out information about identity theft or related issues.

Notable, and alarming, is the response that in almost 20 percent of the cases the victim gave out their personal identifiable information to someone who contacted them over the phone calling out the need for greater educational efforts to be made to inform consumers about the dangers of providing their personal information to unknown entities and individuals – particularly by phone.

When examining the role consumers’ play in their own protection, only 48 percent of the survey respondents identified credit reports as a means by which to find out about fraudulently opened accounts. Heightened educational and awareness efforts should be made so consumers are aware of the importance of being more proactive in monitoring their own credit reports to help thwart the damage done by identity theft.

Going forward, the ITRC will continue to develop informational documents and bring them to consumers through its website, call center, Live Chat and new ID Theft Help mobile app.