Identity Theft: The Aftermath 2013™

Conducted by the Identity Theft Resource Center® (ITRC)[i]

With comparisons to previous *Aftermath Surveys*

Original data analyzed by: The Identity Theft Resource Center
Research Sponsored by: Google

Commentaries: Matt Cullina [ii], Julie Fergerson [iii], Susan Grant[iv], Dr. Charles Nelson [v]
Robert Siciliano [vi] and Eva Velasquez [vii]

Identity Theft: The Aftermath 2013

Table of Contents

Figures in Paper

IDENTITY THEFT: The Aftermath 2013

Executive Summary – *Identity theft affects more than just finances. The emotional and behavioral effects of identity theft are many, and continue well beyond the initial crime.*

The Identity Theft Resource Center's *Identity Theft: The Aftermath 2013* yielded many interesting findings, not the least of which is how little some things have changed, despite growing national efforts to address the many issues faced by victims. The ITRC's *Aftermath* studies have always been recognized for their focus in addressing the impact of identity theft on its victims. The *Aftermath 2013* report is the latest in this series of studies, which began in 2003.

Not surprisingly, the 2013 survey reflects many similarities to the 2009 study regarding the pervasiveness of some types of identity theft crimes. In both studies, financial identity theft involving new accounts ranked as the number one issue, with 61.2 percent reported in 2013, an increase of 6.2 percent over the 55.0 percent reported in 2009.

The issue of medical identity theft was addressed for the first time in the 2008 study, with only nine survey participants (10 percent) responding to that question. The same level of response was reported for 2009, with 18 respondents out of 183. In the 2013 survey, 21.4 percent of the respondents indicated some kind of medical identity theft issue, more than double the percentage reported in previous years.

From an emotional standpoint, the impact of identity theft for some victims continues to be traumatic, as evidenced by their answers. Participant responses covered a broad range of emotions, including suicidal feelings (6.7 percent), shame or embarrassment (29.4 percent), overwhelming sadness (31.6 percent) and disbelief (41.2 percent). Much higher percentages of helplessness (50.3 percent) betrayal (50.8 percent), and rage and anger (65 percent) may be indicative of complex issues involving other types of identity theft, not just financial. Nearly 70 percent of the respondents indicated fear regarding their own personal financial security.

The truth is that identity theft comes in many forms besides financial identity theft, including criminal, medical, and government identity. These types of identity theft often have a greater impact on victims than traditional financial identity theft. They generally take longer to resolve, have a greater out of pocket expense, and leave victims feeling more violated and less trusting.

Something noteworthy is the continued level of dissatisfaction with law enforcement interaction, which is at nearly 41 percent, with 14.4 percent and 26.5 percent of the

respondents indicating “poor” and “terrible,” respectively. This sentiment is expressed despite the fact that 78 percent of victims were able to obtain a police report. Of those victims who did not obtain a police report (22 percent), nearly 36 percent said they tried but were unsuccessful.

It is apparent that even after 15 years of involvement by government/regulatory agencies, advocacy groups, and non-government organizations, more education is needed regarding the critical importance of this tool.

Cell phone capabilities and usage have changed dramatically since our 2009 survey, prompting the ITRC to add new questions regarding mobile device activity. Questions regarding online engagement were also posed to this survey group.

When it comes to identity theft –
***no one is immune, from birth to beyond death* (*Aftermath 2003*[viii])**

This quote, taken from our survey of 10 years ago, demonstrates how long the ITRC has been striving to heighten awareness of this fact. Identity theft can affect ANYONE. This crime crosses many demographic lines. You don’t need to be wealthy or have excellent credit to become a victim. The 2013 survey responses support this position. It seems evident all income levels and ages have their own unique and appealing vulnerabilities to thieves.

Identity Theft: The Aftermath is not a census survey, rather a research survey and white paper regarding the impact of identity theft on the lives of confirmed victims who contacted the ITRC for assistance. It is a reflection of each victim’s case, and of their feelings and attitudes at the time they responded. It may not represent the entire experience of the individual. ITRC has conducted surveys since 2003 allowing us to compare some patterns and trends which continue to occur. We realize that since each was populated by a different group of victims, it is a subjective comparison and that other issues change the picture.

Key Findings:

- **Identity theft continues to victimize people of all ages and income levels**. More than half of survey respondents had a household income level of less than $50,000. Respondent’s age has little to do with victimization rates.

- **New utility and cell phone accounts are appealing to identity thieves.** One out of four victims who had new accounts opened in their name had either utilities or a cell phone account opened.

- **Identity theft involving existing accounts was experienced by more than half (52.4 percent) of the survey participants.** Seven out of 10 (71 percent) of those who experienced this type of activity did not change financial institutions after experiencing unauthorized activity on their existing accounts.

- **Criminal identity theft continues to have an impact.** Approximately 1 in 5 of the survey respondents dealt with this issue in some manner.

- **Nearly 40 percent of the survey respondents reported government identity theft issues.** Regarding IRS tax-related identity theft, only 55 percent of respondents who dealt with the IRS had received their appropriate refund at the time they responded to the survey.

- **More proactive detection measures are needed for medical identity theft.** The most common way victims discovered medical identity theft was when the medical provider, billing department or a collection agency billed them for services they never received.

- **Inability to resolve the issue and lingering effects:** More than half of the respondents indicated they had not yet been able to resolve their identity theft issues. Some of the lingering effects of identity theft reported by the survey respondents included: 35 percent of victims had their ability to obtain credit affected, 22 percent were still being called by collection agencies and nearly 20 percent had their job, or ability to get a job, affected as a result of this crime.

- **Victim satisfaction with law enforcement remains elusive.** More than 40 percent of respondents who dealt with law enforcement were dissatisfied with the interaction, with 14.3 percent rating the experience as “poor” and 26.5 percent rating it as “terrible.”

- **Strong emotions continue to be present when dealing with this crime.** Strong feelings such as “rage and anger,” “fear for personal financial safety,” “powerlessness and helplessness” rank in the top five of emotional responses.

- **Experience is a valuable teacher.** Behavior changes after victimization were reflected in the survey responses. After they had become victims, 50 percent more of respondents checked their credit reports regularly.

- **Despite being victims of identity theft, 94.2 percent of the respondents are still highly engaged online and on their mobile devices.** This level of

activity is relevant to all business and industry sectors seeking to further expand their presence via these types of devices and communication channels.

INTRODUCTION

The Identity Theft Resource Center® developed *Identity Theft: The Aftermath*™ as a means by which anyone interested in identity theft may view this crime through the eyes of a victim. *Identity Theft: the Aftermath 2013* is a one-of-a-kind study, with information from prior *Aftermath* studies included.

These results provide a snapshot of the victim experience for a given year. This is not a random sample study. Survey respondents are victims of identity theft who contacted the ITRC in 2013 for assistance in resolving their cases. ITRC has compared some of the responses in this year's study to those from past years' in order to identify trends which may have influenced identity theft issues year over year. Outcomes and opinions of individual victims are influenced by a multitude of factors, including changes in the law, media coverage of specific issues, changes in the education/advocacy climate and/or assistance provided by the ITRC's skilled advisory staff.

The *Aftermath* survey provides insight not just into what has happened to victims (their experience) and what actions they have taken, but also takes a look at how those victims feel about these experiences with respect to influencing future decisions.

Statements included in some of the sections below are in the words of the victims themselves and are extracted from the open commentary section of the *Aftermath* survey. Inclusion of these statements encourages the reader to remember that behind each of the numbers represented in this survey there exists a person whose life has been impacted.

FINDINGS

A. IDENTITY THEFT CONTINUES TO VICTIMIZE PEOPLE OF ALL AGES AND INCOME LEVELS.

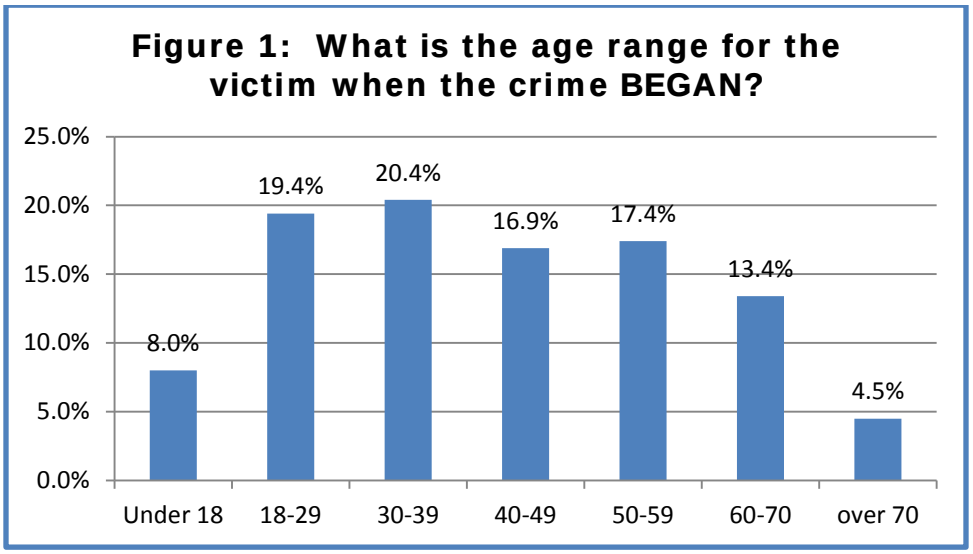
The *2013 Aftermath* study represents victims who contacted the ITRC during the 2013 calendar year. Information, which was mandatory, includes state of residence, age when crime began, and household income level.

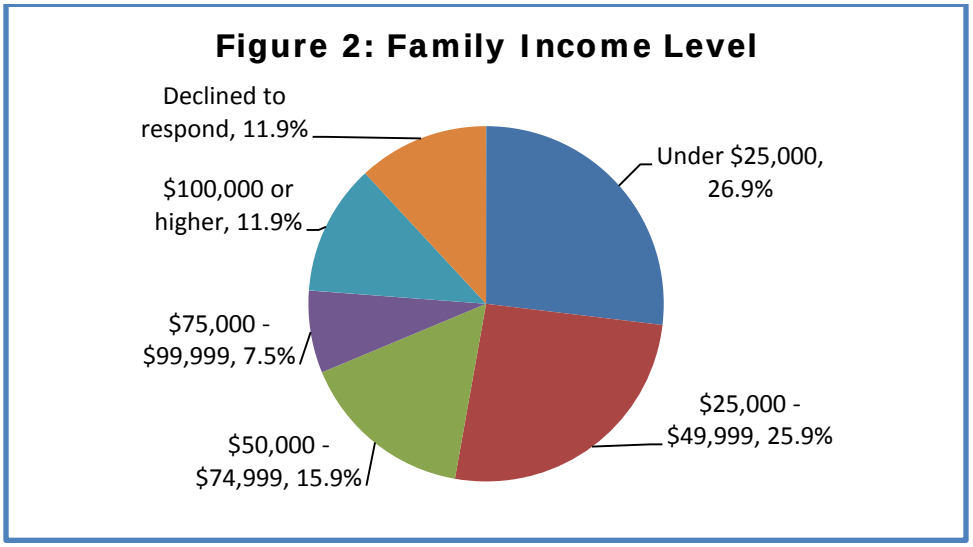
- 201 victims responded from 39 states. It should be noted the area the victim lives in is not to be misconstrued as the location of the crime. Anecdotally, the

ITRC continues to note the vast majority of these cases are multi-jurisdictional in nature. *(Demographics in Appendix)*

- Of the 201 respondents, 8 percent of victims were under the age of 18 when the crime began. All other age groups were almost uniformly represented. Other age categories were as follows: 18-29 (20 percent); 30-39 (15 percent); 40-49 (17 percent); 50-59 (17 percent); and 60+ (17 percent). *(Figure 1)*

- Of the 177 participants who answered the question regarding household income, more than half had household incomes less than $50,000. *(Figure 2)*





B. HOW VICTIM INFORMATION IS USED

The *2013 Aftermath* study captures the ways by which thieves used victim data and information for their own financial gain.

Rather than ask respondents to categorize the "type" of identity theft they may have experienced, we asked them to tell us if they experienced things like NEW accounts being opened, and if so, what type of accounts. We asked about the various ways thieves used their information. Were medical goods or services obtained? Was there a criminal conviction in court under the victim's name? Did a thief file a false tax return using the victim's information?

Overall categories and percentage of survey respondents:

- **New Financial accounts opened (61 percent):** Victim information was used to open new credit cards, loans, checking or savings accounts, cable, internet, utilities, or cell phone accounts.

- **Existing Financial accounts used/taken over (52 percent):** Victim information was used to make charges or conduct transactions on existing credit cards, loans or lines of credit, checking or savings accounts, debit cards, other types of financial accounts (for example, PayPal).

- **Financial "Other" (43 percent)**: Victim information used to rent or lease a dwelling (apartment, house, etc.) or vehicle, or auto insurance was provided in an accident.

- **Criminal (18 percent):** Victim information was given to law enforcement during the commission of a crime (infraction, misdemeanor or felony).

- **Governmental, including tax refund (39 percent):** Victim information was used to obtain a driver's license, file taxes, or to obtain a job (Social Security number provided to employer). Government agency benefits, such as unemployment, food stamps and Social Security, were reported by 11.4 percent of the respondents.

- **Medical (21 percent):** Victim's information was used to obtain medical goods or services, including prescriptions and office visits.

Robert Siciliano, ITRC Board of Directors and Identity Theft Expert:

Identity theft is not something that just happens to other people. It happens to you, me and everyone around us, regardless of our income, age, who we bank with, whether we are dead or alive, our credit scores, or even if we aren't a person but a business instead.

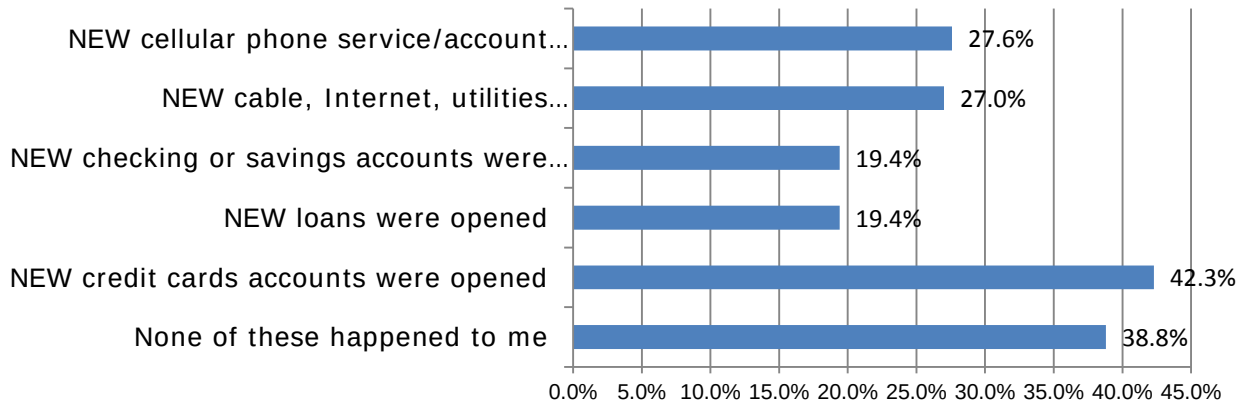
Consumers need to be armed with a basic understanding of how identity theft happens, how to detect it when it does, and finally how to clear their names after discovery. Consumers can't sit on the sidelines and hope that businesses, employers, banks and other financial institutions will be vigilant for them. People need to be proactive – monitoring their financials, protecting their sensitive information and being quick to act once they detect any evidence of identity theft.

C. FINANCIAL IDENTITY THEFT - NEW AND EXISTING ACCOUNTS

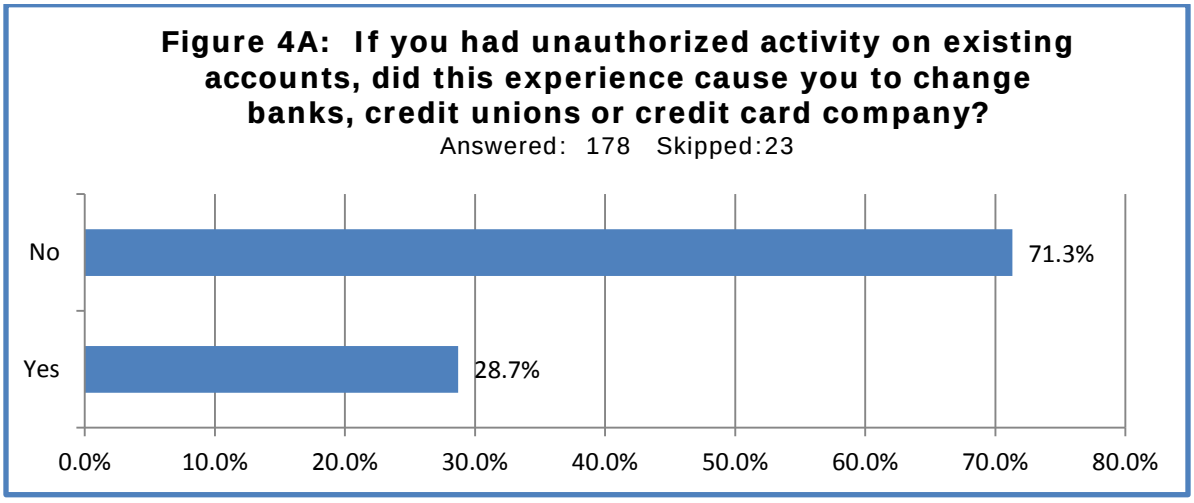
Utilities and cell phones are appealing to thieves. Not all victims experienced NEW account identity fraud but, of those who did, credit cards were the most common type of new account opened (42.3 percent). Of note this year, new cell phone accounts were reported by 27.6 percent of the respondents followed by 27.0 percent reported for new utilities (cable, internet, services). *(Figure 3)*

Figure 3: When you experienced identity theft, did any of the following occur? (Check all that apply)

Answered: 196 Skipped: 5



Identity theft involving existing accounts was experienced by more than half (52.4 percent) of the survey participants. *(Figure 4 in Appendix)*. Seven out of 10 (71.3 percent) of those who experienced this type of activity, did not change financial institutions after experiencing unauthorized activity on their existing accounts. *(Figure 4A)*



Julie Fergerson, ITRC Board Chair and Subject Matter Expert:

Having your financial identity compromised is an intrusive and shocking experience, which can result in consumers having reduced trust and loyalty to their financial institutions. Despite this natural reaction, we are seeing that over 70 percent of the surveyed victims who had unauthorized activity on existing financial accounts stayed with the same financial institution after the identity theft.

Perhaps this is due to consumers becoming more understanding that identity theft can happen to anyone, regardless of what financial institution they use, and are now more concerned with how they are treated in response to said identity theft when determining whether they will continue using the same financial institution.

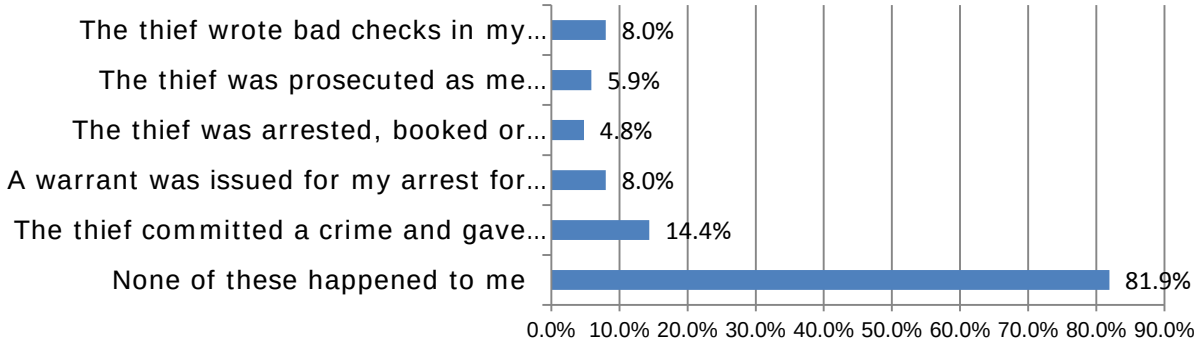
D. CRIMINAL, GOVERNMENT AND MEDICAL IDENTITY THEFT

Criminal identity theft

Nearly one in five of the survey respondents dealt with this issue in some manner, including the thief providing the victim's information during a crime (14.4 percent), bad checks being written (8 percent) and warrants being issued in the victim's name for a crime (8 percent). *(Figure 5)*

Figure 5: When you experienced identity theft, did any of the following occur? (Check all that apply)

Answered: 187 Skipped: 14



Government identity theft

Nearly 40 percent of the survey respondents reported government identity theft issues *(Figure 6).* The largest percentage of these (23.5 percent) involved tax identity theft (taxes filed in the victim's name). Nearly 90 percent of those victims reported the incident to the IRS *(Figure 6A in Appendix).* Only 55 percent of the respondents who communicated with the IRS had received their appropriate refund at the time they responded to the survey. *(Figure 7)*

Other forms of government benefits identity theft, such as social services, unemployment and welfare, were reported by nearly 9 percent of the survey respondents. *(Figure 6C in Appendix)*

Figure 6: When you experienced identity theft, did any of the following occur? (Check all that apply)

Answered: 187 Skipped: 14

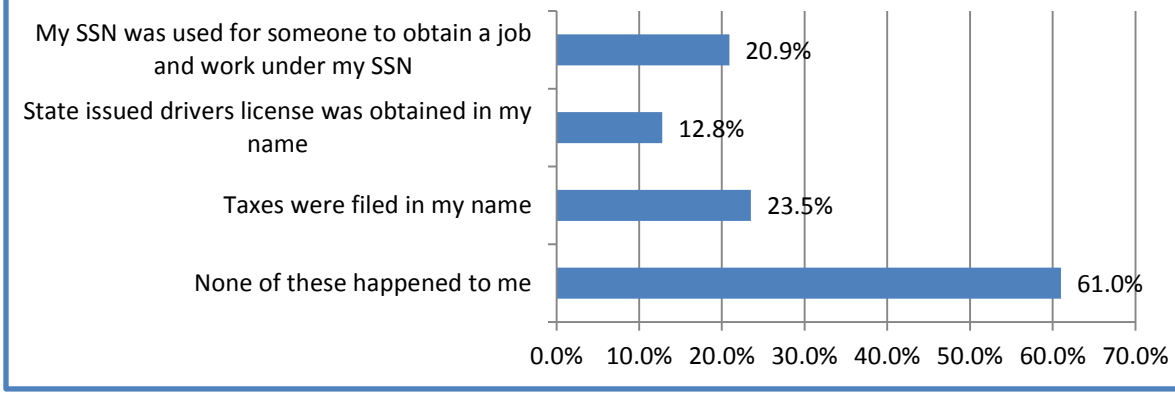
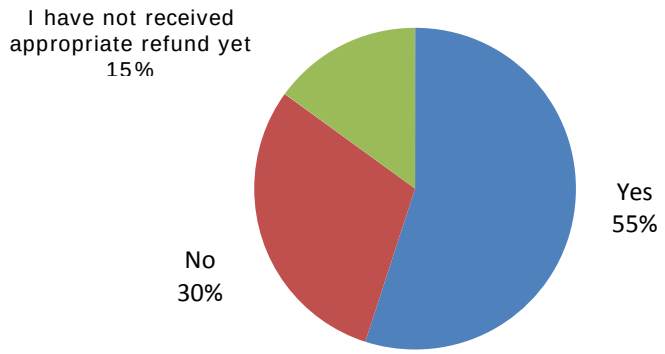


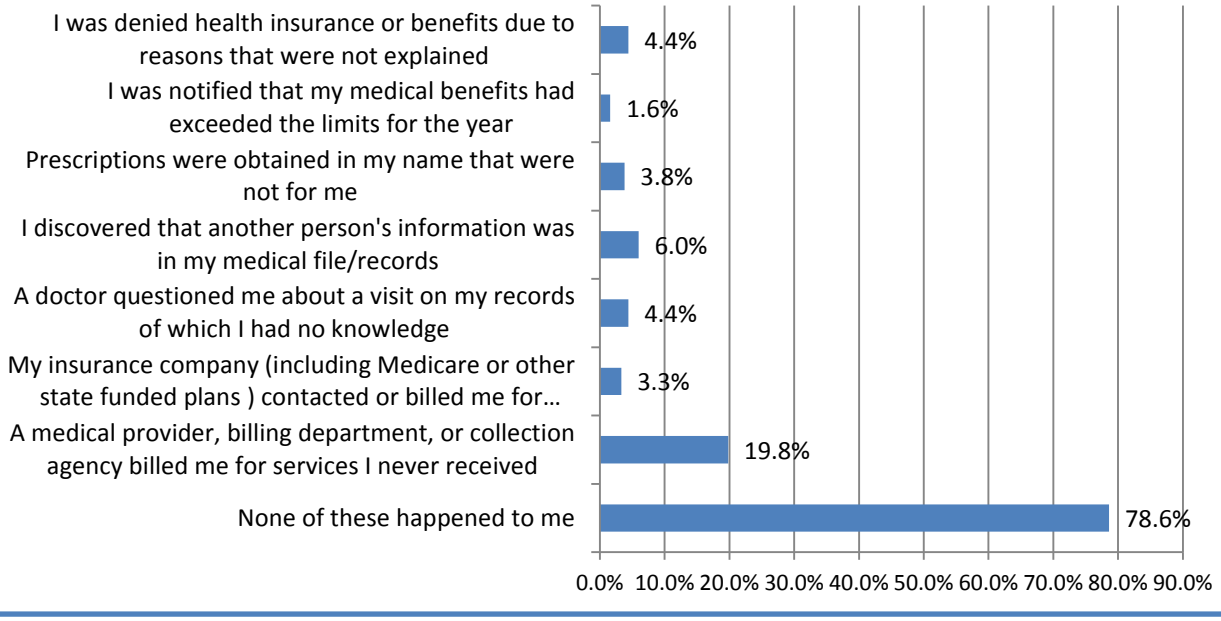
Figure 7: Did you receive your appropriate refund?
Answered: 40 Skipped: 161



Medical identity theft

This type of identity theft, with sometimes dangerous consequences, was reported by 21.4 percent of the survey respondents. Nearly one in five of those who answered this question indicated they found out about the crime via a bill for services they never received. More seriously, 6 percent discovered someone else's health information in their medical records. Inaccurate medical records can have consequences that are further reaching than financial distress alone. *(Figure 8)*

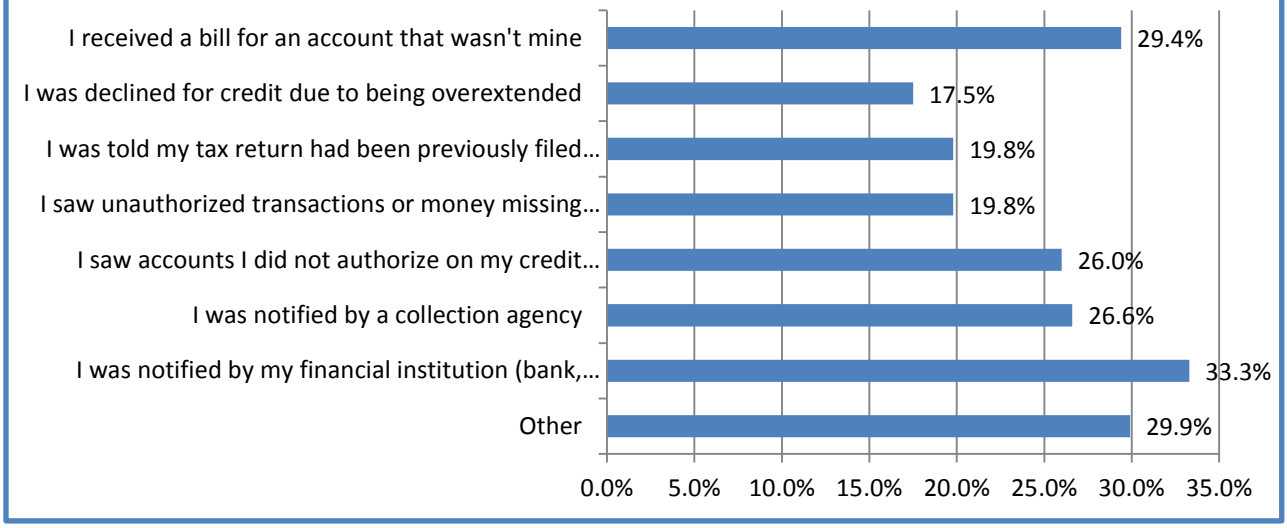
Figure 8: When you experienced identity theft, did any of the following occur? (Check all that apply)
Answered: 177 Skipped: 24



E. MOMENT OF DISCOVERY

How identity theft is discovered: The most common way victims discovered the crime was from notification by their financial institutions (33 percent). *(Figure 9)* We applaud these entities for being proactive and alerting their customers of this issue.

Figure 9: I discovered identity theft had occurred when: Answered: 177 Skipped 24



***Eva Velasquez, President/CEO, Identity Theft Resource Center**:*

How individuals discover they have become victims remains an important detail in our efforts to combat this crime. The sooner victims discover the crime, the less damage thieves are able to inflict. Proactive self-discovery is an essential, but often under used, tool for victims.

In their own words:

It really killed my time to do the things I needed to do. I work for myself and if I do not work, I do not make money. Wasting all the time to resolve this hack on my ID wasted a lot of time and money.

In the "other" category, victims mentioned a variety of ways, many quite unpleasant, by which they found out they had become victims. Some of these statements included:

- *I was taken to court for two child support cases (I don't have any kids)*
- *I was notified that my driver's license was suspended*
- *I saw prescriptions filled that weren't mine*

- *My driver's license was being revoked for DWI in another state that I had never been in*
- *I was taken into custody at a military base and told I had a deportation warrant*
- *I saw checks on my bank statement that were not written by me*
- *I received a package that I did not order*

Time Elapsed Between First Incident and Discovery by Victims

While it is encouraging to note that an increased number of victims were able to detect the identity theft crime in 3 months or less, it's discouraging to see that those falling in the 13 to 24 months has doubled since 2009. It is also unfortunate that the percentages in the "more than three years" category continue to reflect increases. *(Figure 10)*

Figure 10: What was the amount of time between when the crime actually started and when you found out, "the moment of discovery"?

Answered: 181 Skipped: 20

MONTHS PASSED	2013	2009	2008	2007
0-3	48.0%	45.0%	47.0%	42.0%
4-6	8.2%	11.0%	10.0%	11.0%
7-12	10.5%	10.0%	14.0%	11.0%
13 - 24	19.9%	10.0%	8.0%	17.0%
2-3 years	7.7%	9.0%	8.0%	9.0%
More than 3 years	16.2%	14.0%	12.0%	11.0%

Earlier detection has been demonstrated to decrease the time and energy a victim will spend in resolving the issue. The fact we have enjoyed no real increase in early detection rates means we must continue to educate the public regarding the proactive detection methods they can take themselves.

Susan Grant, ITRC Board of Directors and Consumer Advocate:

It is unfortunate to see that the most significant change in the time it takes victims to discover their identity theft is that the number of victims taking 13 to 24 months to discover their identity theft has nearly doubled. This clearly indicates that the battle to spread awareness of identity theft and how to properly monitor your credit and accounts is far from over.

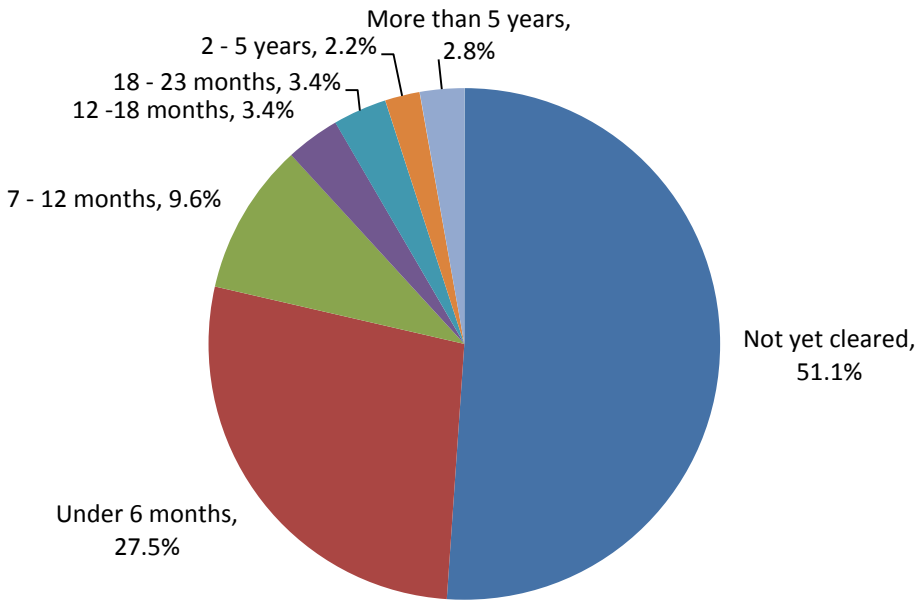
Consumers need to be educated on how to properly review their credit reports, bank account statements, credit card statements, and explanation of benefit statements from their health insurance providers in order to reduce the average time it takes for consumers to discover their victimization. It is simple, easy and free – consumers just need to be aware of the proper monitoring protocols in order to effectively use them, otherwise we will continue to see lackluster change.

F: LONG TERM EFFECTS / INABLITY TO CLEAR RECORDS

Inability to resolve the issue and lingering effects

There are other studies available which measure the direct and indirect costs, in dollars, to victims. ITRC takes a different approach. *The Aftermath* study aims to measure how long it takes to resolve the issue and the lingering effects.

Figure 11: How long did it take for you to resolve your identity theft issue? If it's ongoing, check "Not yet cleared"
Answered: 178 Skipped: 23



Recovering from a crime only starts once the issue is resolved. The consequences of identity theft often linger for significant periods of time. Half of the survey respondents spent more than a year trying to resolve their issue, since their issue was "not yet cleared" at the time they participated in this survey. *(Figure 11)*

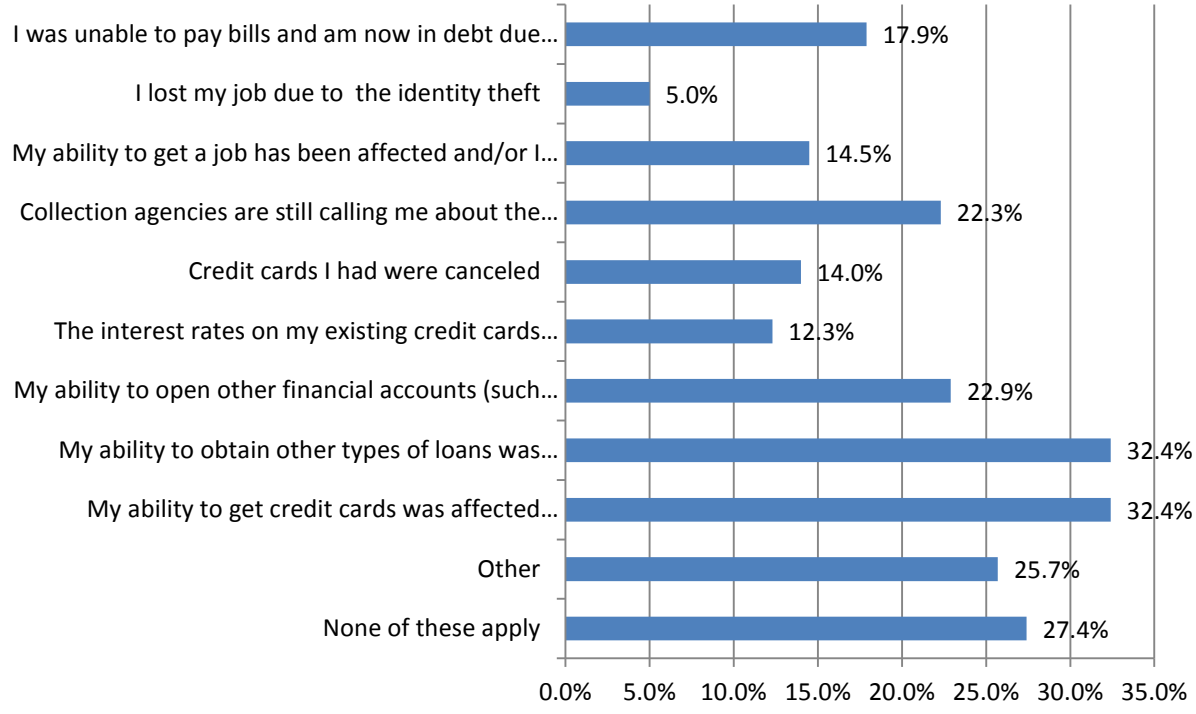
In their own words:

I haven't been able to get a loan to go back to school and finish my degree, which has made finding a job nearly impossible.

Of those who responded to the question regarding how identity theft impacted their life, 32.4 percent had their ability to obtain credit (either credit cards, or other loan types) affected by their identity theft issue; and nearly 20 percent of victims suffered severe impact regarding employment (either lost a current job or were denied employment/unable to get a job). *(Figure 12)*

Figure 12: How has your life been impacted by this crime? (Check all that apply)

Answered: 179 Skipped: 22



Barriers to resolution can often be out of the victim's control. Issues such as fraud alerts being ignored (20.9 percent) and credit agencies not removing incorrect information (18.6 percent) are generally difficult for victims to influence. *(Figure 13)*

And while it seems that giving up (12.4 percent) appears to be within the control of the victim, the question needs to be asked: What causes victims to stop trying to clear their names, an action of obvious benefit to the individual? The response, "I don't know how to clear my report," (22.6 percent) could be more of an indicator of frustration after repeated attempts rather than blind ignorance.

Figure 13: Listed below are some reasons why you may not have been able to elimate or correct negative information. (check all that apply)

Answered: 177 Skipped: 24

REASON	2013	2009	2008	2007
Fraud alerts ignored – imposter is active	20.9%	20.0%	23.0%	19.0%
I do not have a fraud alert and the imposter is active	3.4%	16.0%	8.0%	6.0%
I gave up	12.4%	27.0%	20.0%	25.0%
Credit agencies keep putting information back	14.7%	29.0%	30.0%	31.0%
My SSN is in other people's files	12.4%	18.0%	18.0%	22.0%
Could not prove my innocence - I could not get a police report	7.9%	12.0%	18.0%	19.0%
I could not prove my innocence even with a police report.	12.4%	20.0%	27.0%	26.0%
My accounts keep getting sold to new collection agencies – although cleared by creditor	13.6%	14.0%	28.0%	22.0%
Credit agencies will not remove it	18.6%	29.0%	N/A	32.0%
Civil litigation still on	6.8%	14.0%	15.0%	21.0%
I don't know how to clear my report	22.6%	25.0%	23.0%	16.0%
I clean my report only to have imposter start again	10.7%	7.0%	13.0%	16.0%
Because it was a member of my family	1.1%	4.0%	10.0%	7.0%
Offender is an ex-spouse, I have to go back to court to fix this	3.4%	4.0%	2.0%	6.0%
None of these apply	46.9%	n/a	n/a	n/a

Again it is important to remember that respondents in this survey are not a random population sample, rather they are individuals who contacted the ITRC for, and received, one-on-one case assistance.

Eva Velasquez, President/CEO ITRC:

It is crucial that we continue to capture detection and resolution statistics for this crime. Building an understanding of the victim experience and the roadblocks they face allows us to develop better remediation strategies for future victims.

G: VICTIM EXPERIENCES/SATIFACTION WITH ORGANIZATIONS

Victim satisfaction with law enforcement remains elusive. Victims often need to deal with a significant number of outside organizations in order to remediate their identity theft cases. Their level of satisfaction during those interactions may impact future decisions such as where to do business and how to vote.

In their own words:

Police seem not want to bother even after I found out one of the persons who is doing it. No one is taking this seriously.

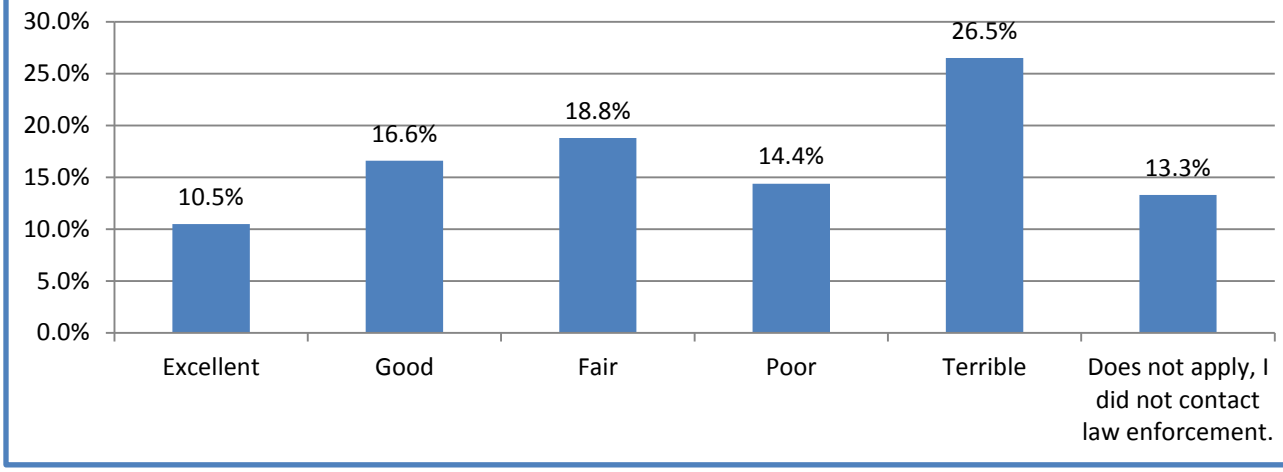
That's why it's important for organizations, including government and law enforcement, to discover where they are doing well and where they are being challenged when it comes to dealing with victims of identity theft. *(Figure 14)*

In their own words:

Worked with two police departments (mine and the perps.) and a special investigator… They took no action…I was also informed that ID theft was so common they were really not very interested.

Figure 14: If you dealt with a law enforcement agency, please rate your level of satisfaction with how they handled your issue/s.

Answered: 181 Skipped: 29



The following three tables (Figure 15 through Figure 17) are representative of respondents' satisfaction levels with other entities with which they may have had to interact in order to resolve their identity theft matters.

Figure 15: If unauthorized transactions were conducted, or new accounts were opened, with a bank, credit union or other financial institution, please rate your level of satisfaction with how they handled the issue/s.

Answered: 192 Skipped: 9

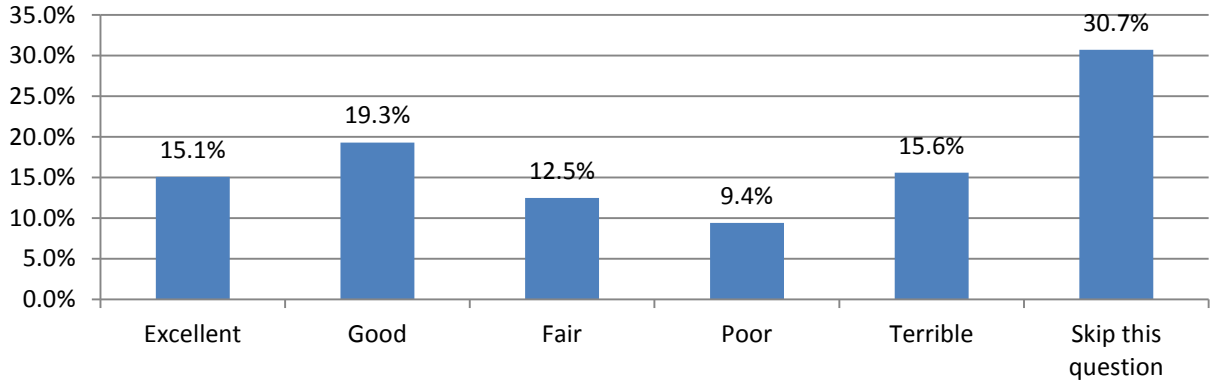
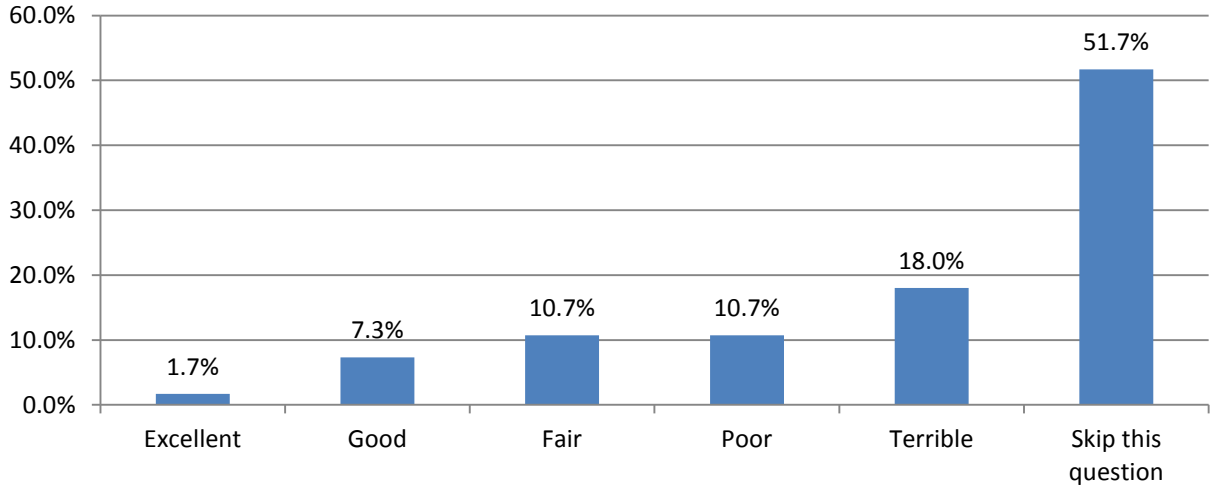
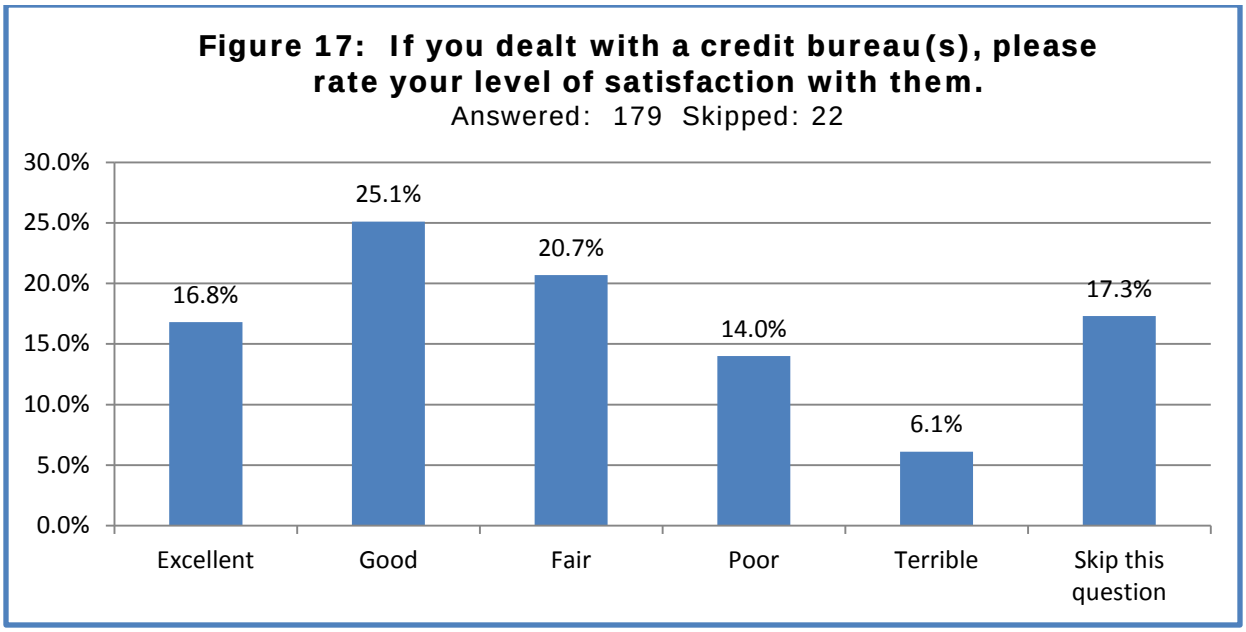


Figure 16: If you dealt with a collection agency, please rate your level of satisfaction with them.

Answered: 178 Skipped 23





Matt Cullina, ITRC Board of Directors and CEO IDT911:

In order to resolve their identity theft, victims will need assistance from various private and public entities, like collection agencies, the fraud department of a financial institution or business, law enforcement, their state Attorney General's office, credit reporting agencies and more. These entities are faced with the opportunity to make a good first impression with victims who are likely in shock and distraught after discovering their personal information has been misused. That first impression is a double edged sword; a negative interaction can result in the loss of trust or loyalty from victims who feel they were mistreated when they attempted to resolve their identity theft.

Additionally, how these entities interact with victims can potentially affect the victims' opinion of said entity, such as swaying their future spending choices and choice in business relationships, and even how they vote on certain measures affecting entities they worked with after discovering their identity theft. It would benefit all organizations to ensure their services are empathetic, attentive, and respectful when assisting identity theft victims.

H: EMOTIONAL IMPACT ON SELF AND OTHERS

Strong emotions continue to be present when dealing with this crime

Identity theft is not just an unforeseen and inconvenient occurrence, such as getting a flat tire. This is a situation that has the impact of both an unforeseen financial event (which often will start a domino effect for low and moderate income households), AND the emotional impact of a crime.

While it is not surprising that the most common feeling was annoyance and frustration, other stronger emotions were experienced by survey respondents. Victims who resolve their issues more quickly will likely be able to more readily overcome the emotional toll. Complex cases that are more difficult to resolve can cause severe distress. For a small but significant number of victims, the effects can be devastating. *(Figure 18)*

- 6 percent of respondents reported feeling suicidal, and 9 percent reported beginning or relapsing into unhealthy addictive behaviors.
- Almost 40 percent reported some sleep disturbances. These strong emotions have declined slightly since the previous survey.
- The marked increase in fear for personal financial security may mean that victims are now understanding that this crime has long term consequences and they many have already experienced them.

Figure 18: Since this crime began, have you experienced any of these emotions *even for a short period of time*? [1] (Check all that apply)

Answered: 177 Skipped:24

	2013	2009	2008	2007
Fear for Personal Financial Security	69%	57%	52%	56%
Rage or Anger	65%	78%	65%	80%
Feelings of Betrayal	50%	49%	60%	48%
Sense of Powerlessness or helplessness	50%	63%	63%	57%
Denial or Disbelief	42%	49%	31%	34%
Shame or Embarassment	29%	27%	24%	29%
Sleep disturbances	40%	43%	40%	47%
Inability to Concentrate	28%	29%	27%	30%
Feeling Suicidal	6%	8%	4%	6%
Frustation or annoyance [2]	81%			
Frustration		74%	68%	74%
Annoyance		67%	64%	66%

[1] These responses from the 2013 respondents, are being compared to the Short Term emotional impact responses from previous year surveys.

[2] In previous studies, the two categories of "Frustration" and "Annoyance" were allowed as separate responses. For the 2013 survey, these two categories were combined.

Dr. Charles Nelson, Psychologist, and ITRC Board of Directors:

It is not at all uncommon for victims of identity theft to experience strong emotions after initially discovering the crime committed against them. This has become an enormous betrayal of trust that the victim may have formerly held regarding the honesty and fidelity of others. As we can see from this survey, frustration and annoyance, rage or anger, powerlessness and betrayal are the responses most often indicated by victims.

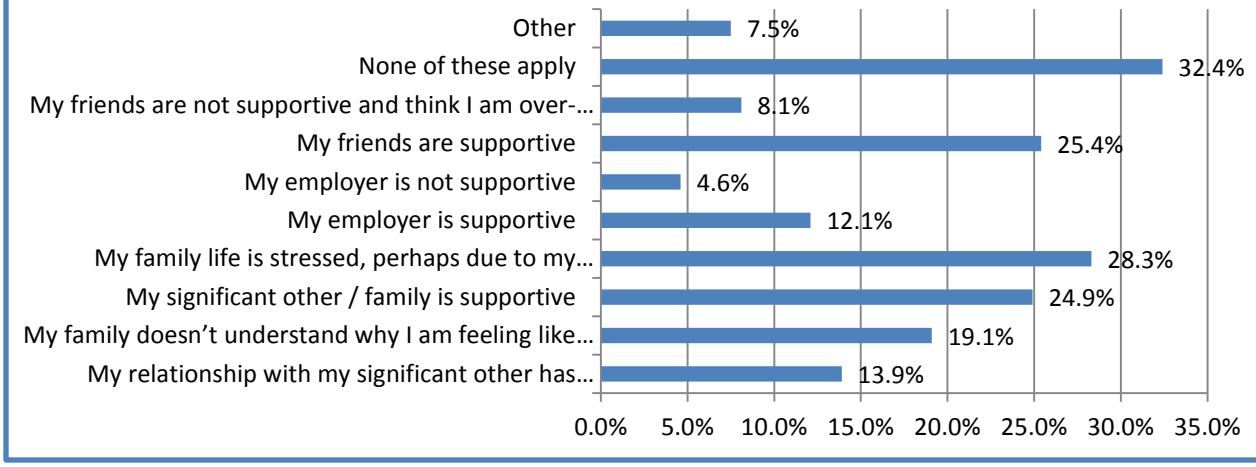
Identity theft is different than most other crimes in that it entails an intimate violation of the victims' basic rights of privacy and control over their own lives. While a small minority, there are a number of victims who are so disturbed by this crime that they may even contemplate suicide. For such severely depressed victims, killing themselves can seem like the only way out of their deep, paralyzing economic cavern that the perpetrator(s) threw them into. The data found in this ITRC survey results serves as a barometer to show just how devastating identity theft can be to one's psychological health.

Entities that commonly work with victims of identity theft should take into consideration the enormous amount of stress the victims are under when assisting them. A few kind words and patience on behalf of those assisting victims can do wonders in settling and reassuring a victim of identity theft.

The emotional impact will often carry over into other aspects of the victim's life, including relationships. Almost 14 percent of respondents reported a severe negative impact on their relationships with significant others, and one in 5 responded there is lack of understanding and support from family members. Additionally, one in 4 reported stress within their family due to this issue. Respondents indicated both employers and friends were more supportive than not. *(Figure 19)*

Figure 19: How has this experience affected your relationships with others?

Answered: 173 Skipped 28



Dr. Charles Nelson:

As with most traumatic experiences, identity theft can not only affect the victims' relationships as a consumer of products and services, but also their personal ones as well. I commonly encourage victims of traumatic experiences such as identity theft to seek out healthy support from friends and family (as long as they are not the perpetrators).

People providing emotional support to victims of identity theft should be understanding and patient with them as they may understandably be paranoid, angry or depressed. Yet, we have discovered the unfortunate fact that many victims reveal that some or all of their family members or other loved ones are not supportive or don't understand their emotional trauma. It is up to the victim to recognize and identify those who do not help or make their emotional trauma worse and to put other more supportive relationships at a higher priority until they have recovered from the stress and trauma of identity theft.

I: CONSUMER BEHAVIORS BEFORE AND AFTER

Experience is a valuable teacher: behavior changes after victimization.

In their own words:

I am far more skeptical and try to take privacy precautions.

When comparing pre-victimization with post-victimization behaviors, all safety precaution behaviors increased. Victims indicated they became more cautious and employed more risk minimization tactics after they became victims. The most dramatic increases were in the following categories.

(Complete list of before and after behavioral questions, see *Figure 23* and *Figure 24* in Appendix.)

- Regularly reviewing credit reports +50 percent
- Security/credit freeze in place +36 percent
- Caution with PII on social profiles +20 percent
- Change online passwords every three months +18 percent
- Review privacy settings on social networks regularly +17 percent

In their own words:

Since I had my identity stolen I am way more conscious of who or what I give my information to.

J: CONSUMER ENGAGEMENT ONLINE

Respondents are highly engaged online and on their mobile devices, despite being identity theft victims.

In their own words:

I don't live in fear nor do I want to. I still shop online, use credit cards and bank online…I prefer to believe systems in place will protect most of us most of the time and don't want to let one instance force me into a life I would rather not live.

Almost 1 in 5 respondents had an issue with email/social media accounts either being taken over or having new ones created in their names *(Figure 20*), yet more than 60 percent of respondents shop or bank online (64 percent and 61 percent, respectively). More than 30 percent of respondents use their banks' mobile banking app and/or use their mobile devices to make purchases. *(Figure 21)*

Despite all of the aftermath victims' experiences as a result of this crime, these respondents are more engaged online than ever. Less than 6 percent of respondents did not engage in any common online activities such as use of email, social media accounts, or online shopping.

Figure 20: When you experienced identity theft, did any of the following occur? (Check all that apply)
Answered: 183 Skipped: 18

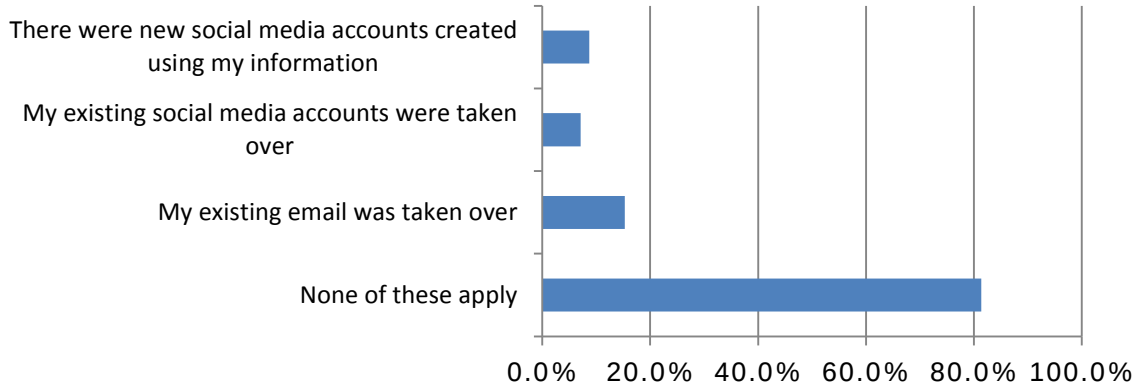
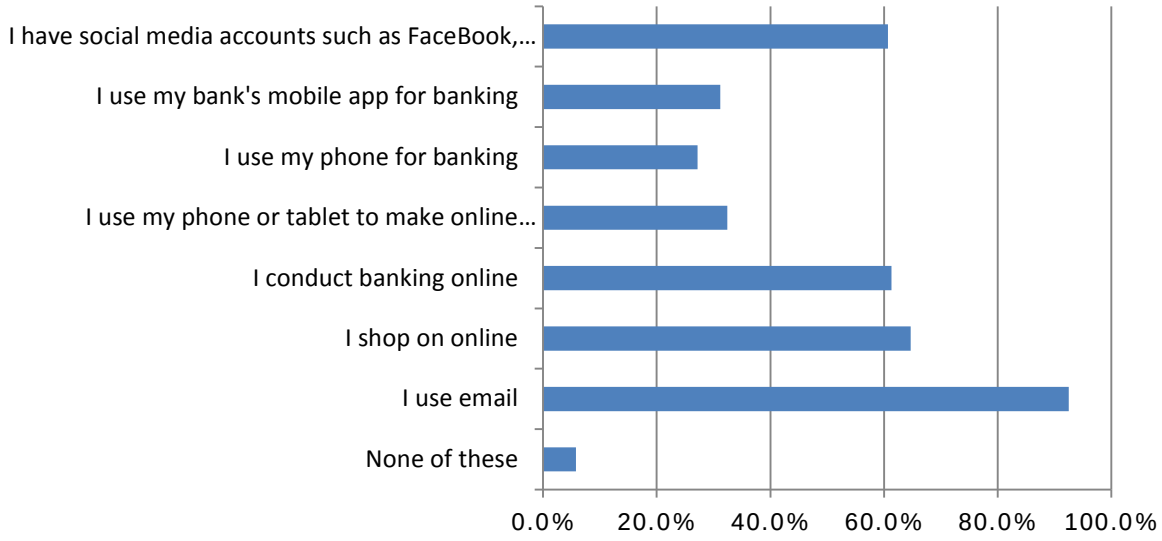


Figure 21: What activities do you currently engage in? (Check all that apply)
Answered: 173 Skipped: 28



K: DATA BREACH NOTIFICATION LETTERS

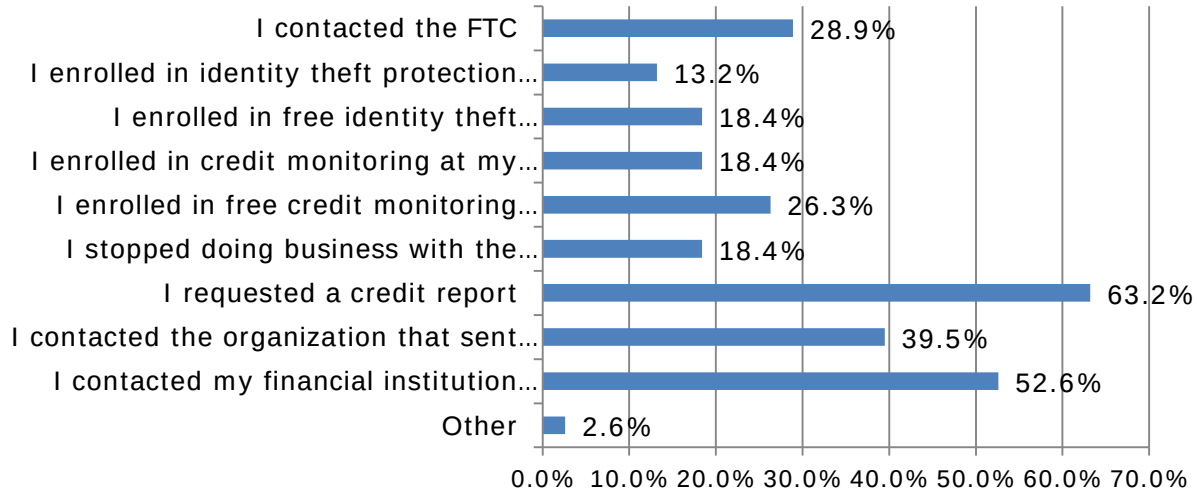
From 2005 to 2013, the ITRC tracked 4,248 breaches in its ITRC Breach Report. This report, which is updated daily and posted on the website weekly, identifies U.S. data breach incidents which have been reported either in the media or on the websites of a small number of Attorneys General.

Recognizing the attention which was has been focused on this issue over the past several years, the ITRC posed the question in this year's Aftermath *study "Did you receive a data breach notification letter in 2013?"* Nearly one quarter (23.9 percent) of the survey respondents said "yes" (*Figure 22 in Appendix*). We followed this question with one asking about their subsequent actions following the receipt of the letter.

Of the nearly 25 percent who indicated they had received a breach notification letter, more than 6 out of 10 followed up by requesting a copy of their credit reports. This is often the first step recommended following a notification letter if it indicated the exposure of a Social Security number. Of those who answered this question, nearly 40 percent contacted the organization who sent the letter and 52.6 indicated they contacted their financial institutions. Only 18.4 percent of the respondents enrolled in the free identity theft protection service which was offered. As always, it is important to remember that these numbers are not to be construed as any kind of overall national average. *(Figure 22A)*

Figure 22A: Did you do any of the following after you received it? (Check all that apply)

Answered: 38 Skipped: 163



Karen Barney, ITRC Program Director and Subject Matter Expert:

It is important for consumers to recognize the need to be proactive following a data breach notification letter in order to minimize the risk of actually becoming an identity theft victim as a result of their information being compromised. While not all data breach incidents result in a serious compromise of personal identifiable information, consumers need to be aware of the increased risk of identity theft that exists due to compromised records.

IN CONCLUSION

Throughout this paper we have allowed the voices of these victims to be heard regarding each of these issues. Perhaps the best closing would be to allow one of them to describe their identity theft experience and how it affected them, as well as how they look to the future.

In their own words:

Identity theft has changed the way I look at lots of things. The only good to come out of the years of ongoing trouble is that I have become super aware of most any scam. I can spot them quite easily now and am suspicious of anyone that contacts me for any reason. Unfortunately though, my information fell into the hands of some persistent criminal or organization's hands back in 2004. To this day, they are still trying to use my personal information to commit fraud and take over my existing accounts. Life did become much easier for me when my state (AR) finally passed the credit freeze legislation a few years ago. This allowed me to finally lock the thieves out of my credit files for good. I will have to be watching things very closely for the rest of my life-that is the worst part of identity theft. Knowing that the persons responsible will likely never be caught or stopped is not a good feeling.

4. METHODOLOGY

The ITRC staff designed and administered the *Identity Theft: The Aftermath 20*13 survey. This is the eighth time the ITRC has undertaken this project. A number of independent industry specialists participated in preparing the final summary.

Respondents to this survey were all assisted by the ITRC during the 2013 calendar year. These respondents were confirmed as identity theft victims by ITRC victim advisors. It is important to remember this survey is not a census survey, rather it reflects the victim population that responded to the survey invitation.

Information includes state of residence, age when crime began, and household income level.

- 201 victims responded from 39 states. It should be noted the area the victim lives in is not to be misconstrued as the location of the crime. Anecdotally, the ITRC continues to note the vast majority of these cases are multi-jurisdictional in nature.

- Of the 201 respondents, 8 percent of victims were under that age of 18 when the crime began. All other age groups were almost uniformly represented. Other age categories were as follows: 18-29 (20 percent); 30-39 (15 percent); 40-49 (17 percent); 50-59 (17 percent); and 60+ (17 percent).

The annual *Aftermath* surveys closely mirror each other in terms of questions asked and reflect details to further understand new methods of identity theft. In 2009, 41 questions were asked.

ITRC emailed 2,092 invitations to participate in the 2013 survey. A total of 201 victims participated in the online (web-based) survey.

Appendix

Figures Referenced in paper:

Q1 What is your state of residence?

Answered: 201 Skipped: 0

Answer Choices	Responses	
AL	1.5%	3
AK	1.0%	2
AZ	2.0%	4
AR	0.5%	1
CA	15.9%	32
CO	4.0%	8
CT	0.5%	1
DE	0.0%	0
FL	9.0%	18
GA	4.0%	8
HI	0.5%	1
ID	0.0%	0
IL	4.0%	8
IN	0.0%	0
IA	2.0%	4
KY	1.0%	2
LA	0.5%	1
ME	0.0%	0
MD	1.0%	2
MA	1.0%	2
MI	2.0%	4
MN	2.5%	5
MS	0.0%	0
MO	2.0%	4
MT	0.0%	0
NE	0.0%	0
NV	0.0%	0
NH	0.0%	0

NJ	2.0%	4
NM	0.5%	1
NY	7.5%	15
NC	2.0%	4
ND	0.0%	0
OH	2.0%	4
OK	1.0%	2
OR	2.5%	5
PA	2.0%	4
RI	0.5%	1
SC	0.5%	1
SD	1.0%	2
TN	2.0%	4
TX	8.0%	16
UT	0.5%	1
VT	0.5%	1
VA	3.5%	7
WA	6.0%	12
WV	1.0%	2
WI	1.5%	3
WY	1.0%	2
Total		**201**

Figure 3A: If a new loan was opened, what type of loan was it? Answered: 37 Skipped: 164

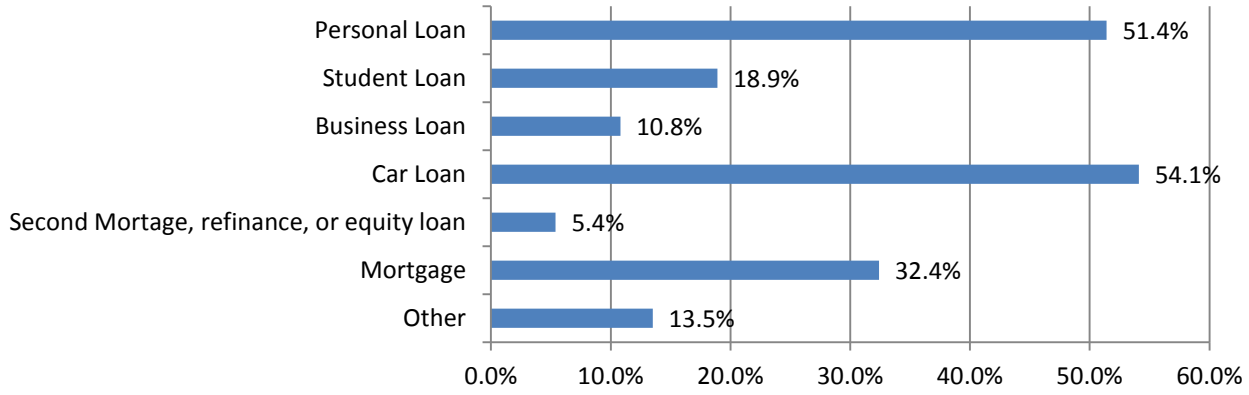


Figure 4: When you experienced identity theft, did any of the following occur? (Check all that apply)

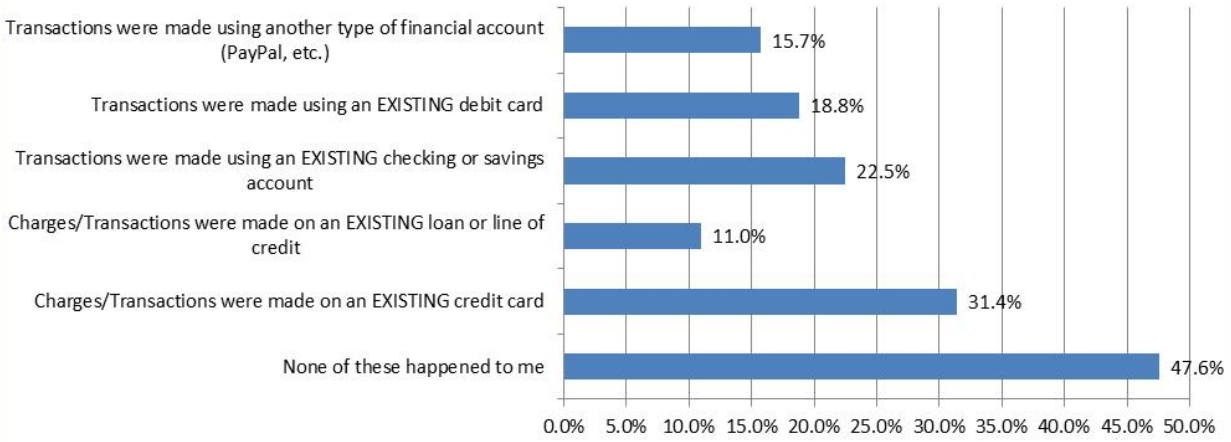


Figure 4B: Financial Existing Accounts - For your existing checking or saving account, did any of the following occur?

Answered: 27 Skipped: 174

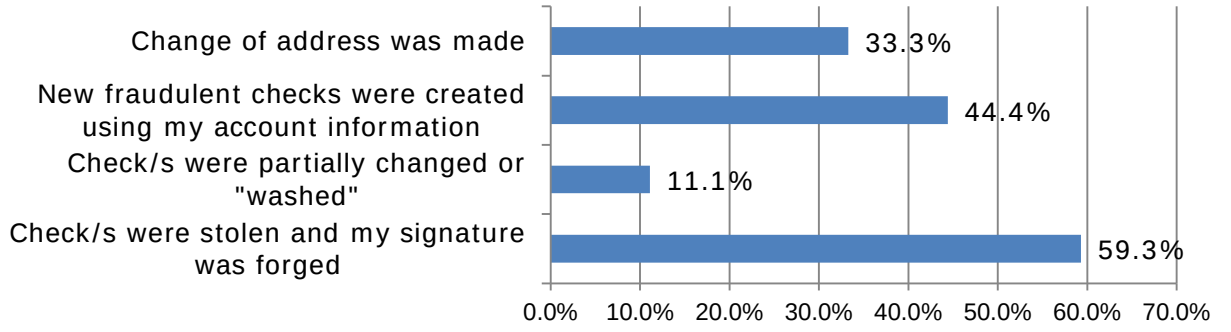


Figure 6A: If taxes were filed in your name, did you contact the IRS? Answered: 47 Skipped: 154

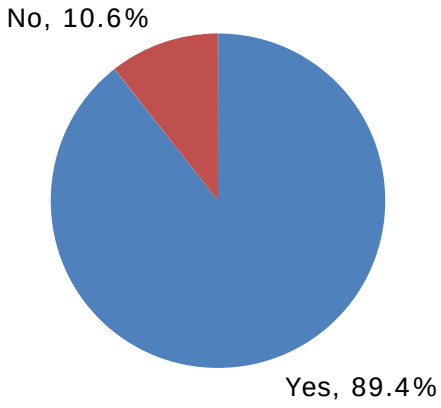


Figure 6B: Governmental - Did any of the following occur during your interaction with the IRS? Answered: 42 Skipped: 159

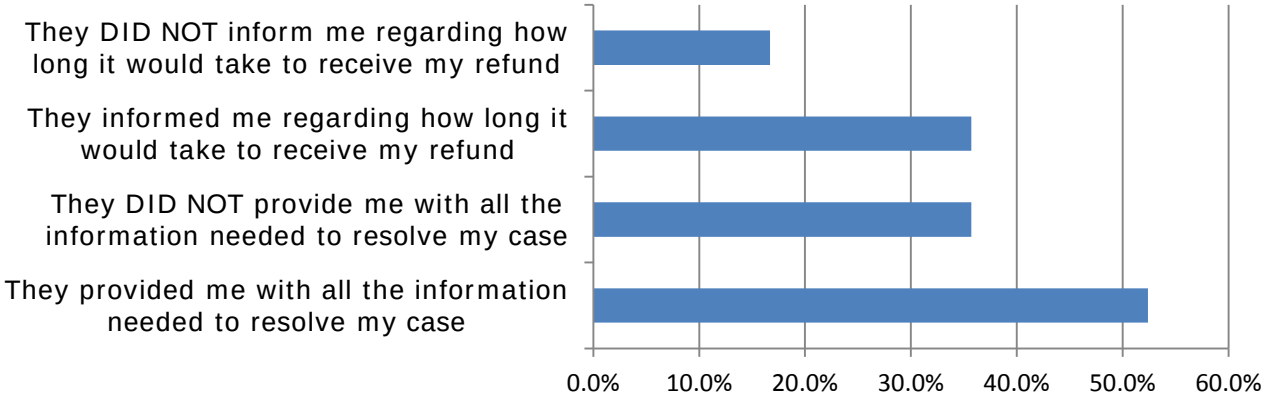


Figure 6C: Governmental - When you experienced identity theft, were government benefits (NOT IRS) such as social services, welfare or food stamps, obtained using your information?
Answered: 184 Skipped:17

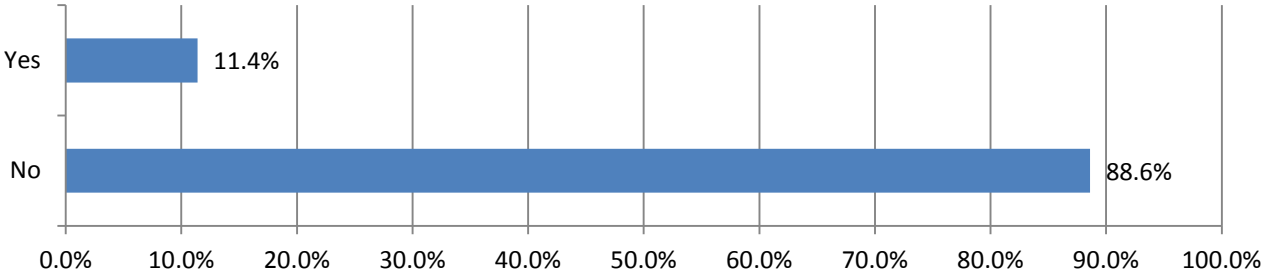


Figure 14A: Did you file a police report?
Answered: 181 Skipped: 20

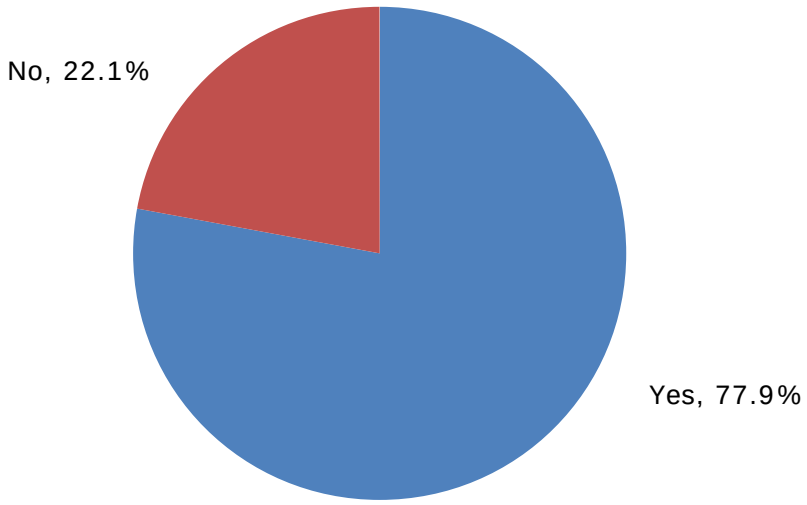


Figure 14B: Why didn't you file a police report?
Answered: 39 Skipped: 162

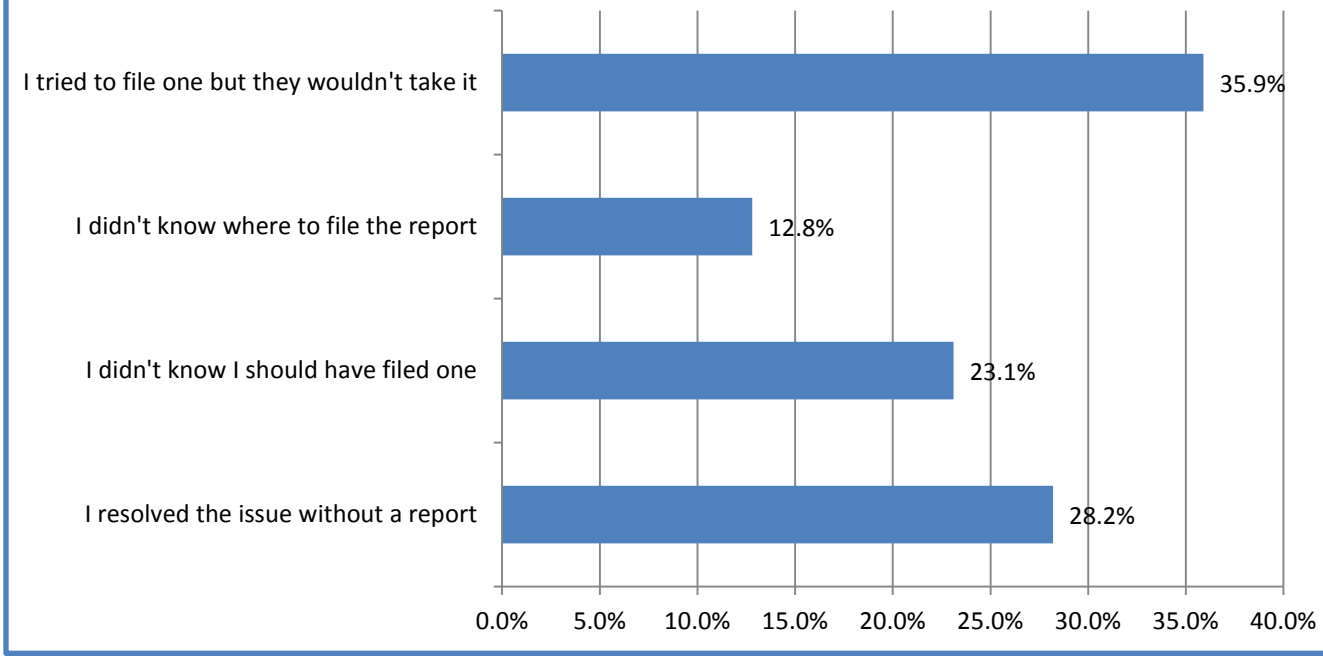


Figure 22: Did you receive a breach notification letter?
Answered: 171 Skipped: 30

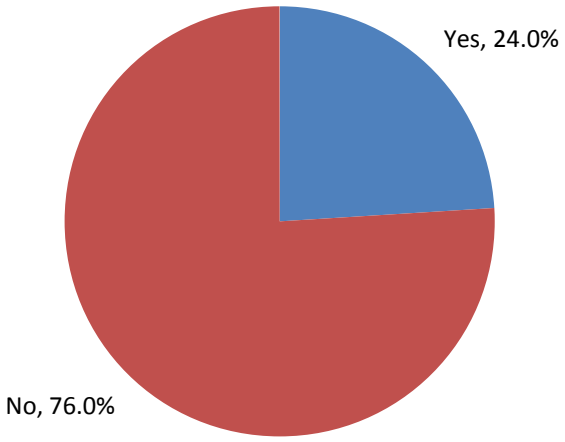


Figure 23: What behaviors did you use BEFORE you found out you were a victim of identity theft? (Check all that apply)

Answer Choices	Responses	
I had a locked mailbox	17.14%	30
I checked my credit reports regularly using the free annualcreditreport.com website	15.43%	27
I checked my credit reports regularly using another method and/or website	8.57%	15
I had a security or credit freeze	6.29%	11
I used a fee-based credit monitoring service (i.e. only looks at credit reports)	10.86%	19
I used a fee-based identity monitoring service	4.57%	8
I shredded documents with account information or Social Security numbers on them	53.71%	94
I deleted scam emails and fraudulent text messages without answering them	63.43%	111
I installed and regularly updated computer security systems, firewalls, anti-virus software, spyware, etc.	51.43%	90
I shopped online only on websites that are known to me.	42.86%	75
I always looked for the yellow padlock and "https:" in the URL	27.43%	48
I didn't carry my Social Security number with me on a daily basis	49.71%	87
I didn't share my Social Security number unless absolutely necessary	61.14%	107
I didn't carry extra credit cards or my checkbook with me on unless I needed them that day	29.14%	51
I kept my credit cards in sight at all times in restaurants and stores when using them	27.43%	48
I had a debit card that required a PIN even when used as a credit card	26.86%	47
I changed the passwords for my online accounts once every 3 months	14.86%	26
I used numbers and letters in my online passwords and made them at least 8 characters long	48.57%	85
I was careful not to put personal information on my social networking profiles	40.57%	71
I reviewed my privacy settings on my social networks regularly to make sure they are adequate	27.43%	48
I didn't use public wifi	20.00%	35
I used a VPN when I was on public wifi	2.29%	4
I regularly checked and set my privacy settings for my social media accounts	21.71%	38
I had a wiping program on my smart phone or tablet	3.43%	6
I had a pin and/or password on my phone or tablet	32.57%	57
None of the above	15.43%	27
Total Respondents: 175		

Figure 24: What behaviors do you CURRENTLY use to minimize your future risk of becoming a victim of identity theft again? (Check all that apply)

Answer Choices	Responses	
I have a locked mailbox	28.49%	49
I check my credit reports regularly using the free annualcreditreport.com website	46.51%	80
I check my credit reports regularly using another method and/or website	27.91%	48
I have a security or credit freeze	42.44%	73
I use a fee-based credit monitoring service (i.e. only looks at credit reports)	18.60%	32
I use a fee-based identity monitoring service	18.02%	31
I shred documents with account information or Social Security numbers on them	62.21%	107
I am familiar with how to deal with scams and fraudulent emails and text messages	59.30%	102
I delete scam emails and text messages without answering them	77.91%	134
I have installed and regularly update computer security systems, firewalls, anti-virus software, spyware, etc.	61.63%	106
I shop online only on websites that are known to me.	49.42%	85
I always look for the yellow padlock and "https:" in the URL	36.63%	63
I don't carry my Social Security number with me on a daily basis	59.88%	103
I don't share my Social Security number unless absolutely necessary	75.00%	129
I don't carry extra credit cards or my checkbook with me on unless I need them that day	43.02%	74
I keep my credit cards in sight at all times in restaurants and stores when using them	41.86%	72
I have a debit card that requires a PIN even when used as a credit card	37.21%	64
I change the passwords for my online accounts once every 3 months	33.72%	58
I use numbers and letters in my online passwords and make them at least 8 characters long	64.53%	111
I am careful not to put personal information on my social networking profiles	59.88%	103
I review my privacy settings on my social networks regularly to make sure they are adequate	44.19%	76
I don't use public wifi	36.05%	62
I use a VPN when I am on public wifi	8.72%	15
I regularly check and set my privacy settings for my social media accounts	32.56%	56
I have a wiping program on my smart phone or tablet	11.63%	20
I have a pin and/or password on my phone or tablet	43.02%	74
None of the above	4.65%	8
Total Respondents: 172		

[i] The Identity Theft Resource Center (ITRC) is a nonprofit, grant and donation funded organization that focuses exclusively on the issues surrounding identity theft and in providing assistance to victims without charge, from the moment of discovery through final resolution. www.idtheftcenter.org. Email: itrc@idtheftcenter.org, 858-693-7935. Victim Hotline: 888-400-5530

[ii] Matt Cullina: Currently on the Board of Directors for the Identity Theft Resource Center, Mr. Cullina has 15 years of insurance industry management, claims and product development experience. He spearheaded MetLife Auto & Home Insurance Co.'s personal product development initiatives, managed complex claims litigation and served as a corporate witness for Travelers Insurance and the Fireman's Fund Insurance Co.

[iii] Julie Fergerson: Currently on the Board of Directors for the Identity Theft Resource Center, Ms. Fergerson is a Senior Vice President of Industry Solutions at Ethoca and is one of the industry's foremost experts on Internet payments fraud. Ms. Fergerson has over 20 years of experience in the online payments and fraud management industry and holds patents for secure transaction order management processing and preventing fraudulent electronic transactions. Prior to joining Ethoca, Ms. Fergerson was Vice President of Emerging Technologies at Debix and Co-Founder and Vice President of Emerging Technologies.

[iv] Susan Grant: Currently on the Board of Directors for the Identity Theft Resource Center, Ms. Grant is the Director of Consumer Protection at the Consumer Federation of America. She works specifically in the areas of privacy, identity theft, online safety and security, telemarketing, electronic and mobile commerce, deceptive marketing, fraud, and general consumer protection issues. Ms. Grant heads CFA's Consumer Protection Institute, conducts CFA's annual Consumer Complaint Survey, and is a recognized authority on combating consumer fraud and deception.

[v] Dr. Charles Nelson, Ph.D.: Currently on the Board of Directors for the Identity Theft Resource Center, Dr. Nelson is a licensed psychologist and the Founder and Director of the Crime and Trauma Recovery Program and the Family Treatment Institute. Dr. Nelson is a nationally respected authority on crime victims, having furnished expert court qualified testimony on murder, domestic violence, post-traumatic stress disorder, and Rape Trauma Syndrome cases since 1971. Besides his work with clients, Dr. Nelson has trained law enforcement, victim assistance counselors, clinical practitioners and graduate students in the area of crime victim trauma since 1976. One of his research projects involved studying the nation's 400 largest police sex crime units and community-based victim assistance centers regarding their attitudes and sensitivity toward victims (1973-1974). He has published numerous works on the impact of crime on individuals and is trained as a NOVA crisis intervention specialist. Dr. Nelson was chosen by the Governor of California to be the recipient of the Doris Tate Crime Victim Provider of the Year Award.

[vi] Robert Siciliano: Currently on the Board of Directors for the Identity Theft Resource Center, Mr. Siciliano is fiercely committed to informing, educating, and empowering Americans so they can be protected from violence and crime in the physical and virtual worlds. For almost 30 years, Mr. Siciliano has been committed to maintaining his expertise in all aspects of security by constantly researching new and upcoming security trends with the goal of informing and educating the consumer so they can avoid becoming a statistic.

[vii] Eva Velasquez: Currently the President and CEO of the Identity Theft Resource Center, Ms. Velasquez is a driven leader with more than 25 years of experience serving the

community and assisting victims of crime. Ms. Velasquez most recently served as the Vice President of Operations for the San Diego Better Business Bureau, where she managed the Bureau's department that supplies the core services of dispute resolution, arbitration, and pre-purchase information to the public. Prior to that appointment, Ms. Velasquez spent 21 years at the San Diego District Attorney's Office, with the last 11 of those years spent investigating and assisting in the prosecution of economic/financial crimes, with a focus on consumer protection issues. In addition, she served as the Chairman of the Consumer Fraud Task Force for 13 years, was a past Vice President of the California Consumer Affairs Association, and most recently was a finalist in the 2012 San Diego Business Journal's Women Who Mean Business Awards.

viii Identity Theft: the Aftermath, 2003, Identity Theft Resource Center