HEALTH CARE FRAUD AND MEDICAL IDENTITY THEFT IN CANADA AND USA

BY JOHN DUMFRIES CGA,CFE,CIA

October 9, 2012

The Institute of Internal Auditors Canada | Institut des vérificateurs internes Canada

Your Presenter

John Dumfries CGA, CFE, CIA

Agenda

- Discuss reasons for the new BC CareCards, the features & limitations of the new BC CareCards.
- Discuss problems with the existing BC CareCard system.
- Examine health care fraud and Medical Identity Theft in BC, Alberta, Ontario, Quebec & USA.

  (problems, solutions and current existing research)
- Discuss results of my survey regarding the public's perception of CareCards and Medical Identity Theft in BC

New Health CareCards

- The BC government announced on May 20, 2011, that they will be replacing the existing health CareCards with new smart cards that have enhanced security features.
- This will cost approximately $10 million to implement and $28 million each year to operate over the next 5 years.
- BC's health ministry estimates it is being defrauded of potentially $260 million every year. This is based on The Canadian Health Care Anti-fraud Association's estimate that health care fraud is between 2% and 10% of total dollars spent.
- The ministry also stated that it would implement anti-fraud detection software and hire more staff to operate the system.
- The government also plans on amending the information and privacy law that will allow secure online access to health records.

Reasons for New CareCards

- There are 9.1 million BC CareCards in circulation for a population of only 4.5 million.

- CareCards currently do not have modern security features and are easy to counterfeit and therefore it is a possibility that medical identity theft occurs.

- The new CareCards will better enable an electronic health care record system.

New CareCard Features

The new BC CareCard will have the following security features:

- Counterfeit-prevention devices like a security chip, holographic overlays and laser engraving of the cardholder's image and signature, plus a second "ghosted" image printed at a different depth.

- New polycarbonate card stock, which is much more tamper-resistant and durable.

The card will be free and only those over 19 will have to re-enrol.

Drivers will be able to re-enrol when they renew their driver's licence every five years. Non-drivers will have a similar cycle.

Present CareCard System

- A fee is not charged for a card issued when a person first enrols with MSP or for the first gold CareCard issued to a senior.
- A fee may be charged to replace a lost, damaged or stolen card.
- If payment is required, the fees are $20 for one card, and more depending on the number of cards that need to be replaced in a family.
- According to the Ministry of Health website, Using a Personal Health Number other than the one issued to you or allowing someone to use your number is an offence under the Medical Protection Act.
- The website also mentions how to report fraud.

http://www.health.gov.bc.ca/msp/infoben/carecard.html#replace

New CareCard Limitations

- No mention by the government that the new cards will detect and prevent other forms of health care fraud and abuse.

- No mention by the government that the new cards will detect and prevent health care practitioner identity theft.

- The new CareCard as part of an electronic health record system may cause information to be more vulnerable to data breaches.

Risks of Electronic Health Records
(According to BC Civil Liberties Association)

1)Privacy breaches from malicious insiders that abuse their right of legitimate access to the system.

2) Insiders collecting the information and selling it on the black market.

3)Risks when health care staff put information on a laptop, smart phone or memory stick.

4)Constant surveillance.

Issues and Possible Solutions

- Are there really approximately 2 cards for every person in BC?

- Is this an internal recordkeeping problem and/or processing coverage change problem?

Since BC residents have to go through the process of card/license renewal and pay for the new cards as taxpayers:

- Do they really think that the extra cards in circulation is a problem?
- Do they think that the benefits of the new cards exceeds the cost to implement the new cards?
- Should the government issue the new cards or pursue other solutions to reduce medical identity theft?

My Research Goals and Methodology

- I researched Medical Identity theft in Alberta, Ontario and Quebec.

- I also researched Medical Identity theft in the United States as well as legislative and technological solutions.

- I conducted an online survey gauging the public's perception of the effectiveness of the new BC Health CareCards in reducing Medical Identity theft.

Polling Question #1

In which industry do you work?

(if internal audit, what is the industry of your employer)

- Health care
- Insurance
- Law enforcement
- Regulatory agency
- Finance
- Accounting and audit (public practice)
- Other

Definition of Medical Identity Theft

The World Privacy Forum's 2006 report "The Information Crime That Can Kill You" defines Medical Identity Theft as "when someone uses a person's name and other parts of their identity without the victim's knowledge or consent to obtain medical services".

Consequences of Medical Identity Theft

- CareCards can be counterfeited and sold on the black market.
- Stolen CareCards or personal health information can be used to conduct financial identity theft.
- Addicts can abuse the system by falsely obtaining drugs.
- People use medical services that they are not entitled to receive. This causes medical records to be inaccurate.

Solutions to Health Care Fraud in BC

- Billing Integrity Program
- Other Investigations
- Identity theft and the Canadian Criminal Code
- Canadian Identity Theft Support Centre

Billing Integrity Program

- The Billing Integrity Program (BIP) provides audit services to the Medical Services Plan (MSP) and the Medical Services Commission (MSC).
- The MSC is authorized and obligated to monitor the billing and payment of claims on behalf of MSP beneficiaries.
- The BIP is supported by the B.C. Medical Association and other respective health care associations.
- Under the Senior Manager of BIP, a staff of medical consultants, research analysts and a team of auditors work closely with the Ministry of Attorney General, ICBC, WorkSafe BC and the RCMP.
- BIP monitors MSP payments and routinely provides utilization information and statistical data to various health regulatory bodies and associations.

Billing Integrity Program (BIP)

The two main methods BIP monitors payments for services rendered by practitioners:

Service Verification Audits – Annually approximately 75,000 letters are sent to patients confirming that they received services which were billed to MSP.

Practitioner Profiles - An analysis of the type and number of insured services, registered specialties, that a practitioner has billed to MSP. Each practitioner within an individual peer group is then compared against the group average statistics.

Billing integrity program since 2005 has recovered $8 million. $1.6 million has been recovered in fiscal year (2011/2012).

In 2010/2011, the Billing Integrity Program conducted 16 on-site medical practitioner audits. It negotiated settlements of approximately $1,080,000 for ten cases. $700,000 was recovered by BIP that year (including recoveries negotiated in previous years).

Examples of the BIP in Action

- In July 2012, the B.C. Medical Services Commission found evidence of patients being charged for publicly insured medical services at two Vancouver private health care clinics.

- Of the 468 cases reviewed by the auditors, 205 had services billed to a beneficiary contrary to Sections 17 and 18 of the Medicare Protection.

- The bills for these services totalled almost $500,000.

Other Examples of Preventing Fraud

- The Ministry of Health states that in 2009/10, it discovered 376 fraud cases with a total dollar value of $936,000.

- A survey of 399 cards in 2010 indicated that 94% of patients claiming MSP coverage were legitimate residents of BC.

Identity Theft and the Canadian Criminal Code

The Identity theft crime bill, enacted on January 8, 2010 created the following offences which are subject to 5-year maximum prison sentences:

- Obtaining and possessing identity information with the intent to use the information in committing a crime;
- Transferring or selling identity information to another person with knowledge of the possible criminal use of the information; and,
- Unlawfully possessing or trafficking in government-issued identity documents that contain information of another person.

The courts can order the offender to pay the identity theft victim for costs incurred to rehabilitate their identity and to pay restitution for actual economic losses.

Canadian Identity Theft Support Centre

- In March 2012, Canada's first support centre to provide resources for identity theft victims opened in Vancouver.
- It is a charitable organization primarily funded by the federal Justice Department.
- The support centre is modelled on the Identity Theft Resource Center based in San Diego who also helped train staff.
- They plan on releasing fiscal & complaints data in 6 months.

SECTION BREAK

Polling Question #2

Where do you primarily work?

- Alberta
- British Columbia
- Ontario
- Quebec
- Other Canada
- USA
- Other Country

Medical Identity Theft in Alberta

In October 2004, Alberta's Auditor General examined the occurrence of medical identity theft. The following are some of the results:

- In some regions near the U.S. border there were twice as many health numbers than residents.
- One Albertan was issued 60 duplicate or replacement health cards, while 32,440 people had received five or more.
- 123 municipalities had at least 2 health numbers for every person counted in the Dec. 2003 census.

The Auditor General also estimated that if 1% of the province's $8-billion annual health spending was lost due to fraud, taxpayers were losing $80 million a year.

Specifically regarding medical identity theft, in 2002-2003, a Health Ministry investigator reviewed 105 cases and found 54 ineligible numbers.

Medical Identity Theft in Quebec

- In February 2010 fraudsters allegedly obtained an RAMQ health card and 750 people used it to obtain medical care with a total value of $500,000.

- The majority of these people do not actually live in Quebec and the RAMQ has only been able to recover $42,000 of the money that was billed to taxpayers.

- The RAMQ has four inspectors in Quebec to investigate health care fraud.

Health Care Cards in Quebec

- Quebec considered smart health care cards in 2003. The cost of implementing the cards would've been $150 million, but would've saved $45 million per year.

- The card was introduced in 1970 it included the SIN of the head of the family.
- In 1976 assigned each card holder a unique permanent number.
- In 1992 The photo and signature of the holder appear on the card. A hologram was added to prevent forgeries.
- In 1995 RAMQ coordinated efforts so that the driver's license had the same photo and signature as the health insurance card.
- In 2003 Micro printing is embedded in the card.

- In December 2009, it was announced that Quebec's health care cards would include bar codes to prevent fraud. These cards will be phased in over a four year period. All cards issued as of January 11, 2010 will have this bar code. All cards are to be renewed every 4 years.

Health Care Cards in Ontario

- In 1995, Ontario issued health care cards with the person's photo and they will have to be renewed every 5 years with proof of residence. This system was estimated to have cost $30 million a year but prevent $65 million a year in fraud.

- The Ontario government estimated that in 1993, 400,000 extra cards existed. In 2005, there was approximately 300,000 extra cards.

- Another 1993 health ministry report estimated that approximately 60,000 ineligible people from outside Ontario received health care services at a cost of $85 million.

- The Ministry of Health concluded that in one investigation approximately 588 Americans might be receiving free health care that lived near the Ontario, Quebec and New York State borders.

Health Care Cards in Ontario

- According to police an Ontario Health care card sells for about $1,000 on the street.
- Of the 300,000 extra cards in 2005, 268,000 of those are in the Toronto area. 10,000 cards are in regions near the US border.
- The health ministry conducted a data integrity audit and they cancelled cards not used and those that did not respond to requests to receive a replacement card with a photo.
- Also, the health ministry cancelled 1,100 cards that had PO boxes as their address.

Health Care Cards in Ontario

- As of July 2012, there are still more than 3.5 million Ontario residents with the old health cards. Since 1995, 75% of Ontario residents have switched from the old cards to new.

- The transition from Ontario's old health cards to new ones could leave some people without coverage in an emergency, especially if they ignored notices to update their card.

- The province replaces about 225,000 of the old cards with the new cards every year. 150,000 people apply for an updated health card each year without being asked.

http://www.theglobeandmail.com/life/health-and-fitness/health/ontario-urges-residents-to-switch-to-new-health-cards/article4442365/

Medical Identity Theft in Ontario

In 1998, the Ontario government also implemented the following security measures:

- Legislation requiring health care providers to report suspected fraud and retain invalid cards;
- Swipe readers and toll-free numbers for hospitals and clinics to validate cards; and
- Special investigations unit to investigate fraud.

Medical Identity Theft in Ontario

- Medical Review Committee recommended charges on 548 physicians from 1991-2002 and $36 million was recovered.
- This committee was cancelled due to doctor backlash.
- Estimated $13 million to $17 million loss in recoveries due to the cancellation of the committee from 2003 to 2006.
- Ontario reinstated the Payment Integrity Program which is similar to BC's Billing Integrity Program.

Medical Identity Theft in Ontario

In 1998 the Ontario Ministry of Health and Long Term Care with the Ontario Provincial Police created a team of 28 officers to investigate health care fraud.

The Ministry of Health and Long Term Care (MOHLTC) funds the OPP Health Fraud Investigations unit.

The OPP health team are mandated to investigate health care frauds and related offences against the Ontario Health Insurance Plan (OHIP) and the Ontario Drug Benefit Plan (ODB).

The OPP health team defines User Fraud as “crimes related to receiving services or products that they are not entitled to or any crimes involving Ontario Health Cards”. The OPP health team also investigates Provider fraud and Drug Diversion.

Examples of User fraud (medical identity theft) are the following:

- Ontario residents who "lend" their cards to non-residents of Ontario;
- Anyone who falsely obtains a legitimate health card; and
- Anyone who receives health services or products illegally in Ontario;

Medical Identity Theft in Ontario

OPP Health Fraud Investigation Unit from 1998 to June 2012 has laid about 10,000 criminal charges and secured 1,800 convictions and had court restitution and forfeitures totalling $9 million.

Detective Staff Sergeant Scott James Unit Commander Health Fraud Investigation Unit states that “The majority of files involve fraudulent billings by physicians, pharmacists and vendors of medical equipment”.

He further states that “Consumer files are mostly persons accessing health care when not entitled because they do not meet residency requirements. Most of the health card fraud cases are residency based”.

The big change since 1998 is that there is greater awareness of the issue of health care fraud through public awareness, media campaigns and public and industry education. Having an enforcement unit for health care fraud has had a significant deterrence impact. He believes the photo health card has reduced incidents of ID crimes against OHIP.

Example of Health Practitioner Identity Theft

Health practitioner identity theft is the theft of medical professionals' identity to obtain insurance payments for services that are either never rendered, or carried out by unqualified personnel. The Insurance Bureau of Canada issued 9 official alerts regarding health practitioner identity theft in 2009 and 12 in 2010.

The following is an example of health practitioner identity theft:

- A rehab clinic investigated by the Financial Services Commission of Ontario was fined $144,000 in 2007 for stealing the identity of a Toronto psychologist and using it to make at least 29 insurance claims worth $136,000.

SECTION BREAK

Polling Question #3

Do you think that your personal health care information is adequately protected?

- Yes
- No
- Unsure

Health Care Data Breaches in Canada

- A nurse at Durham Region Health lost a USB key containing unencrypted personal information of 83,000 people in Dec. 2009.
- The USB key contained personal health information of people vaccinated against H1N1 in eight clinics from October to December 2009. It was dropped somewhere between the parking garage and the building.
- DRH agreed to pay $500,000 in a class action settlement (approx. $6 per record).
- In July 2011, Records containing the personal health information of nearly 6,500 Ontarians who took part in the colon cancer screening program may have gone missing though Canada Post's Express Post service.

Health Care Data Breaches in Canada

- In January 2011, patients at an Ottawa medical centre were warned that some of their personal information may have been on two computers that were stolen.

- The computers did not contain any medical information, but may contain other personal data of patients seen at the clinic between 1971 and July 1, 2006.

- Personal data may include name, date of birth, street address, telephone number or health card number. The data breach could affect up to 60,000 patients.

Health Care Data Breaches in Canada

- July 2011, a Regina doctor is being faulted for poor record-keeping practices after approx. 2,900 patient files were discovered in a paper-recycling bin behind a mall.

- These records were not properly marked and were stored in a non-secure storage area for 5 years prior to being recycled by cleaners.

Health Care Data Breaches in Canada

- In July 2012, a computer server containing personal medical data of nearly 13,000 students and staff at BCIT was breached.
- Information breached includes names, dates of birth, Medical Services Plan numbers, Personal Health Numbers, phone numbers, addresses, treatment billing codes and descriptions.
- A routine security audit revealed that an unauthorized third party accessed a server used by BCIT's Student Health Services Medical Clinic to upload and download movies.
- The records stored on this server contained student information for those who visited the clinic from October 2005 to June 11, 2012.

Health Care Data Breaches in Canada

- As of August 2012, five people have been fired, but none charged, after privacy breaches at Newfoundland and Labrador's Eastern and Western health authorities.
- Eastern Health announced that an employee had inappropriately accessed the medical records of 122 patients. All those patients have been informed of the breach.
- A nurse was later fired for accessing the medical records of patients not under her care.
- The health authority in western Newfoundland said it fired an employee for accessing the medical records of more than 1,000 patients.

Health Care Data Breaches in Canada

- September 2012 a total of five BC Ministry of Health staff have been fired and two remained suspended without pay over the improper use of personal health data.

- RCMP continue to investigate allegations of improper and illegal use of personal health information in medical research at UBC and the University of Victoria.

Health Care Data Breaches in Canada

- Only four provinces presently have mandatory reporting laws in place for data breaches.

- Ontario, New Brunswick and Newfoundland require mandatory reporting, but only for breaches involving health care data.

- In May 2010, Alberta became the first province to enact laws requiring reporting of all types of data breaches.

Canadian Research into Health Care Fraud and Medical Identity Theft

- Canadian Health Care Anti-Fraud Association
  (2004 Canadian Health Care Fraud Survey)
- Dr. Joan Brockman, SFU (May 2005)
- Greyhead Associates (2006)
- Phonebusters/Canadian Anti-Fraud Centre
- Fair Warning Inc.

FairWarning Inc. Study of Canadian Data Breaches

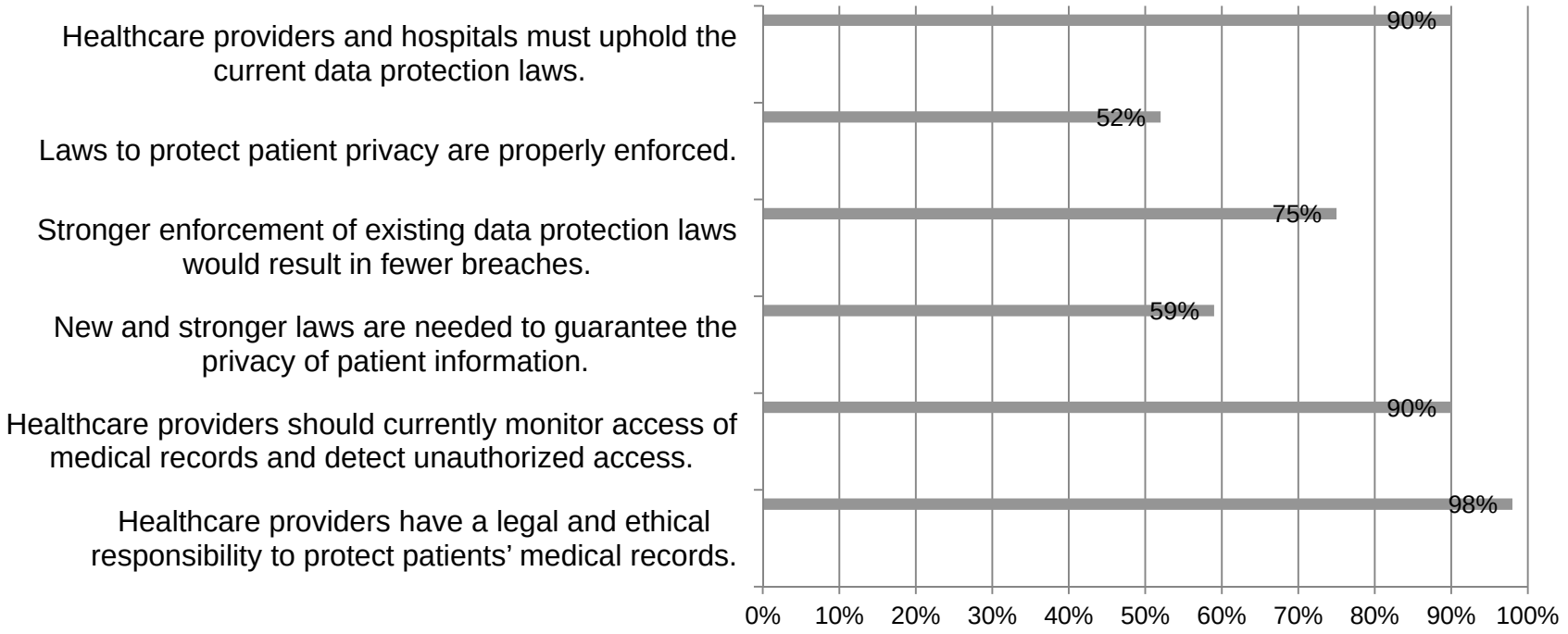
According to a survey of 1,002 patients in October 2011, 3.7% of Canadians have been data breach victims of personal health information. Causes:

- 19% health care provider employee;
- 24% family member, friend or co-worker;
- 5% criminal;
- 8% other; and,
- 43% unknown.

- Of those, 57% of victims were negatively impacted. 11% were victims of Medical Identity Theft and 11% had inaccurate medical records.

FairWarning Inc. Study of Canadian Data Breaches

Patients noted that healthcare providers and hospitals should be held responsible for following the law.



Health Care Fraud in Canada

The 2004 Canadian Health Care Fraud Survey asked 109 senior health-care insurance professionals and claims processors various questions.

The following is a summary of the results:

- 95% were healthcare claim fraud victims, 50% over 30 fraud incidents
- 77% discovered fraud through a claims review process
- 69% detected fraud from receiving external tips
- 87% indicated that Health care providers were responsible for fraud
- 9% indicated that individual policyholders were responsible for fraud

Top 2 types of fraud according to the survey:
90% - Billing for services not provided
68% - Up-coding (charging for a more expensive procedure than provided)

Canadian Medical Identity Theft Research

Greyhead Associates is the only company to perform and publish research (January 2006) in the field of Canadian medical identity theft but they did not quantify their report findings statistically. So it is difficult to draw any inferences or conclusions based on their report.

Greyhead's conclusions and recommendation include the following:

- The banking industry and healthcare operate as silos, due to different privacy requirements. Fraudsters exploit this by stealing personal data and using it for fraudulent purposes.
- Individuals should be notified of unusual activity in their electronic health records.

SECTION BREAK

Polling Question #4

Before today's presentation were you aware of medical identity theft?

Yes

No

Summary of US Researchers

- The Federal Trade Commission has compiled Identity theft statistics since 1998 based on complaints received by the Consumer Sentinel Network. They also have reported medical identity theft specifically since 2001.

- World Privacy Forum (2006) conducted interviews with stakeholders and researched existing medical identity theft statistical reports and medical identity theft civil and criminal cases.

- Booz Allen Hamilton conducted a town hall meeting of industry experts (2009).

- The Exploring Medical Identity Theft paper (2009) conducted a survey of 133 compliance officers that work in the Medical industry.

- Ponemon's Third Annual Survey (2012) on Medical Identity theft surveyed 757 victims of medical identity theft.

Summary of Recommendations from US Researchers:

- Victims of financial identity theft can use the credit reporting system to recover but medical identity theft victims lack similar resources.

- It is difficult for medical identity theft victims to determine where the theft took place because patient records are shared with various medical providers.

- Patients should monitor their credit reports and medical records.

Summary of Recommendations From US Researchers:

- Most cases of medical identity theft occur through the emergency department.
- Time constraints in admitting and registration departments may result in lack of compliance with policies and procedures related to ID verification.
- Ignorance of medical identity theft result in people being vulnerable.
- Victims are willing to share their health care information with family members.

Summary of Recommendations From US Researchers:

- Identity theft prevention should be a condition of licensing or accreditation for health care providers.
- Compliance with medical identity theft policies and procedures should be monitored.
- Reducing use of SSN during Admission and registration could reduce medical identity theft.
- Educate the public, medical staff and law enforcement of medical identity theft.
- Conduct systematic, structured surveys on the frequency of medical identity theft.

Medical Identity Theft in US Ponemon Study

According to the March 2011 Ponemon Institute study, an estimated 1.49 million Americans were medical identity theft victims at an average cost of $20,663.

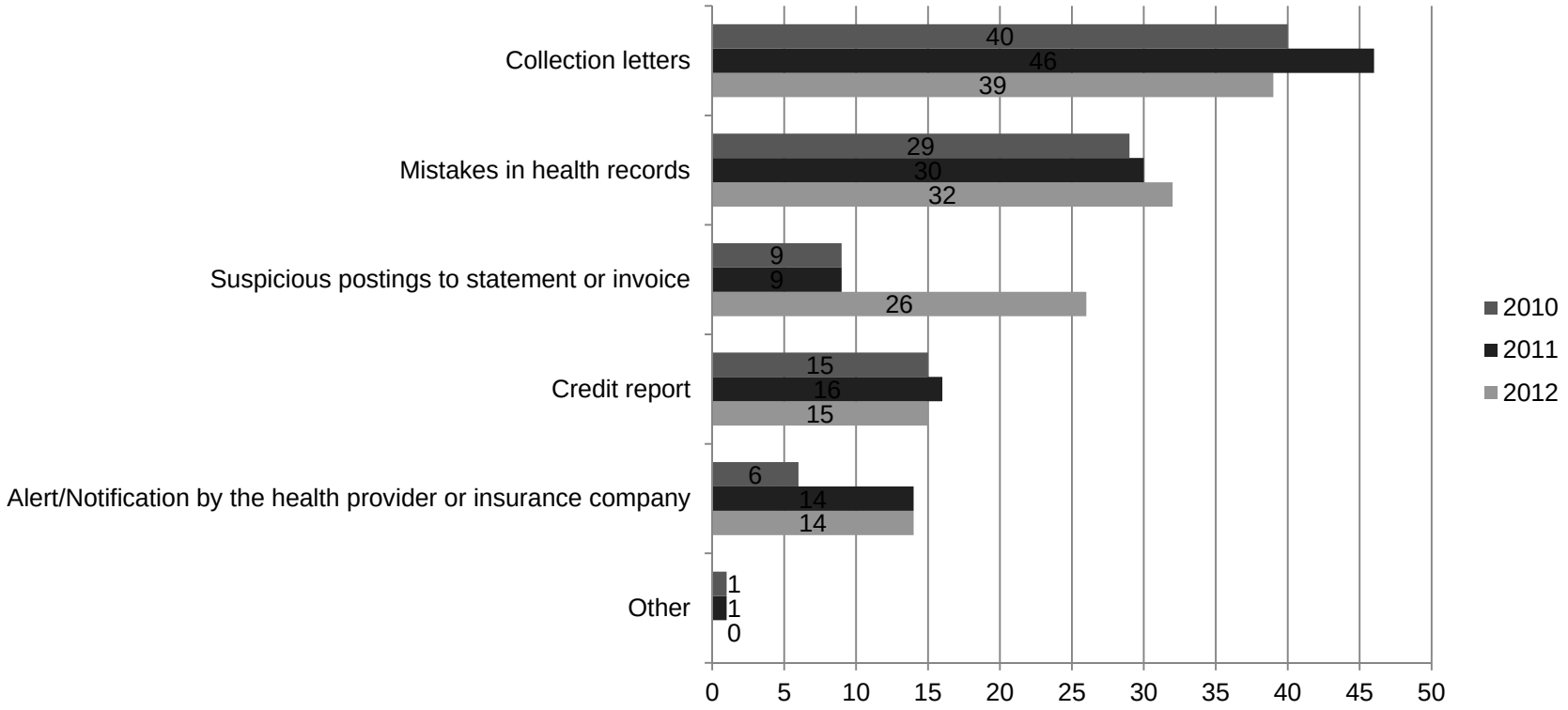
The June 2012 Ponemon Institute study estimated that 1.85 million Americans were medical identity theft victims at an average cost of $22,346.

- 41% of medical identify theft victims lost their health coverage (49% in 2011),
- 47% had to make payments to the healthcare providers in order to regain their health insurance coverage (50% in 2011), and
- 26% received mistreatment due to inaccurate medical records (28% in 2011).

- 31% of the survey respondents said they let family members use their information to obtain medical care (26% in 2011).
- Medical Identity theft is estimated to have a $41.3 billion impact on the U.S. economy, up from $30.9 billion in 2011.
- 90% in 2012 as compared to 77% in 2011 are aware of medical identity theft.

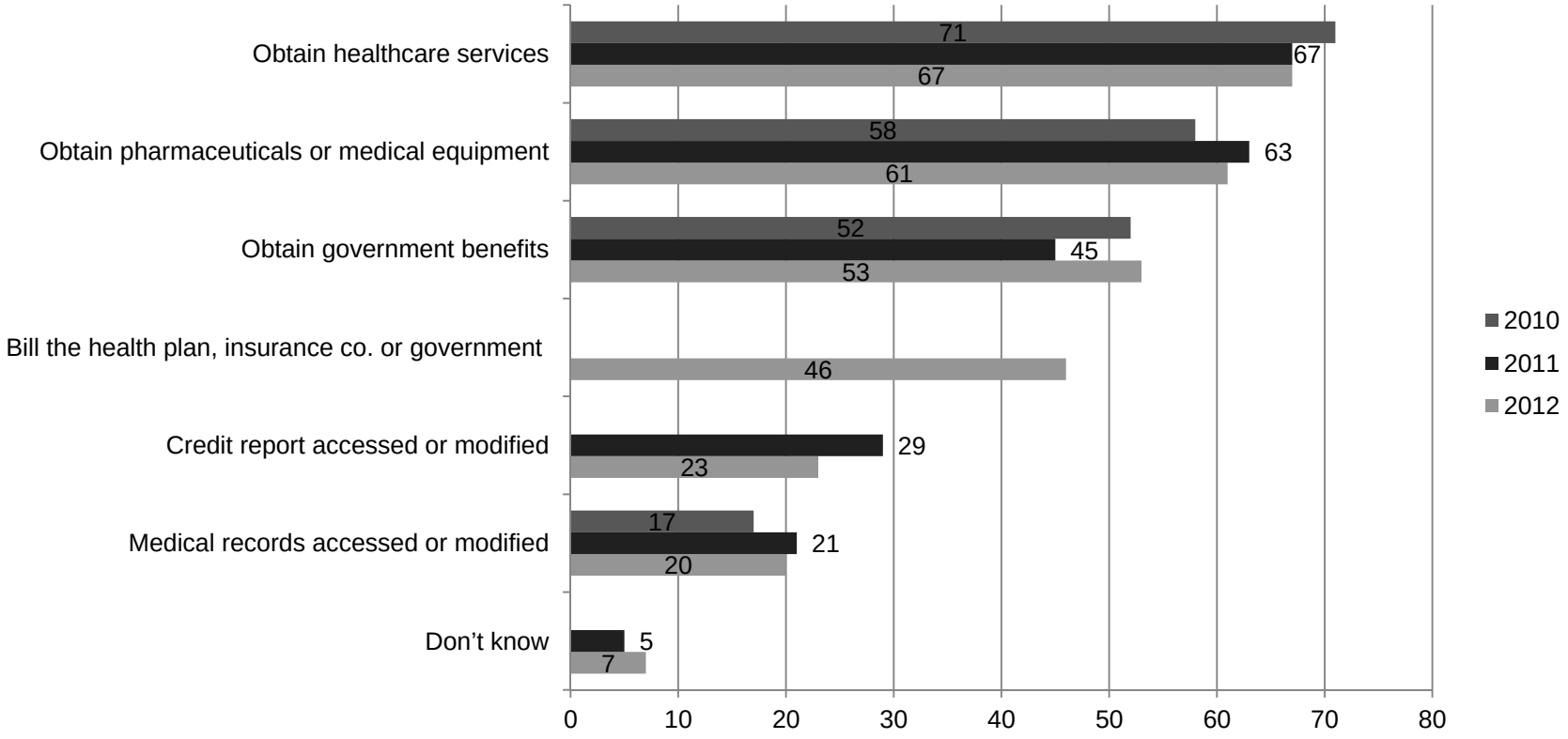
Medical Identity Theft in US Ponemon Study

- Learning of medical identity theft:



Medical Identity Theft in US Ponemon Study

- Description of identity theft incident



Medical Identity Theft in US Ponemon Study

- Cause of medical identity theft:

	2010	2011	2012
Don't know	17	17	15
Phishing attack by criminal or other	9	6	4
Lost wallet	11	9	5
Mailed statement or invoice was intercepted by the criminal	7	8	6
Healthcare provider or insurer had a data breach	11	14	6
Malicious employee in the health provider's office stole health information	12	10	7
Healthcare provider used identification to conduct fraudulent billing			22
A family member took personal identification credentials without my knowledge	33	36	35
	100	**100**	**100**

Medical Identity Theft in US

In the 2011 FTC report, Medical Identity Theft is estimated to be 1.3% of all identity theft complaints (19% of all complaints) received in 2008,2009, 2010.

A 2011 survey conducted by PWC Health Research Institute of 600 executives from US hospitals and physicians, health insurers, and pharmaceutical companies found that 36% of provider organizations had experienced medical identity theft.

A survey by Nationwide Insurance in 2012 among 2,001 adults found that only (15%) of insured adults say they are familiar with medical identity theft. Of that 15% only (38%) could correctly define “medical identity.”

Cost of Health Care Fraud in US

- Health care fraud is estimated by the World Privacy Forum's 2006 report to be between 3% to 10% of all health care costs or 80 to 120 billion dollars per year.

- A stolen medical identity in the US has a $50 street value, according to the WPF – whereas a stolen social security number is only $1.

- According to an 2008 estimate from the FBI, Healthcare fraud is costing American taxpayers between $70 billion to $234 billion annually.

Solutions to Health Care Fraud & Medical Identity Theft in the US

- Smart cards
- Identity theft Red Flags Rules created by the Federal Trade Commission
- Medical record privacy legislation such as HIPAA and the HITECH Act
- Biometrics such as palm vein recognition and iris scanning during the registration process
- Analytical and predictive anti-fraud software

Smart Cards as a Solution in the US

The following is a summary of smart card uses in health care according to the Smart Card Alliance:

- Supporting privacy and security requirements mandated by HIPAA
- Providing a secure carrier for portable medical records
- Reducing administrative costs by reducing paperwork
- Reducing healthcare fraud
- Providing secure access to emergency medical information
- Holding encrypted patient information, compute a digital signature or biometric template.

In 2011, the SCA estimated that a Medicare Fraud is $60 billion per year. SCA stated that a smart Medicare ID could reduce fraud by 66%, for a net annual savings of $37 billion.

International Smart Health Card Solutions

- Taiwan implemented a smart card system in 2002. There are two different cards, one for professionals and one for citizens. They are used to track access to care but also store such data as prescriptions, medical procedures, vaccinations, and allergies.

- In France, the Sesame Vitale program was implemented between 1997 and 2001 and is used by 50 million French citizens. Reducing administration costs was a key focus of the program as supposed to anti-fraud prevention. The previous paper based system took up to 2 months to process claims and reimburse citizens. The electronic process takes just a few days. This new system has saved over 1 billion Euros per year.

- In Germany, 71 million citizens received the health smart card in January 2006, at a cost of 1.6 billion Euros. The German government's plan is to create data exchange within the healthcare industry. One card is issued to citizens that contains prescriptions and patient specific applications and the other to healthcare professionals.

Other Types of Health Care Fraud in the UK

- There are several smart card deployments in the UK such as the health insurance card (HIC), patient data card (PDC), health professional card (HPC), and a multi-application card where health application is part of a National ID.
- The plan is to make e-ID cards mandatory by 2013.
- At least 4,000 NHS staff smart cards have been reported missing since 2008.
- In almost every case, lost or stolen smartcards were reissued automatically without investigation, and no disciplinary action has been taken against any staff member.
- Around one in seven of the eight million UK citizens applying to renew their European Health Insurance Card (EHIC) have unwittingly paid up to £20.
- These cards entitle Britons to medical treatment at no or reduced cost should they fall ill while travelling throughout Europe.

Biometrics

- The Patient Secure Identity (PSI) system identifies patients through palm vein recognition.
- Patients initially enroll by using a photo ID and other verification data but then don’t have to use SSN or ID.
- There is less chance of duplicate patient records or fraudulent use of SSNs, IDs and insurance cards.
- The PSI system integrates with the electronic medical record system and patients can be quickly identified in case of an emergency.
- Health care providers considered palm recognition the most secure of all other biometric options and the least invasive.

Red Flags Rules

The Federal Trade Commission created the Red Flags Rules for creditors in the United States. The Red Flag Rules require:

- Health Care providers (clinic, hospitals but not physicians) to implement a program that will prevent and detect fraud such as suspicious account activity or suspicious documents (personal identifying information).
- Health Care providers to state possible actions that they will take in event of Identity theft.
- The health care providers to train staff and have the program approved by the Board of Directors.

Penalties for non-compliance are up to $2,500 per violation discovered by the FTC.

Legislative Solutions

- American Health care providers have to comply with the Health Insurance Portability and Accountability Act (1996).
- The authors of the Exploring Medical Identity theft study concluded that (HIPAA) does not address medical identity theft and poses barriers for victims.
- Health Information Technology for Economic and Clinical Health Act (HITECH Act), enacted in 2009 addresses the privacy and security concerns associated with the electronic transmission of health information.
- Specifically the HITECH Act states new breach notification requirements and new rules for the accounting of disclosures of a patient's health information.

SECTION BREAK

Office of the Inspector General
Department of Health and Human Services

- The Department of Health and Human Services (HHS) mandate is to protect the health of all Americans and providing essential human services.

- Medicare program is the nation's largest health insurer, handling more than 1 billion claims per year. Medicare and Medicaid together provide health care insurance for one in four Americans.

- Medicare 65 and older, and/or with certain disabilities.

- Medicaid based on various living and income circumstances.

- List of OIG Most Wanted Health Care fraud fugitives on their website.

Medicare Card Fraud

- Medicare cards contain the card holder's Social Security Number.
- The Government Accountability Office estimates that this puts 48 million Americans at risk of identity theft.
- This subject was brought up in 2004 but was considered too costly to change, in 2006 estimates were approximately $300 million to remove the SSN and have a new personal identification number.
- In a 2012 GAO report states costs are now $800 million to remove the SSN and add a new personal ID number.

Results of the OIG HHS Investigations in 2011

- HHS budgeted $1.7 billion in Fraud Detection costs in 2011.
- Healthcare fraud charges against 1,430 defendants, 743 criminal convictions.
- 977 new investigations of civil healthcare fraud and recoveries of about $4.1 billion.
- From May 2007 to September 2012, strike force officials working under the Department of Justice and Department of HHS have charged approx. 1,480 defendants for approx. $4.8 billion in healthcare fraud.

Office of the Inspector General
HHS Investigations in 2012

- February 2012 - A physician, the office manager of his medical practice, and five owners of home health agencies, were charged in a nearly $375 million health care fraud billing scheme.

Office of the Inspector General
Health and Human Services -2012

- May 2012 - Charges were laid against 107 individuals, including doctors, nurses and other licensed medical professionals, for their alleged participation in approximately $452 million Medicare false billing schemes.

Office of the Inspector General
Health and Human Services -2012

- October 2012, 91 doctors, nurses and other licensed medical professionals have been charged for fraudulently billing the government nearly $430 million.
- Phony ambulance trips cost the government $49 million, and the four people arrested represent the largest takedown of alleged ambulance fraud since the special Medical Care Strike Force was activated five years ago.
- In Chicago, a dermatologist and psychologist were charged with falsely billing the government for millions of dollars for unneeded laser treatments and psychotherapy services.
- Other cities where arrests were made are Miami, Dallas, Houston, Brooklyn and Baton Rouge. The indictments alleged more than $230 million in home healthcare fraud, more than $100 million in community healthcare schemes, and the $49 million in ambulance transportation fraud in Los Angeles.

Medicaid Card Fraud

- Medicaid cards do not show an individual's SSN but it does have a person's unique Medicaid ID number.

- In 2006, Federal authorities charged 16 people, including 8 New York City employees, with conspiring to defraud the government by buying, selling or renewing Medicaid identification cards.

- Hundreds of cards were sold for $300 to $400 apiece and then used for medical and prescription-drug benefits in a scheme that cost the government $3.9 million in 2004.

Medicare Fraud Prevention

- Beginning of September 2012, Medicare contractors are required to sign off before power wheelchairs can be delivered to elderly and disabled consumers.

- Nearly 80% of the power wheelchair claims submitted to Medicare don't meet program requirements. That error rate represents more than $492 million in improper payments annually.

- Medicare will only pay after a physician meets with patients face-to-face and prescribes the wheelchair. A supplier recommends the type of wheelchair needed and also submits a claim to Medicare.

http://www.businessweek.com/ap/2012-09-20/medicare-officials-say-program-should-curb-fraud

Medicare Fraud Prevention

- In January 1998, the Centers for Medicare & Medicaid Services (CMS) required each home health agency (HHA) to obtain a surety bond in the amount greater of $50,000 or 15% of the annual amount paid to the HHA by Medicare.
- This regulation remains unimplemented after nearly 15 years.
- As of February 29, 2012, 2,004 HHAs still owed CMS a total of approximately $408 million for $590 million in overpayments between 2007 and 2011.
- CMS could have recovered at least $39 million between 2007 and 2011 if it had required each HHA to obtain a $50,000 surety bond.
- Of the 2,004 HHAs, 21% still had overpayment amounts, excluding interest, of more than $50,000 each, and more than a quarter of these HHAs had outstanding overpayments of greater than $500,000.

Affordable Care Act (2010)

- Tougher sentences for people convicted of health care fraud. 20 to 50% longer sentences for crimes involving more than $1 million in losses.
- Enhanced screenings of Medicare and Medicaid providers and suppliers to keep out fraudsters.
- Suspended payments to providers and suppliers engaged in suspected fraudulent activity.
- The computer program examines 4 million Medicare claims a day looking for outliers.
- Over the next decade, Congress will direct some $340 million in additional funding for government anti-fraud efforts.

- http://www.npr.org/blogs/health/2012/08/22/158761170/health-law-gives-medicare-fraud-fighters-new-weapons

Medicare's New Anti-Fraud Command Center

- $3.6 million command center was opened in Summer 2011.
- Medicare claims run through a predictive modeling tool similar to that used by credit card companies. Near real-time data is examined, providers are given a risk score, and if it's high enough, are subject to payment delays and a follow-up visit from CMS.
- By Christmas 2011, it had stopped just one suspicious payment, for $7,591.
- The administration must report to Congress on the antifraud computer system by the end of 2012.

Detection Techniques

The two primary targeting tools used by CMS contractors and law enforcement are**: (1) Data Mining,** and **(2) Complaints.**

- Government has been accumulating utilization, coding and billing data since the beginning of the Medicare and Medicaid programs in 1965.
- Able to compare providers by practice area, geography, and time.
- They can then effectively identify any “outliers” which may be present when their billing patterns are compared to those of their peers.
- Able to verify whether a person was being treated by two different physicians in two different states on the same day or a variety of other possibilities.

http://pmimd.com/blog/index.php/data-mining-in-medicare-fraud-usage-and-effects-on-healthcare-providers/

Detection Techniques

Only 3 to 5% of fraud is actually detected and usually late in the payment cycle. Additionally, only a fraction of money that could have been used to provide care is recovered

Data tools can be used to review healthcare claims and billing information to target:

- Assess payment risk associated with each provider
- Over-utilization of services in very short-time windows
- Patients simultaneously enrolled in multiple states
- Geographic dispersion of patients and providers
- Patients traveling large distances for controlled substances
- Likelihood of certain types of billing errors
- Billing for “unlikely” services
- Pre-established code pair violation
- Up-coding claims to bill at higher rate

Examine the social networking patterns of known bad actors. Similar to how email spammers almost never reply to comments, a fraudster’s social behaviour pattern also differs from legitimate users.

http://www.govhealthit.com/news/part-3-9-fraud-and-abuse-areas-big-data-can-target

Detection Techniques – Predictive Analysis

- Predictive analytics combats fraud by identifying patterns in claims and by understanding payers' transactional and relationship data.
- Rules-based approach that flags claims that fall outside certain parameters. The first step is to identify potentially fraudulent patterns and then develop the rules to flag them as claims are processed.
- The rules could include specialist providers who bill using a particular code more than a certain number of times a month, or charges for services outside their areas of expertise.
- The most effective, predictive models not only highlight claims with the highest likelihood of fraud but also describe the reasons each claim looks suspicious, so claims can be assessed with high productivity.

http://www.healthcarefinancenews.com/news/fighting-fraud-predictive-analytics-and-link-analysis

Detection Techniques – Link Analysis

- Link analysis examines relationships among claims, people and transactions.
- Link analysis works by analysing related claims in seemingly unrelated instances, such as "crash-for-cash" auto fraud schemes where criminals cause collisions in order to file whiplash and other fraudulent claims.
- Applying link analysis to a wide variety of databases creates a visualization of the relationships between various parties, including doctors, lawyers, vehicle owners, drivers, etc.
- By applying link analysis, payers can see how separate claims may actually be part of a larger scam involving a fraud rings.

http://www.healthcarefinancenews.com/news/fighting-fraud-predictive-analytics-and-link-analysis

Health Care Data Breaches in the US

Department of Health and Human Services and the Office of Civil Rights states that there has been a total of 477 breaches affecting over 21 million individuals (as of August 2012) since breach reporting requirements went into effect in August 2009.

For a breach to be reported, it must affect 500 individuals or more.

39% of breaches occurred on a laptop or other portable device

Cause of breaches:

- 54% Theft
- 20% Unauthorized access or disclosure
- 11% Lost records and devices
- 6% Hacking
- 5% Improper disposal of records
- 4% Unknown

2011 Health Care Data Breaches in the US

According to the Privacy Rights Clearinghouse three of the top 6 breaches in all US based organizations in 2011 were in the health care industry.

- A laptop was stolen containing protected health information of 4.2 million people.
- Nine data servers containing sensitive health information of 1.9 million current and former policyholders went missing from a data center.
- Backup tapes stolen from a car resulted in the exposure of protected health information from approximately 5 million patients of military hospitals and clinics.

2012 Health Care Data Breaches in the US

- **Utah Department of Health.** On March 30, approximately 780,000 Medicaid patients had personal information stolen after a hacker (due to a weak password) from Eastern Europe accessed the Utah Dept. of Technology Service's server.

- Social Security numbers stolen from approximately 280,000 individuals and other sensitive personal data stolen from approximately 500,000 people.

- **South Carolina Department of Health.** An employee of the South Carolina Department of HHS was arrested on April 19th after he compiled data on more than 228,000 people and sent it to a private email account.

- Approximately 22,600 people had their Medicaid ID numbers taken, which were linked to their Social Security numbers.

Cost of HIPAA Violations

HHS announced in March 2012 that Blue Cross Blue Shield (BCBST) has agreed to pay $1.5 million to settle claims that BCBST violated HIPAA in connection with the theft in 2009 of 57 unencrypted hard drives containing protected health information of over 1 million individuals.

Large Enforcement Actions Since 2009

- CVS Caremark Co.: $2.25 million, February 2009
- Alaska DHSS $1.7 million June 2012
- Rite Aid: $1 million, July 2010
- Massachusetts General Hospital: $1 million, February 2011
- Cignet Health fined in February of 2011 - $4.3 million civil money penalty, the largest for such violations.

SECTION BREAK

Polling Question #5

Do you think the benefit of smart health care cards (to deter fraud) outweighs its cost (operating and implementation)?

- Yes, cards are worth the money (our jurisdiction has them)
- Yes, cards are worth the money (our jurisdiction doesn't have them)
- No, cards not worth the money (our jurisdiction has them)
- No, cards not worth the money (our jurisdiction doesn't have them)

Summary of My Research Goals:

- Educate the public on medical identity theft.

- Research other methods to reduce medical identity theft in addition to smart cards as proposed by the Ministry of Health. For instance enhanced or specific privacy legislation and/or stiffer prison sentences, or implementing biometric technology or predictive and analytical software.

- Determine other benefits that the new smart health care cards possess. For instance improving efficiency of registration and billing systems which has occurred in France and Germany.

Research Measurement Model

- I conducted the survey by utilizing the online tool of Surveymonkey.com. The survey consisted of 20 Likert scale (1 strongly disagree to 5 strongly agree) questions, 10 categorical questions and two multiple-choice questions.

- The survey was only open to BC residents, 18 and over.

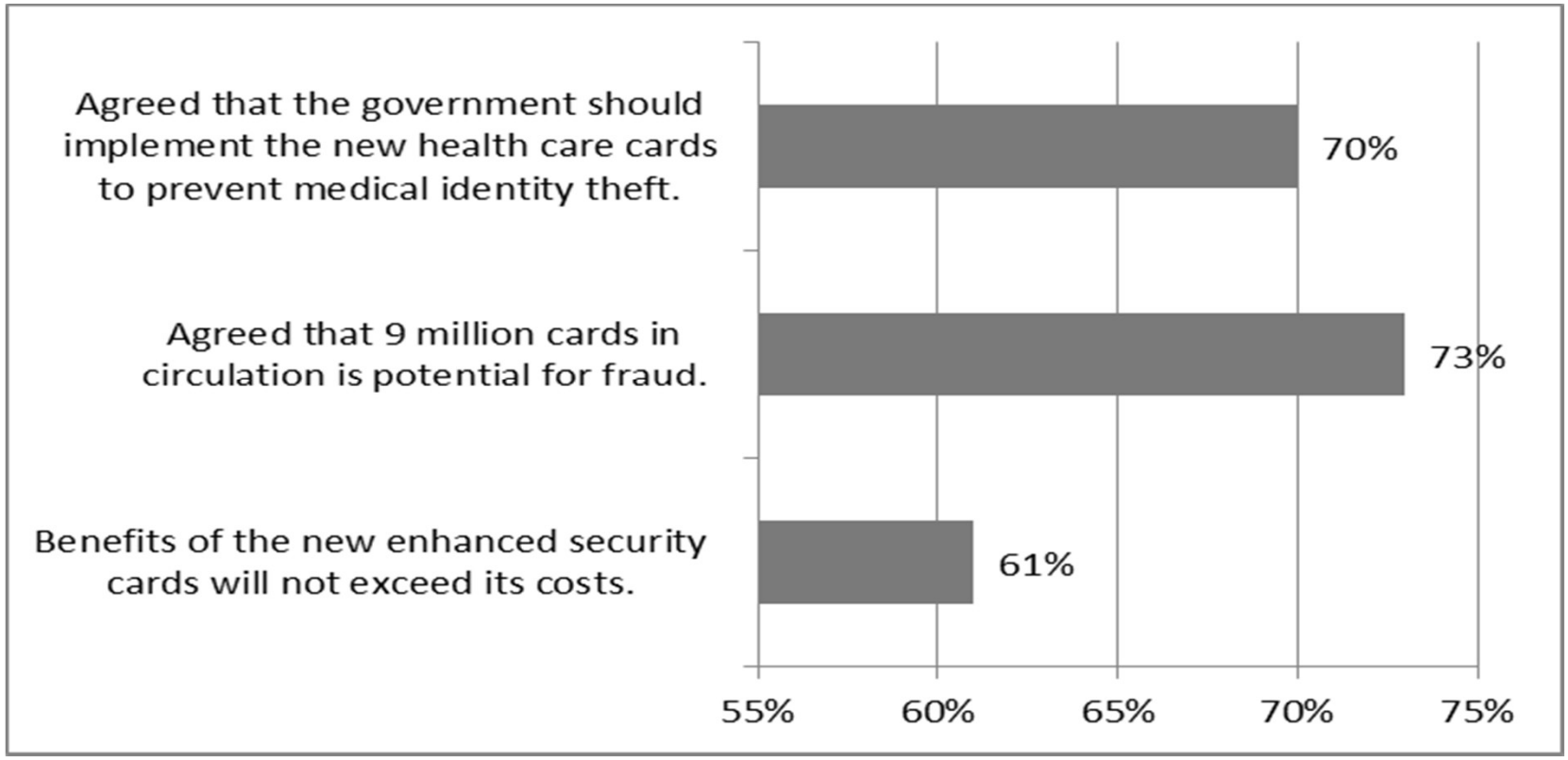
Analysis of Survey Participants

- Total response rate was approximately 36%.
- 70 individuals responded to all questions.
- 35 respondents were female while 35 respondents were male.
- 49 respondents (70%) were in the 30-44 age range.
- Respondents were from a variety of occupations.

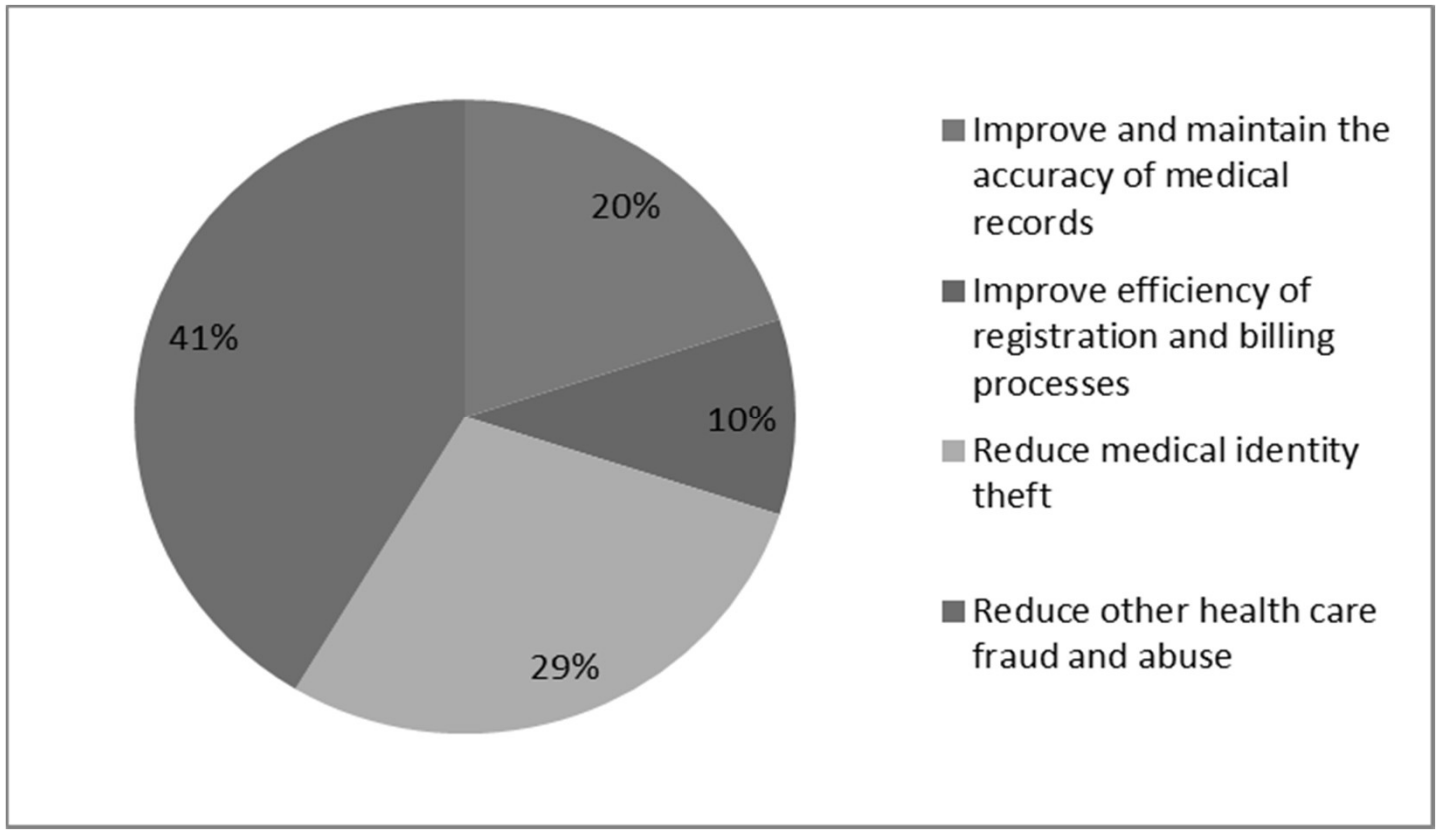
Background Survey Questions Results

- 43 respondents were aware of medical identity theft while 27 were not aware. (ignorance makes potential victims vulnerable)
- 24 respondents (or knew of someone that) had been identity theft victims.
- None of the respondents loaned out their cards to family members.
- 9 respondents lost their card, 5 of those informed the Ministry of Health.
- 22 respondents read the May 20th, 2011 Vancouver Sun article where the government announced the new health CareCards.
- 34 respondents were more concerned with Financial Identity Theft as compared to Medical Identity theft while 30 respondents neither agreed or disagreed.

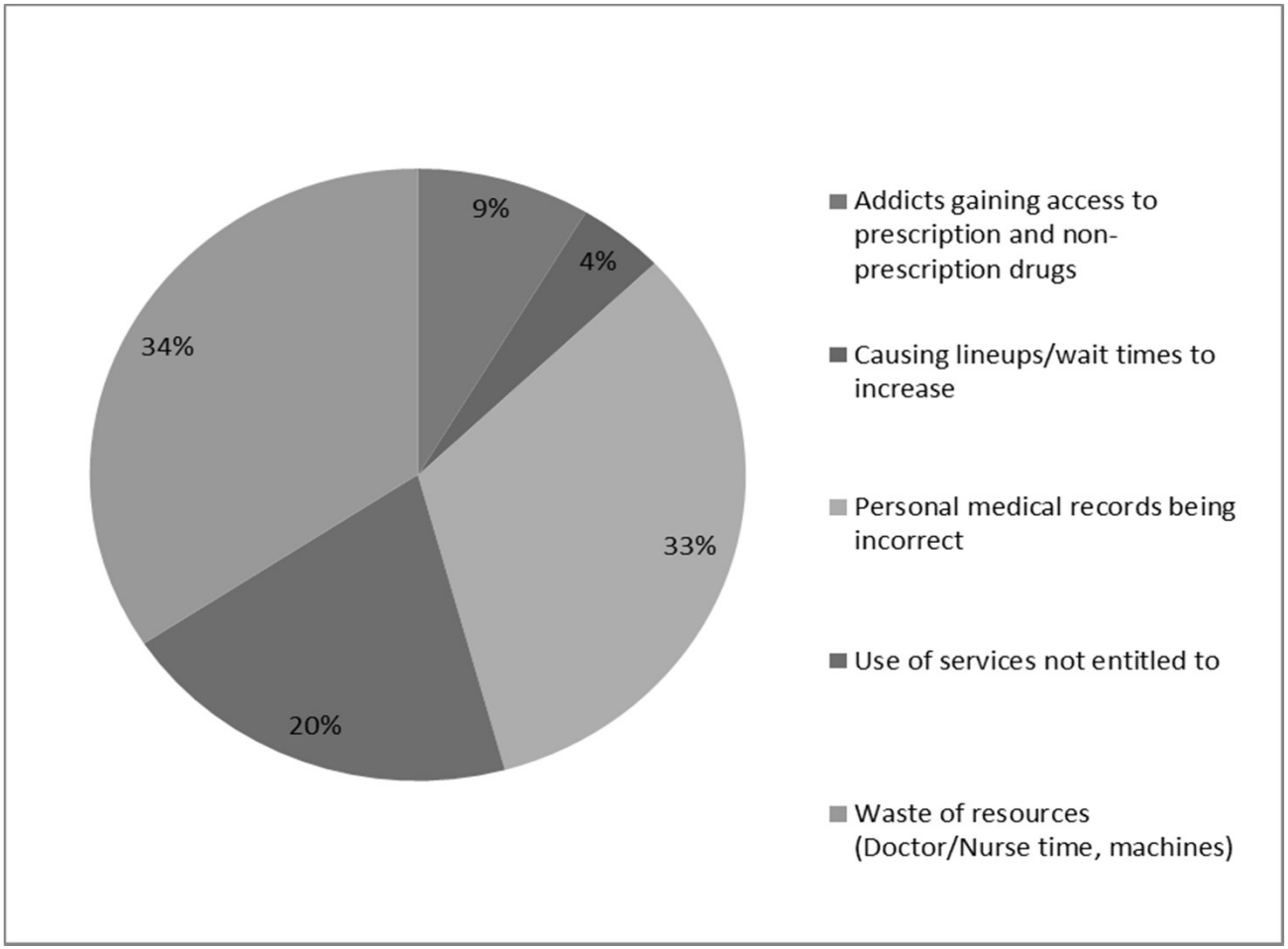
Public Perception of the New Health CareCards



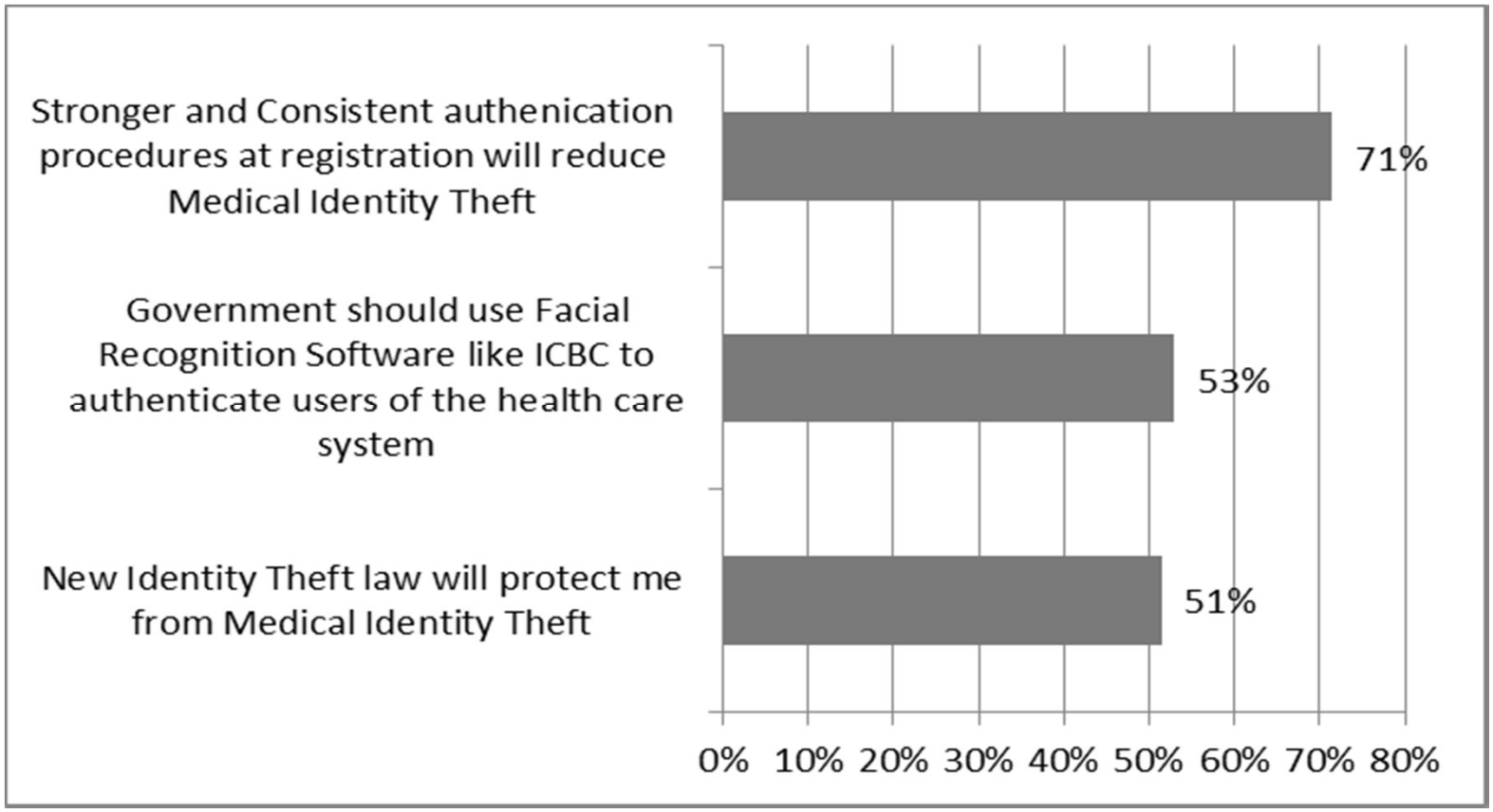
What is the Most Important Impact of the New Smart Health CareCards?



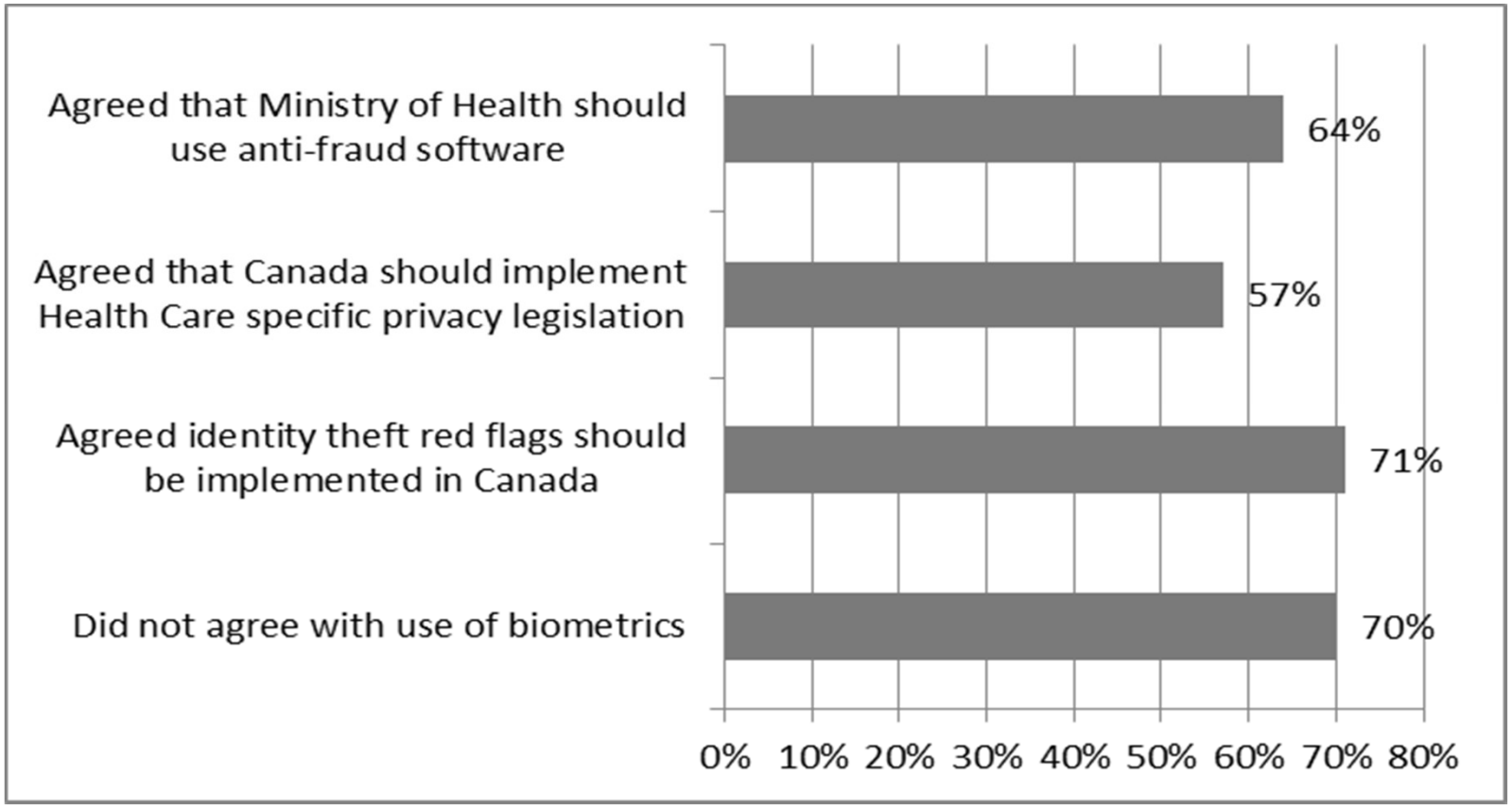
What is the Worst Consequence of Medical Identity Theft?



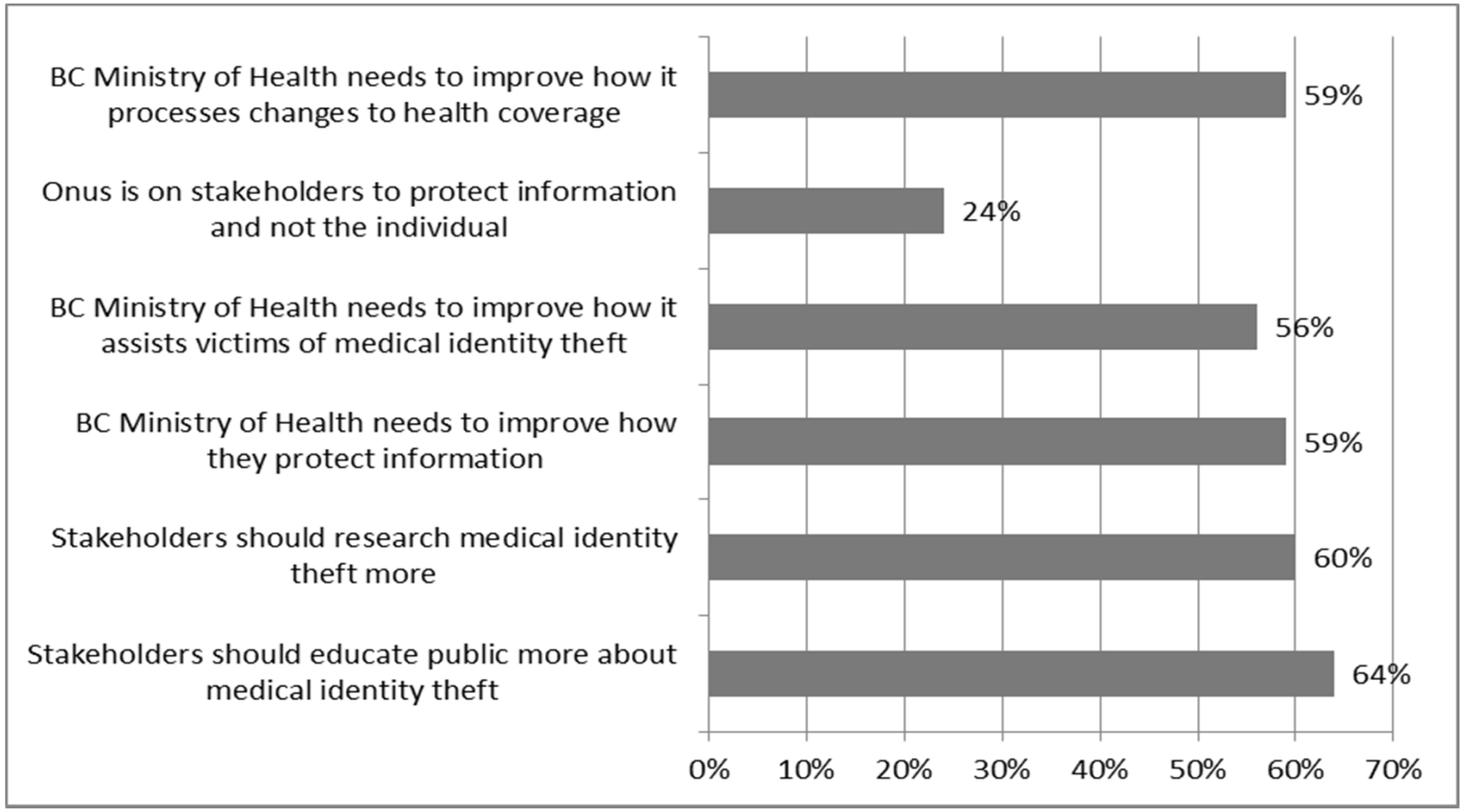
Canadian Alternatives to Reducing Medical Identity Theft



US Alternatives to Reducing Medical Identity Theft



Stakeholders Role in Reducing Medical Identity Theft



Comments From Survey Participants

- I have never really seen fraud but have worked with the Ministry of Health before and the **procedure to get BC Medicare is very easy and I'm sure duplications exist or family members using each others CareCard.**

- **Working in the health care field you see a large number of the families sharing CareCards.**

- Cards should have a picture of the card carrier on them.

More Comments From Survey Participants

- It's too easy to get a name-change on the BC CareCards and also to get replacement cards since all I had to do was make a phone call and one was mailed out.
- There is no proper system of reporting possible id theft in the community pharmacy.
- I know someone that has discontinued the CareCard and not paid the MSP annual fee for many years but the CareCard is still valid. I think Ministry of Health should improve process.
- **As a medical technologist working in the Delta hospital, I have seen Pt. Roberts (U.S) residents using BC CareCard to register on our system and I was told that no question should be asked**.
- **Also, I know a bunch of people have incorrect name on CareCard because of the transcription error in the CareCard issuing process. However, because it is so troublesome and cost money to correct it, none of them request the correction.**

Summary of Survey Results

- Slightly more respondents (73% versus 70%) agreed that the excess cards in circulation being a problem of fraud as suppose to agreeing that the government should issue the cards.
- Respondents stated that the benefits of the new CareCards will not exceed the costs of implementation.
- Respondents agree that stakeholders should become more involved in protecting and educating the public regarding medical identity theft.
- Respondents agree that the Ministry of Health should improve it's processes of CareCard changes, how it assists medical identity theft victims and improve how it protects personal health information.
- Respondents agree that a US style Red Flag reporting system, and stronger and consistent authentication procedures (two forms of ID) would be effective methods of reducing medical identity theft.
- Majority of Respondents are against using biometrics.

Recommendations for BC

- Before implementing new cards, conduct a similar audit that Ontario did in regards to account for the extra cards in circulation.
- Expand BIP to include audit of health care card numbers, coverage change processes, data security.
- Legislation requiring health care providers to report suspected fraud and retain invalid cards.
- Swipe readers and toll-free numbers for hospitals and clinics to validate cards.
- Educate health care providers on preventing data breaches and improving data security.
- Educate health care providers of medical identity theft and ensure they conduct stronger authentication registration procedures consistently.

Conclusion

- Medical Identity theft is a special type of Identity Theft and should be tracked and investigated separately from Identity Theft and Health Care fraud.
- Most people are not aware of Medical Identity Theft and this means that they are vulnerable to become victims. This lack of awareness occurs possibly because individuals aren't as directly effected as compared to "regular" financial identity theft.
- Medical Identity theft is the crime that can kill you, as it may effect an individuals medical records in Canada and the US. Medical Identity Theft victims maybe given the wrong treatment or in the US they may be denied insurance coverage.
- Even if Medical Identity theft and Health Care Fraud doesn't impact people directly creates inefficiencies with the system. We are all taxpayers and have to pay for fraud, waste and abuse, so we should care. One dollar lost to Fraud is one less dollar to spend on Hospitals, Nurses, Doctors and equipment.

Resources:

- BC Ministry of Health CareCards
  http://www.health.gov.bc.ca/msp/infoben/carecard.html#replace
- BC Ministry of Health Billing Integrity Program
  http://www.health.gov.bc.ca/msp/infoprac/bip.html
- Canadian Health Care Anti Fraud Association http://www.chcaa.org/blog/
- Canadian Identity theft Support Centre http://idtheftsupportcentre.org/id-theft/
- Fair Warning Inc. http://www.fairwarning.com/subpages/resources.asp
- Federal Trade Commission http://www.ftc.gov/bcp/edu/microsites/id-theft/
- National Anti-Fraud Centre http://www.antifraudcentre-centreantifraude.ca/english/home-eng.html
- National Health Care Anti Fraud Association http://www.nhcaa.org/
- Office of Inspector General Dept. of HHS http://oig.hhs.gov/
- Ponemon Institute http://www.ponemon.org/index.php
- Smart Card Alliance http://www.smartcardalliance.org/pages/smart-cards-applications-healthcare-identity
- World Privacy Forum http://www.worldprivacyforum.org/medicalidentitytheft.html