Ponemon INSTITUTE

Third Annual Survey on Medical Identity Theft

Sponsored by Experian's ProtectMyID®

Independently conducted by Ponemon Institute LLC

Publication Date: June 2012

Third Annual Survey on Medical Identity Theft

Presented by Ponemon Institute, June 2012

Part 1: Executive Summary

We are pleased to present the findings of the *Third Annual Survey on Medical Identity Theft* conducted by Ponemon Institute and sponsored by Experian's ProtectMyID®. This annual study on medical identity theft is designed to determine how pervasive this crime is in the United States and how it has affected consumers.

In this year's study, we also focused on the importance of healthcare privacy, what consumers would do if they lost trust in the healthcare providers' ability to protect medical records and what is critical in managing the privacy of healthcare records. For purposes of this study, we define medical identity theft as occurring 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.

We surveyed 807 consumers who have self-reported that they had their identity stolen. From the group of identity theft victims participating in this study, 757 say they or their immediate family members have been victims of medical identity theft. This is an increase from last year's sample involving 708 who said they or their immediate family members had their healthcare credentials stolen. In 2010, 716 reported being a victim.

In this year's study, 44 percent of respondents have private insurance, a decrease from 52 percent in 2010. Twenty-one percent have Medicare or Medicaid and 20 percent are not insured. The remaining respondents have government, coop plans or health savings accounts. The percentage of uninsured in 2010 was 13 percent and 22 percent in 2011.

Medical identity theft continues to rise in the United States

Table 1 summarizes our research findings and provides a preliminary extrapolation on the total cost of medical identity theft in the United States over the past three years. In 2012, we assume there are 272 million adult-aged consumers who reside in the US. We then estimate that medical identity theft occurs at a rate of .0068 (.68%) of the total US population, which results in 1.85 million Americans affected by this crime.[1] Our estimate for 2011 was 1.49 million.

Using a mean total cost of $22,346 per incident derived from survey responses, we estimate the economic impact of medical identity theft in the United States at $41.3 billion per annum.[2] This represents a substantial increase from 2011 where we estimated a total cost based on mean value of $30.9 billion dollars. The economic impact using a median sample value in 2011 and 2012 is $7.8 billion and $11.6 billion, respectively.

Table 1. Extrapolated U.S. economic impact	FY 2010	FY 2011	FY 2012
Adult-aged U.S. citizens and residents (millions)	269	271	272
Computed base rate for medical identity theft	0.53%	0.55%	0.68%
Number of people affected by medical identity theft (millions)	1.42	1.49	1.85
Extrapolated average cost per victim ($)	20,160	20,663	22,346
Extrapolated median cost per victim ($)	5,000	5,250	6,250
Impact based on mean value per annum ($billions)	28.6	30.9	41.3
Impact based on median value per annum ($billions)	7.1	7.8	11.6

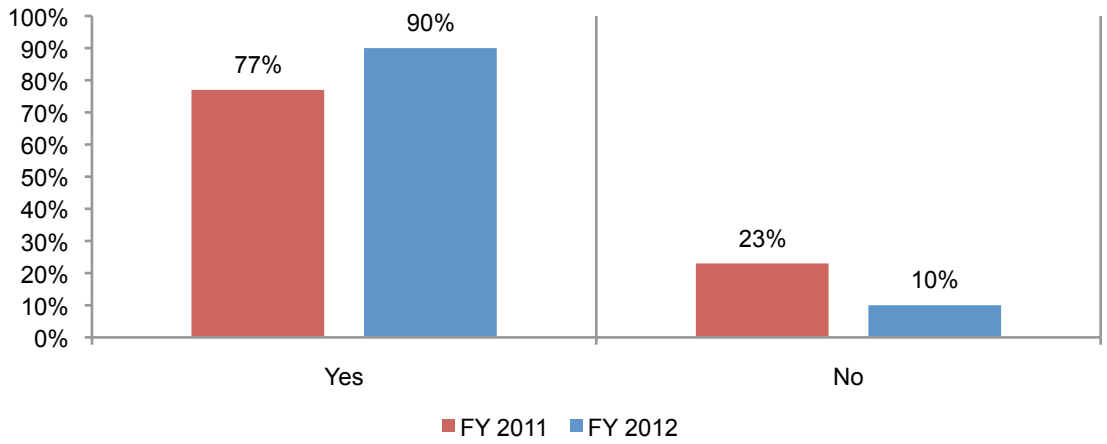
[1]The base rate percentage is determined by the number of respondents from a general adult-aged sample of US residents who self-reported they or their immediate family have been victims of medical identity theft.
[2]The estimated total cost includes all money and value of time spent responding to and resolving the medical identity theft incident.

Part 2: Key Findings

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 three years we have included them in this report.

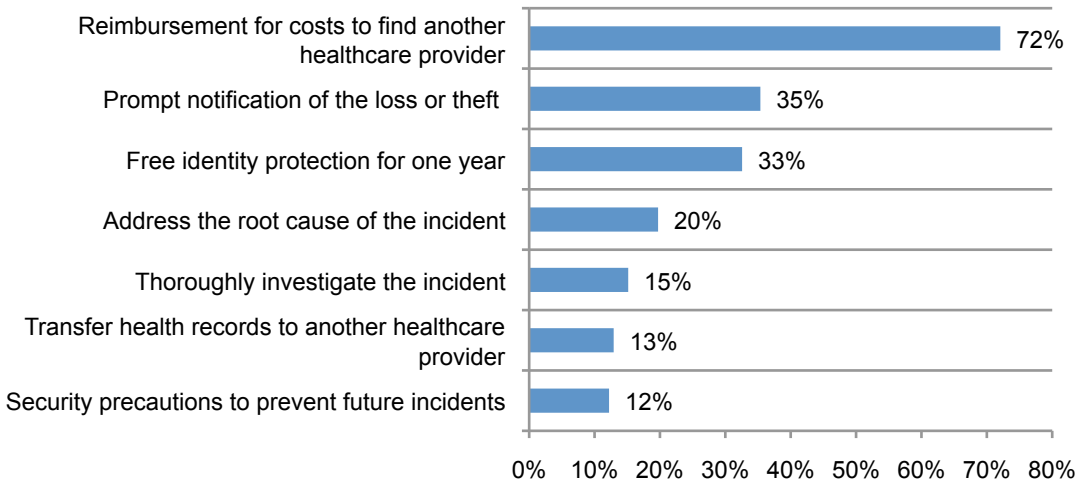
The percentage of participants who understand the definition of medical identity theft has increased from last year. In previous studies, many respondents may have heard about medical identity theft but could not define the crime. This year, 90 percent of identity theft victims in our study report that they knew the definition before taking this survey. This is an increase from 77 percent in last year's survey, as shown in Figure 1.

Figure 1. Knowledge of the definition of medical identity theft



If notified that their medical records were lost or stolen, respondents would want the healthcare provider to reimburse them for what they paid to find another provider. Figure 2 reveals the top three actions desired by respondents following a medical identity theft. These are: reimbursement for costs to change to another healthcare provider, notification within 30 days of the loss or theft and free identity protection for one year.

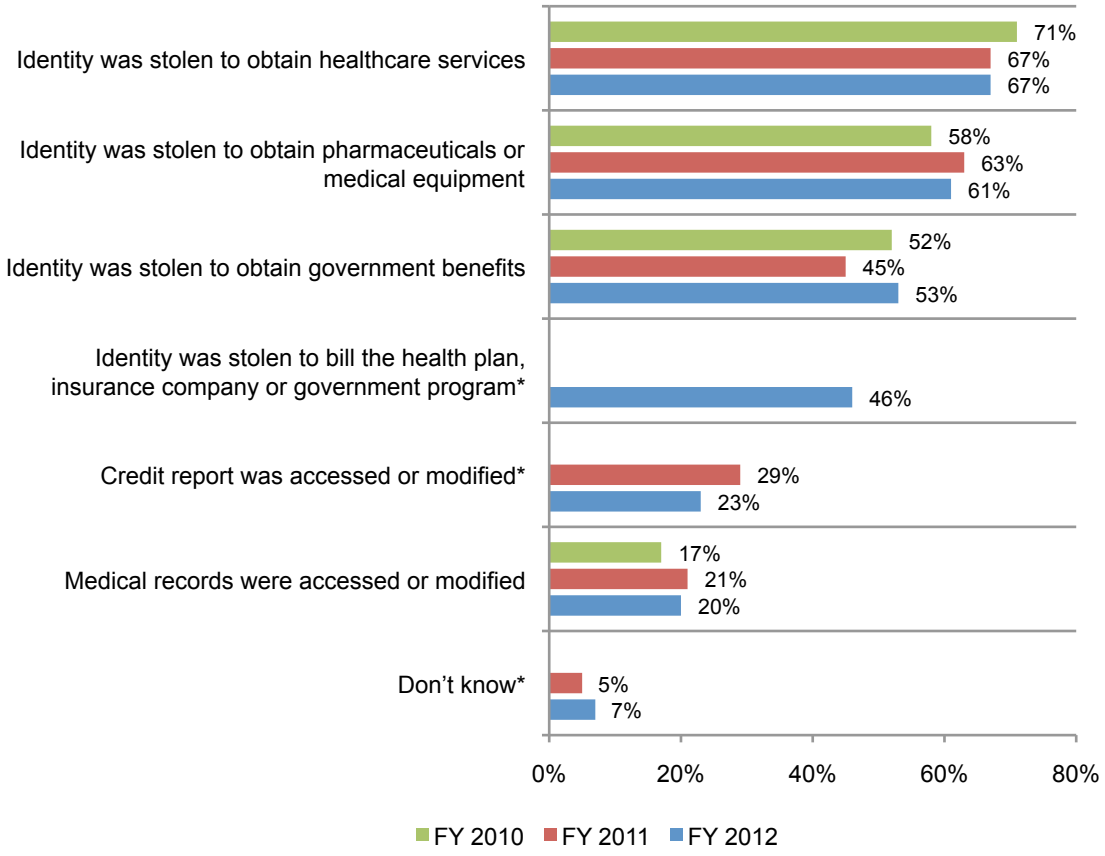
Figure 2. Actions to be taken if notified that medical records were lost or stolen
Two choices permitted



Stolen credentials are most often used to obtain healthcare services, prescriptions or medical equipment. As shown in Figure 3, this finding is consistent since 2010. In this year's study, respondents report that their identity was stolen to obtain healthcare services or treatments (67 percent), prescription pharmaceuticals or medical equipment (61 percent) or government benefits, including Medicare or Medicaid (53 percent).

Only 23 percent say their credit report was accessed or modified and 20 percent say their medical records were accessed or modified. New to this year's study is the finding that 46 percent say their identity was stolen to bill the health plan, insurance company or government program.

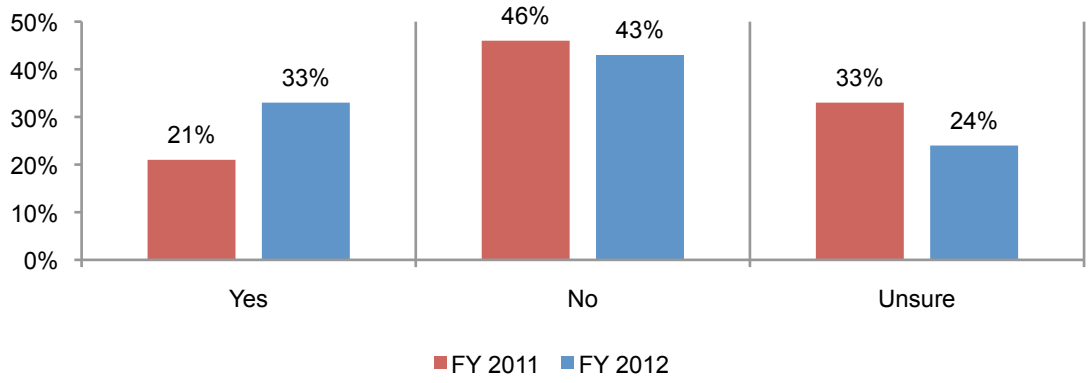
Figure 3. Description of medical identity theft incident
More than one choice permitted



* This choice was not available for all survey years

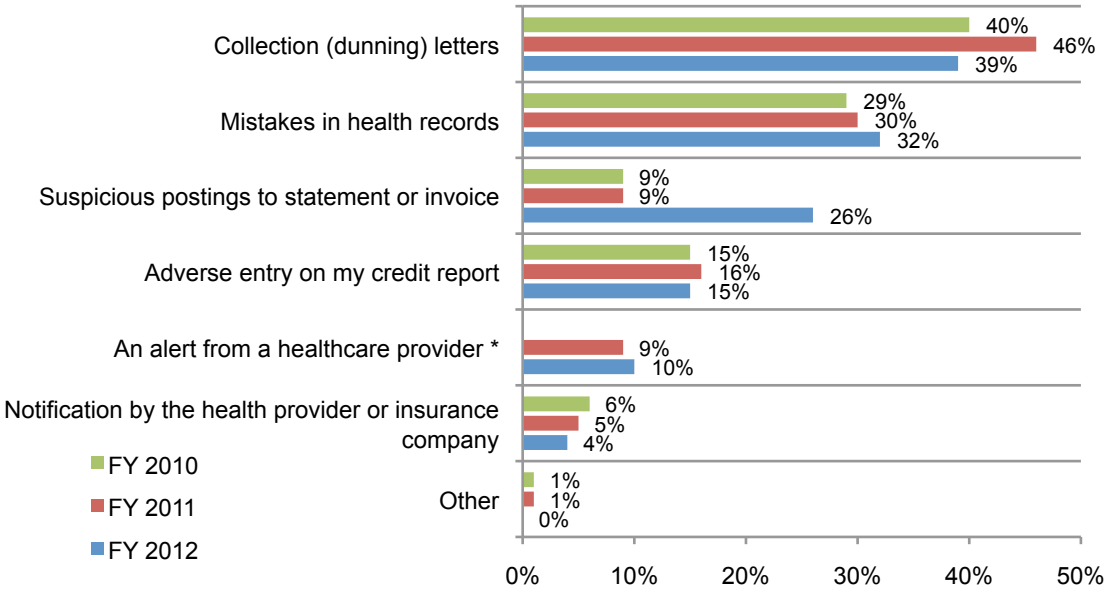
Awareness that medical identity theft can affect credit scores increased slightly from last year. According to Figure 4**,** one-third of all respondents know that their credit score is at risk when they became a victim of medical identity theft. This is an increase from 21 percent in 2011. However, 67 percent did not know this or are unsure. Last year, 79 percent did not know or were unsure. Medical identity theft often results in collections accounts being opened in the victim's name, thus potentially affecting his or her credit scores.

Figure 4. Medical Identity theft affects credit score



Notification of identity theft comes in the form of a collection letter. Figure 5 shows that in the 2010, 2011 and 2012 studies, collection letters are still the number one way of learning about the crime (40 percent, 46 percent and 39 percent, respectively). However, more respondents are learning about the theft from suspicious postings to statements and invoices. This has increased from nine percent to 26 percent. Thirty-two percent say it is mistakes in health records that alerted them to the theft, an increase from 30 percent last year. This seems to indicate that there is more awareness of the importance of carefully reviewing invoices and records from healthcare providers. Especially since only 4 percent this year and 5 percent last year said they found out about the theft from the healthcare provider or insurance company.

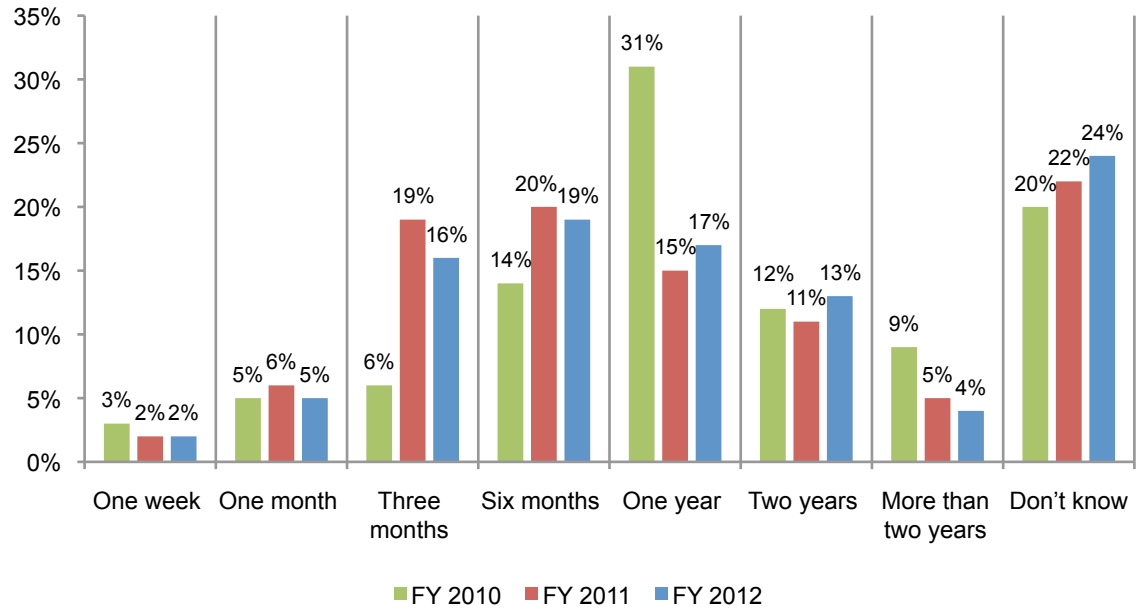
Figure 5. Methods of learning about identity theft
More than one choice permitted



* This choice was not available for all survey years

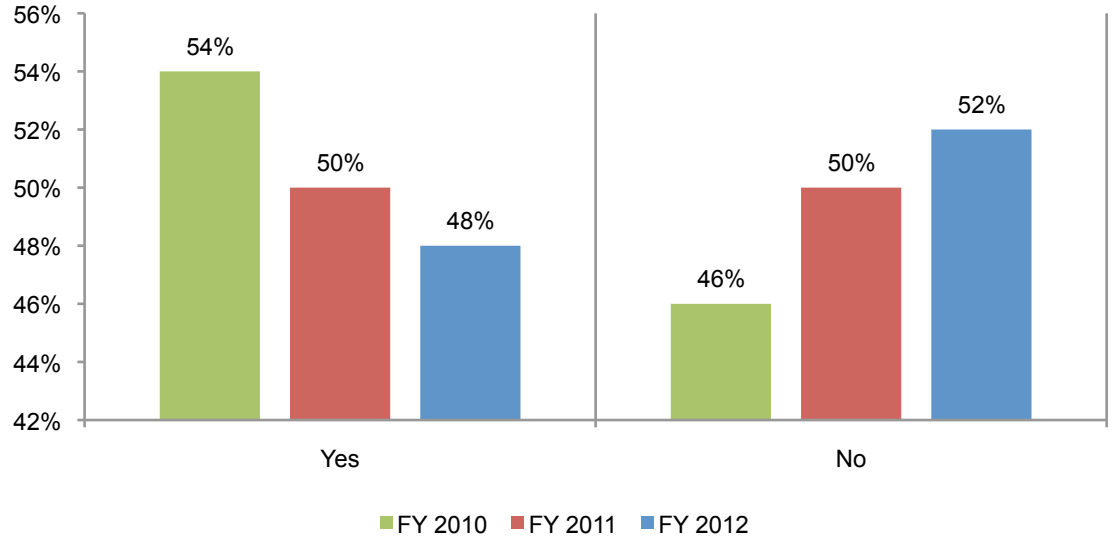
Respondents find it difficult to pinpoint when the crime occurred. When asked when they learned about the incident, 24 percent say they do not know, according to Figure 6. Thirty-four percent say it was one year or later when they found out. Last year, 31 percent said it was one year or more. Since 2010, time to notify has improved. That year, 52 percent said it took more than one year to find out.

Figure 6. Length of time it took to be notified of identity theft



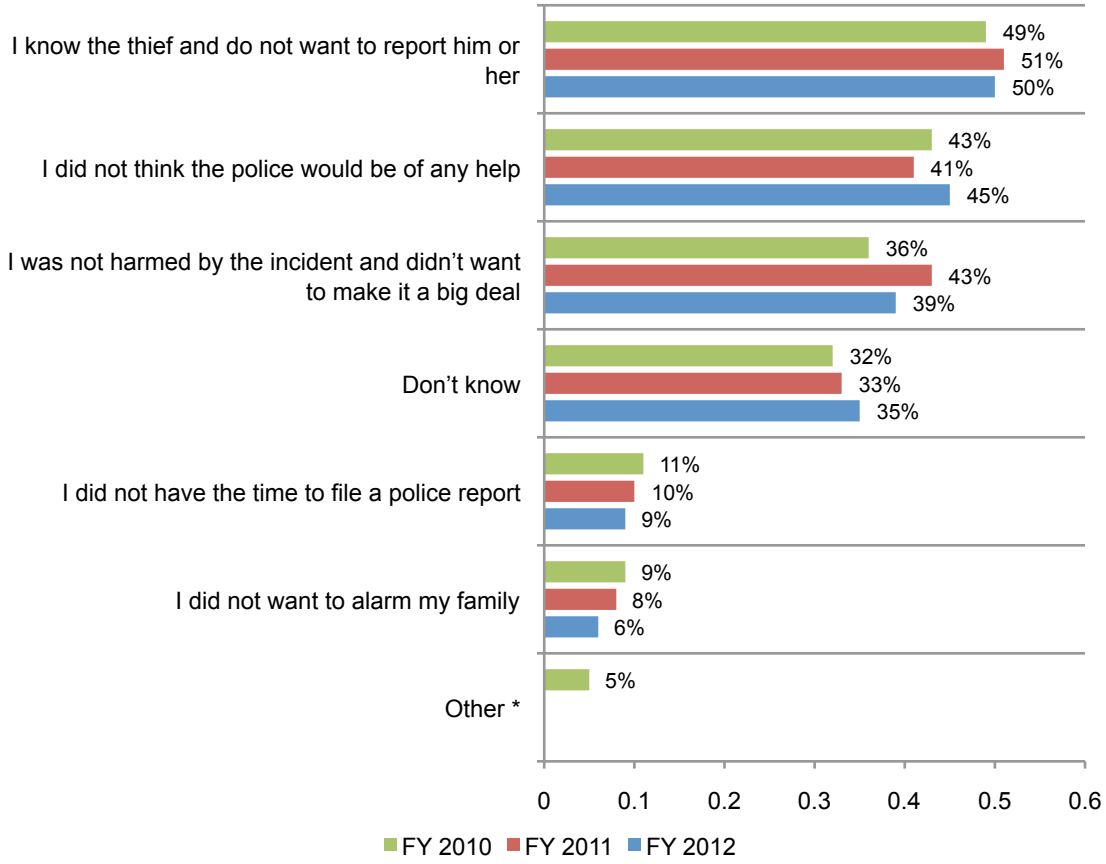
There appears to be reluctance in reporting medical identity theft to law enforcement or other legal authorities. As shown in Figure 7**,** 52 percent say they did not report the crime to law enforcement or other legal authorities. This is a slight increase from 50 percent last year. In 2010 it was 46 percent of respondents who did not contact law enforcement.

Figure 7. Reporting of medical identity theft to law enforcement



The main reason in all three years is that they know the thief and do not want to report him or her (Figure 8). This is followed by doubts that the police would be of any help, there was no harm and don't know.

Figure 8. Reasons the incident is not reported
More than one choice permitted

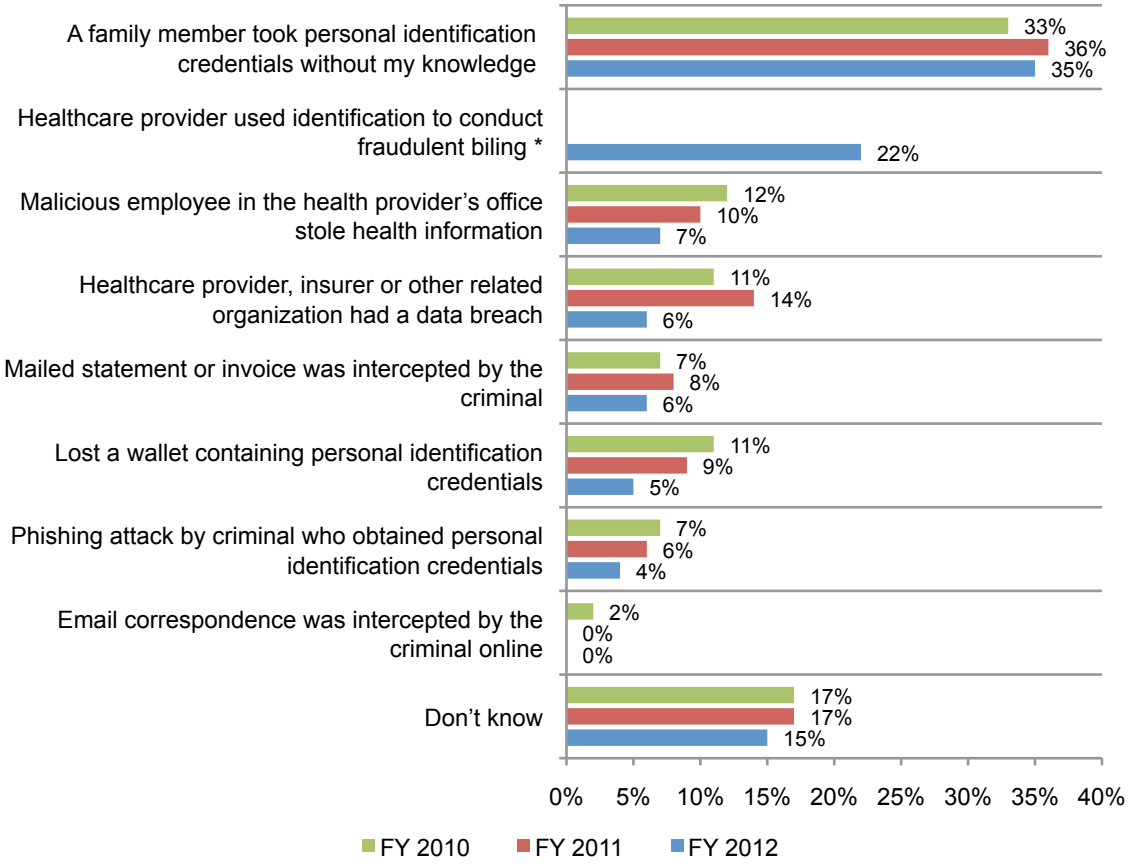


* This choice was not available for all survey years

Medical identity theft continues to be a family affair.

Figure 9 reveals that a family member's theft was the one most likely cause of the crime, according to 35 percent of consumers surveyed this year. Last year 36 percent said a member of the family took their personal identification credentials without their knowledge and in 2010 it was 33 percent of respondents. In this year's study, 22 percent say that the healthcare provider used their identification to conduct fraudulent billing and 15 percent do not know the cause.

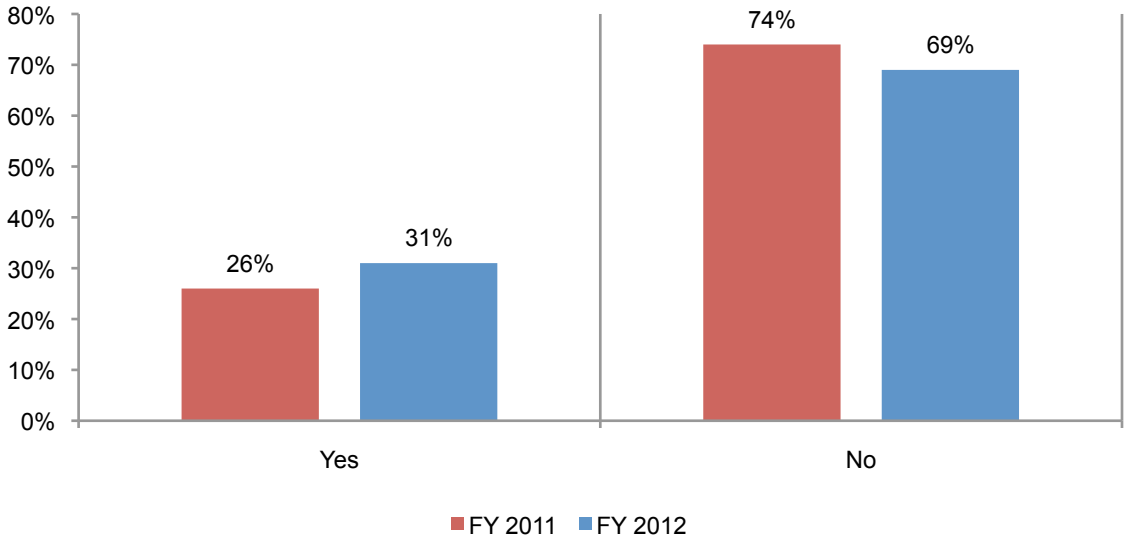
Figure 9. Causes of identity theft



* This choice was not available for all survey years

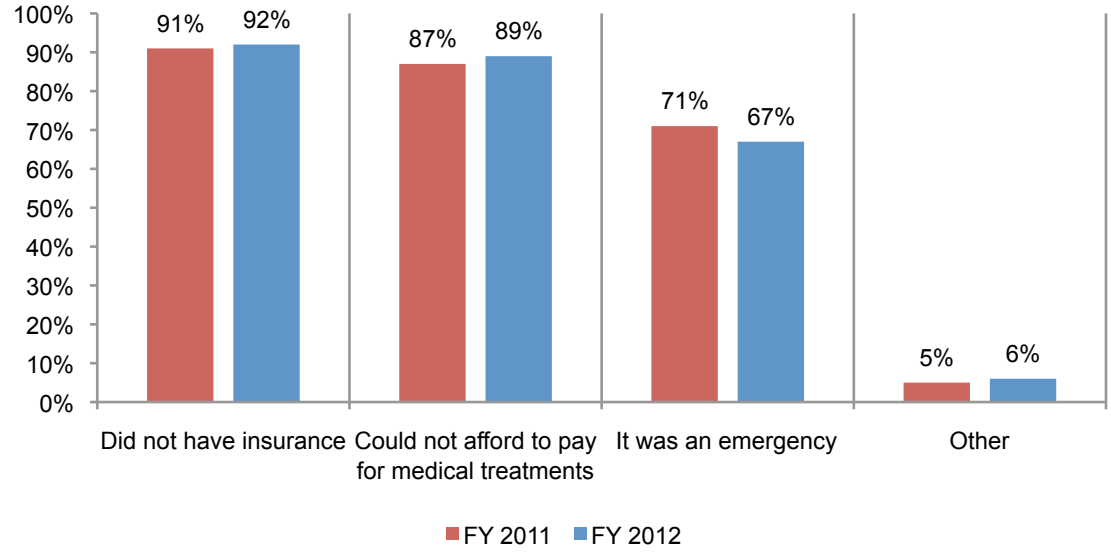
When asked if they had ever shared their personal identification with a family member in order to obtain medical services, 31 percent of respondents said they did. This suggests an increase from 26 percent in last year's study. Please note, however, the sharing of these credentials may or may not have been the cause of the identity theft reported by respondents.

Figure 10. Respondent shared identity credentials with family member



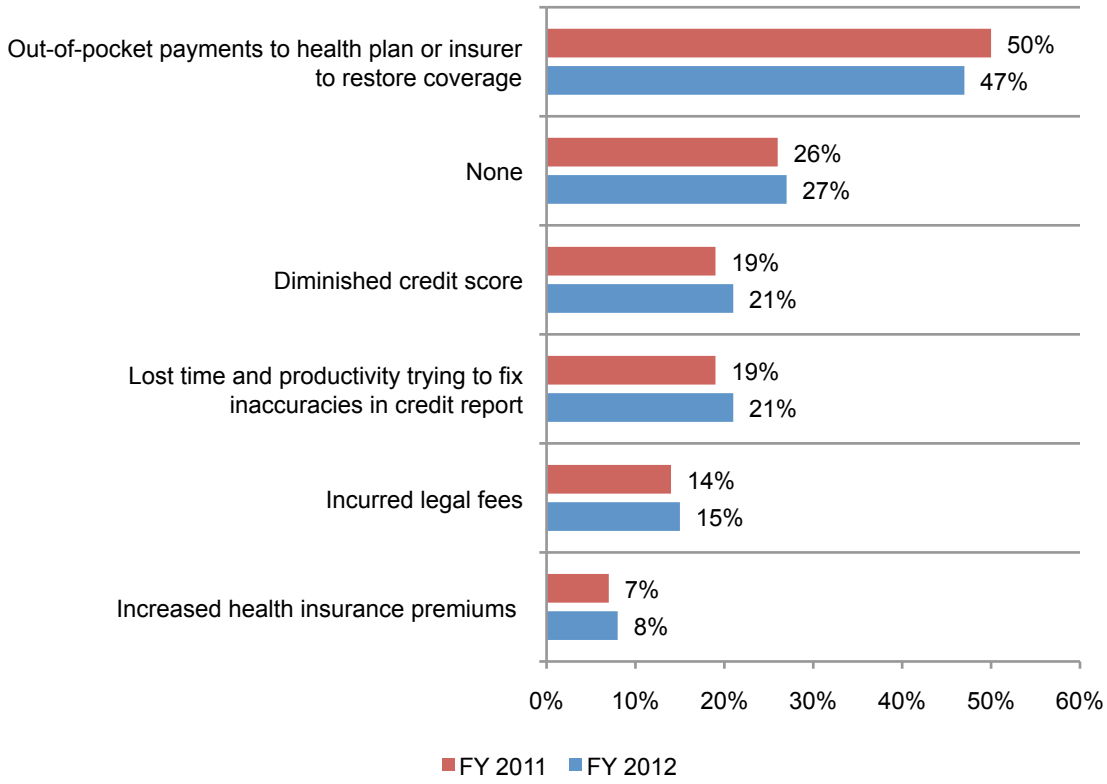
The main reason for sharing credentials is that the family member did not have insurance and could not afford to pay for the medical treatments, as shown in Figure 11. This was the case in last year's study as well. Fifty percent say they did this only once. However, 25 percent cannot recall how often they shared their personal information. This is also consistent with last year's findings.

Figure 11. Reason for sharing personal identification
More than one choice permitted



The financial consequence most often reported was the out-of-pocket payments to health plan or insurer to restore coverage. Figure 12 reveals that 47 percent say they had to pay the health plan or insurer. However, 27 percent say there were no financial consequences. This is followed by 21 percent who say they lost time and productivity trying to fix inaccuracies in credit reports and another 21 percent say it diminished their credit score. In 2011, 50 percent said they made out-of-pocket payments and 26 percent said they had no financial consequences.

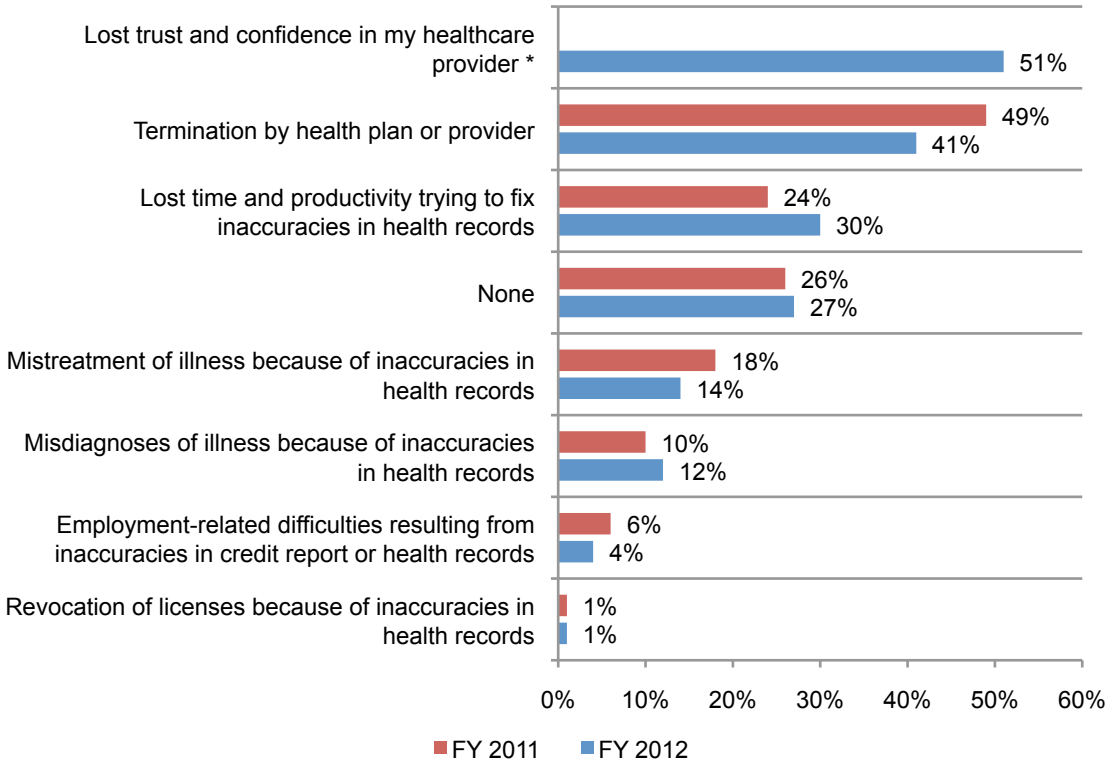
Figure 12. Financial consequences of the medical identity theft
Two choices permitted



The primary non-financial consequence is a loss of trust and confidence in their health care provider, according to 51 percent of respondents. According to Figure 13, this is followed by termination by health plan or provider (41 percent of respondents). Twenty-seven percent say there were no non-financial consequences from the medical identity theft.

In 2011, 49 percent said that termination by health plan or provider was one of the primary non-financial consequences followed by 26 percent who said there were no non-financial consequences.

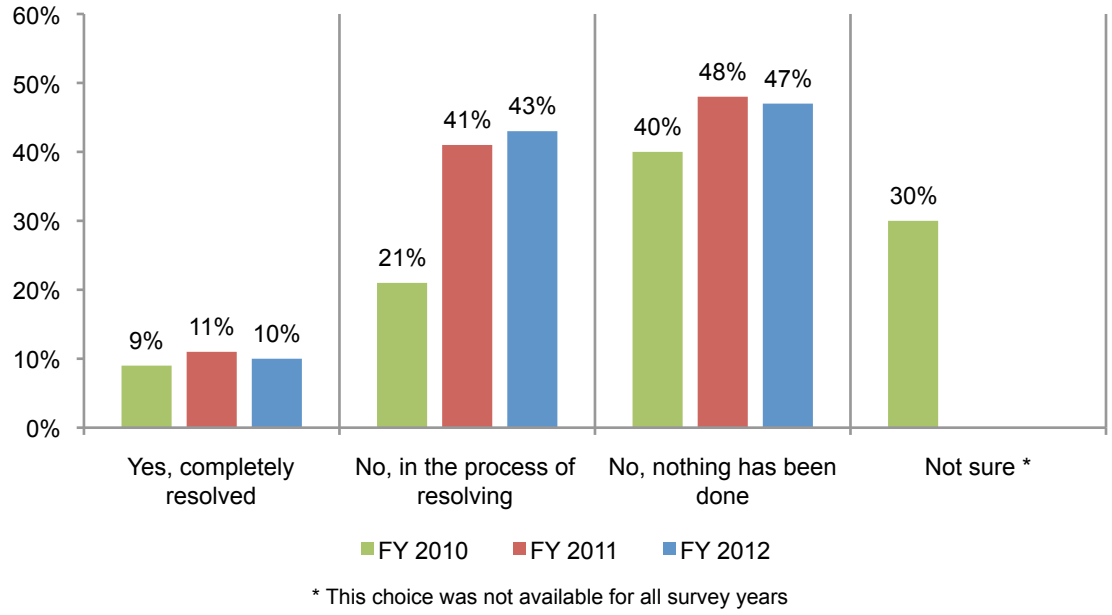
Figure 13. Non-financial consequences of the medical identity theft
Two choices permitted



* This choice was not available for all survey years

Very few are able to resolve the consequences of medical identity theft. Figure 14 reveals that only 10 percent say they have completely resolved the consequences of the theft. Last year 11 percent said they were able to do what was necessary and in 2010 it was only nine percent. Forty-seven percent say they have not done anything to resolve the consequence. Last year, 48 percent said nothing was done. This is an increase from 40 percent in 2010.

Figure 14. Resolution of the identity theft

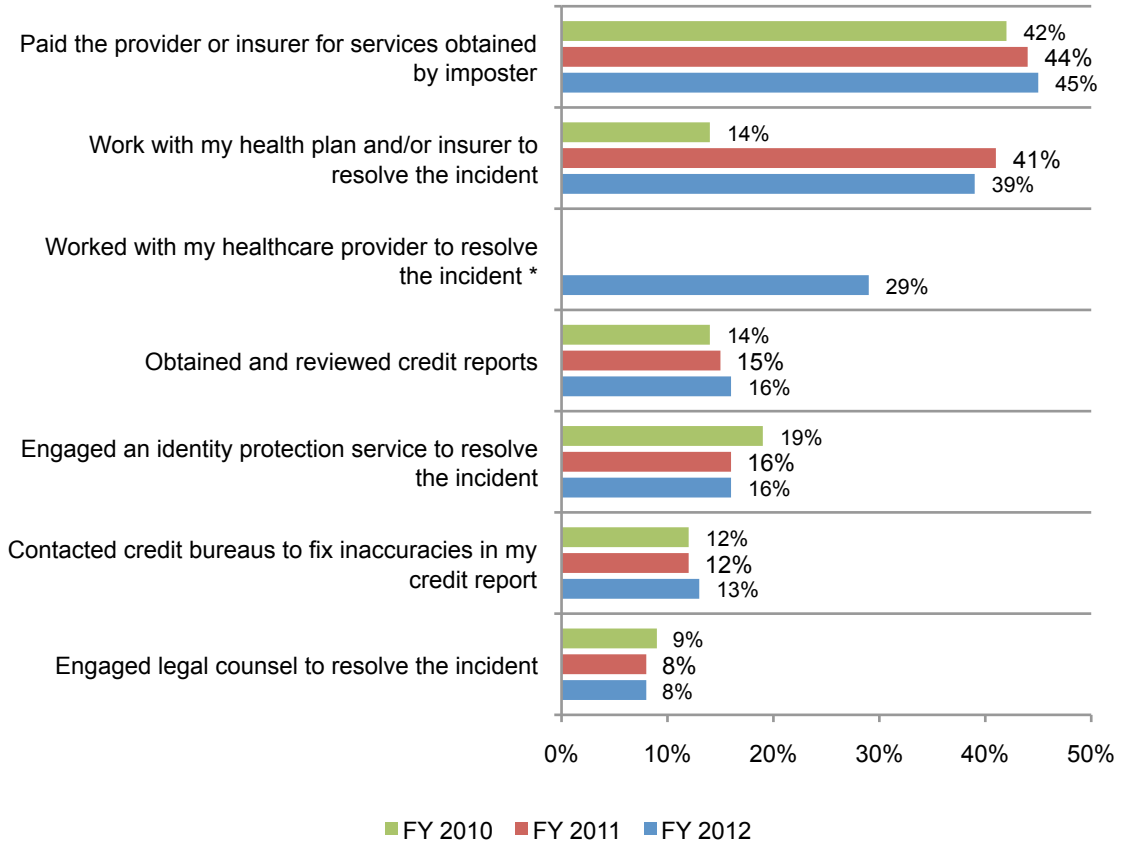


* This choice was not available for all survey years

Reimbursement to the healthcare provider was the primary method used to resolve the theft. According to Figure 15, 45 percent paid the healthcare provider or insurer for services obtained by imposter. This is followed by working with the health plan and/or insurer to help resolve the incident and working with their healthcare provider to help me resolve the incident. It is interesting to note than in 2010 only 14 percent of respondents said they worked with healthcare providers to resolve the theft.

What is not shown in the Figure is that it took respondents 12.1 months (approximately one year) to resolve the theft. Twenty-five percent say it took more than two years to resolve the theft.

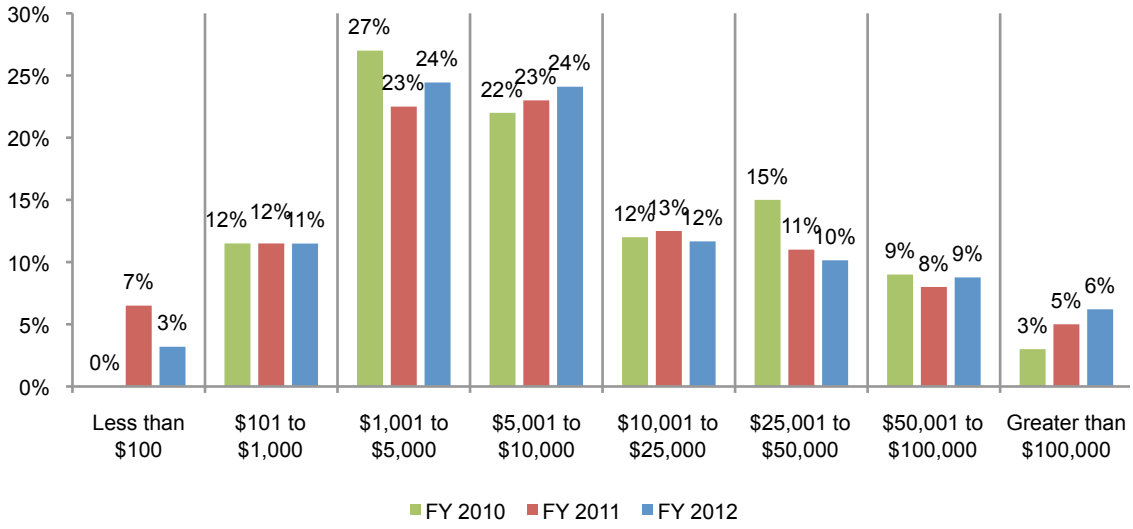
Figure 15. Methods to resolve identity theft
More than one choice permitted



* This choice was not available for all survey years

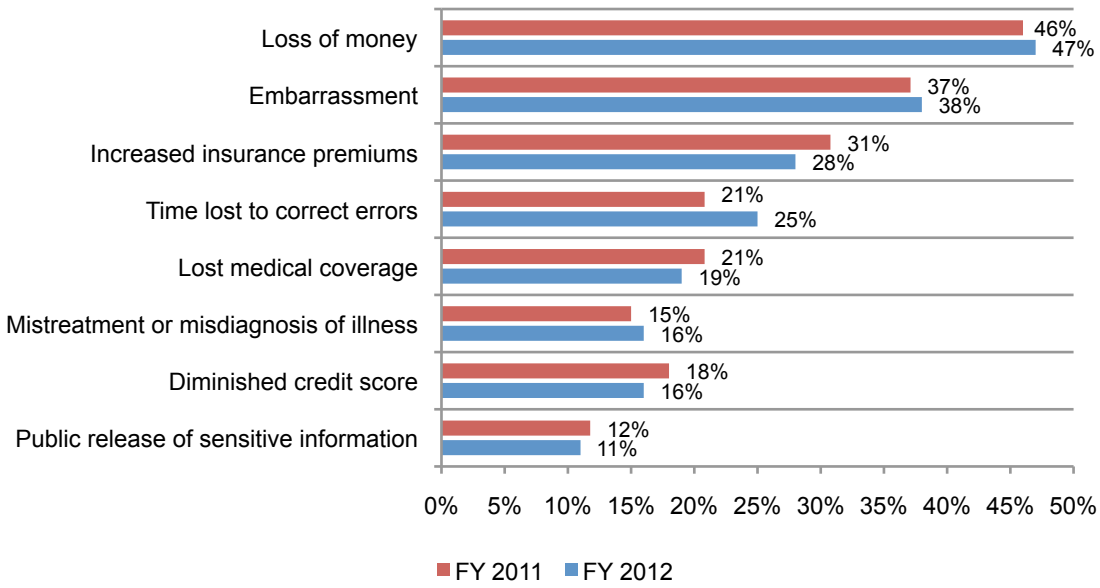
The cost of medical identity theft continues to grow. The extrapolated average cost of medical identity theft is estimated at $22,346 per victim.[3] In 2011 and 2010 the extrapolated costs were $20,663 and $20,160, respectively. In the context of this report, the total cost includes all money and time spent to respond and resolve the medical identity theft incident. Examples of out-of-pocket expenditures include legal services, payment for medical services and medications because of lapse in healthcare coverage; and all reimbursements to healthcare providers to pay for medical services, products or pharmaceuticals obtained by imposters.

Figure 16. Total dollars lost resolving medical identity theft



The biggest negative impact (see Figure 17), according to consumers surveyed, is the loss of money (47 percent of respondents) followed by embarrassment (38 percent of respondents). This finding is consistent with the 2011 findings, 46 percent and 37 percent of respectively.

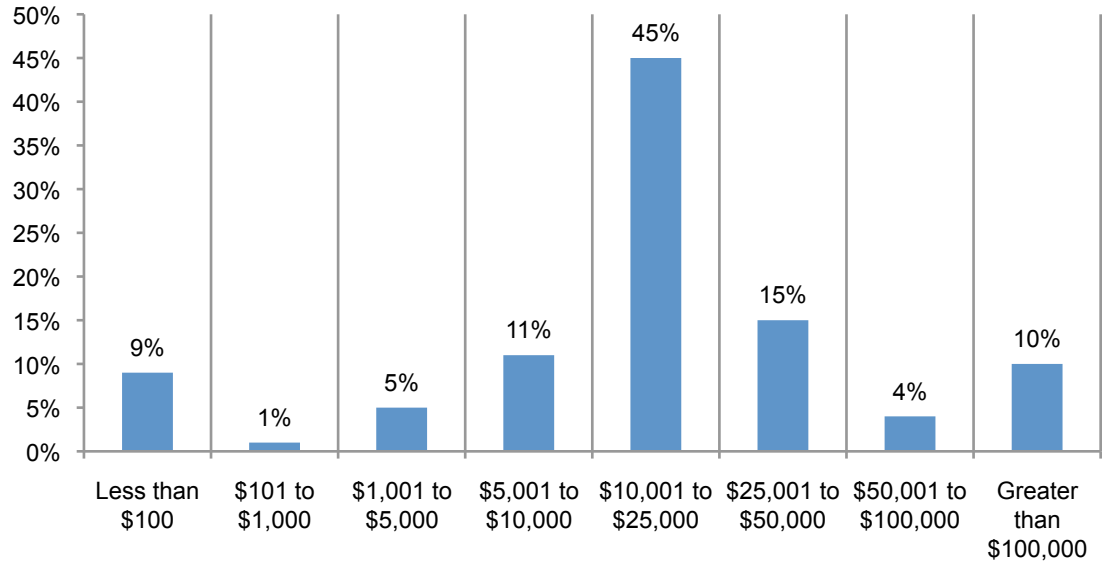
Figure 17. Two most negative impacts



[3]It is important to note that the median value for the 2012 cost estimate is $6,250. The lower median value occurs because the extrapolated average is influenced by a small number of extreme cost estimates.

The value of stolen services, products and pharmaceuticals is costing victims and the healthcare industry. Fifty-six percent of respondents can estimate the approximate value in "dollars" that the imposter obtained in terms of medical services, medical products and pharmaceuticals. For this group, the average value of medical services, medical products and pharmaceuticals was $29,464.[4] As shown in Figure 18, 10 percent of respondents say the total dollar value the thief obtained was in excess of $100,000.

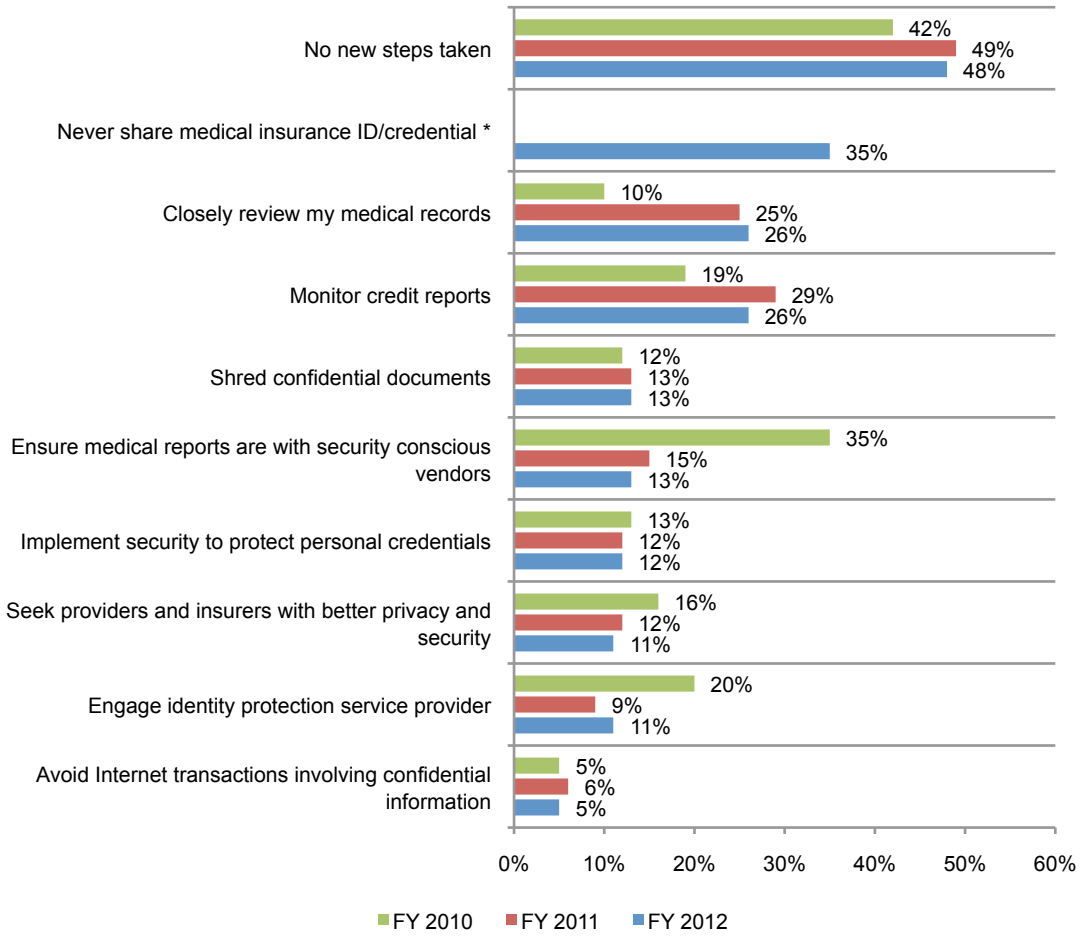
Figure 18. Estimated value of services and products thief obtained by imposters



[4]The median value for this series is $12,500, which is much lower than the computed mean.

Victims need to be more proactive. To prevent future incidents, respondents say they will never share medical insurance ID/credentials with anyone (35 percent) followed by monitoring credit reports (26 percent) and reviewing their medical records (26 percent). However, almost half (48 percent) say no new steps will be taken. As shown in Figure 19, in 2010 and 2011 it was 42 percent and 49 percent, respectively. However, as shown, more respondents are reviewing their medical records.

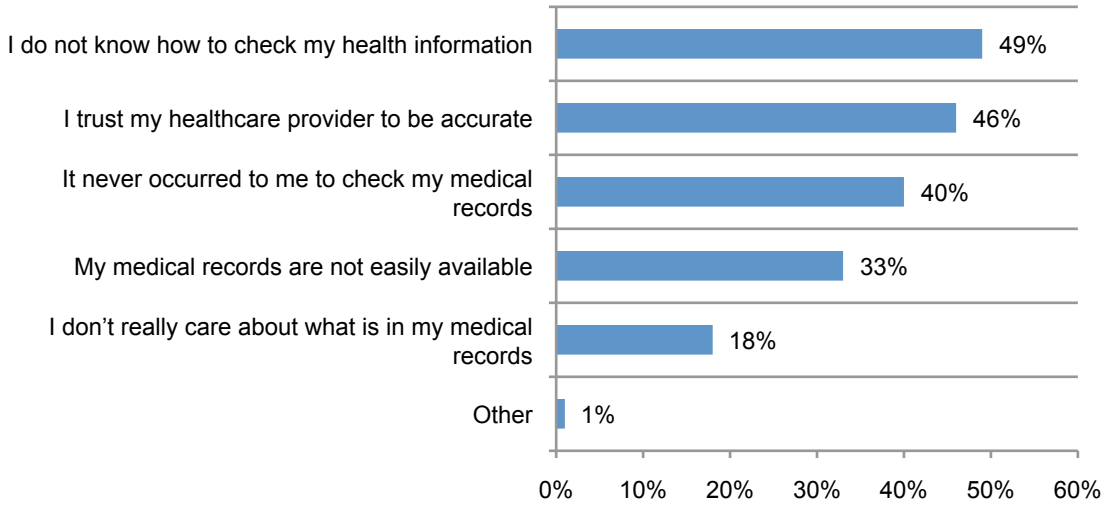
Figure 19. Steps taken to prevent medical identity theft
More than one choice permitted



* This choice was not available for all survey years

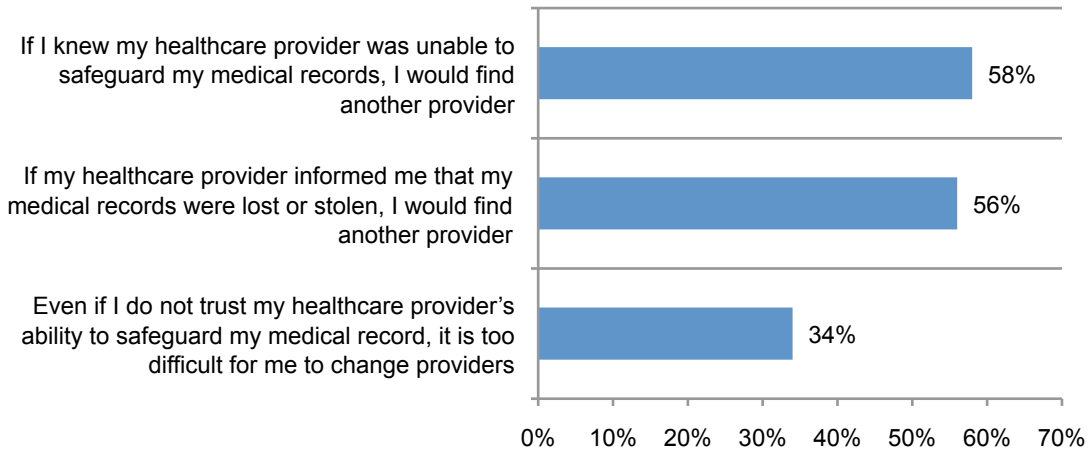
The majority of respondents do not check their medical records for accuracy. For the first time we asked respondents if they check their medical records for accuracy. Fifty-seven percent of respondents say they never check their medical records to determine if the health information about them is accurate. As shown in Figure 20, the primary reason for not doing this is that they do not know how to check their health information (49 percent of respondents) and 46 percent say they trust their health care provider to be accurate. Only 18 percent say they don't really care about what is in their medical records.

Figure 20. Primary reason medical records are not checked for accuracy
More than one choice permitted



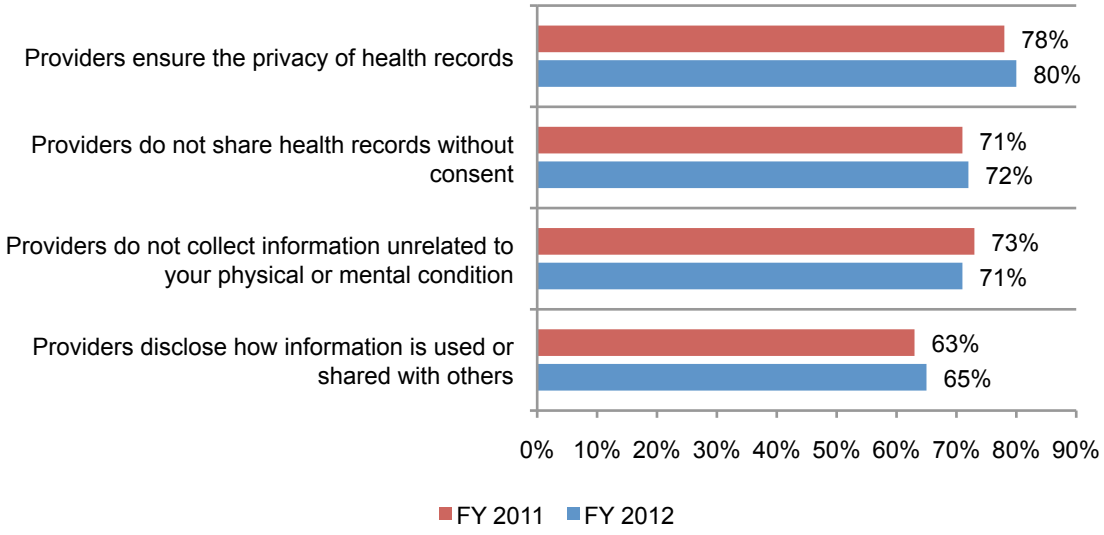
Safeguarding medical records is very important for the majority of respondents. Also new to this year's study is the issue of protecting medical records. According to Figure 21, more than half (58 percent of respondents) say they would change healthcare providers if they lost confidence in their ability to protect their information and 56 percent would look for another provider if their medical records were lost or stolen. Only 34 percent believe it would be too difficult to change providers if they lost trust in the provider's ability to protect medical information.

Figure 21. Attribution about safeguarding medical records
Strongly agree and agree response combined



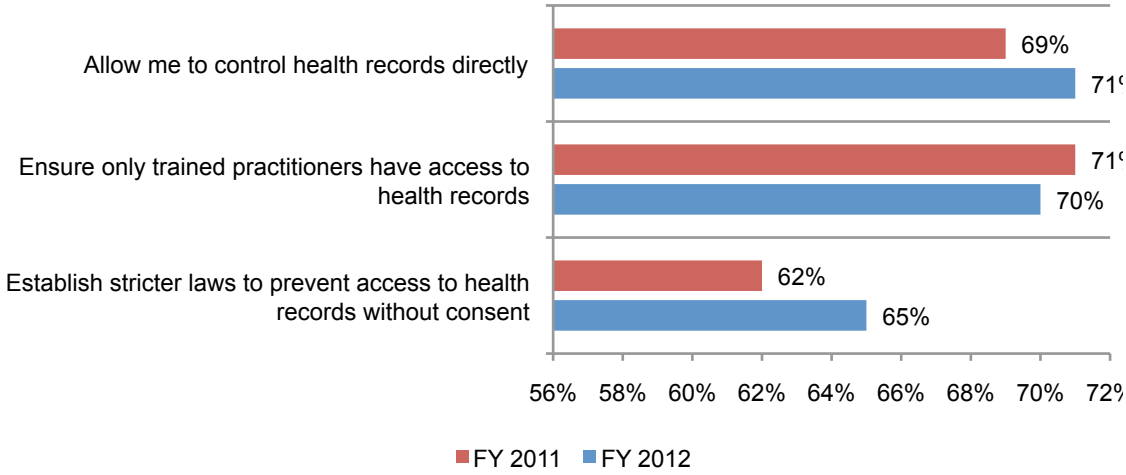
Respondents believe the privacy of health records is very important. According to Figure 22, 80 percent of respondents believe it is important to ensure the privacy of their health records. Seventy-one percent do not want to have information collected about them that is unrelated to their physical or mental condition and 72 percent say they do not want healthcare providers to share their health records with others without their consent. This finding is consistent with the 2011 study.

Figure 22. Attributions regarding healthcare providers
Very important and important response combined



Respondents would like to control their records directly or ensure only trained medical practitioners have access to their health records. As shown in Figure 23, the findings suggest that respondents want control over who can access their health records. Specifically, 71 percent believe it is important to control their health records directly and 70 percent say access should be limited to professionally- trained medical practitioners. Sixty-five percent would like to see stricter laws to prevent companies or government from accessing their health records without their consent. These findings are also consistent with the 2011 study.

Figure 23. Attributions about protecting healthcare records
Very important and important response combined



Part 3: Conclusion

This third annual study on medical identity theft reveals some interesting trends in how Americans are responding to this growing problem. Our results continue to suggest that this is an insidious crime because it is difficult to detect and resolve. However, more respondents are learning about the theft from suspicious postings to statements and invoices. Unfortunately, in many cases it is too late and as a result victims are experiencing significant financial consequences. To protect against this crime we recommend the following:

- 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.

The important thing to remember is that consumers are not helpless. The key is to be vigilant and act promptly if you suspect medical records are at risk. In conclusion, we hope the results of this annual study have heightened the awareness of this important consumer protection issue.

Part 4: Methods

A specialized sampling frame of 40,001 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 experience.[5] Table 1 shows 905 respondents completed the survey. After removing 98 surveys that failed reliability checks, the sample before screening was 807 surveys. Additional screening procedures removed 50 surveys resulting in a final sample of 757 respondents or a 2 percent response rate.

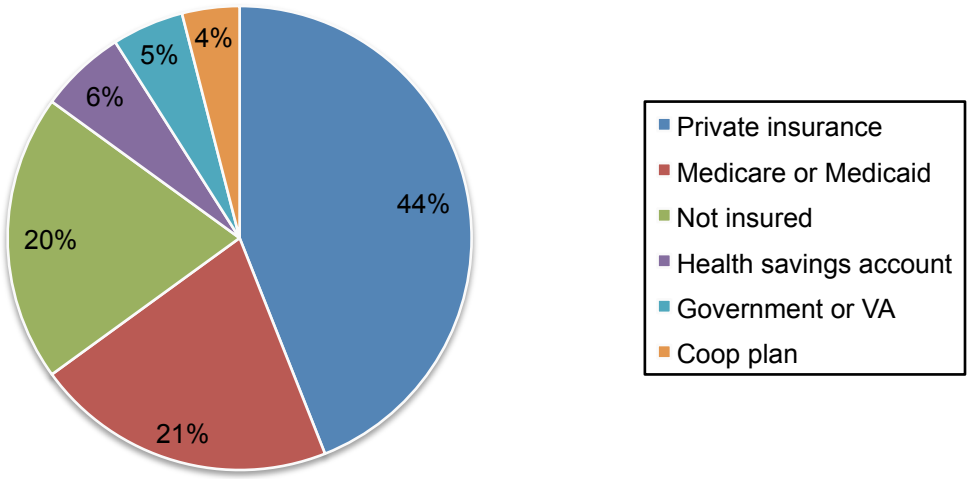
The medical identity theft base rate was determined from a second sampling procedure. Using a discovery sampling method, we randomly surveyed individuals to determine their status. Those that indicated a medical identity theft experience were included in the base rate group. We continued this sampling until we captured 10 bona fide medical identity theft victims.[6]

Table 1. Sample response*	FY 2012	FY 2011	FY 2010
Total sample frame	40,001	36,559	37,383
Invitations sent	36,570	35,998	34,500
Total returns	905	843	1109
Total rejections	98	68	113
Final sample	807	765	996
Medical ID theft victims	757	708	716
Response rate	2.0%	2.1%	1.9%
Medical identity theft base rate	0.068%	0.055%	0.053%

***Note**: The survey instrument and sampling plan has changed significantly from our first medical identity theft study completed in 2010. Therefore, a direct comparison of the 2010 data to the 2011 and 2012 results may not be possible.

Pie Chart 1 shows 44 percent of respondents in the present sample have some form of private insurance. In addition, 21 percent are on Medicare or Medicaid. Another 20 percent say they presently do not have health insurance.

Pie Chart 1. Respondents' current health insurance or plan



[5]The sampling frame of identity theft victims was developed from an original sample of adult-aged individuals residing in the U.S. created for the 2010 Medical Identity Theft Study. This specialized and proprietary sampling frame has been maintained and updated since its inception.
[6]In total, 14,706 individuals were sampled to discover 10 bona fide identity theft victims.

Table 2 shows the distribution of respondents according to their self-reported household income level. As shown, 49 percent of respondents in the 2012 sample report an income level below $50,000 per annum. The extrapolated average income level for the 2012 sample is $74,500, which is slightly lower than the income level for the 2011 sample (at $75,830).

Table 2. Approximately household income per annum	FY 2012	FY 2011	FY 2010
Less than $30,000	25%	22%	23%
$30,001 to $50,000	24%	23%	25%
$50,001 to $80,000	16%	20%	18%
$80,001 to $100,000	16%	16%	14%
$100,001 to $150,000	8%	8%	10%
$150,001 to $200,000	7%	7%	7%
$200,001 to $300,000	3%	3%	2%
$301,000+	1%	1%	1%
Extrapolated average household income	$74,500	$75,830	$73,820

Table 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 Pacific-West and Northeast. The smallest regions are the Southeast and Southwest.

Table 3. Location of respondent by U.S. geographic region	FY 2012	FY 2011	FY 2010
Northeast	19%	20%	20%
Mid-Atlantic	19%	19%	19%
Midwest	17%	17%	18%
Southeast	13%	13%	13%
Southwest	11%	12%	12%
Pacific-West	20%	19%	18%

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 Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in March, 2012.

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.

Part 1. Screening & background

Q1a. Before now, have you heard the term "medical identity theft"?	FY 2012	FY 2011	
Yes	100%	100%	
No	0%	0%	
Total	100%	100%	

Q1b. Before now, did you know the definition of medical identity theft?	FY 2012	FY 2011	
Yes	90%	77%	
No	10%	23%	
Total	100%	100%	

Q1c. If yes, how did you learn about the problem of medical identity theft?	FY 2012	FY 2011	
A story in the media (for example, newspaper, radio, TV, Internet)	11%	4%	
Information provided by my healthcare provider	15%	5%	
Information provided by my employer	5%	5%	
A personal experience	65%	61%	
Stories shared by my friends or family members	58%	56%	
Total	154%	131%	

Q2. If your healthcare provider informed you 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 2012		
Prompt notification of the loss or theft (within 30 days)	35%		
Free identity protection for one year	33%		
Assistance with transferring my health records to another healthcare provider	13%		
Reimbursement for costs incurred to find another healthcare provider	72%		
Assurance that the incident was being thoroughly investigated	15%		
Assurance that steps were taken to address the root cause of the incident	20%		
Assurance that additional security precautions would be taken to prevent future incidents	12%		
Total	200%		

Q3. Please choose the range that best describes your age.	FY 2012	FY 2011	FY 2010
Below 18 years (stop)	0%	0%	0%
Between 18 and 25 years	18%	16%	19%
Between 26 and 35 years	24%	19%	19%
Between 36 and 45 years	21%	19%	22%
Between 46 and 55 years	19%	20%	18%
Between 56 and 65 years	12%	18%	12%
Above 65 years	7%	8%	10%
Total	100%	100%	100%

Part 2. General questions

Q4. Were you or someone else in your immediate family ever the victim of medical identity theft?	FY 2012	FY 2011	
Yes	94%	93%	
No (skip to Part 3)	6%	7%	
Total	100%	100%	

Q5. If yes, who was the identity theft victim?	FY 2012	FY 2011	FY 2010
Me	46%	44%	44%
My spouse	20%	21%	25%
My child or dependent under the age of 13 years*	8%	6%	5%
My child or dependent between 13 and 18 years	2%	1%	
My child or dependent over 18 years	1%	1%	
My parent	19%	18%	20%
Other family member	4%	9%	7%
Total	100%	100%	100%
*FY 2010 does not break out children by age range.			

Q6. How would you describe your medical identity theft incident? Please select all that apply.	FY 2012	FY 2011	FY 2010
My identity was stolen to bill the health plan, insurance company or government program for services I did not receive	46%		
My identity was stolen to obtain government benefits, including Medicare or Medicaid	53%	45%	52%
My identity was stolen to obtain healthcare services or treatments	67%	67%	71%
My identity was stolen to obtain prescription pharmaceuticals or medical equipment	61%	63%	58%
My medical records were accessed or modified	20%	21%	17%
My credit report was accessed or modified	23%	29%	
Don't know	7%	5%	
Total	231%	230%	198%

Q7. OPTIONAL: If you wish, please describe your medical identity theft experience in the space below.

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

Q8. Are you aware that the medical identity theft you experienced can affect your credit score?	FY 2012	FY 2011	
Yes	33%	21%	
No	43%	46%	
Unsure	24%	33%	
Total	100%	100%	

Q9. How did you learn about the medical identity theft?	FY 2012	FY 2011	FY 2010
Collection (dunning) letters	39%	46%	40%
Adverse entry on my credit report	15%	16%	15%
Suspicious postings to statement or invoice	26%	9%	9%
Mistakes in health records	32%	30%	29%
An alert from a healthcare provider	10%	9%	
Notification by the health provider or insurance company	4%	5%	6%
Other	0%	1%	1%
Total	126%	116%	100%

Q10. When did you learn you were a victim of medical identity theft?	FY 2012	FY 2011	FY 2010
Immediately after the incident	0%	0%	0%
About one week after the incident	2%	2%	3%
About one month after the incident	5%	6%	5%
About three months after the incident	16%	19%	6%
About six months after the incident	19%	20%	14%
About one year after the incident	17%	15%	31%
About two years after the incident	13%	11%	12%
More than two years after the incident	4%	5%	9%
Don't know	24%	22%	20%
Total	100%	100%	100%

Q11a. 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 2012	FY 2011	FY 2010
Yes	48%	50%	54%
No	52%	50%	46%
Total	100%	100%	100%

Q11b. If no, why wasn't the medical identity theft incident reported?	FY 2012	FY 2011	FY 2010
I know the thief and do not want to report him or her	50%	51%	49%
I did not want to alarm my family	6%	8%	9%
I did not think the police would be of any help	45%	41%	43%
I did not have the time to file a police report	9%	10%	11%
I was not harmed by the incident and didn't want to make it a big deal	39%	43%	36%
Don't know	35%	33%	32%
Total	184%	186%	180%

Q12. To the best of your knowledge, how did this medical identity theft happen? Please select only one most likely cause.	FY 2012	FY 2011	FY 2010
Lost a wallet containing personal identification credentials	5%	9%	11%
Mailed statement or invoice was intercepted by the criminal	6%	8%	7%
Email correspondence was intercepted by the criminal online	0%	0%	2%
Phishing attack by criminal who obtained personal identification credentials	4%	6%	7%
Malicious employee in the health provider's office stole health information	7%	10%	12%
Healthcare provider used my identification to conduct fraudulent billing	22%		
Healthcare provider, insurer or other related organization had a data breach	6%	14%	11%
A member of my family took my personal identification credentials without my knowledge	35%	36%	33%
Don't know	15%	17%	17%
Total	100%	100%	100%

Q13a. What were the financial consequences of the medical identity theft? Please select the top two choices only.	FY 2012	FY 2011	
Lost time and productivity trying to fix inaccuracies in credit report	21%	19%	
Increased health insurance premiums as a result of inaccuracies in health records.	8%	7%	
Out-of-pocket payments to health plan or insurer to restore coverage	47%	50%	
Diminished credit score	21%	19%	
Incurred legal fees	15%	14%	
Other	0%	0%	
None	27%	26%	
Total	139%	135%	

Q13b. What were the non-financial consequences of the medical identity theft incident? Please select the top two choices only.	FY 2012	FY 2011	
Lost trust and confidence in my healthcare provider	51%		
Lost time and productivity trying to fix inaccuracies in health records	30%	24%	
Termination by health plan or provider	41%	49%	
Misdiagnoses of illness because of inaccuracies in health records	12%	10%	
Mistreatment of illness because of inaccuracies in health records	14%	18%	
Employment-related difficulties resulting from inaccuracies in credit report or health records	4%	6%	
Revocation of licenses because of inaccuracies in health records	1%	1%	
None	27%	26%	
Total	180%	134%	

Q14a. Did you ever permit a family member to use your personal identification to obtain medical services including treatment, healthcare products or pharmaceuticals?	FY 2012	FY 2011	
Yes	31%	26%	
No	69%	74%	
Total	100%	100%	

Q14b. If yes, why did you do this?	FY 2012	FY 2011	
They did not have insurance	92%	91%	
They could not afford to pay for the medical treatments	89%	87%	
It was an emergency	67%	71%	
Other	6%	5%	
Total	254%	254%	

Q14c. If yes, how often did you share your personal healthcare information with a family member?	FY 2012	FY 2011	
Only 1	50%	56%	
2 to 5	13%	9%	
6 to 10	9%	8%	
> 10	3%	3%	
Cannot recall	25%	24%	
Total	100%	100%	

Q15a. Did you or your immediate family members resolve the consequences of identity theft?	FY 2012	FY 2011	FY 2012
Yes, completely resolved	10%	11%	9%
No, in the process of resolving	43%	41%	21%
No, nothing has been done	47%	48%	40%
Not sure			30%
Total	100%	100%	100%

Q15b. If yes, how did you resolve this medical identity theft? Please select all that apply.	FY 2012	FY 2011	FY 2010
Paid the healthcare provider or insurer for services obtained by imposter	45%	44%	42%
Engaged an identity protection service provider to help resolve the incident	16%	16%	19%
Worked with my healthcare provider to help me resolve the incident	29%		
Work with my health plan and/or insurer to help resolve the incident	39%	41%	14%
Obtained and carefully reviewed credit reports	16%	15%	14%
Contacted credit bureaus to fix inaccuracies in my credit report	13%	12%	12%
Engaged legal counsel to help me resolve the incident	8%	8%	9%
Total	166%	136%	110%

Q15c. If yes, how long did it take to resolve this medical identity theft?	FY 2012	FY 2011	FY 2010
Less than 1 month	4%	4%	5%
1 to 3 months	5%	6%	4%
4 to 6 months	41%	43%	41%
7 to 12 months	10%	8%	9%
1 to 2 years	15%	12%	13%
More than 2 years	25%	27%	28%
Total	100%	100%	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 medical services, products or pharmaceuticals provided to imposters; (4) the value of the time incurred by you and others in your immediate family in trying to resolve the medical identity theft incident.

Q16a. Approximately, what were the **total dollars** lost in trying to resolve this medical identity theft?	FY 2012	FY 2011	FY 2010
Less than $100	3%	7%	0%
Between $101 and $1,000	11%	12%	12%
Between $1,001 and $5,000	24%	23%	27%
Between $5,001 and $10,000	24%	23%	22%
Between $10,001 and $25,000	12%	13%	12%
Between $25,001 and $50,000	10%	11%	15%
Between $50,001 and $100,000	9%	8%	9%
Greater than $100,000	6%	5%	3%
Total	100%	100%	100%

Q16b. Approximately, how many hours were spent trying to resolve this medical identity theft?	FY 2012		
< 5	2%		
5 to 10	6%		
11 to 25	5%		
26 to 50	10%		
51 to 75	11%		
76 to 100	13%		
101 to 200	32%		
> 200	21%		
Total	100%		

Q17. In terms of impact to you or your immediate family members, please select the two most negative outcomes.	FY 2012	FY 2011	
Loss of money	47%	46%	
Diminished credit score	16%	18%	
Time lost to correct errors	25%	21%	
Increased insurance premiums	28%	31%	
Lost medical coverage	19%	21%	
Mistreatment or misdiagnosis of illness	16%	15%	
Embarrassment	38%	37%	
Public release of sensitive information	11%	12%	
Total	200%	200%	

Q18a. Do you know the approximate value in "dollars" that the thief obtained in terms of medical services, medical products and pharmaceuticals?	FY 2012		
Yes	56%		
No	44%		
Total	100%		

Q18b. If yes, please select the approximate dollar range?	FY 2012		
Less than $100	9%		
Between $101 and $1,000	1%		
Between $1,001 and $5,000	5%		
Between $5,001 and $10,000	11%		
Between $10,001 and $25,000	45%		
Between $25,001 and $50,000	15%		
Between $50,001 and $100,000	4%		
Greater than $100,000	10%		
Total	100%		

Q19. What new steps are you or your immediate family members taking to prevent medical identity theft incidents? Please check all that apply.	FY 2012	FY 2011	FY 2010
Engage identity protection service provider	11%	9%	20%
Monitor credit reports	26%	29%	19%
Closely review of my medical records	26%	25%	10%
Seek healthcare providers and insurers with better privacy and security practices	11%	12%	16%
Ensure medical reports are with security conscious vendors	13%	15%	35%
Implement security precautions to protect personal credentials	12%	12%	13%
Shred confidential documents	13%	13%	12%
Avoid Internet transactions involving confidential information	5%	6%	5%
Never share medical insurance ID/credential with anyone	35%		
No new steps taken	48%	49%	42%
Total	200%	170%	172%

Part 3: Healthcare privacy

Healthcare providers include physicians, dentists, nurses, pharmacists and others who provide health services for you and your family.

Q20a. Do you ever check your medical records to determine if the health information about you is accurate?	FY 2012		
Yes, all the time	19%		
Yes, sometimes	24%		
Never	57%		
Total	100%		

Q20b. If never, why don't you check?	FY 2012		
My medical records are not easily available	33%		
I do not know how to check my health information	49%		
I trust my healthcare provider to be accurate	46%		
It never occurred to me to check my medical records	40%		
I don't really care about what is in my medical records	18%		
Other	1%		
Total	187%		

Attributions: Please rate the following statements using the scale provided below each item. Strongly agree and agree response combined.	FY 2012		
Q21a. If I knew my healthcare provider was unable to safeguard my medical records, I would find another provider.	58%		
Q21b. If my healthcare provider informed me that my medical records were lost or stolen, I would find another provider.	56%		
Q21c. Even if I do not trust my healthcare provider's ability to safeguard my medical record, it is too difficult for me to change providers.	34%		

How important are the following issues? Very important and important response combined.	FY 2012	FY 2011	
Q22a. Healthcare providers ensure the privacy of your health records.	80%	78%	
Q22b. Healthcare providers do not share your health records with others without your consent to do so.	72%	71%	
Q22c. Healthcare providers disclose how your information is used or shared with others.	65%	63%	
Q22d. Healthcare providers do not collect information about you and your family that is unrelated to your physical or mental condition.	71%	73%	

What do you see as the most important steps to protecting the privacy of your health records? Very important and important response combined.	FY 2012	FY 2011	
Q23a. Allow me to control my health records directly.	71%	69%	
Q23b. Establish stricter laws to prevent companies or government from accessing my health records without consent.	65%	62%	
Q23c. Ensure that only professionally trained medical practitioners has access to my health records.	70%	71%	

Part 4. Demographics

D1. What best describes your present health plan?	FY 2012	FY 2011	FY 2010
Private insurance	44%	44%	52%
Medicare or Medicaid	21%	20%	19%
Government or VA	5%	5%	4%
Coop plan	4%	5%	5%
Health savings account	6%	5%	7%
Not insured	20%	22%	13%
Total	100%	100%	100%

D2. What is your highest level of education attained?	FY 2012	FY 2011	FY 2010
High School	29%	27%	28%
Vocational	23%	24%	23%
College or University (attended or earned a degree)	41%	42%	41%
Post Graduate	6%	6%	7%
Doctorate	1%	1%	1%
Total	100%	100%	100%

D3. What best describes your present employment status?	FY 2012	FY 2011	FY 2010
Business owner/partner	6%	6%	7%
Full time employee (including homemaker)	56%	52%	43%
Part time employee	10%	9%	9%
Retired	11%	13%	16%
Military	1%	2%	3%
Student	6%	7%	8%
Unemployed	9%	11%	14%
Total	100%	100%	100%

D4. Approximately, what is your total household income?	FY 2012	FY 2011	FY 2010
Less than $30,000	25%	22%	23%
$30,001 to $50,000	24%	23%	25%
$50,001 to $80,000	16%	20%	18%
$80,001 to $100,000	16%	16%	14%
$100,001 to $150,000	8%	8%	10%
$150,001 to $200,000	7%	7%	7%
$200,001 to $300,000	3%	3%	2%
$301,000+	1%	1%	1%
Total	100%	100%	100%

D5. Are you the head of your household?	FY 2012	FY 2011	FY 2010
No	53%	52%	39%
Yes	47%	48%	61%
Total	100%	100%	100%

D6. Gender:	FY 2012	FY 2011	FY 2010
Female	52%	52%	52%
Male	48%	48%	48%
Total	100%	100%	100%

D7. Geographic region in the United States	FY 2012	FY 2011	FY 2010
Northeast	19%	20%	20%
Mid-Atlantic	19%	19%	19%
Midwest	17%	17%	18%
Southeast	13%	13%	13%
Southwest	11%	12%	12%
Pacific-West	20%	19%	18%
Total	100%	100%	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.