Medical Identity Theft

Smart Card Alliance Webinar
June 8, 2010

Introduction: Medical Identity Theft

Randy Vanderhoof
Executive Director, Smart Card Alliance

Who We Are

- **Smart Card Alliance mission**

  To stimulate the understanding, adoption, use and widespread application of smart card technology through educational programs, market analysis, advocacy, and industry relations in the United States and Latin America.

- **Over 150 members, including participants from financial, retail, government, corporate, and transit industries and technology providers to those users**
- **Major activities**
  - **Conferences, symposia, web seminars**
  - **Educational workshops and on-line training**
  - **Web-based resources: white papers, reports, industry product and services**
  - **Industry and Technology Councils**
    - **Identity Council**
    - **Contactless Payments Council**
    - **Healthcare Council**
    - **Physical Access Council**
    - **Transportation Council**

Webinar Topics

- Scope of medical identity theft in the U.S.
- Consumer attitudes toward medical identity theft
- Emerging risks to personal healthcare information
- Opportunities in the current electronic health record adoption process to address medical identity theft with policies and technical standards
- Impact of medical identity theft on healthcare providers

Speakers

- **Randy Vanderhoof**, Executive Director, **Smart Card Alliance**

- **Larry Ponemon**, *Chairman & Founder*, **Ponemon Institute**

- **Deven McGraw**, *Director of Health Privacy Project*, **Center for Democracy and Technology**

- **Paul Contino**
  Vice President of Information Technology
  Mount Sinai Medical Center

National Study on Medical Identity Theft Sponsored by ProtectMyID, A Part of Experian

Independently conducted by Ponemon Institute LLC
Presentation by Dr. Larry Ponemon
June 8, 2010

Ponemon INSTITUTE

Ponemon Institute LLC

- ✓ The Institute is dedicated to advancing responsible information management practices that positively affect privacy and data protection in business and government.
- ✓ The Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations.
- ✓ Ponemon Institute is a full member of **CASRO** (Council of American Survey Research Organizations). Dr. Ponemon serves as CASRO's chairman of Government & Public Affairs Committee of the Board.
- ✓ The Institute has assembled more than 50 leading multinational corporations called the **RIM Council**, which focuses the development and execution of ethical principles for the collection and use of personal data about people and households.
- ✓ The majority of active participants are privacy or information security leaders.

What Is Medical Identity Theft?

Definition by the World Privacy Forum:

- Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity - such as insurance information - without the person's knowledge or consent to obtain medical services or goods, or uses the person's identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim's name.
- Medical identity theft is a crime that can cause great harm to its victims. Yet despite the profound risk it carries, it is the least studied and most poorly documented of the cluster of identity theft crimes. It is also the most difficult to fix after the fact, because victims have limited rights and recourses. Medical identity theft typically leaves a trail of falsified information in medical records that can plague victims' medical and financial lives for years.

See www.worldprivacyforum.org for additional details.

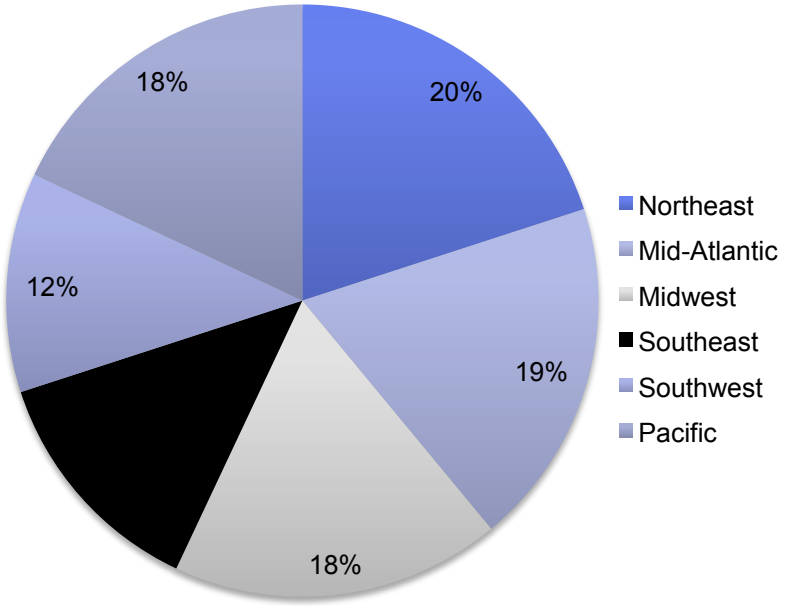
Purpose of our Study

- This is the first national study that focuses on medical identity theft crimes in the United States.
- Using scientific survey methods, our research seeks to better understand the scope, nature and impact of medical identity theft and how this crime differs from ordinary identity theft.
- The results of this research are used to extrapolate the number of adult-aged Americans who have been victimized by this crime over the past few years. Also, we attempt to measure economic impact on a per capita and national basis.
- In addition to sizing the problem, this research examines:
  - Root causes of the crime
  - Detection of the crime by victims
  - Consequences to victims in terms of direct cost, productivity losses, increased insurance premiums, reputational damage and so forth
  - Actions taken to resolve the crime

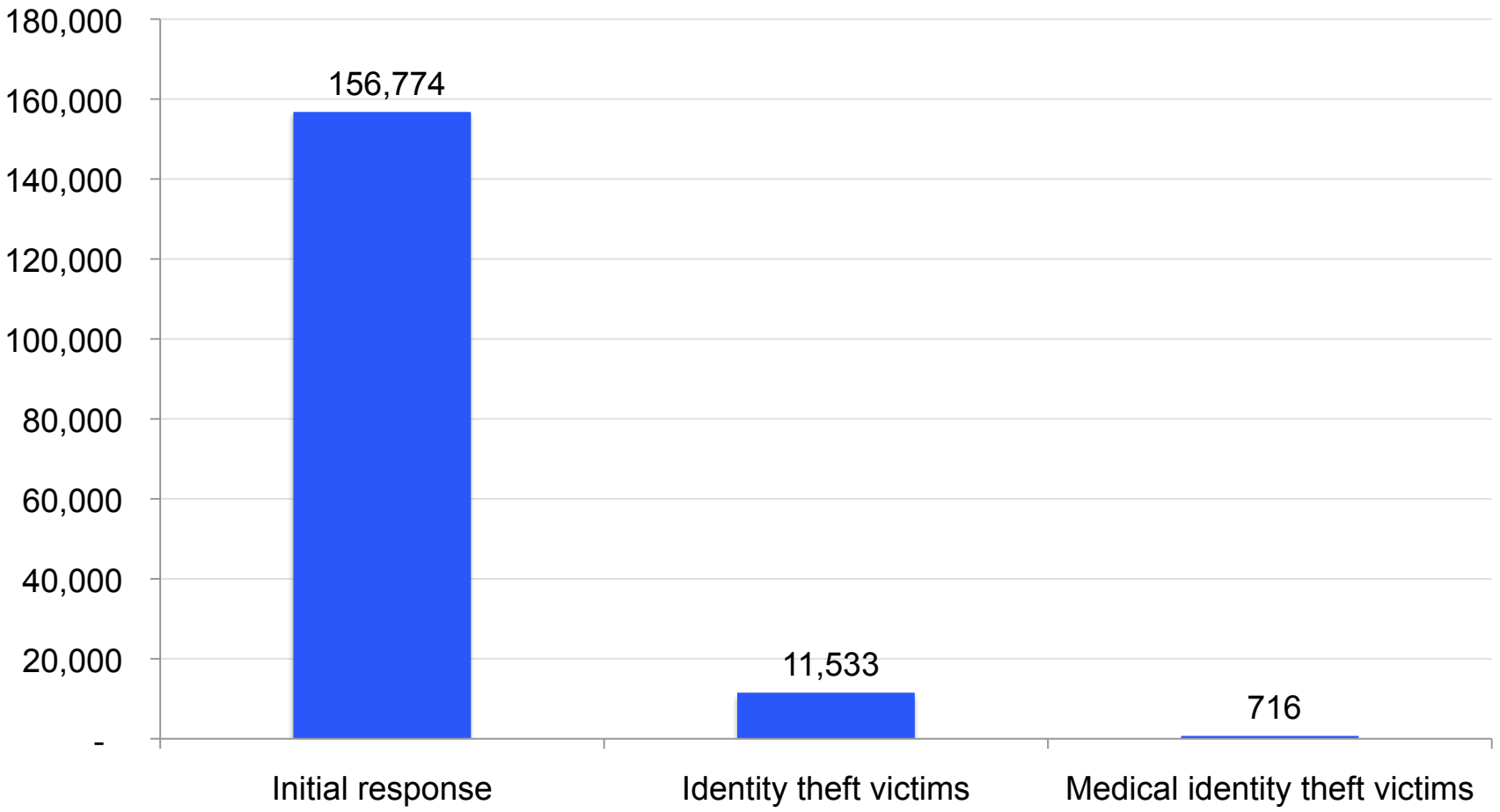
Sample & Survey Methods

- Launched in early January 2010.
- Established a standardized survey containing approximately 30 fixed formatted items.
- Obtained input from experts in the privacy and identity protection fields.
- Conducted readability tests for qualified consumer panels.
- Utilized a large, nationally balanced consumer sampling frame representing Americans located in all regions of the United States.
- Obtained confidential responses using web and telephone collection channels.
- Concluded field work on February 28, 2010.

Pie chart shows the distribution final sample by geographic region in the United States

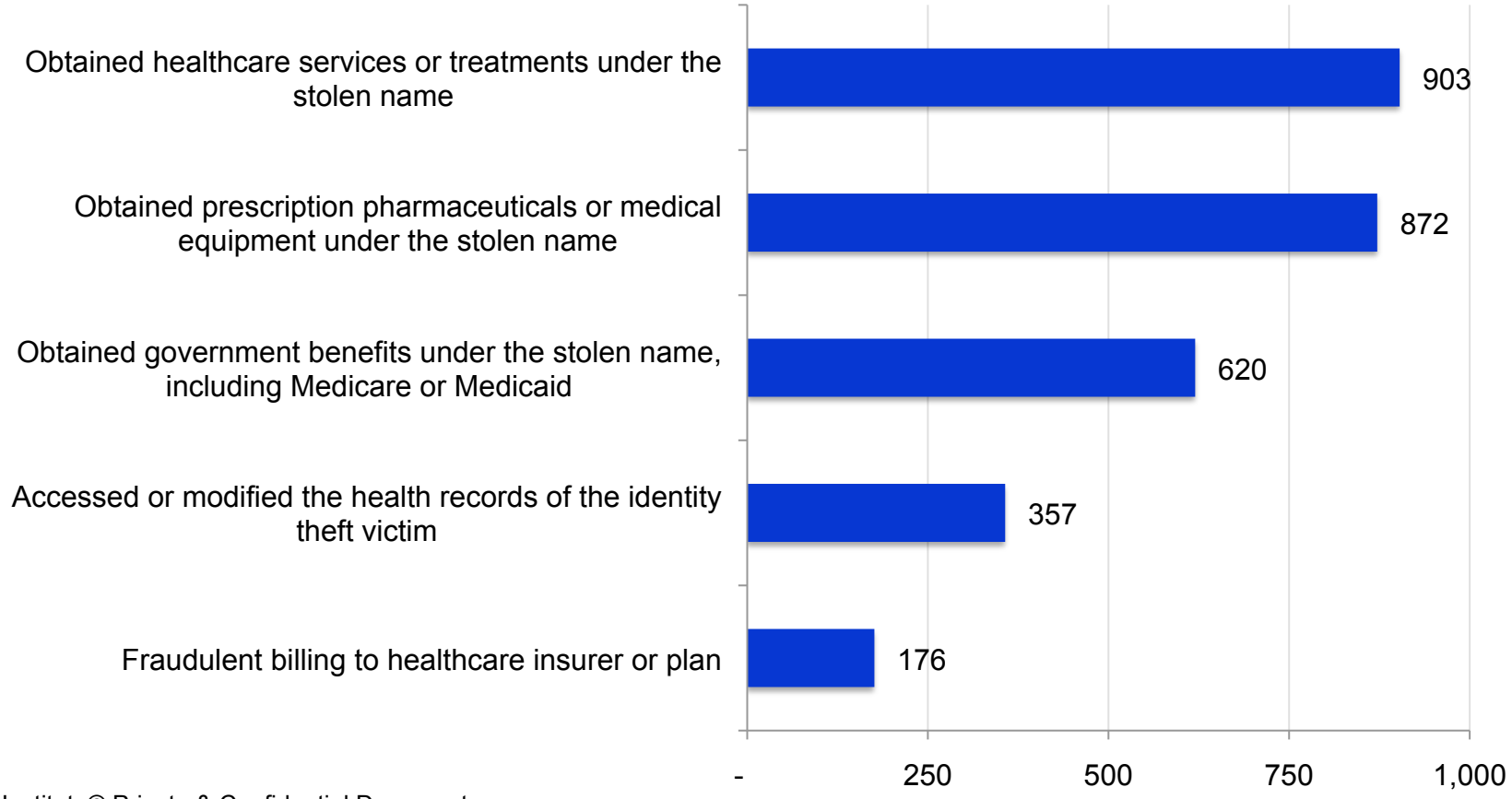


Response & Screening Procedures

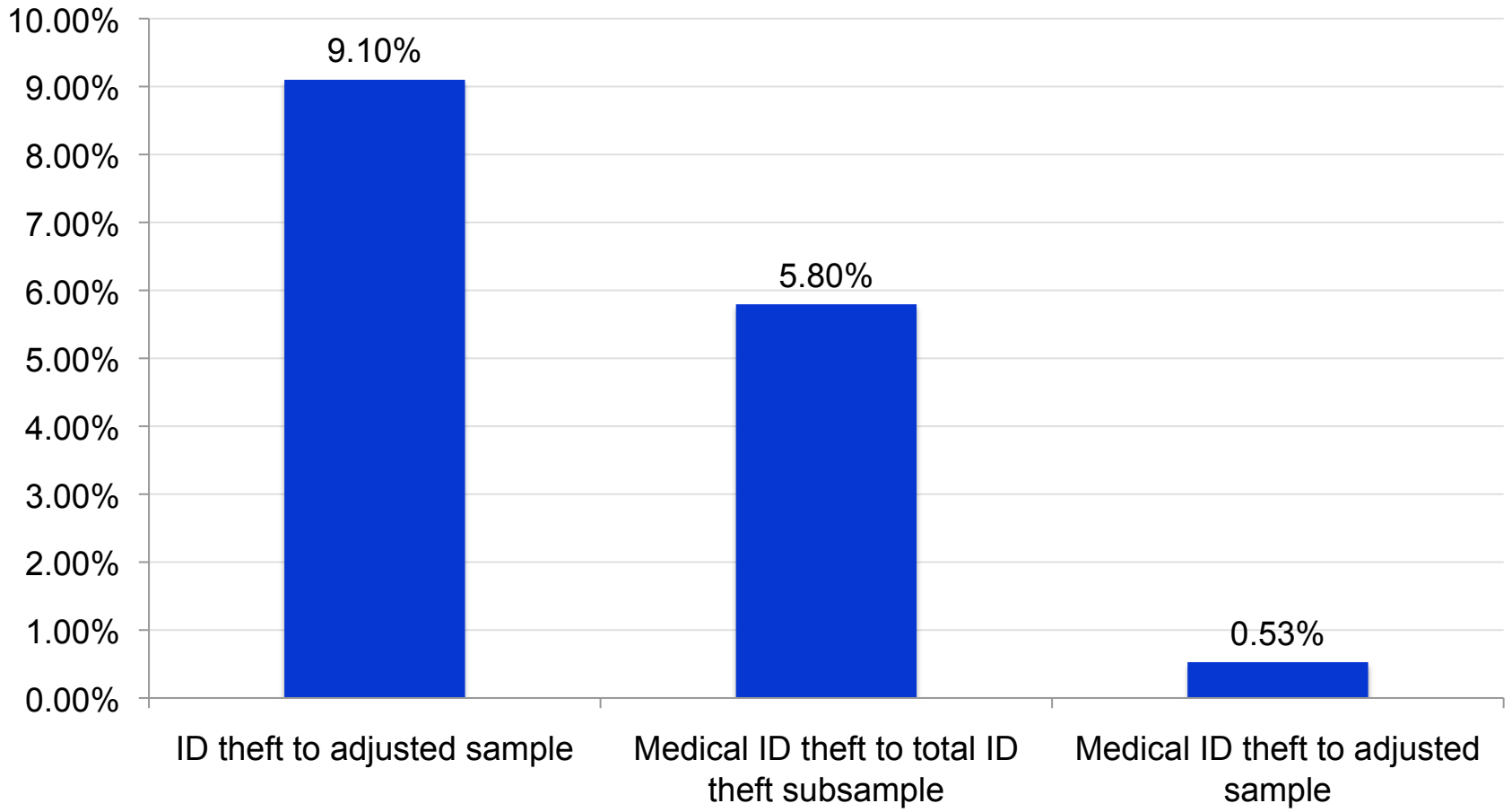


Events Surrounding Medical Identity Theft

This chart reports five events surrounding the medical identity theft incident. Please note that the existence of one or more events was not a sufficient condition for determining inclusion in the final sample of 716 individuals.



Key Percentage Responses



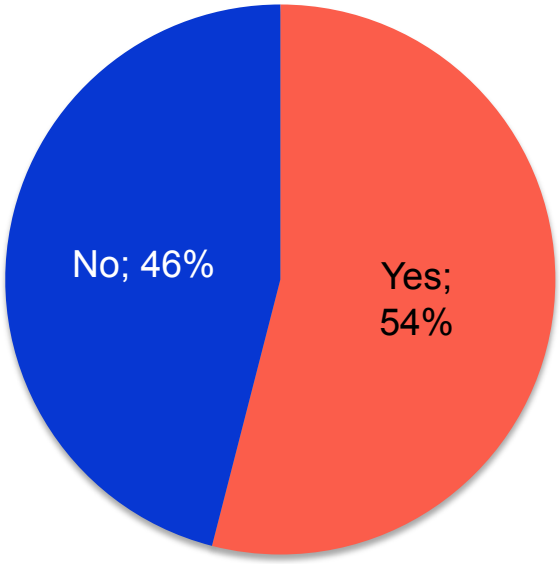
Facts about the Incident

How did you learn about the medical identity theft?	Pct%
Collection letters from creditors	40%
Actual mistakes in medical file	29%
Credit report inconsistencies	15%
Errors or inconsistencies on invoices	9%
Data breach notification	6%
Other	1%
Total	100%

How long ago did this medical identity theft incident take place?	Pct%
Less than three months	8%
Between three and six months	9%
Between six and twelve months	26%
Between one and two years	18%
More than two years	10%
Don't have the facts	29%
Total	100%

Low Fraud Reporting Rate

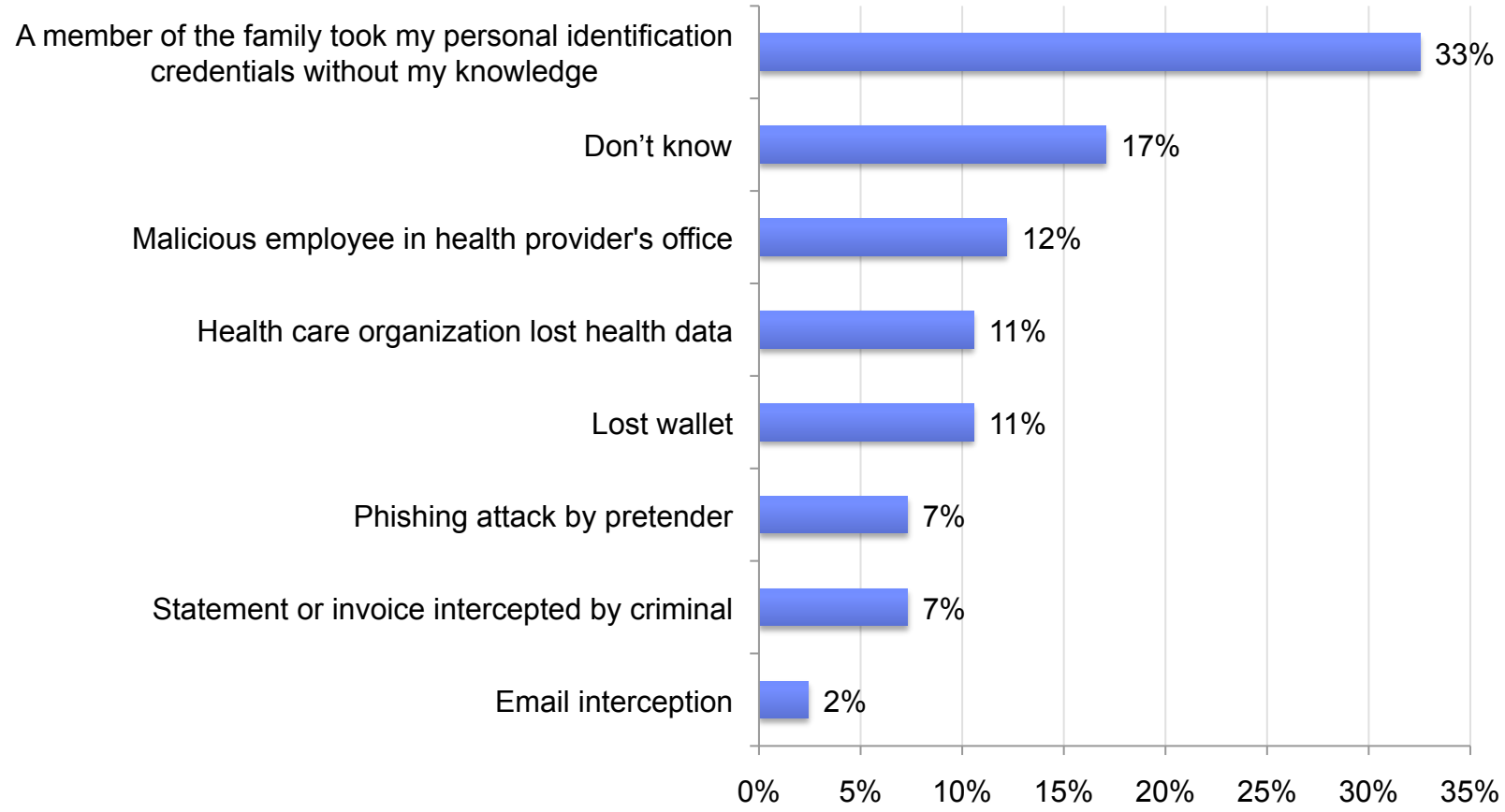
Was the medical identity theft incident reported to law enforcement or other legal authorities?



If no, why wasn't this incident reported?	Pct%
I knew the identity of the thief and did not want to snitch on him or her.	49%
I did not think the police would be of any help.	43%
I was not harmed by the incident and didn't want to make a fuss.	36%
Don't know	32%
I did not have the time to file a police report.	11%
I did not want to alarm my family.	9%
Other	5%

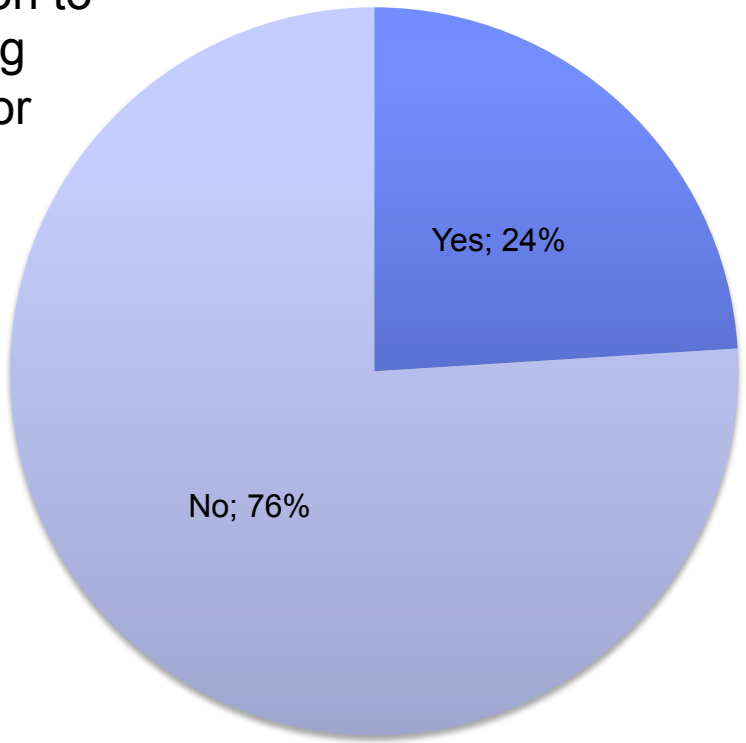
Root Causes of the Crime

To the best of your knowledge, how did this medical identity theft happen?



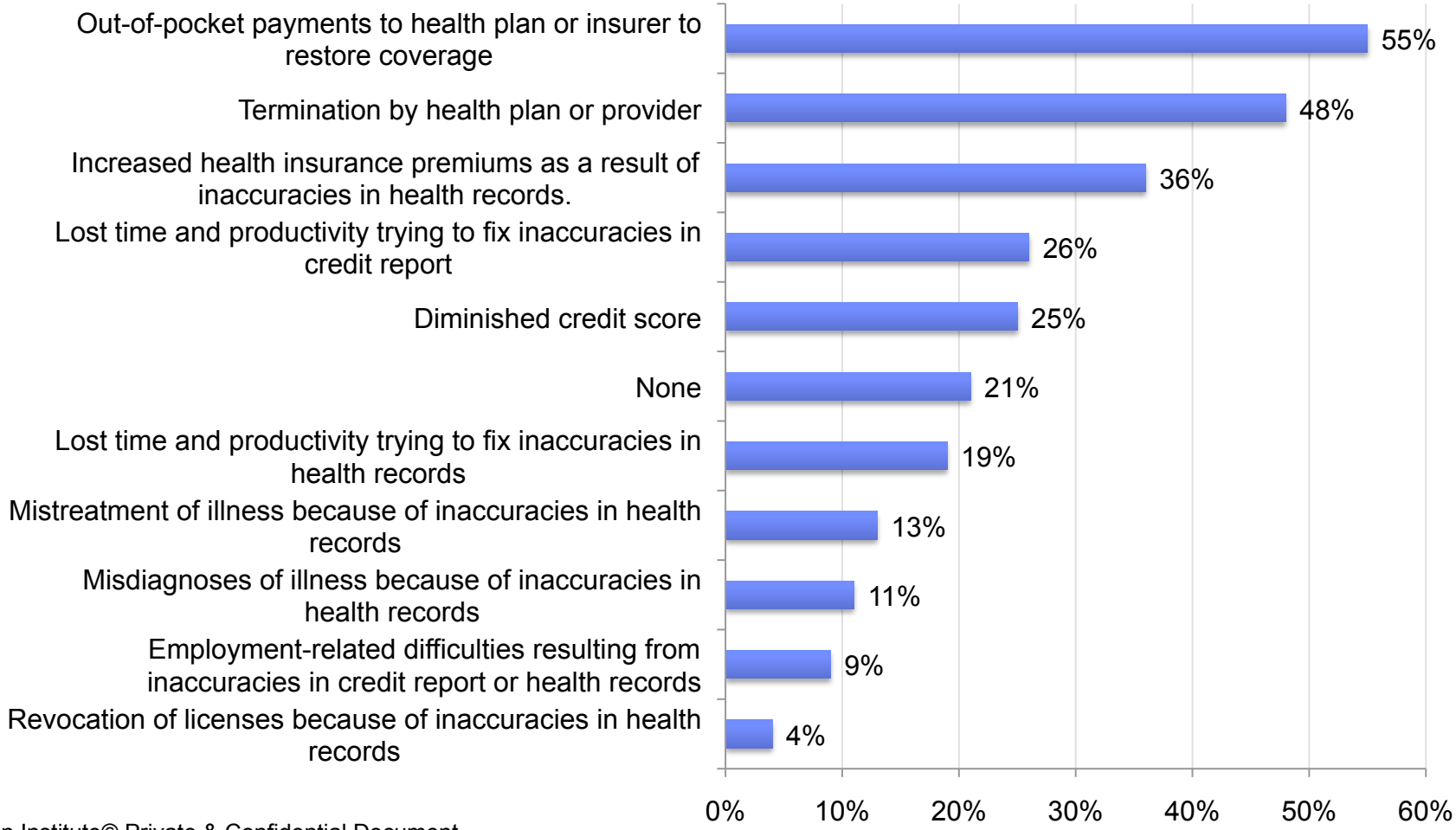
Family Members Share Medical Identification Credential

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



Consequences of the Crime

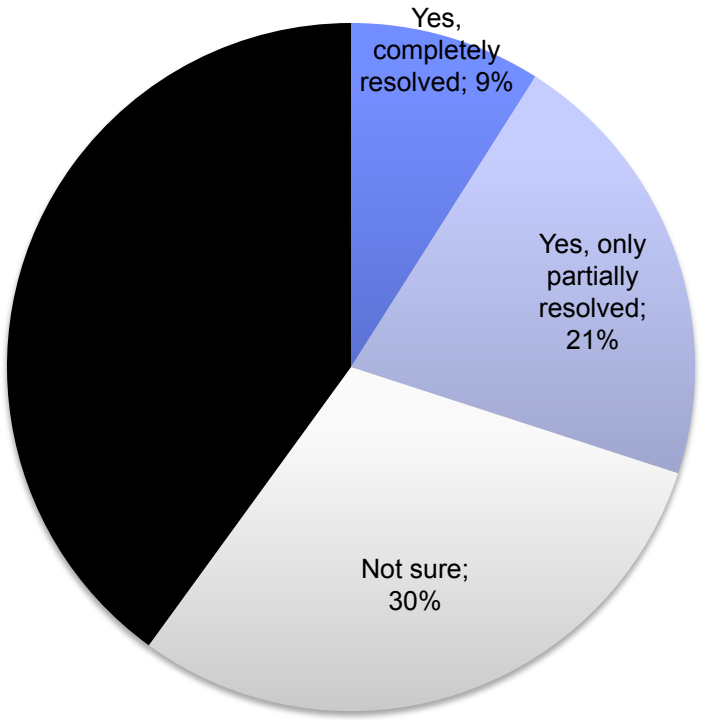
What were the consequences of the medical identity theft?



Resolution of the Crime

If yes, how did you resolve this medical identity theft incident? Please select all that apply.	Pct%
Paid healthcare provider (or repaid insurer) for services obtained by imposter	42%
Worked with law enforcement to track down identity thieves	20%
Engaged an identity protection service provider to assist in restoring records	19%
Contacted health plan and/or insurer to fix inaccuracies in medical records	14%
Obtained and carefully reviewed credit reports	14%
Contacted credit bureaus to fix inaccuracies in the credit report	12%
Placed a fraud alert on credit report	10%
Contacted credit bureaus to freeze credit report	9%
Engaged law firm to assist in restoring identity	9%

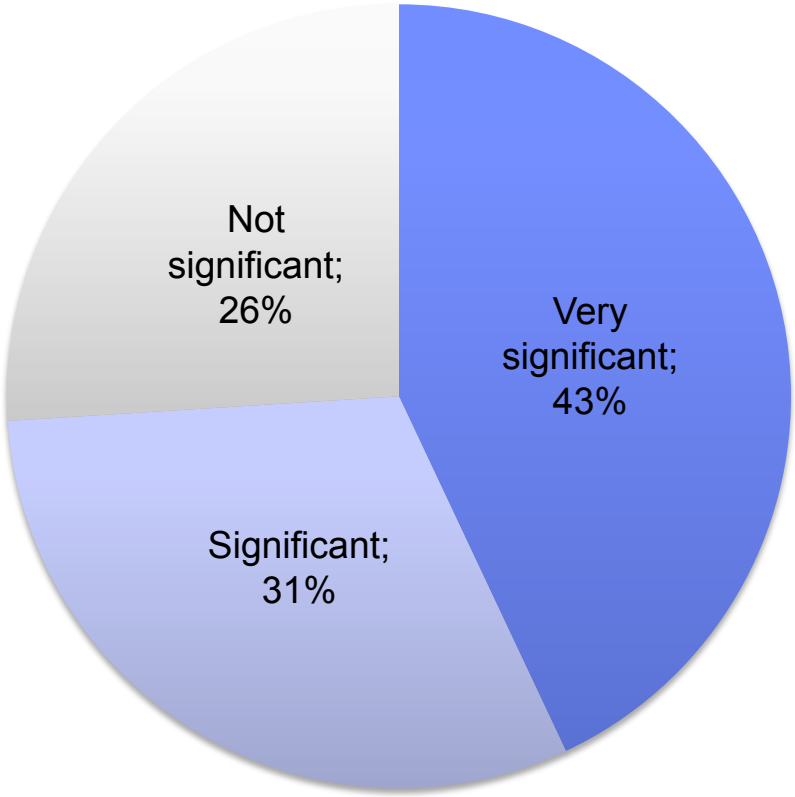
Did you or your immediate family members resolve this crime and restore identity?



Cost in Resolving the Crime

Approximately, what were the **total dollars** lost in trying to resolve this medical identity theft incident?	Pct%
None	0%
Less than $100	0%
Between $101 and $1,000	12%
Between $1,001 and $5,000	27%
Between $5,001 and $10,000	22%
Between $10,001 and $25,000	12%
Between $25,001 and $50,000	15%
Between $50,001 and $100,000	9%
Greater than $100,000	3%
Total	100%

In your opinion, how much effort was expended to resolve this medical identity theft incident?



Attributions

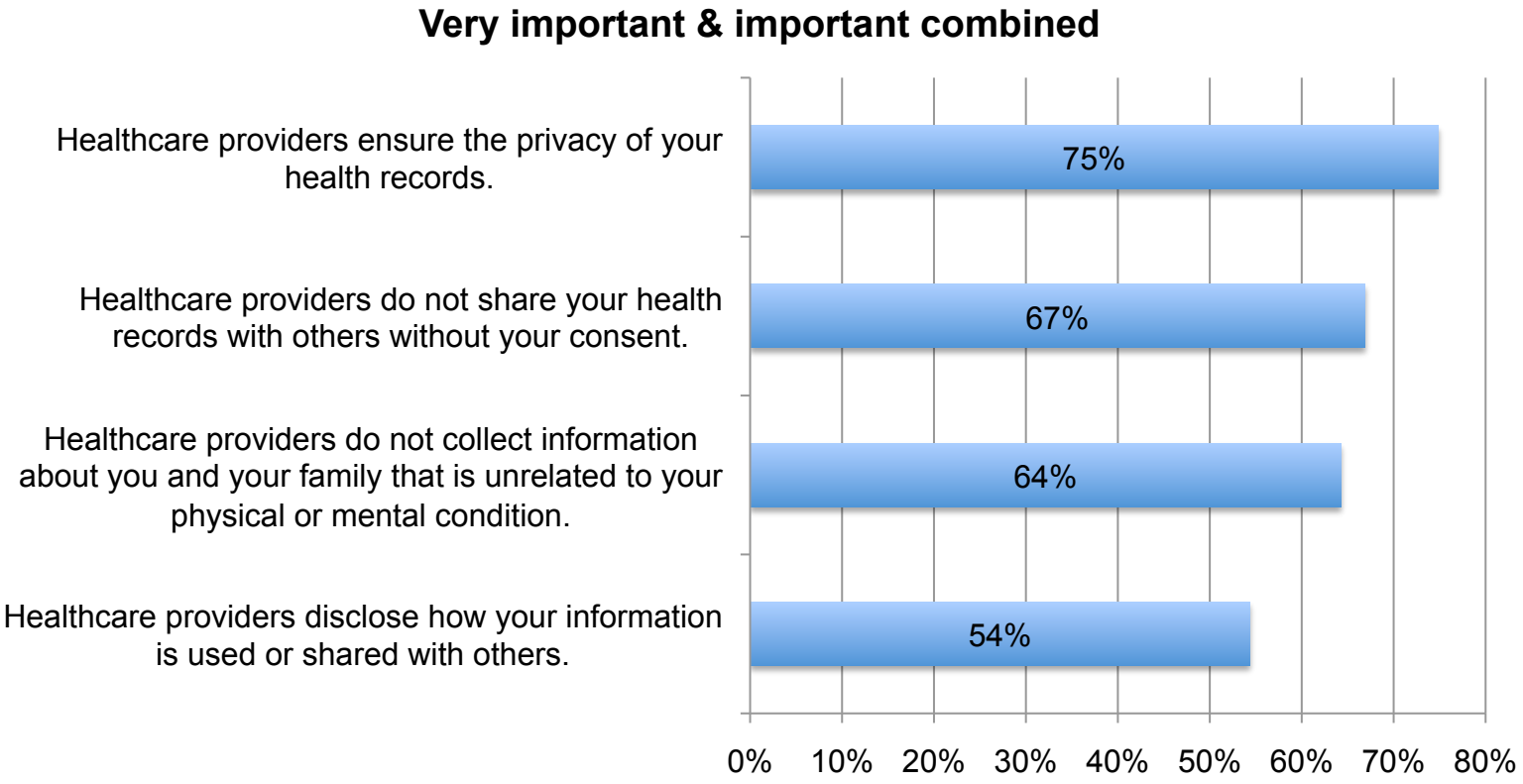
A five-point adjective scale from strongly agree to strongly disagree was used to rate each statement listed below. Only the strongly agree and agree response combined are reported in percentage terms.

Attributions. Please rate each one of the following seven statements using the scale provided.	Strongly agree & Agree responses
The protection of my personal health information is very important.	74%
The medical identity theft caused me to lose **trust and confidence** in healthcare organizations.	55%
Healthcare providers did a **good job** in helping to restore identity.	35%
Government authorities did a **good job** in helping restore identity.	21%
Credit bureaus did a **good job** in helping restore identity.	19%
Law enforcement did a **good job** in helping restore identity.	18%
Health insurer or plan did a **good job** in helping restore identity.	16%


Smart Card
Alliance
Americans' Perceptions about Healthcare Privacy
Ponemon
INSTITUTE

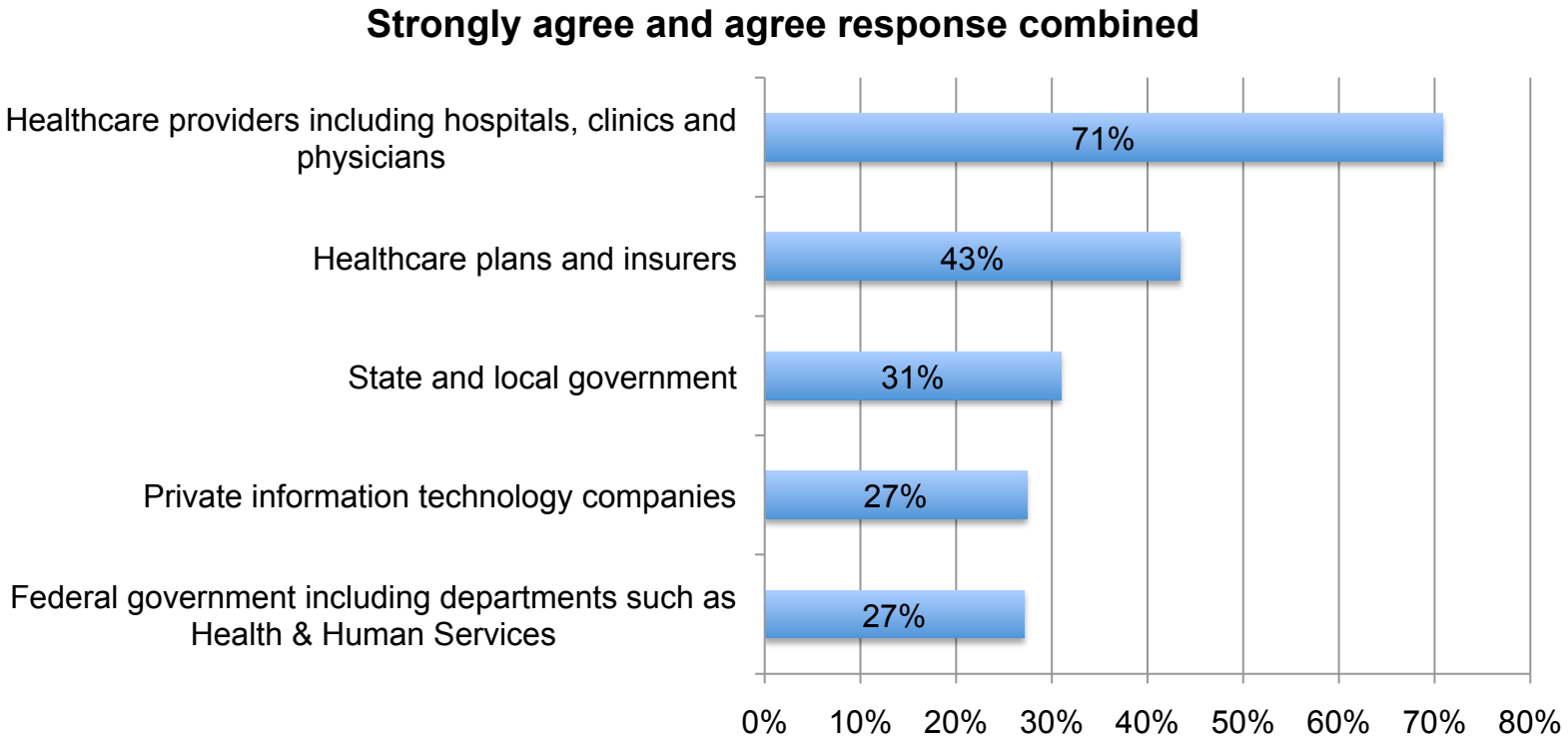
How Important Are the Following Issues?

Based on an independent sample of 883 adult-aged respondents. See Americans' Opinions about Healthcare Privacy (dated February 1, 2010).



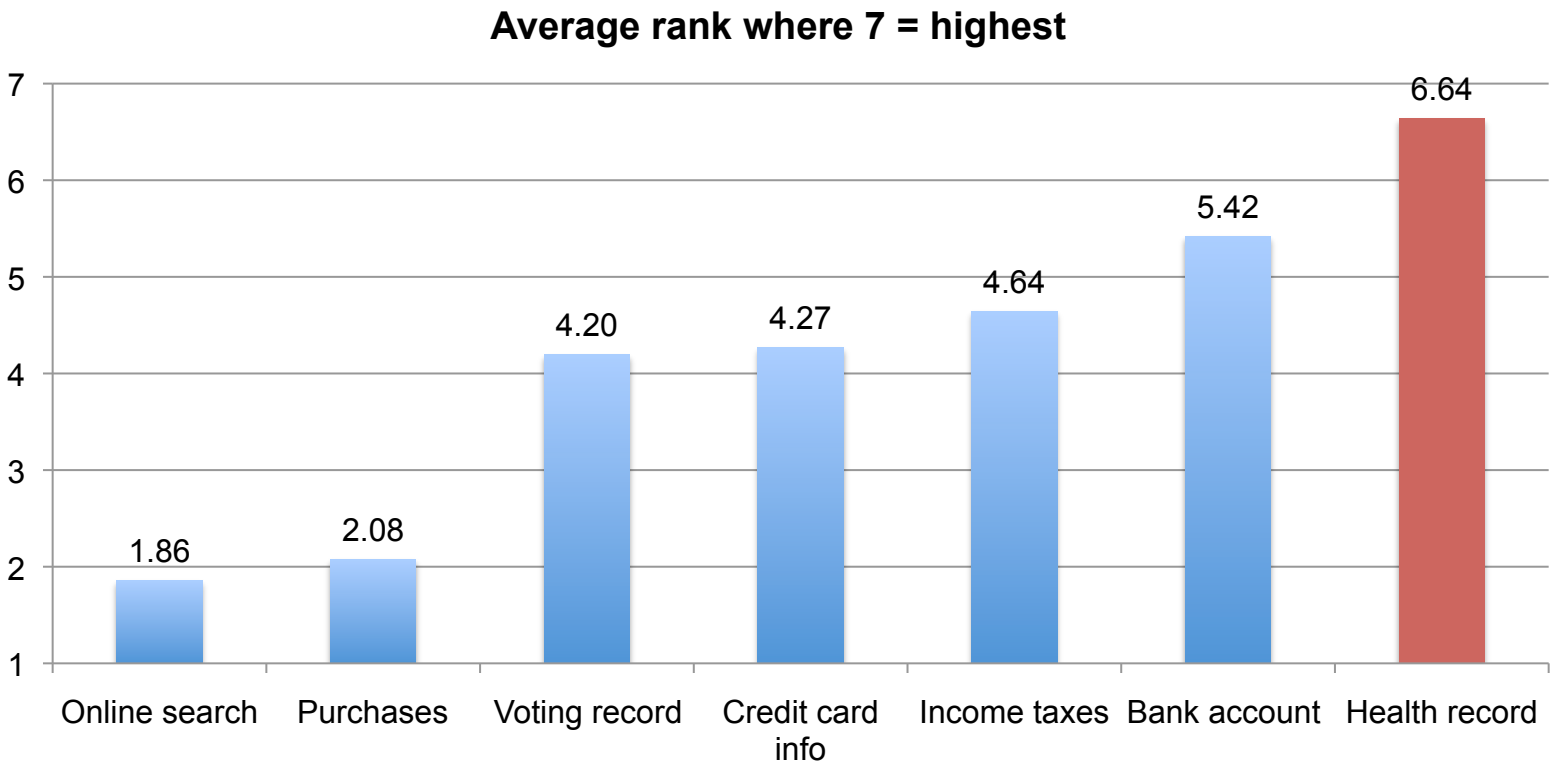
Who Do You Trust for Privacy of your Healthcare Records?

Based on an independent sample of 883 adult-aged respondents. See Americans' Opinions about Healthcare Privacy (dated February 1, 2010).



How Important Is the Privacy of the Following Seven Data Types?

Based on an independent sample of 883 adult-aged respondents. See Americans' Opinions about Healthcare Privacy (dated February 1, 2010).



What We Learned

- More than 73 percent of respondents do not trust the federal government, including departments such as the U.S. Department of Health and Human Services, to protect the privacy of their health records.
- In contrast, 71 percent of respondents do trust healthcare providers such as hospitals, clinics and physicians to protect the privacy of their health records.
- The protection of the privacy of healthcare records is considered very important or important by 75 percent of respondents.
- Sixty-seven percent believe it is very important or important not to share their health records without their consent.

Electronic Medical Record Security and Privacy

Deven McGraw
Director, Health Privacy Project
Center for Democracy and Technology

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

Health Privacy Project at CDT

- Health IT and electronic health information exchange are engines of health reform and have tremendous potential to improve health, reduce costs and empower patients.
- Some progress has been made on resolving the privacy and security issues raised by e-health – but gaps remain and implementation challenges loom.
- Project's aim: Develop and promote workable privacy and security policy solutions for electronic personal health information.

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

People Want Health IT - but Also Have Significant Privacy Concerns

- Survey data shows the public wants electronic access to their personal health information.
- But a majority - 67% - also have significant concerns about the privacy of their medical records (California Healthcare Foundation 2005; more recent AHRQ focus groups confirm).

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

Health IT Can Protect Privacy – Also Magnifies Risk

- Technology can enhance protections for health data (encryption; role-based access; identity proofing & authentication)
- But moving & storing health information in electronic form - in the absence of strong privacy and security safeguards - magnifies the risks.
  - Recent thefts of laptops, inadvertent posting of data on the Internet, "snooping," medical identity theft
  - Cumulative effect of these reports deepens consumer distrust

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

A Comprehensive Approach Is Needed

- Privacy and security protections are not the obstacle - enhanced privacy and security can be an **enabler** to health IT.
- A comprehensive privacy and security framework is needed to facilitate health IT and health information exchange.
  - Build on HIPAA for traditional health care entities (ARRA took first steps here)
  - Establish new protections to address concerns raised by access to information outside of the health care system
  - Hold all who handle health data accountable for complying with baseline protections

KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

Opportunities to Strengthen Protections in Post HITECH Era

- Modifications to HIPAA Privacy and Security Rules
- "Meaningful Use" and EHR Certification Criteria
  - Medicare and Medicaid incentive payments under HITECH only available to providers and hospitals who are "meaningful users" of certified EHR technology
- NHIN standards/requirements
- FTC Red Flag Rules

KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

HIPAA Rule Changes in HITECH

- New breach notification rules for HIPAA covered entities (in effect)
  - Individuals and federal authorities required to be notified in the event of a "breach"
  - Definition of breach is broad – but must cause significant risk of harm
  - Safe harbor for encryption
- Strengthened right of patients to receive accounting of disclosures (in effect on 2011 at the earliest)
  - Entities using EHRs cannot rely on TPO exemption
  - Certification standard in IFR; recent HHS RFI
- Increased civil penalties; state AG enforcement

KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

Meaningful Use Criteria – Stage 1

- Must do security risk assessment and address deficiencies (in proposed rule from CMS)
- Not meaningful user if fined for significant violation of HIPAA rules (proposed by Health IT Policy Committee, not in proposed rule)
- May be more specific requirements in Stage 2 (begins 2013)

Certification Criteria – Stage 1

- EHRs must include the capability to (from IFR):
  - Assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information.
  - Permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency.
  - Terminate an electronic session after a predetermined time of inactivity.
  - Encrypt and decrypt electronic health information according to user-defined preferences (e.g., backups, removable media, at log-on/off) in accordance with the standard specified in Table 2B row 1.

KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

Certification Criteria – Stage 1 (cont.)

- **EHRs must include the capability to (from IFR):**
  - **Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified in Table 2B row 2.**
  - **Record actions (e.g., deletion) related to electronic health information in accordance with the standard specified in Table 2B row 3 (i.e., audit log), provide alerts based on user-defined events, and electronically display and print all or a specified set of recorded information upon request or at a set period of time.**
  - **Verify that electronic health information has not been altered in transit and detect the alteration and deletion of electronic health information and audit logs in accordance with the standard specified in Table 2B row 4 (secure hashing algorithm).**

Certification Criteria – Stage 1 (cont.)

- **EHRs must include the capability to (from IFR):**
- **Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information.**
- **Verify that a person or entity seeking access to electronic health information across a network is the one claimed and is authorized to access such information in accordance with the standard specified in Table 2B row 5.**
- **Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in Table 2B row 6 (date, time, patient ID, user ID, and a description of the disclosure).**

NHIN Standards/Requirements

- NHIN Direct technical working group establishing technical standards/protocols (www.nhindirect.org)
- Health IT Policy Committee working on NHIN policies, including trust framework (identification, authentication, secure routing) and governance
- State HIE national and state policies and standards – less clear (further work by ONC & Health IT Policy Committee)
  - According to HITECH, must be business associates under HIPAA.

KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

FTC Red Flag Rules

- Adopted in 2008 in response to enactment of Fair and Accurate Credit Transactions Act
- FTC interpreted "creditor" to apply to any business (including physicians and hospitals) that sell services now and bill customers later
- Provider groups have filed lawsuits challenging this interpretation
- FTC keeps extending enforcement deadline due to controversy (recently extended thru 12/31/10)
- Bill to exempt medical practices with 20 or fewer employees unanimously passed the House

FTC Red Flag Rules (cont.)

- Businesses/organizations subject to rules must develop written identity theft prevention programs to detect warning signs or "red flags" of identity theft and mitigate potential harm to consumers.
- An identity theft prevention program must include reasonable policies and procedures to:
  - Identify relevant Red Flags for those accounts covered by the rules and incorporate those Flags into its program
  - Detect Red Flags that have been incorporated into the program
  - Respond appropriate to any detected Red Flags
  - Update the program periodically to reflect changes in risk
    - (See worldprivacyforum.org paper with suggestions for health care providers)

Identity Theft in Healthcare

A Provider Perspective

Paul Brian Contino
Vice President of Information Technology
Mount Sinai Medical Center

Mount Sinai

M S S M

Mount Sinai Medical Center

- Founded in 1852
- 1,171-bed tertiary-care teaching hospital
- Mount Sinai Hospital of Queens (235 bed)
- Medical School and Graduate School

- 1,000,000 patient visits per year
- 100,000 emergency room visits

- Database of over
  3.7 million patients

Importance of Patient Identity

- **Is the patient in front of us who they say?**
  - Patient Safety - appropriate medical care
  - Avoid potential medical errors
- **Link patient to existing medical records**
  - Continuity of Care
  - Provide clinical data to healthcare providers
- **Medical billing and claims processing**
  - Fraud and Abuse
  - Medical Identity Theft

Identity Theft – A Difficult Crime

LifeLock CEO's Identity Stolen 13 Times

May 18, 2010

http://www.wired.com/threatlevel/2010/05/lifelock-identity-theft

Medical Identity Theft

- Considered one of the fastest growing crimes in America (FTC, FBI)
- Nearly 1.5 million Americans have been victims of medical identity theft with an estimated total cost of $28.6 billion. (Ponemon Institute)
- Average personal expense $20,000 per incident

Medical Identity Theft

- "Fraud resulting from exposure of health data has risen from 3% in 2008 to 7% in 2009, a 112% increase (Javelin Strategy and Research)
- It takes more than twice the time to detect medical information fraud and more than twice the cost as compared to other types of identity theft. (Javelin Strategy and Research)
- Despite requirements that data be encrypted, the U.S. Department of Health and Human Services has announced that between January 1 and March 9, 2010 at least 74,962 unencrypted health records had already been breached. (HHS)"

Medical Identity Theft

- **2006 report - The World Privacy Forum Medical Identity Theft : The Information Crime that Can Kill You**

- **Medical Identity Theft can cause** significant financial impact **but also risk physical harm**
- **Inaccurate medical information may be recorded in a patient records.**
- Real danger of erroneous diagnosis and treatment due to false information contained in medical records.
- **Blood type, current medications and chronic medical conditions**

The Ill Effects of MIT

You may be a victim of Medical Identity Theft if:

- **You get a bill for medical services you didn't receive**
- **A debt collector contacts you about medical debt you don't owe**
- **You order a copy of your credit report and see medical collection notices you don't recognize**
- **You try to make a legitimate insurance claim and your health plan says you've reached your limit on benefits**
- **You are denied insurance because your medical records show a condition you don't have.**

Medical Identity Theft

- Denial of Insurance Coverage
- Insurance Caps
- Loss of Reputation
- Credit Rating
- Medical Record clean up

Detecting Medical Identity Theft

Pay close attention to your medical, insurance and financial records

- **Read the explanation of benefits (EOB) statements**
- **Review credit reports**
- **Obtain copies of your medical records**

The Challenges Ahead

ARRA (Carrot) / HITECH (Stick)

The proliferation of electronic medical records, (insurance and payment data), health information exchanges

- **Health Networks (RHIO, HIE, HIO, NHIN)**
- **Large sets of data available online, frequent data breaches**
- **Rapid exchange of data can exacerbate issues**
- **Healthcare traditionally a lower security sector**

An Ounce of Prevention

You can minimize your risk of Medical Identity Theft

- **Verify a source before sharing information**
- **Safeguard medical and insurance information**
- **Careful what you throw in the trash**
- **Careful what you share online (social media etc)**

Mount Sinai Health Card

- **Identity Management**
  - Photograph
  - Patient Name
  - Medical Record Number
  - Demographics (chip)
- **Registration Efficiency**
  - Positive ID
  - Barcoded MRN
  - Linkage to Patient Records

Conclusions

Randy Vanderhoof
Executive Director, Smart Card Alliance

Questions and Answers

- Randy Vanderhoof, rvanderhoof@smartcardalliance.org
- Larry Ponemon, research@ponemon.org
- Deven McGraw, deven@cdt.org
- Paul Contino, paul.contino@mountsinai.org

Smart Card Alliance

191 Clarksville Rd. · Princeton Junction, NJ 08550 · (800) 556-6828

rvanderhoof@smartcardalliance.org • www.smartcardalliance.org