



Second Annual Survey on Medical Identity Theft

Sponsored by Experian's ProtectMyID

Independently conducted by Ponemon Institute LLC

Publication Date: March 2011

Second Annual Survey on Medical Identity Theft

Presented by Ponemon Institute, March 1, 2011

Part 1. Executive Summary

We are pleased to present the findings of the *Second Annual Survey on Medical Identity Theft* conducted by Ponemon Institute and sponsored by Experian's ProtectMyID. This is the second year we conducted this study to rigorously determine how pervasive medical identity theft is in the United States and how it has affected American consumers. In this year's study, we also surveyed consumers on how recent healthcare legislation and the government's plan to create a national database to house healthcare records might affect the security of their medical 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. As the results of this study show, consumers are at risk of having their medical credentials stolen by a family member, of becoming a victim of a data breach, or of having someone access their credit or personal health record.

More than 1,672 adult-aged individuals from two independent samples participated in this study. Of these respondents, 633 are known individuals who have experienced identity theft either directly or through the experience of a close family member.¹ Forty-four percent of respondents have private insurance and 18 percent have Medicare or Medicaid. Fifty percent attended college or have an advanced degree.

Medical identity theft continues to be a billion dollar crime 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 for the 2010 and 2011 studies. In 2011, we assume there are 271 million adult-aged consumers who reside in the US. We then estimate that medical identity theft occurs at a rate of .55 percent of the total US population and results in 1.49 million Americans affected by this crime. Based on the number of Americans in 2010, the number of victims was estimated at 1.42 million.

Using an extrapolated cost of \$20,663 per incident derived from our present survey, we estimate the economic impact of medical identity theft in the United States at \$30.9 billion per annum. Our assessment of the economic impact in 2010 was \$28.6 billion.²

Table 1: Extrapolated U.S. economic impact of medical identity theft	FY 2010	FY 2011
Adult-aged Americans and legal residents	269 million	271 million
Base rate for medical identity theft	0.53%	0.55%
Number of Americans affected by medical identity theft	1.42 million	1.49 million
Extrapolated cost per victim	\$20,160	\$20,663
National impact of medical identity theft crimes	28.6 billion	30.9 billion

¹ This specialized panel of adult-aged respondents who are likely identity theft victims was created and used in our *First Annual National Survey on Medical Identity Theft* published in February 2010.

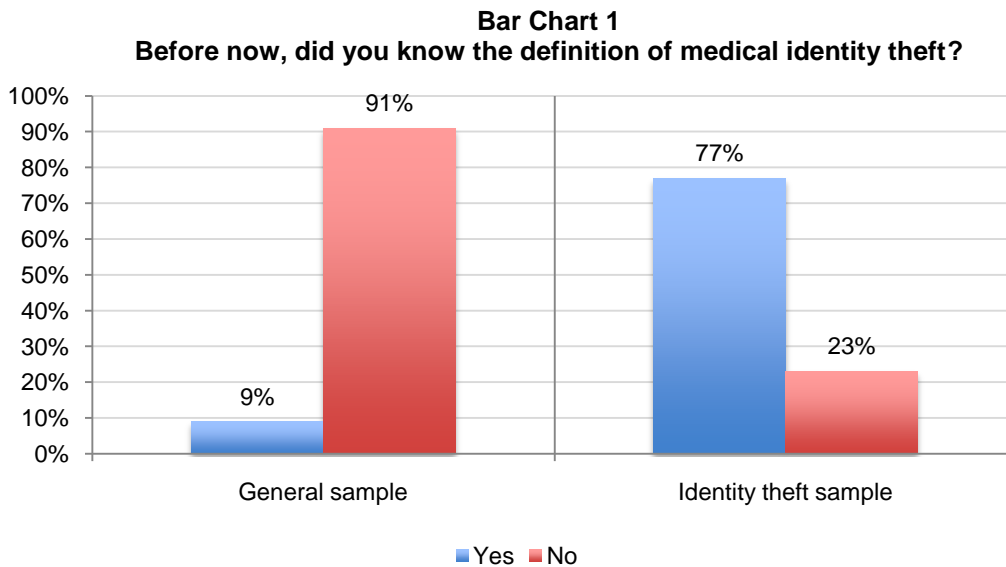
² The base rate percentage is determined by the number of respondents from a general adult-aged panel of US residents who self-reported they or their immediate family have been victims of medical identity theft.

Part 2. Key findings

Following are the study's findings presented as bar charts, pie charts and tables.

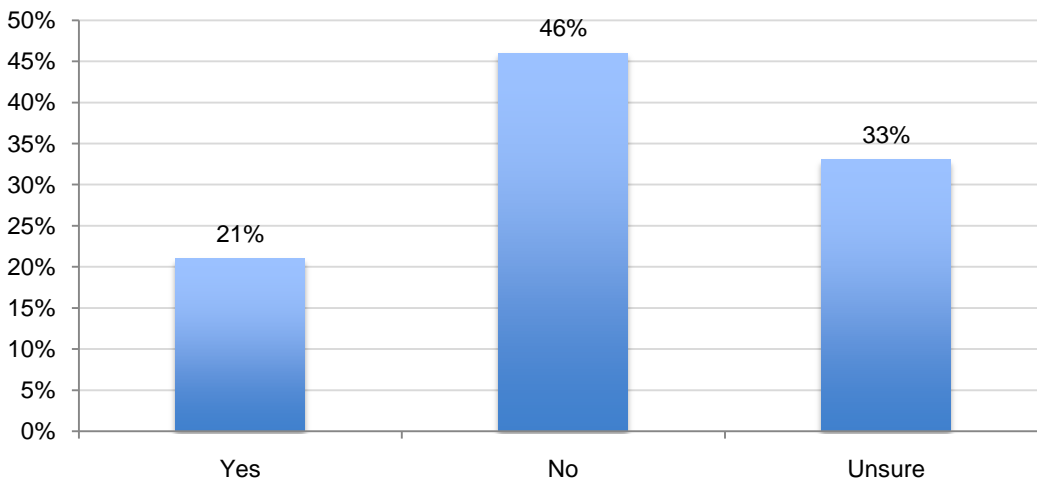
Ignorance about medical identity theft leaves many unprepared and vulnerable to this serious crime.

The vast majority of respondents in our general sample (91 percent) did not know the definition of medical identity theft before completing this survey (see Bar Chart 1). In contrast, 77 percent of respondents in the identity theft sample say they were aware of medical identity theft before completing our survey. The best sources of information about medical identity theft seem to be friends or family members who share stories or their personal experience.



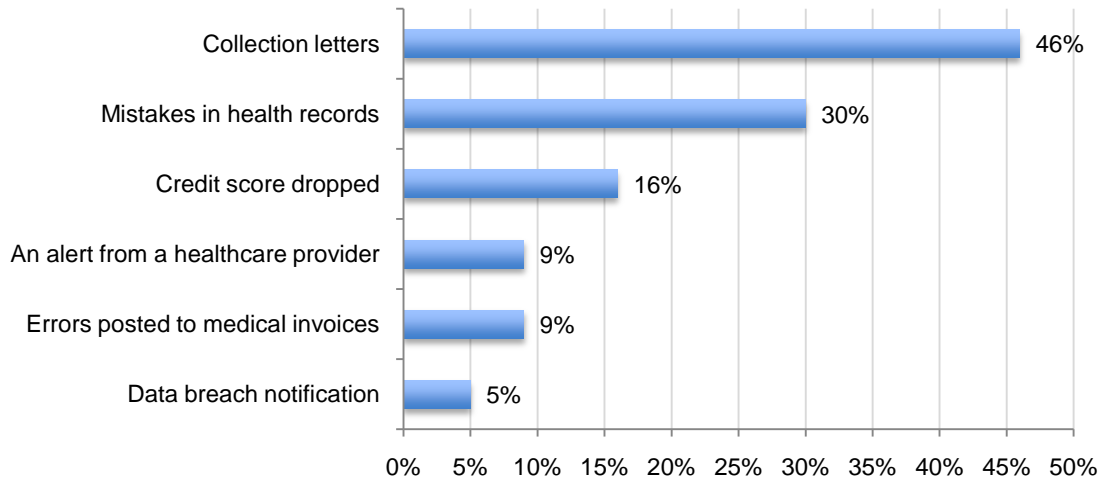
As a further indication that respondents may not understand the risk of medical identity theft, 79 percent (46 + 33 percent) of respondents say they are not aware or unsure about how medical identity theft may affect their credit score (see Bar Chart 2).

Bar Chart 2
Are you aware that medical identity theft you experienced can affect your credit score?



Most respondents learned about the theft of their medical credentials after the damage has been done. According to Bar Chart 3, it took a collection letter, a mistake in their health records or a decline in credit score before becoming aware they were victims.

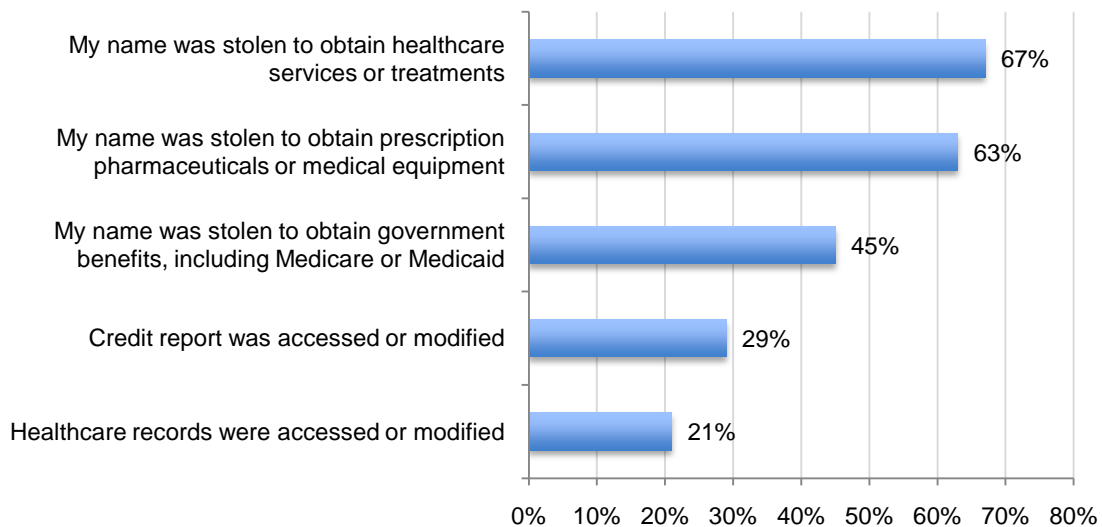
Bar Chart 3
How did you learn about the medical identity theft?



Medical identity theft is an easy crime to commit.

According to Bar Chart 4, thieves stole the respondents' name to obtain medical services, prescription drugs or medical equipment and government benefits. This suggests that medical identity theft is an easy crime to commit. About 29 percent say their identity was stolen by accessing a credit report or healthcare records.

Bar Chart 4
How would you describe your medical identity theft incident?

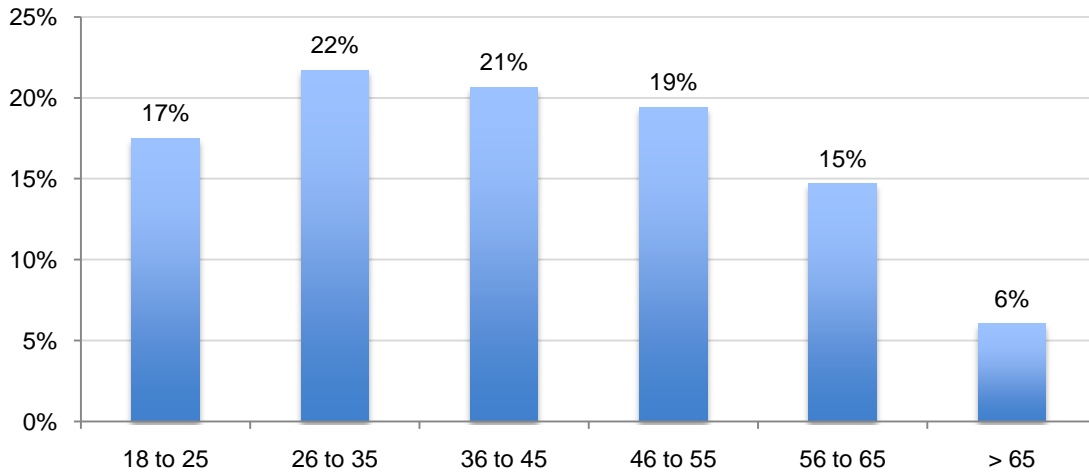


Medical identity theft victims tend to be older.

Bar Chart 5 shows the age distribution of respondents. Sixty-one percent of these medical identity theft victims are 36 years and older. This is understandable given that respondents in this age

group are most likely to have access to more medical benefits and services. Further, older respondents are more likely to have Medicare or other Social Security benefits.

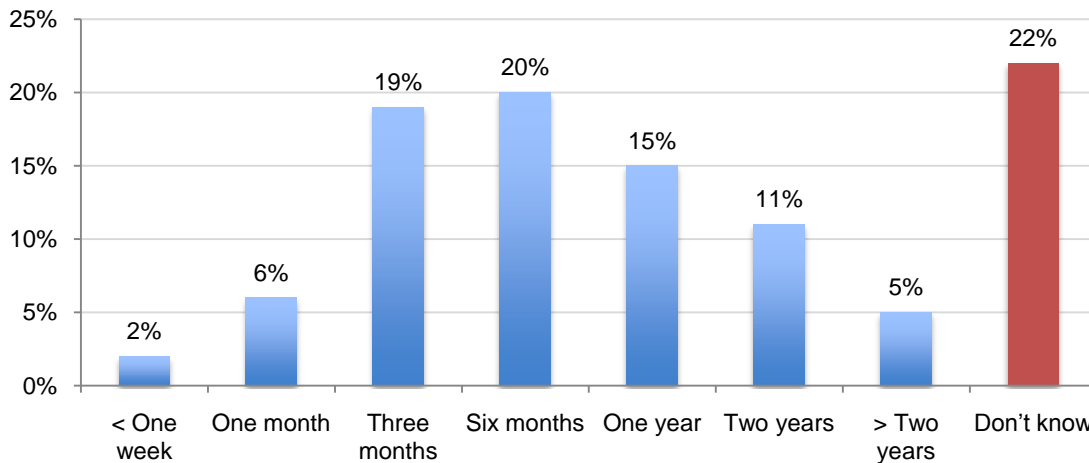
Bar Chart 5
Age range of respondents



Respondents find it difficult to pinpoint when the crime occurred.

Twenty-two percent of respondents did not know when the medical identity theft incident occurred. Approximately 31 percent say they first discovered the theft more than one year after the incident (see Bar Chart 6).

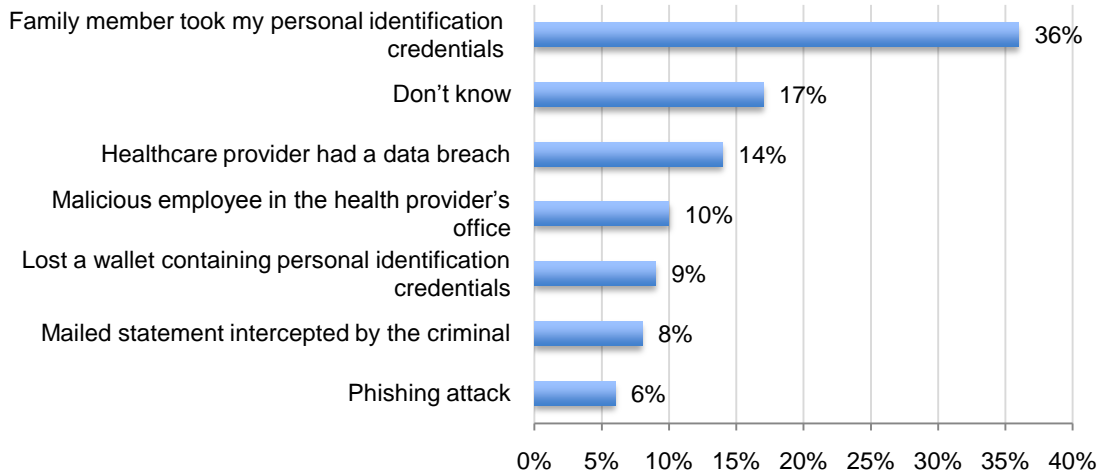
Bar Chart 6
How long after the incident did you learn you were a victim of medical identity theft?



Medical identity theft is a family affair.

A family member is the mostly likely person to steal your medical identity. According to 36 percent of respondents surveyed, a member of the family stole personal identification credentials without the victim's knowledge (see Bar Chart 7). This was followed by 17 percent of respondents who did not know how the medical identity theft happened. Another 14 percent say the root cause of the medical identity theft was a healthcare provider's data breach. Ten percent say a malicious employee in the medical office likely stole the medical information and credentials of the victim.

Bar Chart 7
How did this medical identity theft happen?



As we mentioned above, medical identity theft is often committed by a family member or a close acquaintance. Consequently, 50 percent of respondents in our study were probably reluctant to report the crime to authorities. Table 2 shows the reasons for not reporting the medical identity theft. Specifically, 51 percent knew the thief and did not want to report the incident. This was followed by 43 percent who did not think they were harmed, and 41 percent who did not believe the police would be of any help.

Pie Chart 1
Once you became aware of the medical identity theft, did you or someone in your immediate family report the medical identity theft to law enforcement?

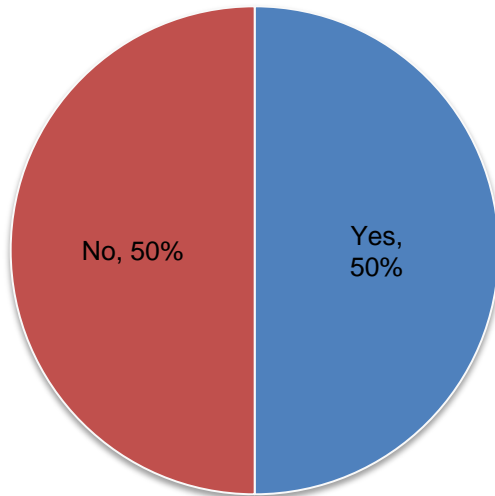


Table 2
If no, why wasn't the medical identity theft reported to law enforcement?

I knew the thief and did not want to snitch on him or her	51%
I was not harmed by the incident and didn't want to make it a big deal	43%
I did not think the police would be of any help	41%
Don't know	33%
I did not have the time to file a police report	10%
I did not want to alarm my family	8%

*More than one response could be provided.

Respondents in this study admit to sharing their health credentials with family members.

Twenty-six percent of respondents say they shared their credentials (see Pie Chart 2). Of these respondents who shared their credential with family members, 56 percent say they did this only once – probably because they began to worry about the consequences of letting their credentials be used by other persons. Another 24 percent cannot recall how many times they shared their health credentials. By forfeiting control of their credentials, these respondents have put their medical identity at great risk.

Pie Chart 2
Did you ever permit a family member to use your personal identification to obtain medical services including treatment, healthcare products or pharmaceuticals?

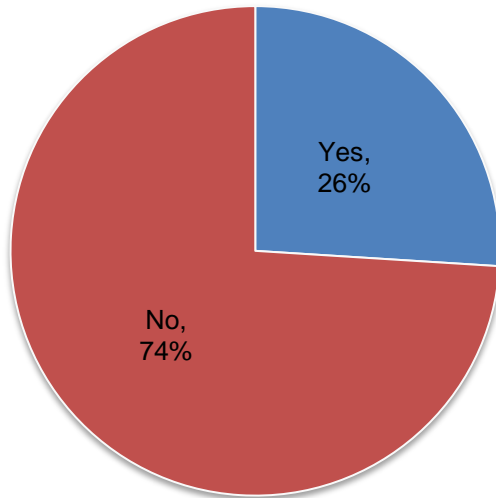
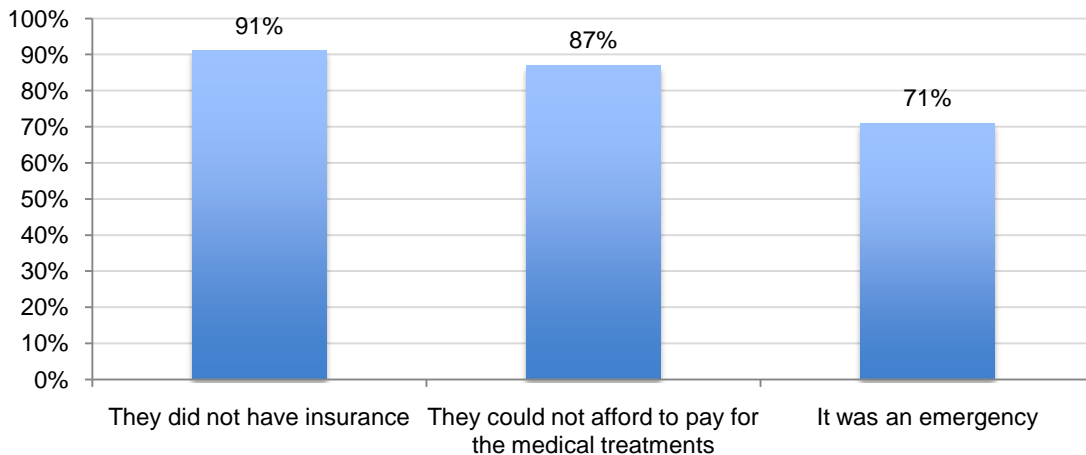


Table 3
If yes, how often did you share your personal healthcare information with a family member?

Once	56%
2 to 5 times	9%
6 to 10 times	8%
More than 10 times	3%
Cannot recall	24%

Compassion seems to be the reason respondents say they shared their private medical identity credential (such as an ID card) with family (see Bar Chart 8). Ninety-one percent say the family member did not have insurance and 87 percent say the family member could not afford needed treatment. Thus, respondents believe they are doing a good deed by sharing their credentials.

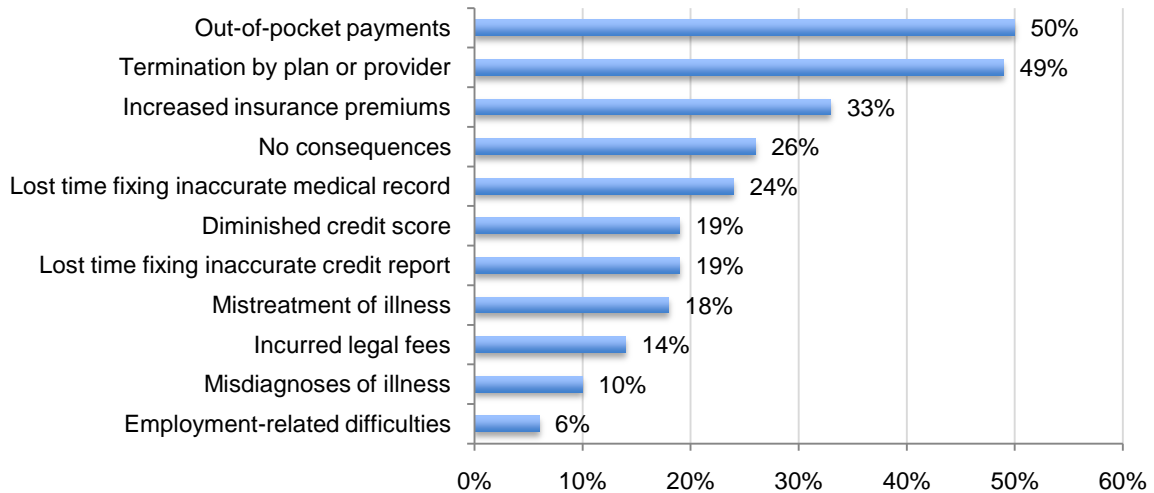
Bar Chart 8
Why respondents shared their medical identity credential



The primary consequences of medical identity theft are financial harms and loss of health coverage.

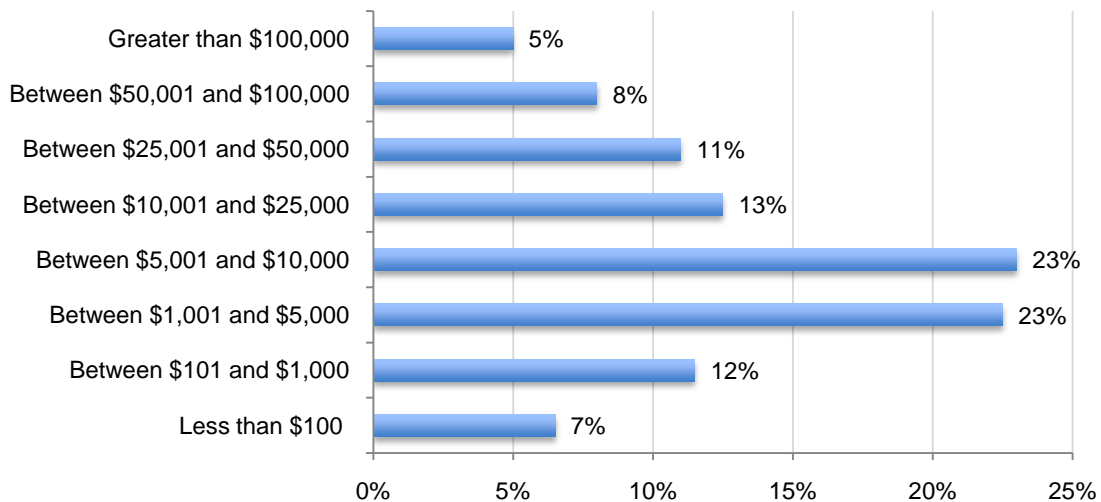
According to 50 percent of medical identity theft victims in our study, the most harmful consequence was paying for services illegally rendered to the thief. Forty-nine percent say they lost their insurance. However, 26 percent claim there was no consequence or harm as a result of the theft. Another 24 percent say they lost time trying to correct their medical records. Bar Chart 9 lists all consequences in descending order.

Bar Chart 9
The consequences of the medical identity theft incident



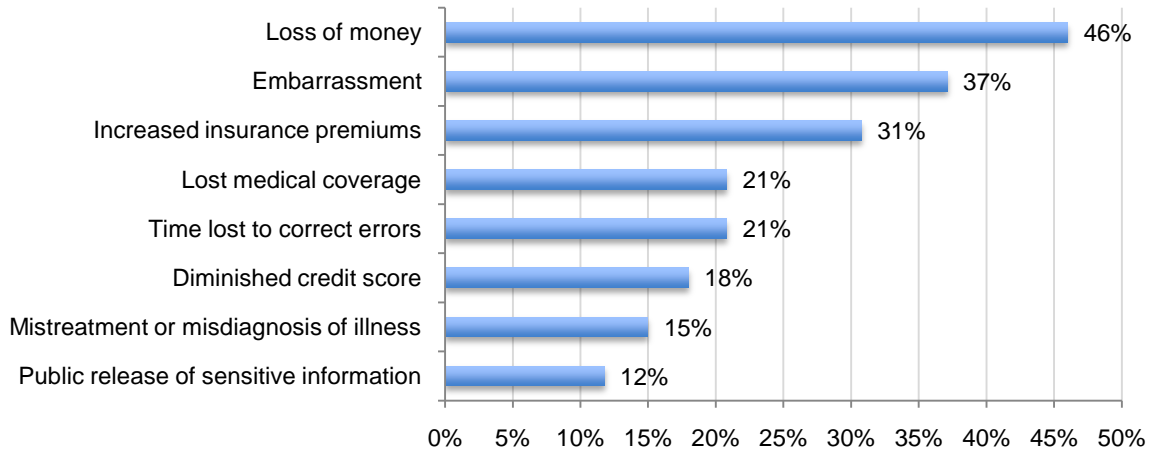
Bar Chart 10 shows the distribution of economic harms experienced by medical identity theft victims. On average it cost the victim \$20,663 to resolve the medical identity theft and several months. The extrapolated average cost in last year's study was \$20,160.

Bar Chart 10
The financial impact of the medical identity theft incident to the victim and families



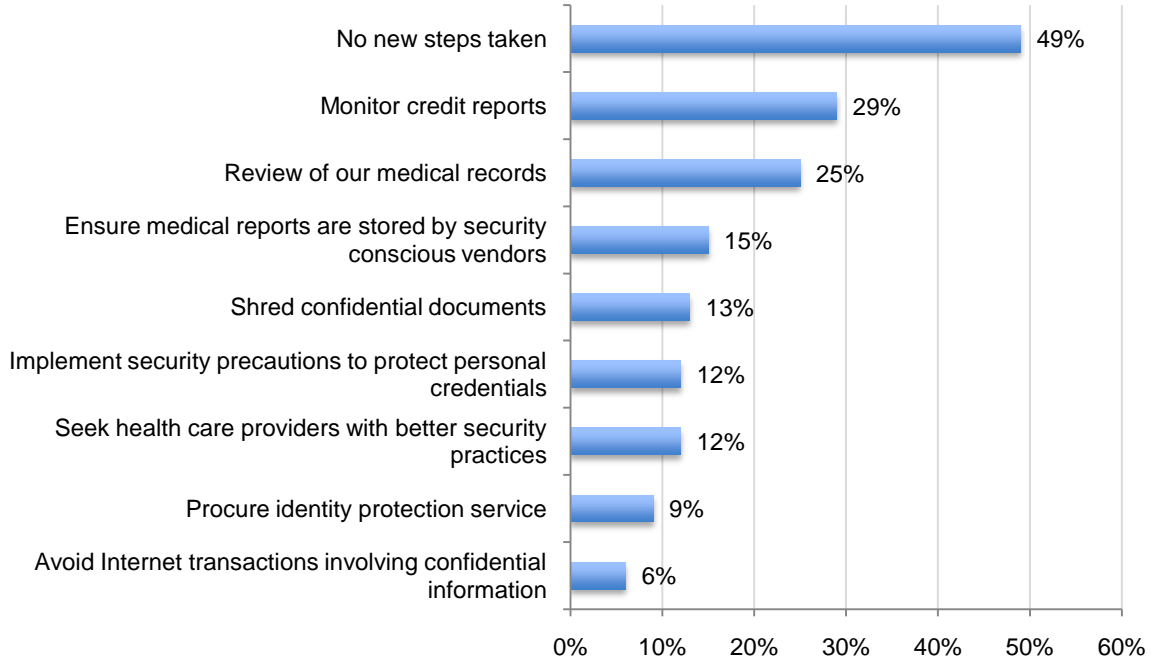
As shown in Bar Chart 11, the most negative consequences of medical identity theft are the loss of money, embarrassment, increased insurance premiums, and lost medical coverage.

Bar Chart 11
The impact of the medical identity theft on respondents and their immediate families



To prevent future incidents, respondents say they will monitor credit reports (29 percent) and review their medical records (25 percent). It is surprising that 49 percent say they will not take any new precautions to prevent medical identity theft in the future.

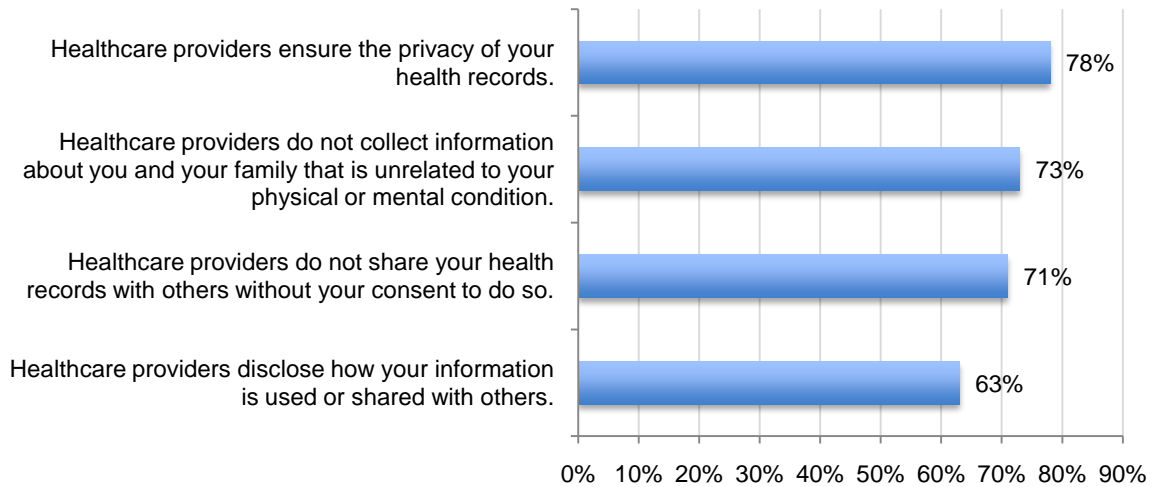
Bar Chart 12
What steps taken to prevent medical identity theft in the future?



Healthcare privacy is an important issue for medical identity theft victims.³

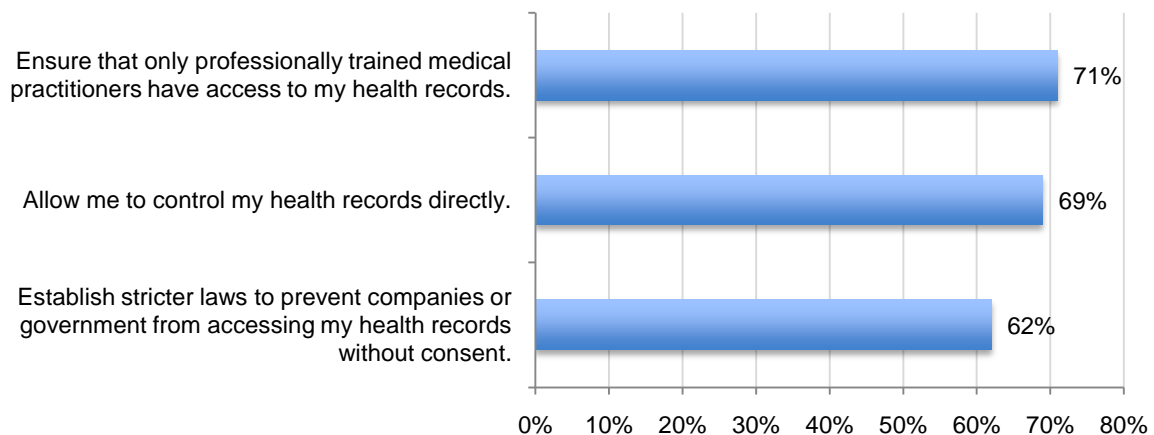
The majority of respondents in our study believe it is important for healthcare providers to take steps to ensure the privacy of their healthcare records. Other perceptions about healthcare providers are shown in Bar Chart 13.

Bar Chart 13
Importance of health information privacy
 Strongly agree and agree response combined



To protect patient privacy, respondents want their healthcare providers to take the following precautions: ensure that only professionally trained medical practitioners have access to their health records, allow patients to control their health records directly and establish stricter laws to prevent companies or government from accessing their health records without consent.

Bar Chart 14
Steps taken to protect health information privacy
 Strongly agree and agree response combined

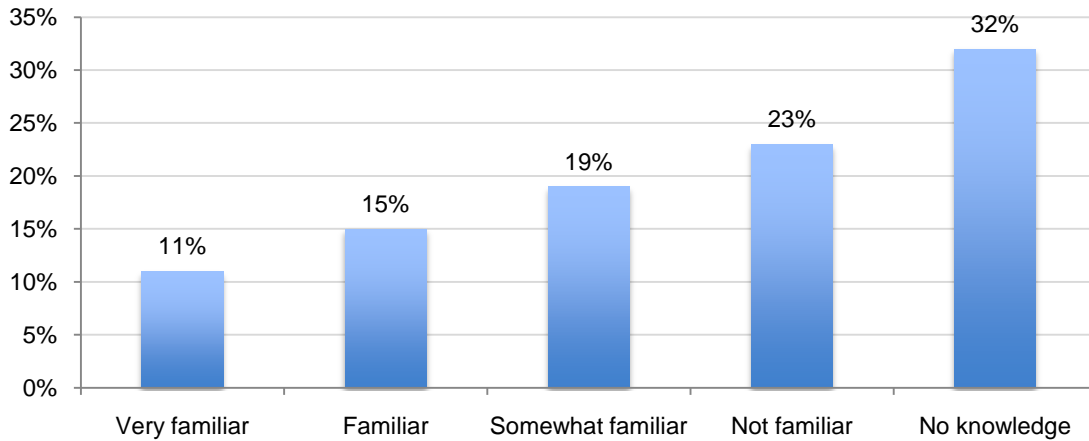


³These questions are derived from an earlier study entitled, "Americans' Opinion about Healthcare Privacy, Ponemon Institute, January 2010.

Only 26 percent of respondents are familiar with the new healthcare reform bill passed in 2010. Thirty-two percent have no knowledge about the bill.

We believe that the lack of familiarity about the new healthcare bill is due in large measure to its complexity. However, those who are familiar are not confident or are unsure that the new law will reduce their risk of medical identity theft.

Bar Chart 15
How familiar are you with the new healthcare law?



Seventy-nine percent of respondents are not aware of the initiative to have an electronic database for patient information. If aware, respondents are uncertain how the database will affect the security of their personal health information. Forty-five percent say it will have no affect on medical identity theft. However, 33 percent believe it will actually increase the risk of medical identity theft. In any event, an overwhelming majority of respondents in this study believe security of such a national electronic database is very important or important.

Pie Chart 3
Are you aware of the plan to create a national database of Americans' health information

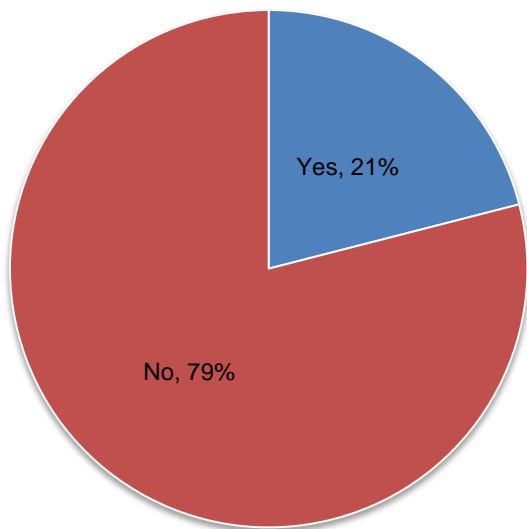


Table 4
How will the creation of a national database affect medical identity theft?

Increase the risk of medical identity theft	33%
Decrease the risk of medical identity theft	9%
No affect on medical identity theft	45%
Not sure	13%

Part 3. Methods

Our sampling plan consisted of two parts: A general sample of US consumers was used to estimate the base rate for medical identity theft victims and a special sample of likely identity theft victims (that was developed for our 2010 study). This special sample was necessary because our survey required responses from individuals who either experienced medical identity theft directly or through a close family relationship.

Using a discovery sampling method, we were able to determine a medical identity theft base rate for adult-aged consumers in the United States, as follows:⁴

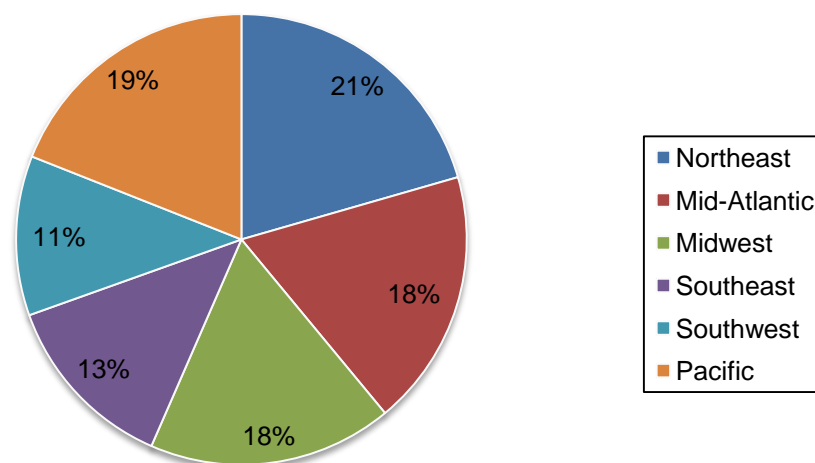
- A total of 907 individuals from the general sample of consumers responded to our survey.
- A total of 5 individuals passed screening criteria for medical identity theft (either directly or through family relationships).
- Five divided by 907 equals .55 percent, which is our medical identity theft base rate in 2011.

Table 5 summarizes our sample response. As can be seen, nearly 74,000 individuals were invited to participate in this research. This resulted in a combined response of 1,672 individuals (2.26 percent combined response rate). Those who passed screening criteria for medical identity theft in the general and identity theft samples were combined, thus resulting in a total of 633 individuals who responded to questions about medical identity theft.

Table 5 Sample response	General sample	Identity theft sample	Combined
Total sample frame	37,332	36,559	73,891
Final sample	907	765	1,672
Bona fide medical identity theft victim	5	628	633
Response rate	2.43%	2.09%	2.26%
Sample weighting	54.2%	45.8%	100.0%

Pie Chart 4 shows the geographic distribution of respondents. The northeast at 21 percent represents the largest region, while the southwest at 11 percent represents the smallest region.

Pie Chart 4: Sample distribution across geographic regions



⁴ The discovery sampling method is commonly used to assess the existence of an attribute in a population. In this case, we sampled from a large consumer sampling frame of over 37,000 records until we found five individuals who passed objective criteria for medical identity theft.

The remaining tables provide the percentage frequency of all respondents (n = 1,672) from the combination of the general and identity theft samples. A total of 48 percent of respondents state they are the head of household. Fifty-two percent are female and 48 percent are male. Table 6 summarizes respondents' healthcare coverage. Forty-four percent have private insurance, 22 percent do not have insurance (at present), and 18 percent have Medicare or Medicaid.

Table 6 Respondents' present health coverage or plan	Pct%
Private insurance	44%
Medicare or Medicaid	18%
Government or VA	5%
Coop plan	5%
Health savings account	6%
Not insured	22%
Total	100%

Table 7 summarizes the education level of respondents. As shown, 42 percent of respondents say they attended or graduated from a college or university.

Table 7 Highest level of education attained by respondents	Pct%
High School	27%
Vocational	23%
College or University (attended or earned a degree)	42%
Post Graduate	7%
Doctorate	1%
Total	100%

Table 8 summarizes the employment status of respondents. As shown, over 52 percent of respondents are full-time employees or homemakers. Nearly 12 percent are retired and 11 percent are unemployed.

Table 8 Employment status of respondents	Pct%
Full time employee (including homemaker)	52%
Retired	12%
Unemployed	11%
Part time employee	10%
Student	7%
Business owner/partner	6%
Military	2%
Total	100%

Table 9 summarizes the self-reported household income of respondents. A total of 47 percent of respondents say they earn \$50,000 or less per annum.

Table 9 Respondents' annual household income	Pct%
Less than \$30,000	23%
\$30,001 to \$50,000	24%
\$50,001 to \$80,000	19%
\$80,001 to \$100,000	15%
\$100,001 to \$150,000	9%
\$150,001 to \$200,000	7%
\$200,001 to \$300,000	2%
\$301,000+	1%
Total	100%

Part 4. Limitations and Conclusion

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 representative 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.

Concluding Thoughts

The findings reveal the lack of awareness many Americans have about medical identity theft and the devastating consequences it can have. These include financial loss, incorrect medical records and harm to their credit scores. Moreover, medical identity theft appears to be an easy crime to commit. Sharing credentials with family members or enabling thieves to steal their names to access healthcare goods and services was very common among the consumers surveyed.

However, as we discussed in last year's report, consumers are not helpless. Taking steps to monitor your health records and credit reports can ensure that if your medical identity theft has been stolen you will be able to resolve the incident as soon as possible.

Appendix 1: Detailed Results

The following tables summarize the frequency of results for the general (sample 1) and identity theft (sample 2) samples, respectively. Fielding for this survey was completed in February 2011.

Sample response	Sample 1	Sample 2	Combined
Total sample frame	37,332	36,559	73,891
Invitations sent	36,501	35,998	72,499
Total returns	991	843	1,834
Total rejections	84	68	152
Final sample	907	765	1,672
Bona fide medical identity theft victim	5	628	633
Response rate	2.43%	2.09%	2.26%
Sample weighting	54.2%	45.8%	100.0%

Part 1. Background			n=907
Q1a. Before now, have you heard the term "medical identity theft"?	Sample 1	Sample 2	Combined
Yes	21%		
No	79%		
Total	100%		

Q1b. Before now, did you know the definition of medical identity theft?			n=1672
Sample 1	Sample 2	Combined	
Yes	9%	77%	40%
No	91%	23%	60%
Total	100%	100%	100%

Q1c. If yes, how did you learn about the problem of medical identity theft?	Sample 1	Sample 2	Combined
A story in the media (for example, newspaper, radio, TV, Internet)	9%	4%	6%
Information provided by my healthcare provider	11%	5%	8%
Information provided by my employer	6%	5%	6%
A personal experience	30%	61%	44%
Stories shared by my friends or family members	47%	56%	51%
Total	103%	131%	116%

Q2. Please choose the range that best describes your age.	Sample 1	Sample 2	Combined
Below 18 years (stop)	0%	0%	0%
Between 18 and 25 years	19%	16%	17%
Between 26 and 35 years	24%	19%	22%
Between 36 and 45 years	22%	19%	21%
Between 46 and 55 years	19%	20%	19%
Between 56 and 65 years	12%	18%	15%
Above 65 years	4%	8%	6%
Total	100%	100%	100%

Part 2. General questions			n=1,672
Q3. Were you or someone else in your immediate family ever the victim of medical identity theft?	Sample 1	Sample 2	Combined
Yes	1%	93%	43%
No (skip to Part 3)	99%	7%	57%
Total	100%	100%	100%

n=633

Q4. If yes, who was the identity theft victim?	Consolidated
Me	44%
My spouse	21%
My child or dependent under the age of 13 years	6%
My child or dependent between 13 and 18 years	1%
My child or dependent over 18 years	1%
My parent	18%
Other family member	9%
Total	100%

Q5. How would you describe your medical identity theft incident? Please select all that apply.	Consolidated
My name was stolen to obtain government benefits, including Medicare or Medicaid	45%
My name was stolen to obtain healthcare services or treatments	67%
My name was stolen to obtain prescription pharmaceuticals or medical equipment	63%
Healthcare records were accessed or modified	21%
Credit report was accessed or modified	29%
Don't know (Skip to Part 3)	5%

Q5a. OPTION: If you wish, please describe your medical identity theft experience in the space below.	Contextual
Please answer the following questions with specific focus on medical identity theft experienced by you or your immediate family members.	

Q6. Are you aware that the medical identity theft you experienced can affect your credit score?	Consolidated
Yes	21%
No	46%
Unsure	33%
Total	100%

Q7. How did you learn about the medical identity theft?	Consolidated
Collection letters	46%
Credit score dropped	16%
Errors posted to medical invoices	9%
Mistakes in health records	30%
An alert from a healthcare provider	9%
Data breach notification	5%
Other (please specify)	1%
Total	116%

Q8. Approximately, what time of the year did the medical identity theft occur?	Consolidated
Fall (September through December)	12%
Winter (January through March)	15%
Spring (April through May)	20%
Summer (June through August)	15%
Don't know	38%
Total	100%

Q9. With respect to time of the incident, when did you learn you were a victim of medical identity theft?	Consolidated
Immediately	0%
About one week later	2%
About one month later	6%
About three months later	19%
About six months later	20%
About one year later	15%
About two years later	11%
More than two years later	5%
Don't know	22%
Total	100%

Q10a. Once you became aware of the medical identity theft, did you or someone in your immediate family report the medical identity theft to law enforcement or other legal authorities?	Consolidated
Yes	50%
No	50%
Total	100%

Q10b. If no, why wasn't the medical identity theft reported?	Consolidated
I know the thief and do not want to snitch on him or her	51%
I did not want to alarm my family	8%
I did not think the police would be of any help	41%
I did not have the time to file a police report	10%
I was not harmed by the incident and didn't want to make it a big deal	43%
Don't know	33%
Total	186%

Q11. To the best of your knowledge, how did this medical identity theft happen? Please select only <u>one</u> most likely event.	Consolidated
Lost a wallet containing personal identification credentials	9%
Mailed statement or invoice was intercepted by the criminal	8%
Email correspondence intercepted by the criminal online	0%
Phishing attack by criminal who obtained personal identification credentials	6%
Malicious employee in the health provider's office stole health information	10%
Health care provider, insurer or other related organization had a data breach	14%
A member of the family took my personal identification credentials without my knowledge	36%
Don't know	17%
Total	100%

Q12. What were the consequences of the medical identity theft? Please select all that apply.	Consolidated
Lost time and productivity trying to fix inaccuracies in credit report	19%
Lost time and productivity trying to fix inaccuracies in health records	24%
Increased health insurance premiums as a result of inaccuracies in health records.	7%
Termination by health plan or provider	49%
Out-of-pocket payments to health plan or insurer to restore coverage	50%
Diminished credit score	19%
Misdiagnoses of illness because of inaccuracies in health records	10%
Mistreatment of illness because of inaccuracies in health records	18%
Employment-related difficulties resulting from inaccuracies in credit report or health records	6%
Revocation of licenses because of inaccuracies in health records	1%
Incurred legal fees	14%
Other (please specify)	0%
None	26%
Total	243%

Q13a. Did you ever permit a family member to use your personal identification to obtain medical services including treatment, healthcare products or pharmaceuticals?	Consolidated
Yes	26%
No	74%
Total	100%

Q13b. If yes, why did you do this?	Consolidated
They did not have insurance	91%
They could not afford to pay for the medical treatments	87%
It was an emergency	71%
Other	5%
Total	254%

Q13c. If yes, how often did you share your personal healthcare information with a family member?	Consolidated
Only one time	56%
Between two and five times	9%
Between six and 10 times	8%
More than 10 times	3%
Can't remember how many times	24%
Total	100%

Q14a. Did you or your immediate family members resolve the consequences of identity theft?	Consolidated
Yes, completely resolved	11%
No, in the process of resolving	41%
No, nothing has been done	48%
Total	100%

Q14b. If yes, how did you resolve this medical identity theft? Please select all that apply.	Consolidated
Paid healthcare provider (or repaid insurer) for services obtained by imposter	44%
Engaged an identity protection service provider to assist in restoring records	16%
Contacted health plan and/or insurer to fix inaccuracies in medical records	41%
Obtained and carefully reviewed credit reports	15%
Contacted credit bureaus to fix inaccuracies in the credit report	12%
Hired legal counsel	8%
Total	136%

Q14c. If yes, how long did it take to resolve this medical identity theft?	Consolidated
Less than one month	4%
Between one and three months	6%
Between four and six months	43%
Between seven months and one year	8%
Between one and two years	12%
More than two years	27%
Total	100%

Q15. Approximately, what were the total dollars lost in trying to resolve this medical identity theft?	Consolidated	Extrapolated dollars
Less than \$100	7%	5
Between \$101 and \$1,000	12%	58
Between \$1,001 and \$5,000	23%	563
Between \$5,001 and \$10,000	23%	1,725
Between \$10,001 and \$25,000	13%	2,188
Between \$25,001 and \$50,000	11%	4,125
Between \$50,001 and \$100,000	8%	6,000
Greater than \$100,000	5%	6,000
Total	100%	\$20,663

Q16. In terms of impact to you or your immediate family members, please select the two most negative outcomes.	Consolidated
Loss of money	46%
Diminished credit score	18%
Time lost to correct errors	21%
Increased insurance premiums	31%
Lost medical coverage	21%
Mistreatment or misdiagnosis of illness	15%
Embarrassment	37%
Public release of sensitive information	12%
Total	200%

Q17. What new steps are you or your immediate family members taking to prevent medical identity theft? Please check all that apply.	Consolidated
Engage identity protection service provider	9%
Monitor credit reports	29%
Review of our medical records	25%
Seek health care providers and insurers with better privacy and security practices	12%
Ensure medical reports are with security conscious vendors	15%
Implement security precautions to protect personal credentials	12%
Shred confidential documents	13%
Avoid Internet transactions involving confidential information	6%
Other (please specify)	0%
No new steps taken	49%
Total	170%

Part 3: Healthcare privacy

	n=1672		
Q18. How important are the following issues?	Very important	Important	Combined
Q18a. Healthcare providers ensure the privacy of your health records.	40%	38%	78%
Q18b. Healthcare providers do not share your health records with others without your consent to do so.	38%	33%	71%
Q18c. Healthcare providers disclose how your information is used or shared with others.	34%	29%	63%
Q18d. Healthcare providers do not collect information about you and your family that is unrelated to your physical or mental condition.	39%	34%	73%

Q19. What do you see as the most important steps to protecting the privacy of your health records? Please use the scale provided below to rate each statement.	Very important	Important	Combined
Q19a. Allow me to control my health records directly.	33%	36%	69%
Q19b. Establish stricter laws to prevent companies or government from accessing my health records without consent.	29%	33%	62%
Q19c. Ensure that only professionally trained medical practitioners have access to my health records.	34%	37%	71%

Q20a. A healthcare reform bill was passed in 2010. How familiar are you with the new healthcare law?	Consolidated
Very familiar	11%
Familiar	15%
Somewhat familiar	19%
Not familiar	23%
No knowledge	32%
Total	100%

Q20b. If you are familiar, do you believe the new healthcare law will reduce your risk of medical identity theft?	Consolidated
Yes	19%
No	45%
Don't know	36%
Total	100%

Q21a. Are you aware of the plan to create a national electronic database of Americans' health information?	Consolidated
Yes	21%
No	79%
Total	100%

Q21b. How will the creation of this national electronic database affect medical identity theft?	Consolidated
Increase the risk of medical identity theft	33%
Decrease the risk of medical identity theft	9%
No affect on medical identity theft	45%
Not sure	13%
Total	100%

Q21c. In your opinion, how important is the security of a national electronic database of Americans' health information?	Very important	Important	Combined
Five-point scale	35%	44%	79%

Part 4. Demographics

	n=1,672		
Q22. What best describes your present health plan?	Sample 1	Sample 2	Combined
Private insurance	45%	43%	44%
Medicare or Medicaid	16%	21%	18%
Government or VA	5%	5%	5%
Coop plan	5%	5%	5%
Health savings account	6%	5%	6%
Not insured	23%	21%	22%
Total	100%	100%	100%

Q23. What is your highest level of education attained?	Sample 1	Sample 2	Combined
High School	26%	28%	27%
Vocational	23%	24%	23%
College or University (attended or earned a degree)	43%	41%	42%
Post Graduate	7%	6%	7%
Doctorate	1%	1%	1%
Total	100%	100%	100%

Q24. What best describes your present employment status?	Sample 1	Sample 2	Combined
Business owner/partner	6%	6%	6%
Full time employee (including homemaker)	51%	53%	52%
Part time employee	10%	9%	10%
Retired	11%	14%	12%
Military	2%	2%	2%
Student	8%	6%	7%
Unemployed	12%	10%	11%
Total	100%	100%	100%

Q25. Approximately, what is your total household income?	Sample 1	Sample 2	Combined
Less than \$30,000	23%	22%	23%
\$30,001 to \$50,000	24%	23%	24%
\$50,001 to \$80,000	19%	20%	19%
\$80,001 to \$100,000	15%	16%	15%
\$100,001 to \$150,000	9%	8%	9%
\$150,001 to \$200,000	7%	7%	7%
\$200,001 to \$300,000	2%	3%	2%
\$301,000+	1%	1%	1%
Total	100%	100%	100%

Q26. Are you the head of your household?	Sample 1	Sample 2	Combined
No	51%	52%	51%
Yes	49%	47%	48%
Total	100%	99%	100%

Q27. Gender:	Sample 1	Sample 2	Combined
Female	53%	51%	52%
Male	47%	49%	48%
Total	100%	100%	100%

Q28. Geographic region in the United States	Sample 1	Sample 2	Combined
Northeast	21%	20%	21%
Mid-Atlantic	18%	19%	18%
Midwest	18%	17%	18%
Southeast	13%	13%	13%
Southwest	11%	12%	11%
Pacific	19%	19%	19%
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.