Ponemon INSTITUTE

2013 Survey on Medical Identity Theft

Sponsored by the Medical Identity Fraud Alliance with support from ID Experts®

Independently conducted by Ponemon Institute LLC

Publication Date: September 2013

2013 Survey on Medical Identity Theft

Presented by Ponemon Institute, September 2013

Part 1: Executive Summary

The *2013 Survey on Medical Identity Theft* conducted by Ponemon Institute and sponsored by the Medical Identity Fraud Alliance (MIFA), with support from ID Experts, measures the prevalence of medical identity theft in the United States and its impact on consumers. The survey found that consumers are at increased risk of medical identity theft and as a result face serious medical and financial consequences.

Survey incorporates feedback from key federal agencies

Several federal agencies charged with fighting the medical identity theft problem in the U.S., reviewed and contributed to the development of the 2013 survey, in order to get a more detailed view of the complex issue of medical identity theft. Additional questions were added to expand our understanding of how victims were affected by the theft, the costs they incurred and the actions they took to resolve the crime.

We surveyed 788 adult-aged (18+ years old) individuals who self-reported they or close family members were victims of medical identity theft. For purposes of this study, medical identity theft occurs when someone uses an individual's name and personal identity to fraudulently receive medical service, prescription drugs and goods, including attempts to commit fraudulent billing.

Medical identity theft is increasing and consumers need to take steps to protect their personal information.

The estimated number of medical identity theft victims continues to be significant. Table 1a provides the estimate of the size and cost of medical identity theft in the United States for 2013. Based on this year's study, it is estimated that 1.84 million adult-aged Americans or close family members at some point in time became victims of medical identity theft. Last year's estimate, adjusted for more recent census data, was 1.52 million individuals.[1]

Table 1a. U.S. population of medical identity theft victims	Value
U.S. population in 2013 (Census Bureau)	315,655,265
U.S. population below 18 years of age	29%
U.S. adult-aged population	223,940,455
Base rate for medical identity theft in 2013 (sample estimate)	0.0082
Number of medical identity theft victims in 2013	1,836,312

The following are key findings from the study

The number of medical identity theft victims increased. The number of new cases over the past year is estimated at 313,000. This estimated increase in the base rate of identity theft victims climbed from .0068 to .0082, which represents a 19 percent increase over one year.

Medical identity theft can put victims' lives at risk. The individuals in this study understand what medical identity theft is and have had personal experience with this crime either directly or through an immediate family member. However, 50 percent are not aware that medical identity theft can create inaccuracies in their permanent medical records.

Most medical identity theft victims lose trust and confidence in their healthcare provider following the loss of their medical credentials. The most frequent medical consequence of a

[1] Please note that last year's estimate for the number of U.S. residents who were at or above 18 years of age was approximately 272 million individuals. More accurate census data provided an estimate of 224 million people.

medical identity theft is that respondents lost trust and confidence in their healthcare provider (56 percent). This is an increase from 51 percent in last year's study.

Individuals lack awareness of the seriousness of the crime. The majority of respondents have yet to realize the negative consequences of medical identity theft. As a result, it seems they are slow to take steps to protect themselves and resolve the crime. In fact, 50 percent of respondents do not take any steps to protect themselves from future medical identity theft. This might be a result of many victims not experiencing any financial consequences.

Resolution of the crime is time-consuming. The amount of time it takes to deal with the crime may discourage many victims from trying to resolve the theft and stop future incidents. Those who did try to resolve the incident say that they worked with their health plan and/or insurer to help resolve the incident (35 percent) or worked with the healthcare provider (31 percent). Such activities consumed almost a year or more, according to 36 percent of respondents. Almost half (48 percent) of respondents say the crime is still not resolved.

Individuals rarely take steps to check their medical records. Seventy-eight percent of respondents say that it is very important or important to control their health records directly but they are not taking steps to do so. Specifically, 56 percent of respondents do not check their medical records to determine if the health information is accurate.

Reviews of Explanation of Benefits can protect individuals. In this year's research, we asked respondents if they read the EOB form or document that is sent by insurance companies following a healthcare service paid for by the insurance company. Taking the time to check the accuracy of the form could red flag any possible incidents of medical identity theft.

Sharing of personal identification to obtain medical services is prevalent. Thirty percent of respondents knowingly permitted a family member to use their personal identification to obtain medical services including treatment, healthcare products or pharmaceuticals. The frequency of sharing varies among respondents. Fifty-three percent say they did it only once. However, 21 percent could not count the number of times they shared their identification.

Many cases of medical identity theft are preventable. The majority of respondents say the crime happened because they knowingly shared their personal identification or medical credentials with someone they knew (30 percent) or a member of the family took their personal identification or medical credentials without consent (28 percent).

Part 2: Key Findings

We surveyed adult-aged individuals who self-reported that they or close family members had their identity stolen participated in this research. From the group of identity theft victims, 788 say they or their immediate family members have been victims of medical identity theft.

For purposes of this study, medical identity theft occurs when someone uses an individual's name and personal identity to fraudulently receive medical services, prescription drugs and/or goods, including attempts to commit fraudulent billing.

In this year's study, 42 percent of respondents have private insurance and 24 percent have Medicare or Medicaid. Twenty one percent say they are presently uninsured. The remaining respondents have government, coop plans or health savings accounts.

In this section, we provide an analysis of the findings. Since first conducting the study in 2010, questions have been replaced or modified. For those questions that have remained consistent over the four years we have included them in this report.

In this year's study, we have identified six themes from the research. They are as follows:

1. Medical identity theft continues to be a costly crime.
2. The dangers and consequences of medical identity theft are not fully understood by consumers surveyed.
3. Steps to protect against medical identity theft and resolve the crime are often ignored.
4. The risk of medical identity theft can be reduced.
5. Certain individuals are more likely to knowingly share their medical credentials.
6. Certain individuals are more likely to suffer negative medical and financial consequences.

Medical identity theft continues to be a costly crime.

The Tables below show how the economic impact of medical identity theft was calculated and provides an estimate of the number of individuals affected and the total costs incurred.

The estimated number of medical identity theft victims continues to be significant. Table 1a provides preliminary extrapolations on the size and cost of medical identity theft in the United States for 2013. Based on this year's study, it is estimated that 1.84 million adult-aged Americans or close family members at some point in time became victims of medical identity theft. This is an increase from 1.52 million individuals in last year study.

Table 1a. U.S. population of medical identity theft victims	Extrapolated Value
U.S. population in 2013 (Census Bureau)	315,655,265
U.S. population below 18 years of age	29%
U.S. adult-aged population	223,940,455
Base rate for medical identity theft in 2013 (sample estimate)	0.0082
Number of medical identity theft victims in 2013	1,836,312

Total costs to the victims who paid out-of-pocket to resolve the crime. Sixty-four percent of individuals in this study self-reported that they did not incur any out-of-pocket costs as a result of the crime. However, 36 percent did pay an average of $18,660, as shown in Table 1b. These costs are: (1) identity protection, credit reporting and legal counsel; (2) medical services and medications because of lapse in healthcare coverage; (3) reimbursements to healthcare providers to pay for services to imposters. Based on our extrapolation, we estimate the total out-of-pocket costs incurred by medical identity theft victims in the United States at $12.3 billion.[2]

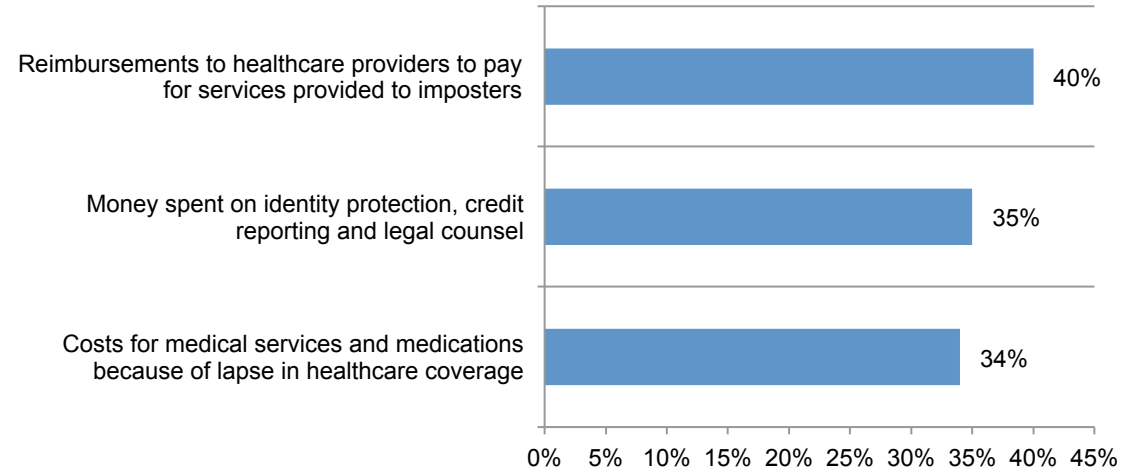
Table 1b. Total costs incurred by medical identity theft victims	Extrapolated Value
Percentage of victims who said they incurred out-of-pocket costs	36%
Number of victims who incurred out-of-pocket costs	661,072
Average out-of-pocket costs incurred by medical identity theft victims	$18,660
Total value of out-of-pocket costs incurred by U.S. victims	$12,335,607,684

The number of medical identity theft victims increased. Table 1c shows that the number of new cases over the past year is estimated at 313,000. This estimated increase in the base rate of identity theft victims climbed from .0068 to .0082, which represents a 19 percent increase over one year.

Table 1c. Increase in the number of medical identity theft victims	Extrapolated Value
Number of medical identity theft victims in 2013 (base rate = .0082)	1,836,312
Number of medical identity theft victims in 2012 (base rate = .0068)	1,522,795
Net increase in the number of medical identity theft victims	313,517
Net increase in base rate	0.0014
Percentage increase in base rate over one year	19%

Figure 1 reveals that an average of 36 percent of respondents in our study spent money to resolve the consequences of medical identity theft. As shown, 40 percent of respondents say they reimbursed healthcare providers, 35 percent incurred costs associated with identity restoration and legal counsel, and 34 percent paid for medical services and medications because of a lapse in coverage.

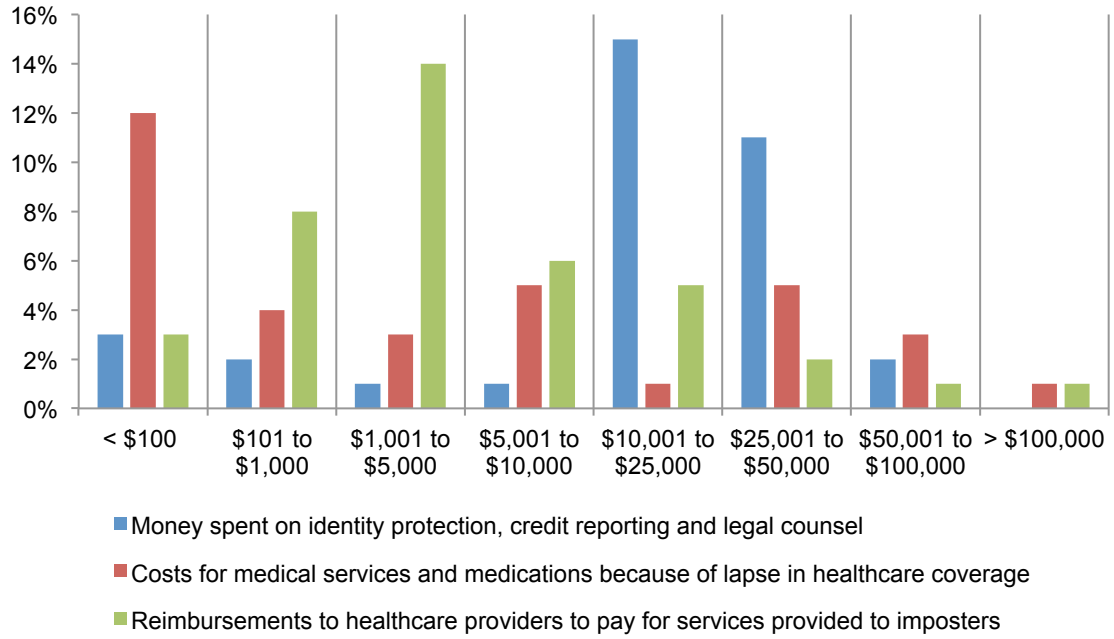
Figure 1. Percentage of respondents who incurred out-of-pocket costs



[2]The estimated total economic value shown here cannot be directly compared to last year's total value because the method used to calculate per capita cost changed (e.g., becoming more precise). Assuming this year's per capita cost applied to last year's estimated population would result in a total cost of $10.2 billion or a net increase of $2.1 billion between 2012 and 2013.

Figure 2 provides a breakdown of out-of-pocket costs incurred by 36 percent of medical identity theft victims who self-reported that they had to spend funds to resolve the crime. It is estimated that on average they spent $18,660 to restore their medical identity. On average, the greatest amount was spent on identity protection, legal counsel and credit reporting for an average of $8,369, followed by $5,899 on medical services because of a lapse in health insurance and $4,392 to healthcare providers for health services provided to imposters in their name.

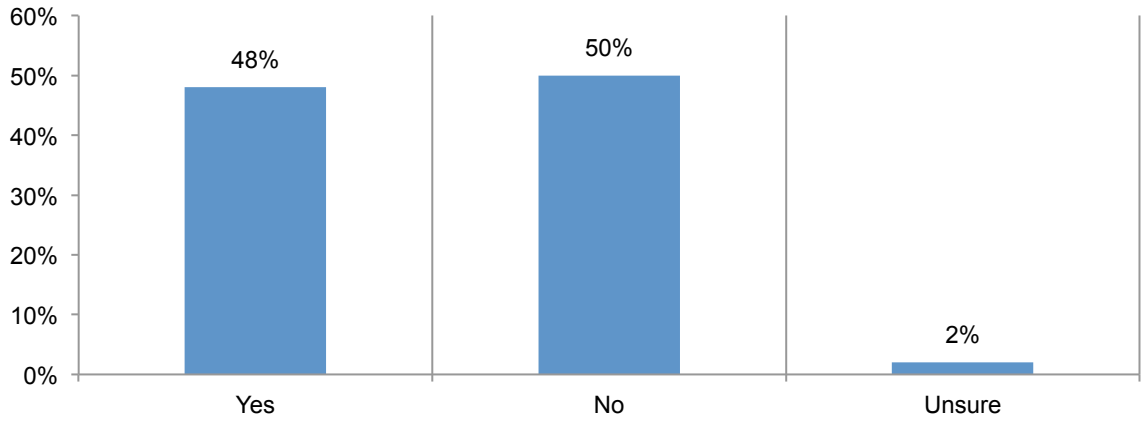
Figure 2. Percentage breakdown of out-of-pocket costs



Individuals are unaware of the dangers and consequences of medical identity theft.

Medical identity theft can put victims' lives at risk. The individuals in this study understand what medical identity theft is and have had personal experience with this crime either directly or through an immediate family member. However, 50 percent are not aware that medical identity theft can create inaccuracies in their permanent medical records as shown in Figure 3. Such inaccuracies can result in misdiagnosis, errors in prescriptions, delay in receiving medical treatment and mistreatment.

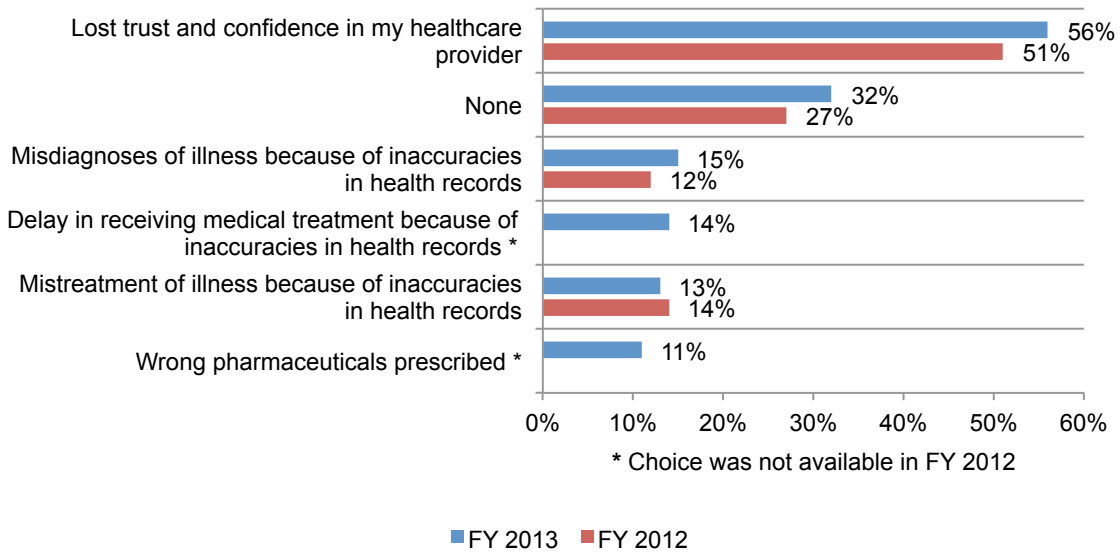
Figure 3. Can inaccuracies occur in medical records because of medical identity theft?



Most medical identity theft victims lose trust and confidence in their healthcare provider following the loss of their medical credentials. Figure 4 shows that the most frequent medical consequence of a medical identity theft is that respondents lost trust and confidence in their healthcare provider (56 percent). This is an increase from 51 percent in last year's study.

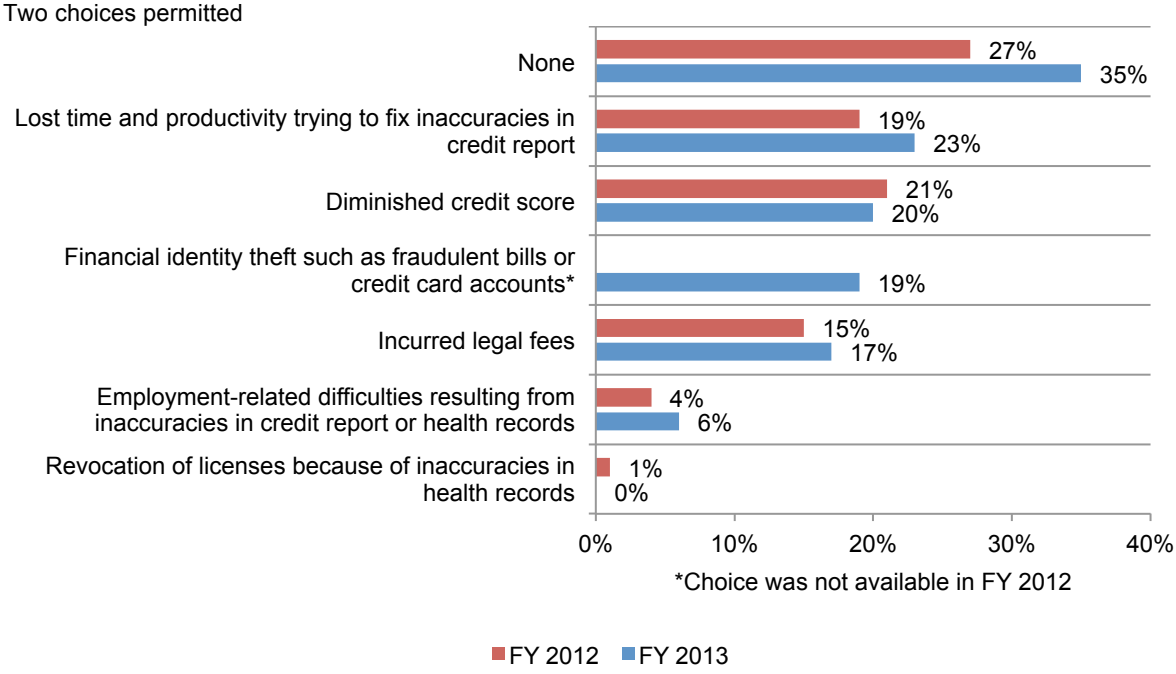
Thirty-two percent say they had no medical consequences from the theft of their medical credentials. However, some of the respondents are aware that medical identity theft can be life threatening. Specifically, 15 percent say they were misdiagnosed when seeking treatment, 14 percent say there was a delay in receiving treatment, 13 percent say they received the wrong treatment and 11 percent say the wrong pharmaceuticals were prescribed.

Figure 4. Medical consequences of the medical identity theft incident
Two choices permitted



Many medical identity theft victims say they did not experience any financial impact. Figure 5 shows that 35 percent of respondents say they did not suffer a financial consequence as a result of the identity theft incident. This is an increase from 27 percent in last year's study. Twenty-three percent say they incurred costs associated with lost time and productivity trying to fix inaccuracies in credit reports. This is a nominal increase from 19 percent in the 2012 study.

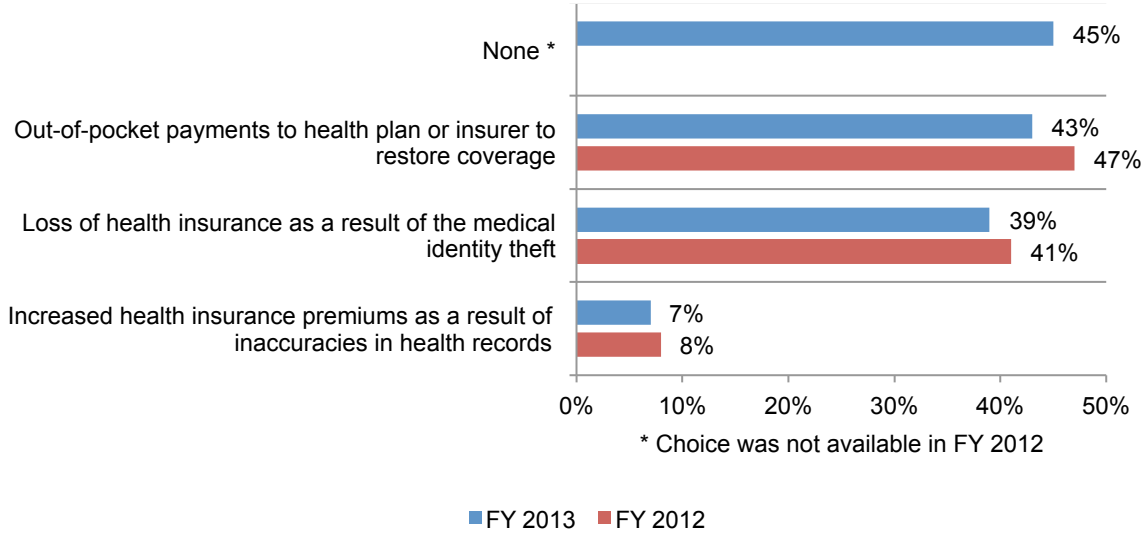
Figure 5. Financial consequences of the medical identity theft incident
Two choices permitted



In this year's study, we also wanted to determine if medical identity theft caused victims to lose their insurance coverage, pay higher premiums or pay fees to restore coverage. As shown in Figure 6, 45 percent say they did not suffer any of these consequences.

However, 43 percent did have to make out-of-pocket payments to their health plan or insurer to restore coverage and 39 percent lost their health insurance coverage. These findings are slightly lower than in 2012. Very few respondents saw their health insurance premiums increase as a result of inaccuracies in health records.

Figure 6. Health insurance consequences of the medical identity theft incident
Two choices permitted



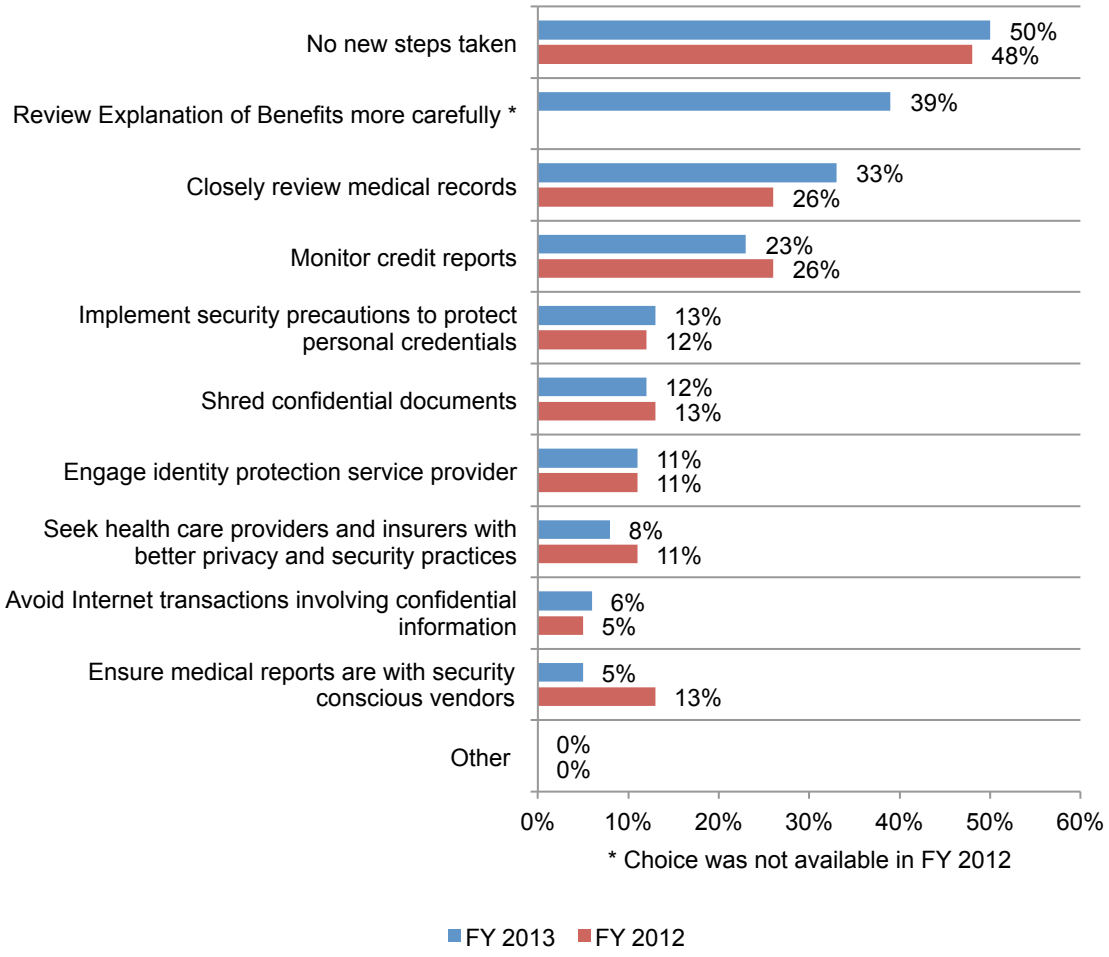
Steps to resolve the crime and prevent future incidents are often ignored.

Individuals lack awareness of the seriousness of the crime. The majority of individuals have yet to realize the negative consequences of medical identity theft. As a result it seems they are slow to take steps to protect themselves and resolve the crime.

As shown in Figure 7, 50 percent of participants do not take steps to protect themselves from future medical identity theft incidents. This is virtually unchanged since last year. Thirty-nine percent of respondents say they will review their Explanation of Benefits and 33 percent say they will more carefully review their medical records.

When asked if they or their immediate family members resolved the identity theft incident, 50 percent say they have done nothing. Only 11 percent say it was completely resolved.

Figure 7. Steps taken to prevent future medical identity theft incidents
More than one choice permitted

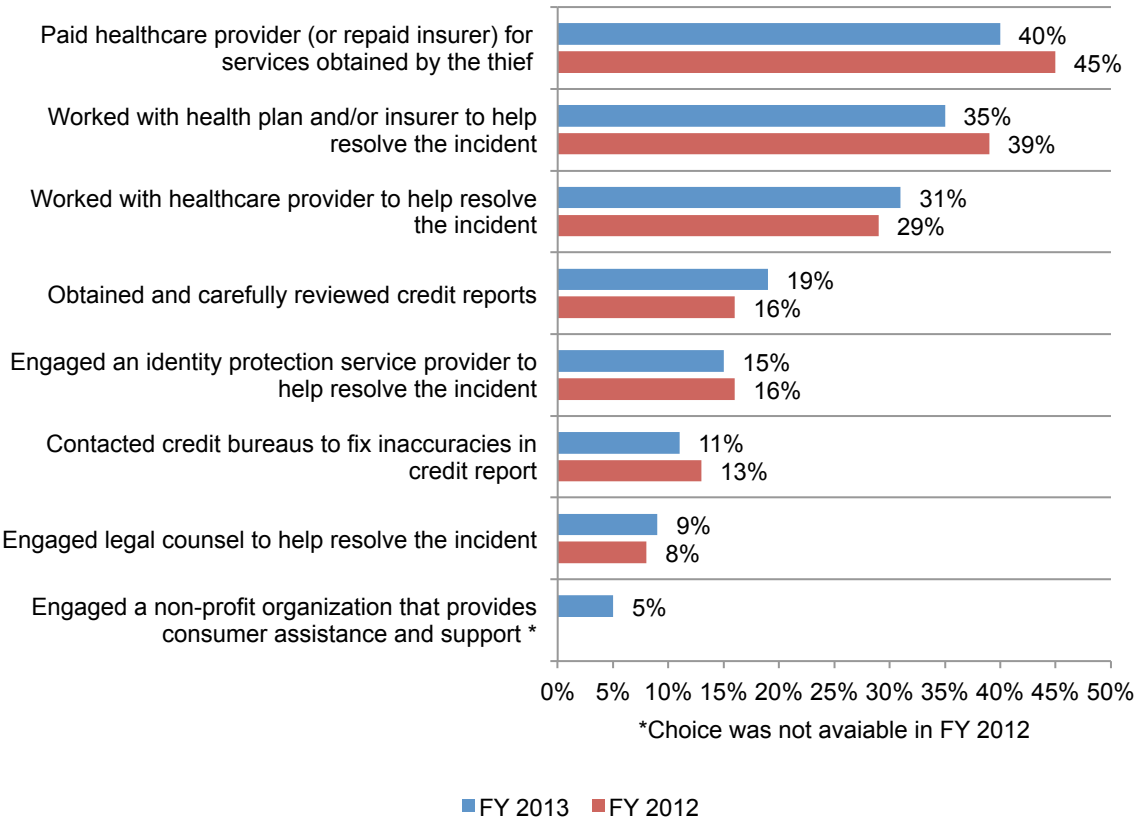


Resolution of the crime is time-consuming. The amount of time it takes to deal with the crime may discourage many victims from trying to resolve the theft and stop future incidents.

Those who did try to resolve the incident say that they worked with their health plan and or insurer to help resolve the incident (35 percent) or worked with the healthcare provider (31 percent), according to Figure 8.

Such activities consumed almost a year or more, according to 36 percent of respondents. Almost half (48 percent) of respondents say the crime is still not resolved.

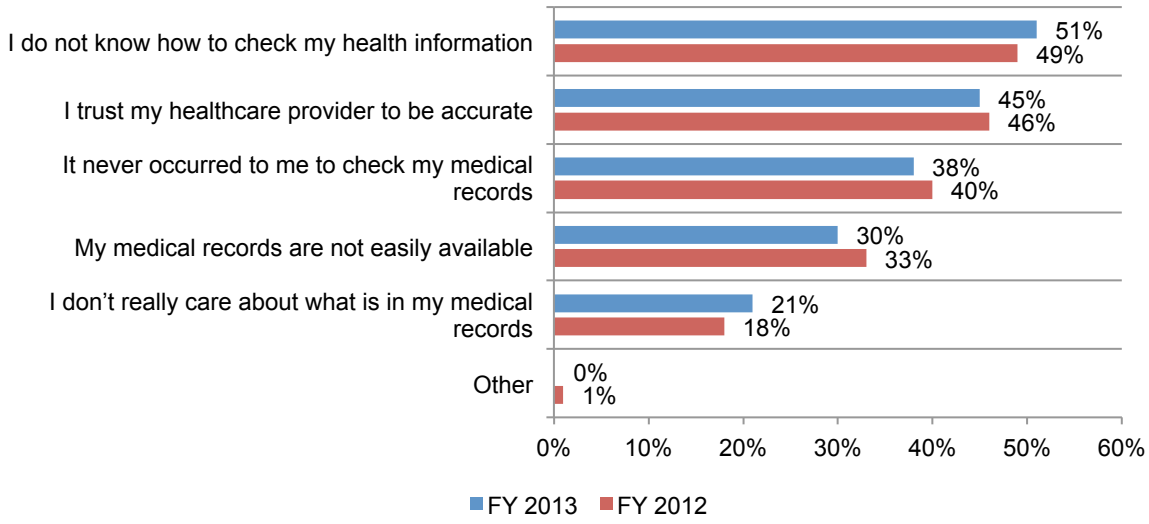
Figure 8. Methods for resolving the medical identity theft
More than one response permitted



Individuals rarely take steps to check their medical records. Seventy-eight percent of respondents say that it is very important or important to control their health records directly but they are not taking steps to do so. Specifically, 56 percent of respondents do not check their medical records to determine if the health information is accurate.

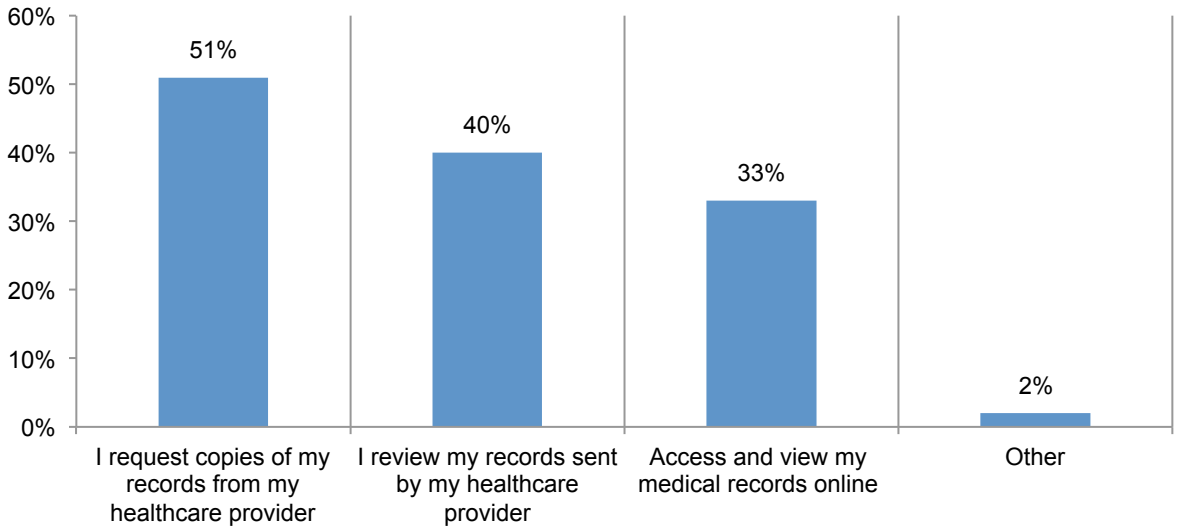
According to Figure 9, they don't know how to check their medical records (51 percent) and they trust their healthcare provider to be accurate (45 percent) are the primary reasons for not checking medical records.

Figure 9. Reasons medical records are not checked for accuracy
More than one response permitted



The steps taken by the 44 percent of respondents who say they do check their health records for accuracy most of the time or sometimes are shown in Figure 10. They are most likely to request copies from their healthcare provider or they review their records such as explanation of benefits.

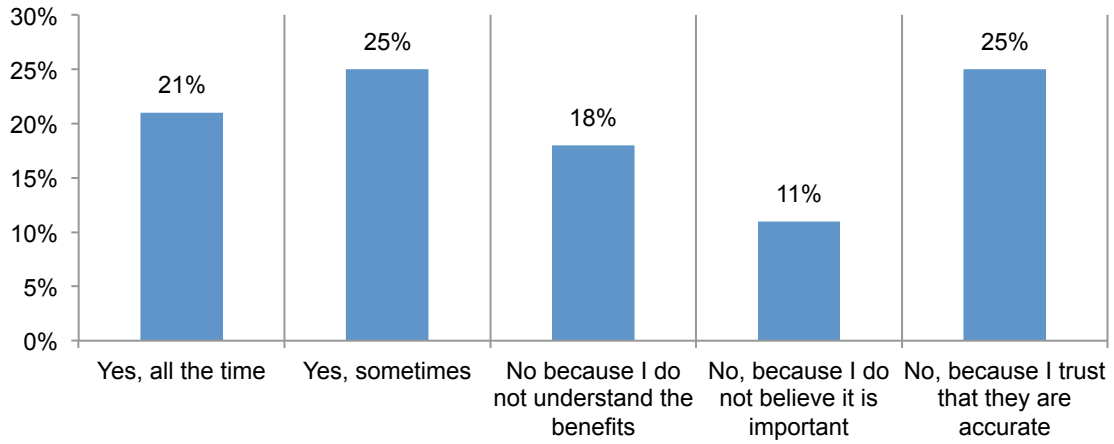
Figure 10. Methods used for checking health records for accuracy
More than one response permitted



Reviews of Explanation of Benefits can protect individuals. In this year's research, we asked respondents if they read the EOB form or document that is sent by insurance companies following a healthcare service paid for by the insurance company. Taking the time to check the accuracy of the form could red flag any possible incidents of medical identity theft.

As shown in Figure 11, the majority of respondents do not review these documents. Forty-six percent of respondents read these documents all or some of the time. If they don't, 25 percent say it is because they believe they are accurate and their review is not necessary.

Figure 11. Do victims read their EOB?



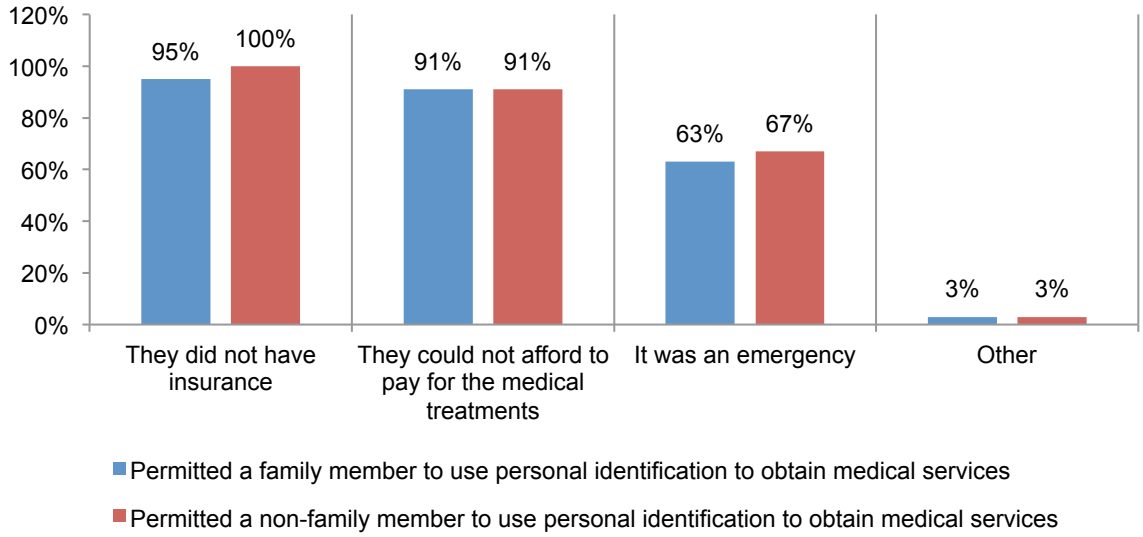
Of those who read the EOBs, they believe the most important information to check is the nature of the procedure or type of exam and the total claim amount such as the amount covered by insurance. Fifty-one percent say that when reviewing the EOB there was a claim they did not recognize. Unfortunately, if inaccuracies are found 52 percent say they do not report them.

The risk of medical identity theft can be reduced.

Sharing of personal identification to obtain medical services is prevalent. Thirty percent of respondents knowingly permitted a family member to use their personal identification to obtain medical services including treatment, healthcare products or pharmaceuticals. The frequency of sharing varies among respondents. Fifty-three percent say they did it only once. However, 21 percent could not count the number of times they shared their identification.

As shown in Figure 12 the most common reasons were because the family member did not have insurance or could not afford to pay for the treatments. In the case of non-family members, only 17 percent of respondents admit to sharing. Again the reasons were similar as shown in the figure. Once again the frequencies range from once to cannot recall. Fifty-one percent say they only did it once and 22 percent can't remember.

Figure 12. Why respondents shared their medical ID credentials
More than one response permitted



Many cases of medical identity theft are preventable. The majority of respondents say the crime happened because they knowingly shared their personal identification or medical credentials with someone they knew (30 percent) or a member of the family took their personal identification or medical credentials without consent (28 percent), according to Figure 13.

In both cases, not sharing credentials or being more protective of their credentials could have prevented the crime. Very few respondents say that a data breach, malicious insider, identity thief or loss of their credentials resulted in the crime.

Figure 13. Most likely causes of medical identity theft
One choice permitted

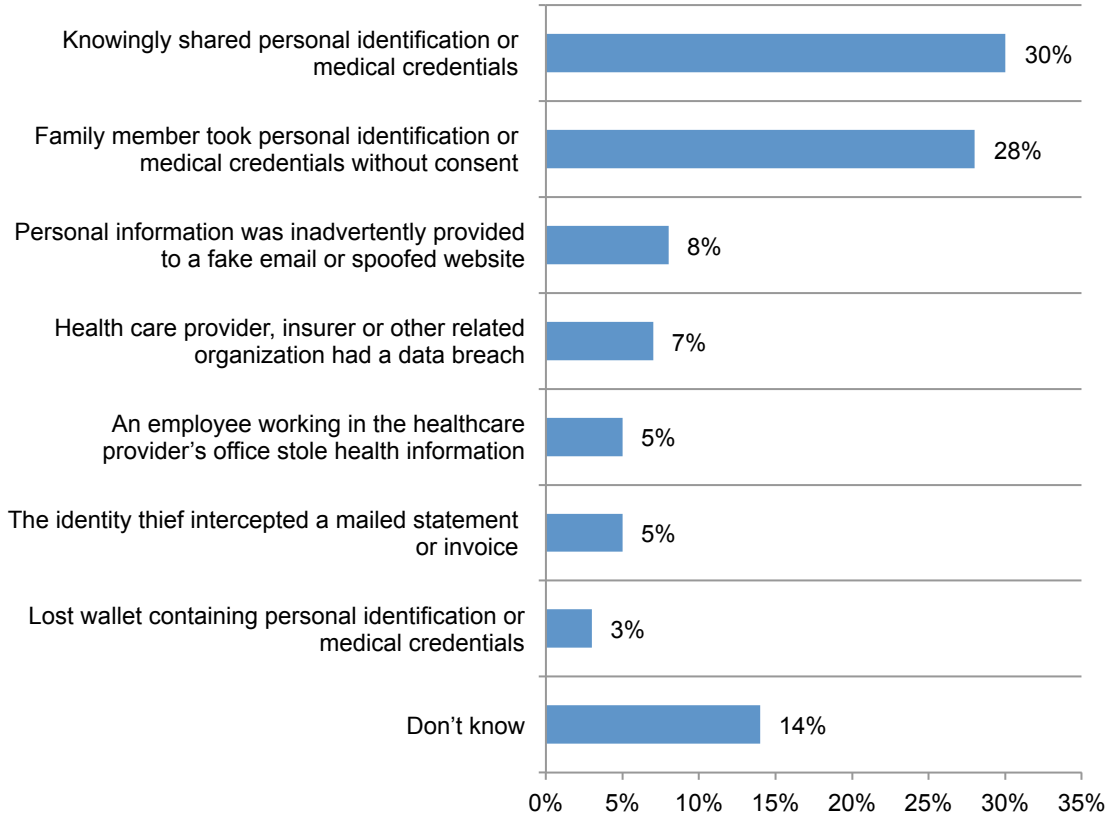


Figure 14 summarizes how respondents learned that they were medical identity theft victims. Respondents say they found out about the crime when they uncovered mistakes in health records (29 percent), errors in EOB from insurer (26 percent), errors posted to medical invoices by my healthcare provider (25 percent) or a collection letter (24 percent).

Figure 14. How the medical identity theft was discovered

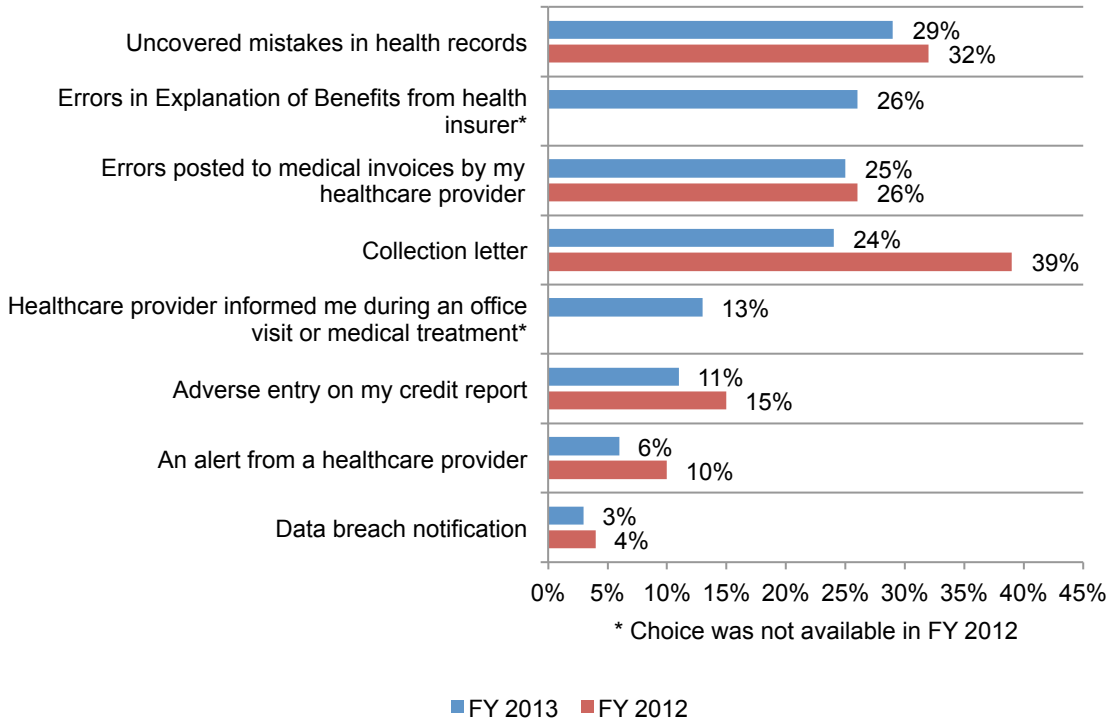
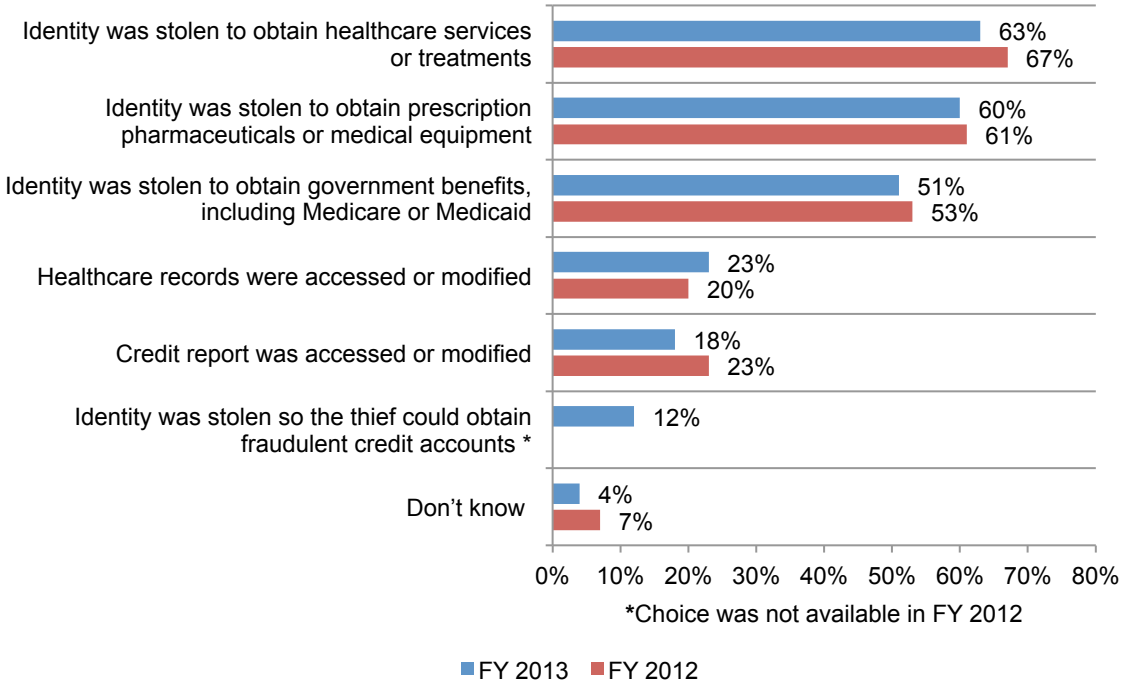


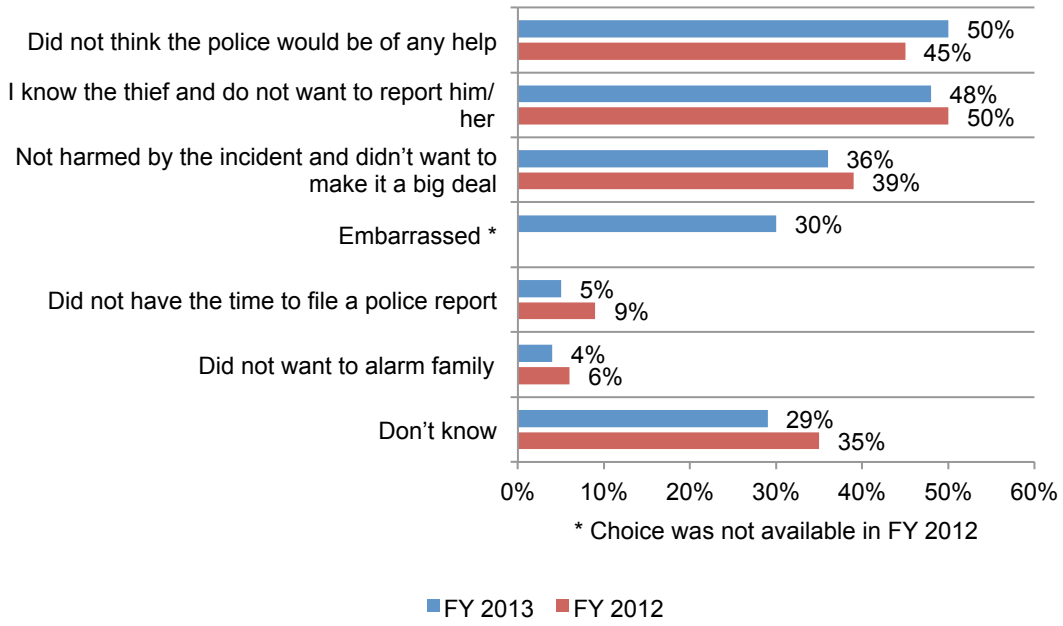
Figure 15 describes the incident. The objective of the thief was to obtain healthcare services or treatments, prescription pharmaceuticals, medical equipment or government benefits.

Figure 15. Description of medical identity theft incident
More than one response permitted



Very often the crime is unreported. Only 43 percent of respondents say they notified law enforcement or legal authorities. The main reason for not reporting the crime is because they did not think the police would be of help (50 percent) or they knew the thief and did not want to report him or her (48 percent), as shown in Figure 16.

Figure 16. Why the medical identity theft wasn't reported
More than one response permitted

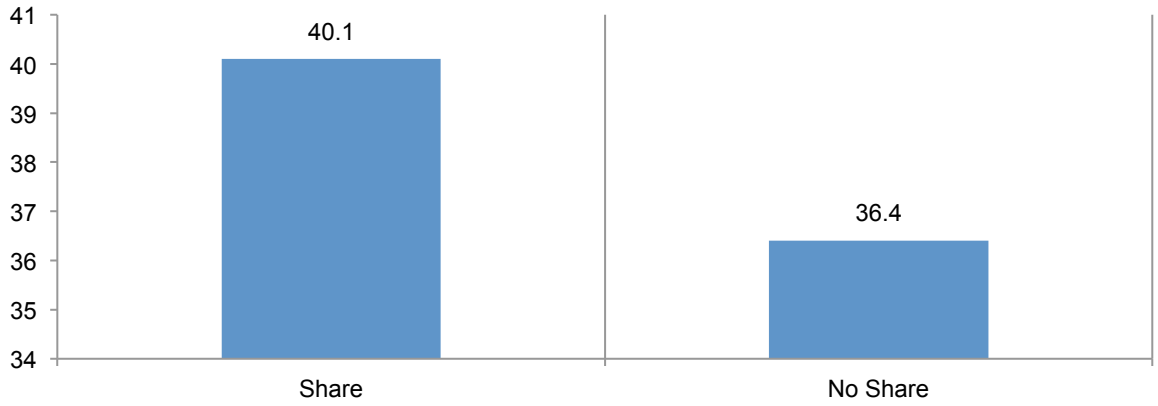


Certain individuals are more likely to share medical credentials.

Who is most likely to knowingly share their medical credentials with someone they know? A deeper analysis of the findings enables us to profile the most likely individuals to share their credentials, which is shown in Figures 17 to 21.

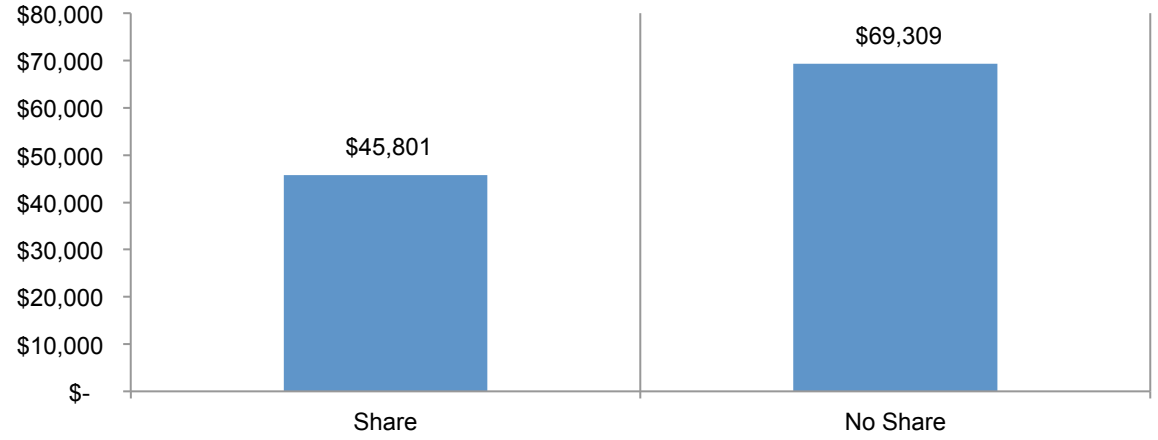
The average age of respondents who share their medical credentials is 40.1 years. In contrast, respondents who do not share have an average age of 36.4 years.

Figure 17. Average age by share and no share subsamples
Share subsample = 217 respondents (28%); No share subsample = 571 respondents (72%)



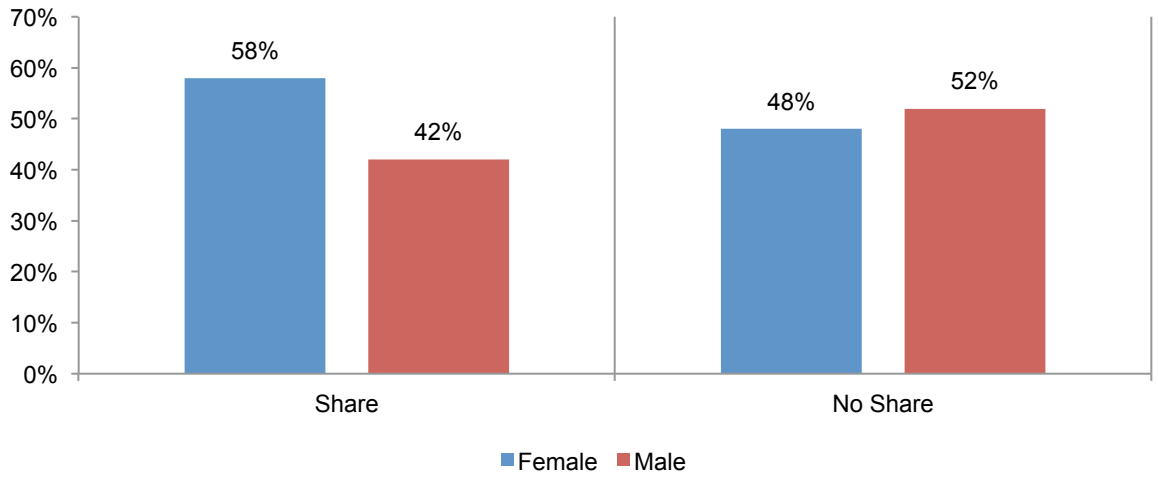
The average self-reported household income appears to be related to the share/no share decision. Specifically, the estimated average household income for those who share is $45,801 versus $69,309 for those who do not share.

Figure 18. Average household income by share and no share subsamples
Share subsample = 217 respondents (28%); No share subsample = 571 respondents (72%)



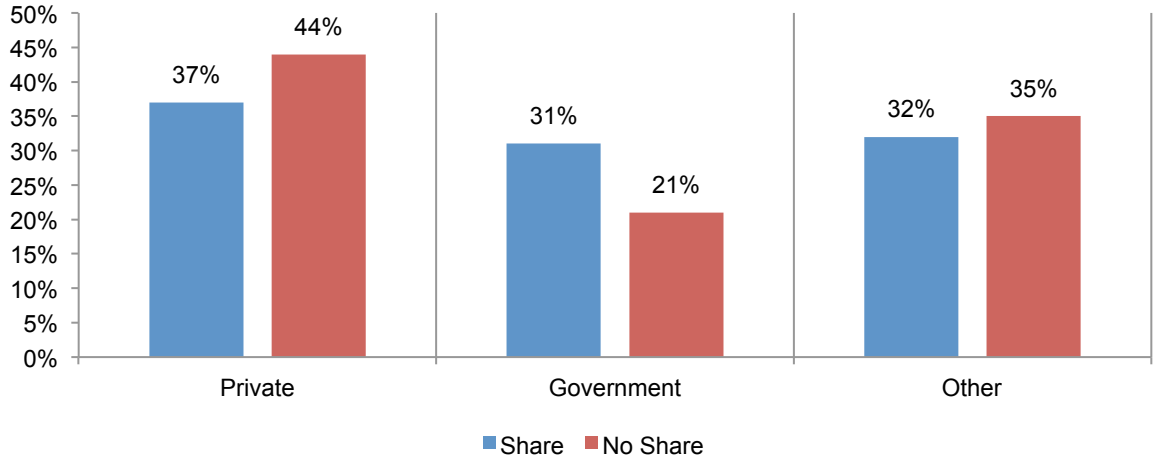
The respondents' gender appears to be related to the share/no share decision. Accordingly, 58 percent of the share subsample are women and 42 percent men. In sharp contrast, 52 percent of the no share subsample are male and 48 percent female.

Figure 19. Gender of respondents by share and no share subsamples
Share subsample = 217 respondents (28%); No share subsample = 571 respondents (72%)



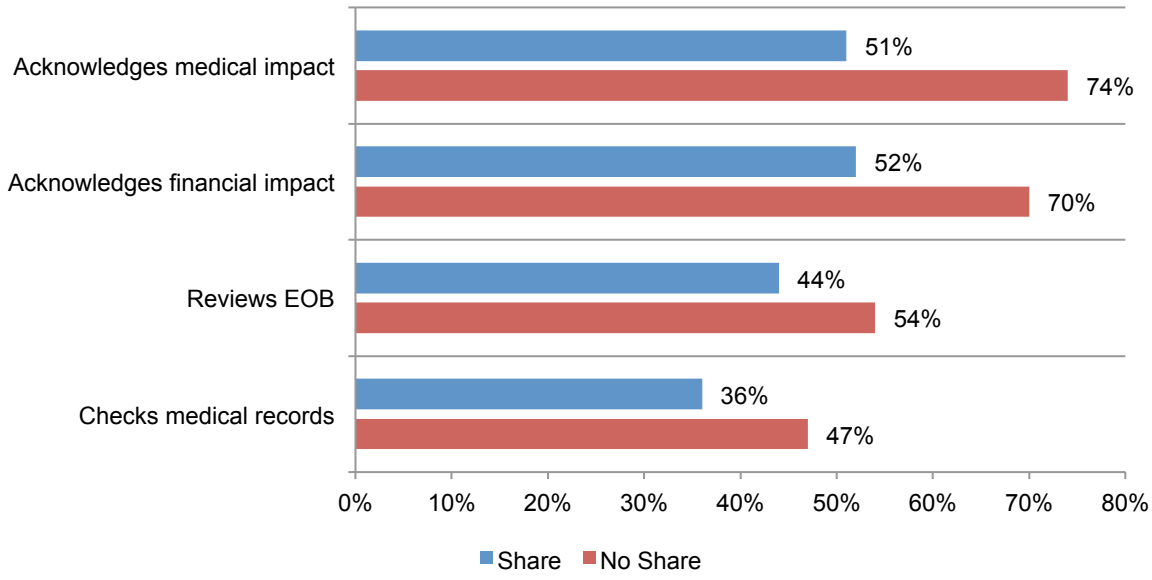
The respondents' insurance type is also related to the respondents' share/no share decision. As shown, respondents who have private health insurance are less likely to share than not share their medical ID credential (37 vs. 44 percent). On the other hand, those respondents who have government insurance are more likely to share than not share (31 vs. 21 percent).

Figure 20. Insurance type by share and no share subsamples
Share subsample = 217 respondents (28%); No share subsample = 571 respondents (72%)
Government insurance includes Medicare, Medicaid, VA benefits and other plans



The next figure summarizes four yes/no questions completed by respondents in the share or no share subsamples. In comparison to the share subsample, respondents who do not share are more likely to acknowledge the medical and financial impacts of medical identity theft. In addition, they are more likely to review their EOB and check their health records.

Figure 21. Respondents' actions by share and no share subsamples
Share subsample = 217 respondents (28%); No share subsample = 571 respondents (72%)

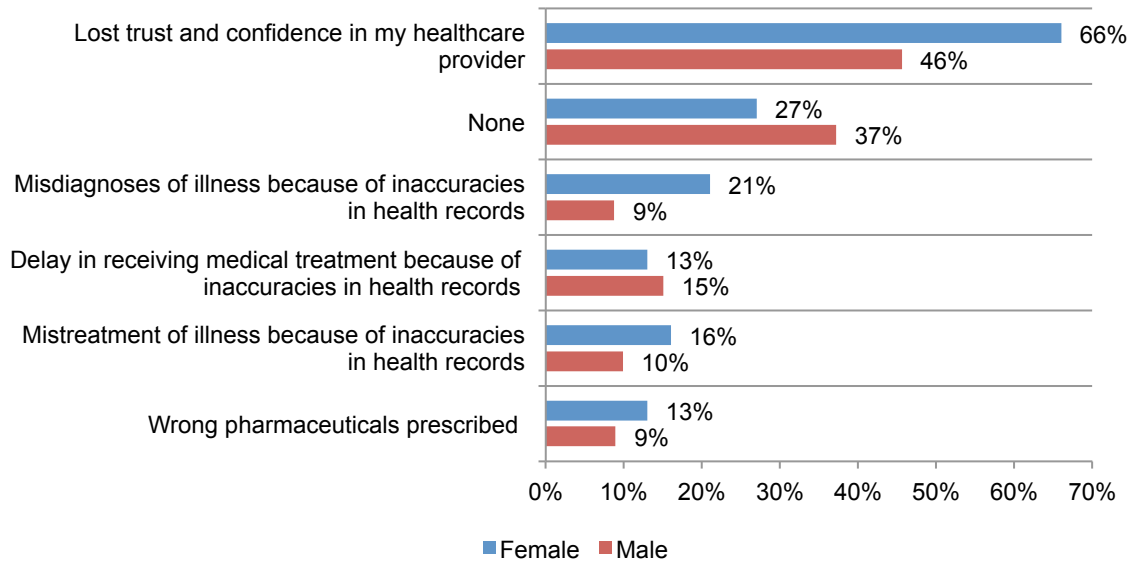


Who is most likely to suffer negative medical and financial consequences?

We also analyzed the medical consequences based on the gender, age and type of insurance of the respondent. In general, women, older individuals and those with private insurance believe they have suffered more negative medical consequences resulting from medical identity theft.

Figure 22 shows that women are more likely to lose the trust of their healthcare provider.

Figure 22. Medical consequences by gender
Two responses permitted



Older respondents, defined as individuals who are more than 35 years of age, have greater awareness about the consequences and are more concerned about the possibility of a misdiagnosis as a result of inaccuracies in their medical records as shown in Figure 23.

Figure 23. Medical consequences by age group
Younger respondents are 18 to 35 years; older respondents are above 35 years
Two responses permitted

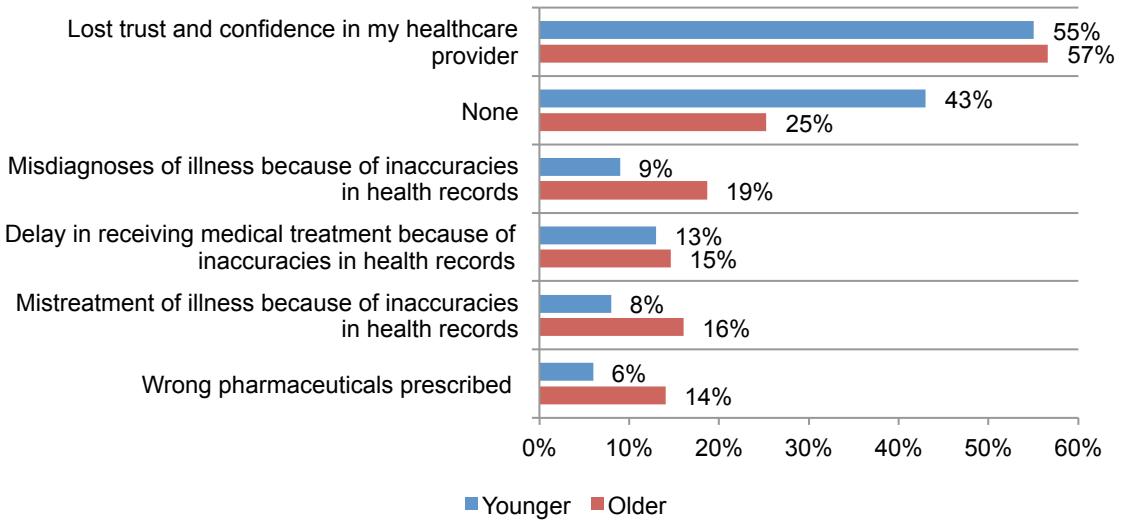
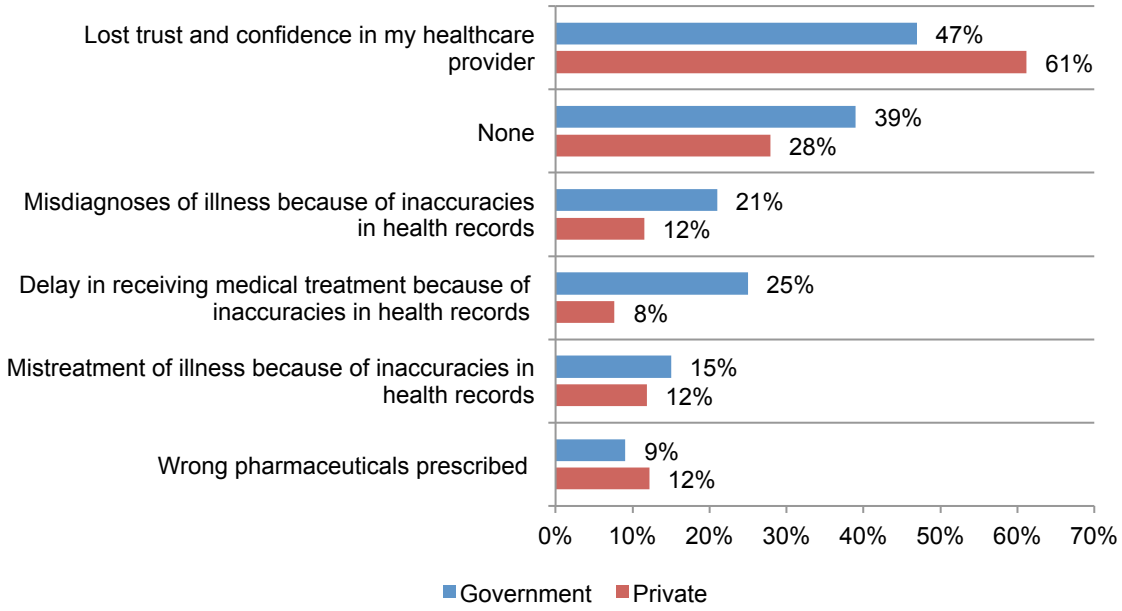


Figure 24 shows differences for respondents who have private health insurance versus those with government insurance (such as Medicare, Medicaid, veterans' benefits and others). Accordingly, respondents with private insurance are more likely to lose trust in a healthcare provider. However, respondents with government coverage appear to be more likely to worry about delays in receiving medical treatment and misdiagnosis because of inaccuracies in health records.

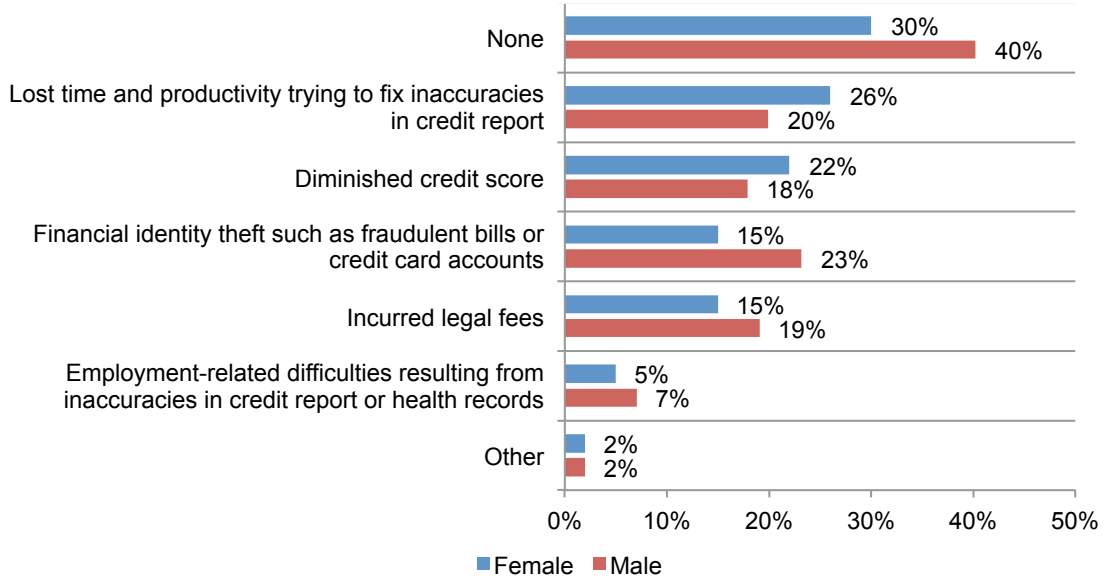
Figure 24. Medical consequences by insurance type
Government insurance includes Medicare, Medicaid, VA benefits and other plans



Differences in the financial consequences of medical identity theft also are shown according to gender, age, household income and type of insurance. Once again, women, older and higher income respondents are more aware of the negative consequences of medical identity. Those with private insurance are also more aware of the cost to them.

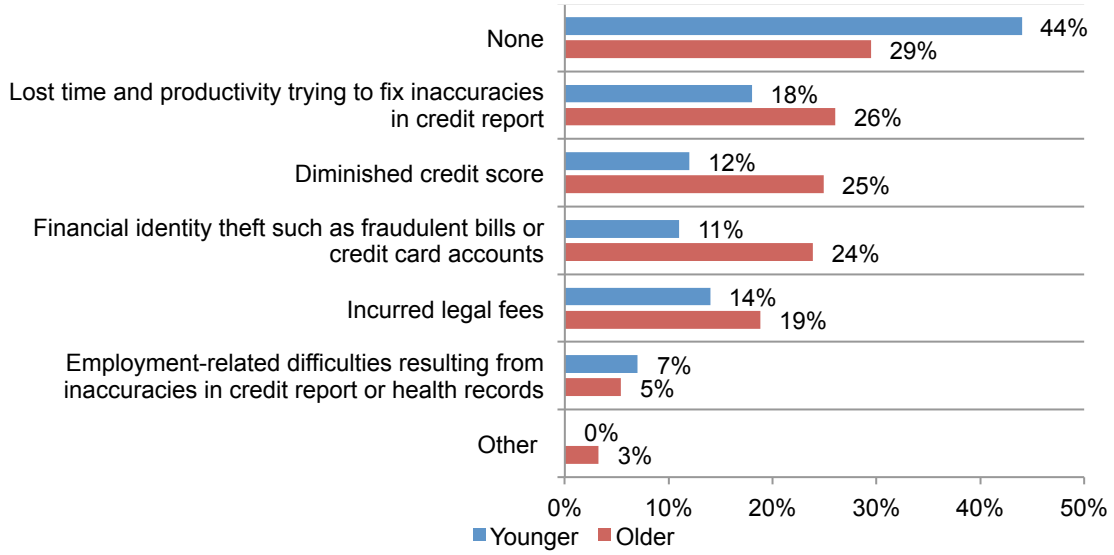
Figure 25 shows that more women report lost time and productivity trying to fix inaccuracies. However men are more aware of having their financial identity stolen.

Figure 25. Financial consequences by gender
Two choices permitted



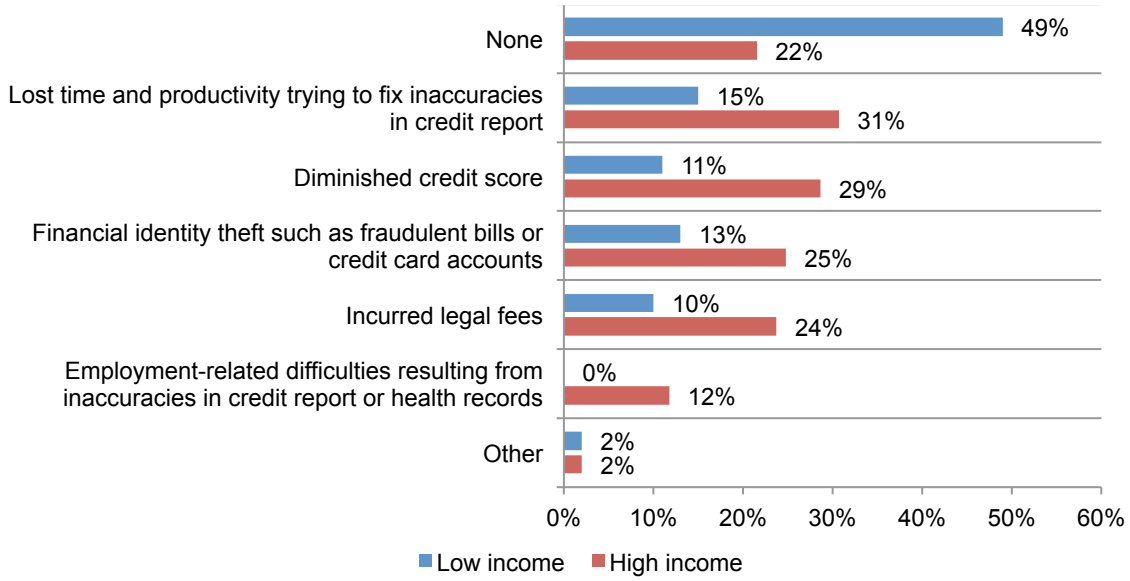
According to Figure 26, there are significant differences between younger and older respondents about the awareness of financial consequences. Specifically, older respondents are more aware of financial identity theft and diminished credit score.

Figure 26. Financial consequences by age group
Younger respondents are 18 to 35 years; older respondents are above 35 years
Two choices permitted



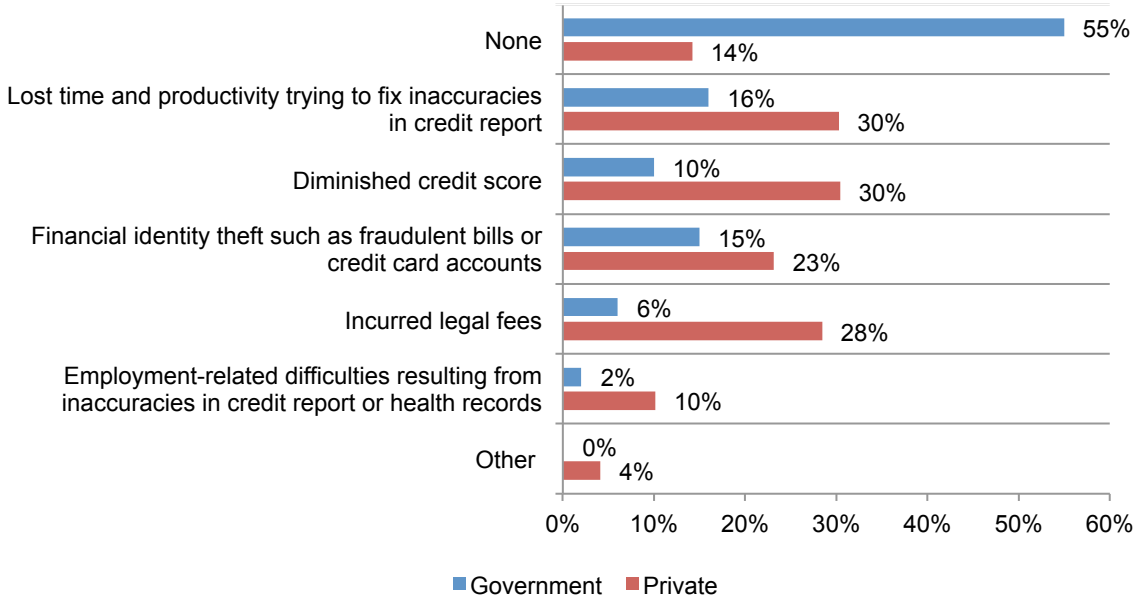
Respondents in the higher income bracket (defined as more than $50,000) also are most likely to know that their credit score has been diminished and have had to incur legal fees, as shown in Figure 27.

Figure 27. Financial consequences by income level
Low income is defined as below $50,000; high income is at or above $50,000
Two choices permitted



According to Figure 28, respondents with private insurance are more likely to be aware of the financial consequences suffered as a result of the medical identity theft. They are more likely to have lost time trying to fix inaccuracies in their credit report, to understand that their credit score has been diminished and incurred legal fees to resolve the crime.

Figure 28. Financial consequences by insurance type
Government insurance includes Medicare, Medicaid, VA benefits and other plans
Two choices permitted



Part 3: Conclusion: Solving the medical identity theft problem

Medical identity theft is costly and on the rise according to this research. The number of cases increased more than 300,000 since last year's study. For the first time, we calculated that the total out-of-pocket costs for the 36 percent of respondents who paid to resolve the crime averaged $18,660 per victim. Based on this calculation, we estimate that the total value of out-of-pocket cost to victims who had to pay is approximately $12.3 billion.

Many cases of medical identity theft reported in this study result from the sharing of personal identification with family and friends. In some cases, family members take the victim's personal credentials without consent. Rarely does it occur from data breaches, malicious insiders, an identity thief or loss of medical credentials. This finding that medical identity theft is a family affair is consistent with previous studies conducted by Ponemon Institute.

While costly for some, many individuals are spared the need to spend money to resolve the crime. However, while they may not feel a financial loss they could be risking their lives by having inaccuracies in their medical records as a result of someone using their medical credentials

Individuals, healthcare and government working together can reduce the risk of medical identity theft. Individuals need to be aware of the negative consequences of sharing their credentials. Healthcare organizations and government must improve their authentication procedures to insure imposters are not obtaining medical services and products.

Following are recommendations to curb the rise of medical identity theft:

- Never share personal medical identity credentials with anyone, even close family members or friends.
- Monitor credit reports and billing statements for possible medical identity fraud. For example, an unpaid balance on a statement for medical procedures or products may suggest someone has committed fraud.
- Periodically check with the primary physician to ensure the accuracy of medical records. Specially, check to see if the records accurately reflect the procedures, treatments, prescriptions and other medical activities that have been conducted. Also, look for any inaccuracies concerning health profile such as blood type, pre-existing conditions, allergies and so forth.
- Engage the services of an identity protection provider if there are any concerns about the ability to monitor and protect your identity.
- Individuals should be made aware that sharing their personal identification is fraud and could result in significant costs to the government and healthcare industry and, ultimately, the taxpayer as a result of medical services products and pharmaceuticals illegally obtained.
- In turn, healthcare providers, government agencies and insurance companies should understand the financial impact to their organizations. In addition to safeguarding the patient data entrusted to their care from breaches, their responsibility should be to ensure that all patients are properly authenticated prior to receiving medical services and products. By doing so, both the medical and financial consequences of this crime could be minimized.

Part 4. Methods

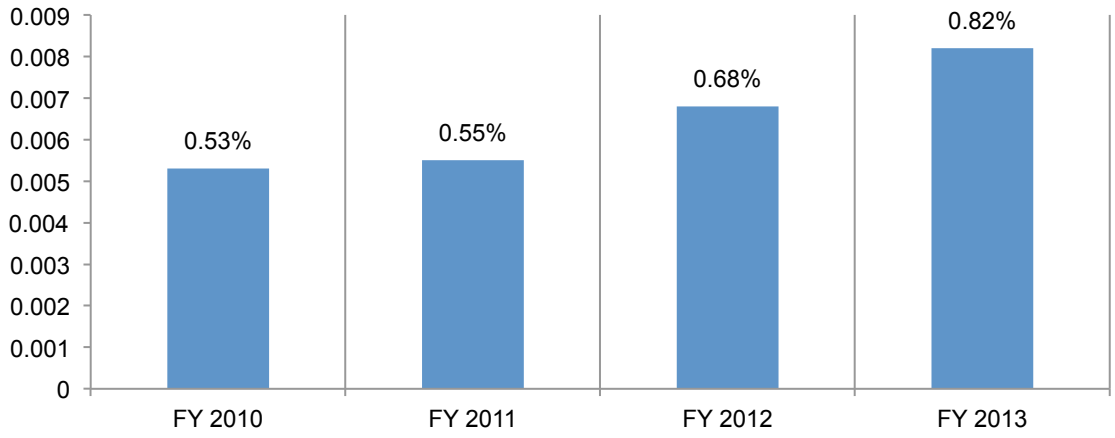
A sampling frame of 43,778 adult-aged individuals located in all regions of the United States was selected as participants to this survey. This sampling frame contained individuals who were pre-screened from a larger sample on the basis of their identity theft or identity fraud experience.[3] Table 2 shows 901 respondents completed the survey. Screening and reliability checks removed 111 surveys, which resulted in a final sample of 790 respondents or a 1.8 percent response rate.

Table 2. Sample response	Freq.
Total sample frame	43,778
Total response	901
Screened responses	111
Usable sample	788
Response rate	1.8%

The medical identity theft base rate of .0082 was determined from a second (independent) survey sampling procedure. Using discovery methods, we randomly surveyed a representative panel of adult-aged U.S. consumers to determine status. Specifically, those who indicated they were medical identity theft victims were included in the base rate group. We collected 41 bona fide respondents after sampling 5,000 individuals.[4]

Figure 30 shows the medical identity theft base rates over the past four years. Using the same discovery sampling methods, we see the base rate steadily rising since our first study in 2010. As can be seen, the increase over the past year is calculated at 19 percent.

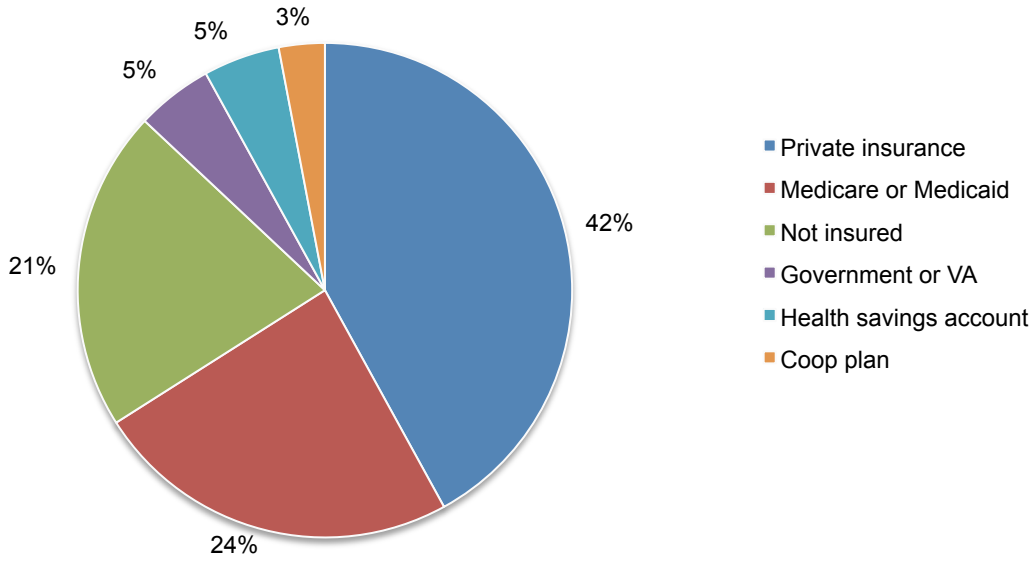
Figure 30. Medical identity theft base rates over four years



[3]The sampling frame of identity theft victims was developed from an original sample of adult-aged U.S. consumers, which was created for the first Medical Identity Theft Study conducted in 2010. This specialized and proprietary sampling frame has been maintained and updated since its inception.
[4]Exactly 5,000 individuals were randomly sampled from a general population of adult-aged consumers in the United States to discover 41 bona fide medical identity theft victims.

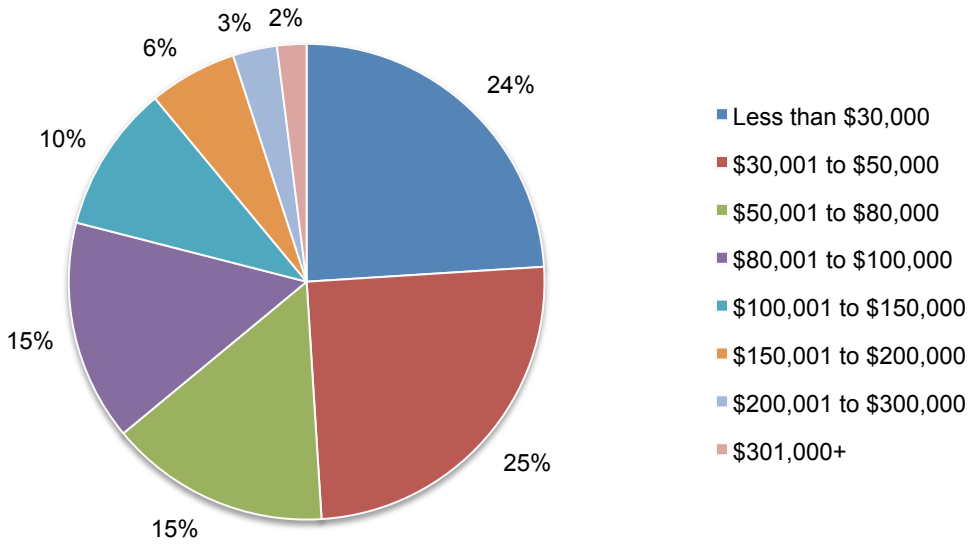
Pie Chart 1 shows 42 percent of respondents in the present sample have some form of private insurance. In addition, 24 percent are on Medicare or Medicaid. Another 21 percent say they presently do not have health insurance.

Pie Chart 1. Respondents' current health insurance or plan



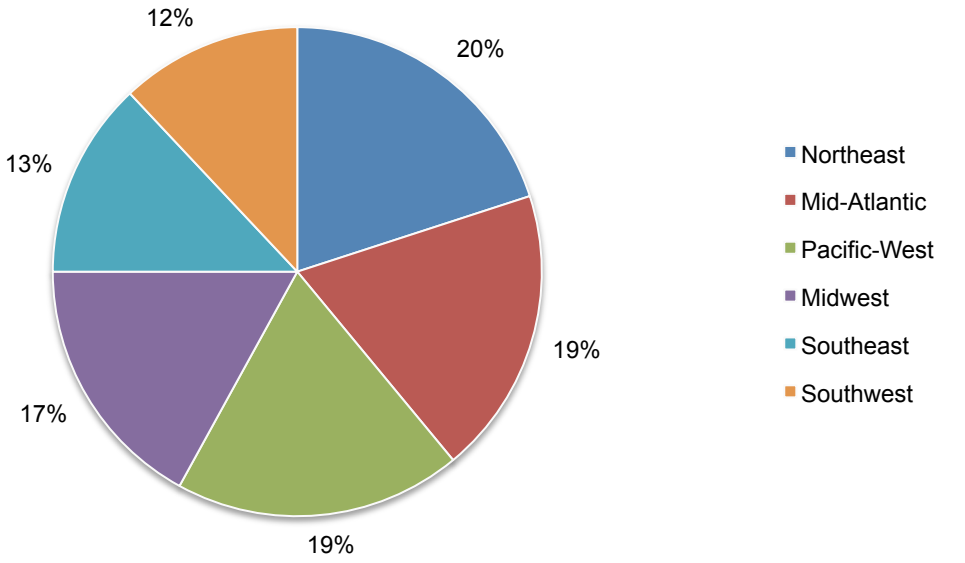
Pie Chart 2 shows the distribution of respondents according to their self-reported household income level. As shown, 49 percent of respondents in the 2013 sample report an income level at or below $50,000 per annum. The extrapolated average household income level for the 2013 sample is $62,821.

Pie Chart 2. Respondents' current health insurance or plan



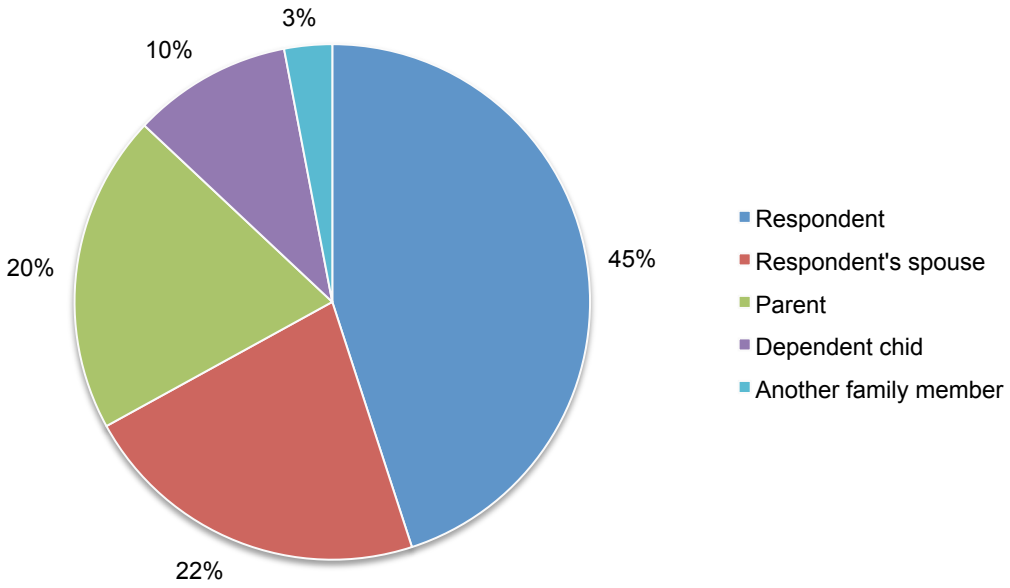
Pie Chart 3 shows the distribution of sample respondents by geographic region. As shown, the distribution by geographic region has remained relatively constant over year years. The largest regions are Northeast and Pacific-West. The smallest regions are the Southwest and Southeast.

Pie Chart 3. Respondents' location by U.S. region



When asked who was the subject of the crime, 45 percent say they were the victim followed by 22 who say it was their spouse or partner. Another 20 percent say it was a parent and 10 percent say it was a dependent child.

Pie Chart 4. Who is the medical identity theft victim?



Part 5. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to many consumer-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a sample of adult-aged consumers located in all regions of the United States, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the sample is representative of individuals who are likely to suffer from an identity theft crime. We also acknowledge that the results may be biased by external events such as media coverage at the time we fielded our survey.

  We also acknowledge bias caused by compensating respondents to complete this research within a holdout period. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that certain respondents did not provide accurate responses.

Appendix: Detailed Results

The following tables provide the frequency of responses to all survey questions contained in this study. All survey responses were captured in June 2013.

Sample response	**FY 2013**
Total sample frame	43,778
Total response	899
Screened responses	111
Usable sample	788
Response rate	1.8%

Medical identity theft occurs when someone uses an individual's name and personal identity to fraudulently receive medical services, prescription drugs and/or goods, including attempts to commit fraudulent billing. This includes medical identity theft that occurs when an individual shares his or her credentials with others.

Part 1. Background	
Q1a. Before now, have you heard the term "medical identity theft"?	FY 2013
Yes	100%
No	0%
Total	100%

Q1b. Before now, did you know the definition of medical identity theft?	FY 2013
Yes	92%
No	8%
Total	100%

Q1c. If yes, how did you learn about medical identity theft?	FY 2013
A story in the media (for example, newspaper, radio, TV, Internet)	16%
Information provided by my healthcare provider	14%
Information provided by my employer	4%
A personal experience	69%
Stories shared by my friends or family members	59%
Total	162%

Q2. If you were informed that your medical records were lost or stolen, what actions listed below would be most important to you? Please select the two most important actions.	FY 2013
Prompt notification of the loss or theft by the organization responsible for safeguarding your confidential information (within 30 days)	38%
Free identity protection for one year	30%
Assistance with transferring my health records to another healthcare provider	17%
Reimbursement for costs incurred to find another healthcare provider	76%
Assurance that the incident was being thoroughly investigated	14%
Assurance that steps were taken to address the root cause of the incident	16%
Assurance that additional security precautions would be taken to prevent future incidents	9%
	200%

Q3. Please choose the range that best describes your age.	FY 2013
Below 18 years (Stop)	0%
Between 18 and 25 years	17%
Between 26 and 35 years	21%
Between 36 and 45 years	23%
Between 46 and 55 years	20%
Between 56 and 65 years	11%
Above 65 years	8%
Total	100%

Q4. Are you aware that medical identity theft can create **inaccuracies** in your permanent medical records?	FY 2013
Yes	48%
No	50%
Unsure	2%
Total	100%

Part 2: Healthcare provider privacy	
Q5a. Do you check your medical records to determine if the health information about you is accurate?	FY 2013
Yes, most of the time	18%
Yes, sometimes	26%
No	56%
Total	100%

Q5b. If no, why don't you check?	FY 2013
My medical records are not easily available	30%
I do not know how to check my health information	51%
I trust my healthcare provider to be accurate	45%
It never occurred to me to check my medical records	38%
I don't really care about what is in my medical records	21%
Other (please specify)	0%
Total	185%

Q5c. If yes, how do you check?	FY 2013
Access and view my medical records online (web portal)	33%
I request copies of my records from my healthcare provider	51%
I review my records sent by my healthcare provider (such as the explanation of benefits)	40%
Other (please specify)	2%
Total	126%

Please rate the following statements using the strongly agree to strongly disagree (5-point) scale provided below each item.	FY 2013
Q6a. If I knew my healthcare provider was unable to safeguard my medical records, I would find another provider.	56%
Q6b. If my healthcare provider informed me that my medical records were lost or stolen, I would find another provider.	57%
Q6c. Electronic medical records will increase my chances of becoming a victim of identity theft.	39%

How important are the following issues? Use the five-point scale from very important to irrelevant.	FY 2013
Q7a. Healthcare providers ensure the privacy of your health records.	82%
Q7b. Allow me to control my health records directly.	78%

Part 3. Healthcare insurer privacy
An Explanation of Benefits (EOB) is a form or document that may be sent to you by your insurance company several months after you had a healthcare service that was paid by the insurance company. You should get an EOB if you have private health insurance, a health plan from your employer, or Medicare.

Q8a. My healthcare insurer is concerned about medical identity theft.	FY 2013
Yes	67%
No	23%
Don't know	10%
Total	100%

Q8b. If no, would you consider changing healthcare insurance providers if you had a choice?	FY 2013
Yes	44%
No	49%
Don't know	7%
Total	100%

Q9a. Do you read your health care Explanation of Benefits (EOB) from your health insurer?	FY 2013
Yes, all the time	21%
Yes, sometimes	25%
No because I do not understand the benefits	18%
No, because I do not believe it is important	11%
No, because I trust that they are accurate	25%
Total	100%

Q9b. If yes, what information is most important to ensure the EOB is correct? Two top choices.	FY 2013
Healthcare provider information	23%
Date of service	39%
Nature of visit such as procedure, type of exam or testing/imaging	56%
Total claim amount, amount covered by insurance/benefit and amount owed	54%
Don't know	2%
Total	174%

Q10a. Did you ever review your EOB and see a claim from a health care provider that you did not recognize?	FY 2013
Yes	51%
No	49%
Total	100%

Q10b. If yes, whom did you report the claim to?	FY 2013
Insurance company	26%
Healthcare provider	17%
Identity protection service provider	5%
Other	0%
No one (because I did not know whom to report the claim to)	52%
Total	100%

Q11. If your health insurance plan offered a free medical identity theft monitoring service, would you use it?	FY 2013
Yes	65%
No	19%
Unsure	16%
Total	100%

Part 4. Medical identity theft experience	
Q12a. Did you ever knowingly permit a family member to use your personal identification to obtain medical services including treatment, healthcare products or pharmaceuticals?	FY 2013
Yes	30%
No	70%
Total	100%

Q12b. If yes, why did you do this?	FY 2013
They did not have insurance	95%
They could not afford to pay for the medical treatments	91%
It was an emergency	63%
Other	3%
Total	252%

Q12c. If yes, how often did you share your personal healthcare information with a family member?	FY 2013
Only 1 time	53%
Between 2 and 5 times	15%
Between 6 and 10 times	7%
More than 10 times	4%
Can't remember how often	21%
Total	100%

Q13a. Did you ever permit someone you know (non-family member) to use your personal identification to obtain medical services including treatment, healthcare products or pharmaceuticals?	FY 2013
Yes	17%
No	83%
Total	100%

Q13b. If yes, why did you do this?	FY 2013
They did not have insurance	100%
They could not afford to pay for the medical treatments	91%
It was an emergency	67%
Other	3%
Total	261%

Q13c. If yes, how often did you share your personal healthcare information with someone you know?	FY 2013
Only 1 time	51%
Between 2 and 5 times	16%
Between 6 and 10 times	8%
More than 10 times	3%
Can't remember how often	22%
Total	100%

Q14. Were you or someone else in your immediate family ever the victim of medical identity theft?	FY 2013
Yes	92%
No (skip to Part 5)	8%
Total	100%

Please answer the following questions with specific focus on medical identity theft experienced by you or your immediate family members.

Q15. If yes, who was the identity theft victim?	FY 2013
Me	45%
My spouse/partner	22%
My child or dependent under the age of 13 years	7%
My child or dependent between 13 and 18 years	3%
My child or dependent over 18 years	0%
My parent	20%
Another family member living in my household	3%
Total	100%

Q16. How would you describe your medical identity theft incident? Please select all that apply.	FY 2013
My identity was stolen to obtain government benefits, including Medicare or Medicaid	51%
My identity was stolen to obtain healthcare services or treatments	63%
My identity was stolen to obtain prescription pharmaceuticals or medical equipment	60%
My identity was stolen so the thief could obtain fraudulent credit accounts in my name	12%
My healthcare records were accessed or modified	23%
My credit report was accessed or modified	18%
Don't know	4%
Total	231%

Q17. How did you learn about the medical identity theft?	FY 2013
Collection letter	24%
Adverse entry on my credit report	11%
Errors posted to medical invoices by my healthcare provider	25%
Errors in Explanation of Benefits from health insurer	26%
Uncovered mistakes in health records	29%
An alert from a healthcare provider	6%
Healthcare provider informed me during an office visit or medical treatment	13%
Data breach notification	3%
Other (please specify)	0%
Total	137%

Q18. When did you learn you were a victim of medical identity theft?	FY 2013
Almost immediately	0%
Less than 1 week after the incident	0%
Less than 1 month after the incident	4%
Less than 3 months after the incident	14%
Less than 6 months after the incident	20%
Less than 1 year after the incident	18%
Less than 2 years after the incident	15%
More than 2 years after the incident	6%
Don't know	23%
Total	100%

Q19a. Once you became aware of the incident, did you or someone in your immediate family report the medical identity theft to law enforcement or other legal authorities?	FY 2013
Yes	43%
No	57%
Total	100%

Q19b. If no, why wasn't the medical identity theft incident reported?	FY 2013
I know the thief and do not want to report him or her	48%
I did not want to alarm my family	4%
I did not think the police would be of any help	50%
I did not have the time to file a police report	5%
I was not harmed by the incident and didn't want to make it a big deal	36%
I was embarrassed	30%
Don't know	29%
Total	202%

Q20. To the best of your knowledge, how did this medical identity theft happen? Please select only one most likely cause.	FY 2013
I lost a wallet containing personal identification or medical credentials	3%
The identity thief intercepted a statement or invoice mailed to my address	5%
Email correspondence containing medical information was intercepted online by the identity thief	0%
I inadvertently provided my personal information to a fake email or spoofed website (phishing attack)	8%
An employee working in the healthcare provider's office stole my health information	5%
My health care provider used my ID to conduct fraudulent billing	
My health care provider, insurer or other related organization had a data breach	7%
A member of the family took my personal identification or medical credentials without my consent	28%
I shared my personal identification or medical credentials with someone I know	30%
Don't know	14%
Total	100%

Q21a. What were the **financial** consequences of the medical identity theft incident? Please select the top two choices only.	FY 2013
Lost time and productivity trying to fix inaccuracies in credit report	23%
Employment-related difficulties resulting from inaccuracies in credit report or health records	6%
Revocation of licenses because of inaccuracies in health records	0%
Financial identity theft such as fraudulent bills or credit card accounts	19%
Diminished credit score	20%
Incurred legal fees	17%
Other (please specify)	2%
None	35%
Total	122%

Q21b. What were the **medic**al consequences of the medical identity theft incident? Please select the top two choices only.	FY 2013
Lost trust and confidence in my healthcare provider	56%
Misdiagnoses of illness because of inaccuracies in health records	15%
Mistreatment of illness because of inaccuracies in health records	13%
Wrong pharmaceuticals prescribed	11%
Delay in receiving medical treatment because of inaccuracies in health records	14%
Other (please specify)	0%
None	32%
Total	141%

Q21c. What were the **health insurance** consequences of the medical identity theft incident? Please select the top two choices only.	FY 2013
Increased health insurance premiums as a result of inaccuracies in health records	7%
Loss of health insurance as a result of the medical identity theft	39%
Out-of-pocket payments to health plan or insurer to restore coverage	43%
Other (please specify)	0%
None	45%
Total	134%

Q22a. Did you or your immediate family members resolve the identity theft incident?	FY 2013
Yes, completely resolved	11%
No, but I am in the process of resolving this incident	39%
No, nothing has been done as yet to resolve the incident	50%
Total	100%

Q22b. If yes, how did you resolve this medical identity theft? Please select all that apply.	FY 2013
Paid healthcare provider (or repaid insurer) for services obtained by the thief	40%
Engaged an identity protection service provider to help me resolve the incident	15%
Worked with my healthcare provider to help me resolve the incident	31%
Worked with my health plan and/or insurer to help me resolve the incident	35%
Obtained and carefully reviewed credit reports	19%
Contacted credit bureaus to fix inaccuracies in my credit report	11%
Engaged legal counsel to help me resolve the incident	9%
Engaged a non-profit organization that provides consumer assistance and support (such as the Identity Theft Resource Center)	5%
Total	165%

Q22c. If yes, how long did it take you or your immediate family members to resolve this medical identity theft incident?	FY 2013
Less than 1 month	0%
Less than 3 months	6%
Less than 6 months	10%
Less than 1 year	13%
Less than 2 years	12%
More than 2 years	11%
Not resolved as yet	48%
Total	100%

When responding to the following question, please include in your calculation of total cost the following: (1) Money spent on identity protection, credit reporting and legal counsel; (2) All out-of-pocket costs for medical services and medications because of lapse in healthcare coverage; (3) All reimbursements to healthcare providers to pay for services provided to imposters.

Q23. Approximately, what were the **costs** incurred in trying to resolve the medical identity theft incident? From the table below, please select one cost range for each one of the three cost categories presented.

Q23a. Money spent on identity protection, credit reporting and legal counsel	FY 2013
None	65%
Less than $100	3%
$101 and $1,000	2%
$1,001 and $5,000	1%
$5,001 and $10,000	1%
$10,001 and $25,000	15%
$25,001 and $50,000	11%
$50,001 and $100,000	2%
Greater than $100,000	0%
Total	100%

Q23b. All out-of-pocket costs for medical services and medications because of lapse in healthcare coverage	FY 2013
None	66%
Less than $100	12%
$101 and $1,000	4%
$1,001 and $5,000	3%
$5,001 and $10,000	5%
$10,001 and $25,000	1%
$25,001 and $50,000	5%
$50,001 and $100,000	3%
Greater than $100,000	1%
Total	100%

Q23c. All reimbursements to healthcare providers to pay for services provided to imposters	FY 2013
None	60%
Less than $100	3%
$101 and $1,000	8%
$1,001 and $5,000	14%
$5,001 and $10,000	6%
$10,001 and $25,000	5%
$25,001 and $50,000	2%
$50,001 and $100,000	1%
Greater than $100,000	1%
Total	100%

Q24. Approximately, how much time did you and your immediate family members spend trying to resolve this medical identity theft incident?	FY 2013
None	5%
Less than 5 hours	8%
5 and 10 hours	3%
11 and 20 hours	2%
21 and 30 hours	6%
31 and 40 hours	3%
41 and 50 hours	11%
51 and 100 hours	17%
More than 100 hours	45%
Total	100%

Q25. What steps are you or your immediate family members taking to prevent future medical identity theft incidents? Please check all that apply.	FY 2013
Engage identity protection service provider	11%
Monitor credit reports	23%
Closely review medical records	33%
Seek health care providers and insurers with better privacy and security practices	8%
Ensure medical reports are with security conscious vendors	5%
Implement security precautions to protect personal credentials	13%
Shred confidential documents	12%
Avoid Internet transactions involving confidential information	6%
Never share medical insurance ID/credential with anyone	
Review Explanation of Benefits more carefully	39%
Other (please specify)	0%
No new steps taken	50%
Total	200%

Part 5. Demographics	
D1. What best describes your present health plan?	FY 2013
Private insurance	42%
Medicare or Medicaid	24%
Government or VA	5%
Coop plan	3%
Health savings account	5%
Not insured	21%
Total	100%

D2. What is your highest level of education attained?	FY 2013
High School	28%
Vocational	23%
College or University	43%
Post Graduate	5%
Doctorate	1%
Total	100%

D3. What best describes your present employment status?	FY 2013
Full time employee	53%
Part time employee	11%
Business owner/partner	5%
Stay-at-home parent	11%
Retired	7%
Military	0%
Student	5%
Unemployed	8%
Total	100%

D4. Approximately, what is your total household income?	FY 2013
Less than $30,000	24%
$30,001 to $50,000	25%
$50,001 to $80,000	15%
$80,001 to $100,000	15%
$100,001 to $150,000	10%
$150,001 to $200,000	6%
$200,001 to $300,000	3%
$301,000+	2%
Total	100%

D5. Gender:	FY 2013
Female	51%
Male	49%
Total	100%

D6. Geographic region in the United States [state pull down menu], or region:	FY 2013
Northeast	20%
Mid-Atlantic	19%
Midwest	17%
Southeast	13%
Southwest	12%
Pacific-West	19%
Total	100%

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**,we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.