ORIGINAL

PUBLIC [redacted]

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION
OFFICE OF THE ADMINISTRATIVE LAW JUDGES

In the Matter of

LabMD, Inc.,
a corporation.

[redacted]

DOCKET NO. 9357

RESPONDENT LABMD, INC.'S MOTION *IN LIMINE* TO EXCLUDE THE EXPERT TESTIMONY OF RICK KAM

FACTS

FTC hired Rick Kam to provide his expert opinion regarding the "risk of injury to consumers caused by the unauthorized disclosure of their sensitive personal information." Exhibit 1, Rick Kam Report ("R.K. Report"), 5. Kam applied a novel, personally-developed four-factor methodology for analyzing risk of harm to the information FTC provided him. Specifically, he provided estimates of risk of harm to "consumers" whose Personal Health Information ("PHI") was located in three places: (1) LabMD's 1,718-page file containing Insurance Aging Reports, which was allegedly available over LimeWire, a peer-to-peer ("P2P") network; (2) LabMD's Day Sheets, discovered by police in a house in Sacramento; and (3) on LabMD's computer networks. Kam has no relevant qualifications or degrees and his experience remains a secret due to nondisclosure agreements with his clients. His invented four-factor method has not been peer-reviewed, or applied before. His analysis is not even tailored to the facts of this case. And it is in his business interest to criticize LabMD, so his analysis is infected with bias. For these reasons, his testimony should be excluded.

STANDARD

FRE 702 governs the admissibility of expert testimony:

> [A] witness qualified as an expert by knowledge, skill, experience, training, or education, may testify…if [1] the testimony is based upon sufficient facts or data, [2] the testimony is the product of reliable principles and methods, and [3] the witness has reliably applied the principles and methods to the facts of the case.

Under Rule 702, courts perform a "gatekeeping" function, screening "expert" scientific and technical evidence to exclude unreliable testimony. *Daubert v. Merrell Dow Pharm.*, 509 U.S. 579, 597 (1993); *In re McWane*, 2012 FTC LEXIS 142, *8 (August 16, 2012); *Kilpatrick v. Breg*, 613 F.3d 1329, 1335 (11th Cir. 2010). Rule 702 applies to experts who rely on their purported skill or experience. *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 148 (1999).

The *Daubert* standards of relevance and reliability for scientific evidence apply to bench trials. *Seaboard Lumber v. U.S.*, 308 F.3d 1283, 1302 (Fed. Cir. 2002); *Stryker Spine v. Biedermann Motech*, 684 F. Supp. 2d 68, 100 n.35 (D.D.C. 2010); *Duncan Pipeline v. Walbridge Aldinger*, 2013 U.S. Dist. LEXIS 45982, *13-*25 (S.D. Ga. Mar. 29, 2013). Motions *in limine* are the appropriate mechanism to challenge admissibility of expert testimony. *In re Pom Wonderful*, 2011 FTC LEXIS 97, *2-3 (April 20, 2011).

Daubert mandates a "rigorous three-part inquiry" assessing: (1) the expert's qualifications; (2) the reliability of the expert's methodology; and (3) whether the expert's testimony assists the factfinder,"through the application of scientific, technical, or specialized expertise…." *Hendrix v. Evenflo*, 609 F.3d 1183, 1194 (11th Cir. 2010). FTC bears the burden of showing by preponderant evidence that Kam's proposed testimony independently satisfies all three prongs. *Id.*; *See generally Amorgianos v. Amtrak*, 303 F.3d 256, 267 (2d Cir. 2002)("expert's analysis [must] be reliable at every step").

An expert must have relevant "knowledge, skill, experience, training, or education." FRE 702. In *Daubert* the Supreme Court specified several factors for whether an expert's methodology is reliable: (1) whether the expert's theory can be and has been tested; (2) whether the theory has been subjected to peer-review and publication; (3) the known or potential rate of error of the particular scientific technique; and (4) whether the technique is generally accepted in the scientific community. *Daubert*, 509 U.S. at 593-94; *Kilpatrick v. Breg, Inc.*, 613 F.3d 1329, 1335 (11th Cir. 2010); *see also Kumho Tire Co. v. Carmichael,* 526 U.S. 137, 151 (1999). This list is not exhaustive, and, ultimately, the expert's testimony must concern matters that are at issue in a case and beyond the understanding of the average lay person. *See Daubert*, 509 U.S. at 591; *Frazier,* 387 F.3d at 1262.

ARGUMENT

I. Kam's Invented Four-Factor Methodology Is Unreliable.

The four-factor method used by Kam lacks any basis in data, literature, or common acceptance within the field of medical-information privacy. In his expert report, Kam lays out the four factors he personally developed and used to analyze risk of harm. R.K. Report 17-18. FTC cannot meet its burden of showing that these factors are reliable.

A. Kam's Method Is Not Generally Accepted.

Kam's personally-developed methodology has not been accepted in the fields of medical or data privacy or statistical analysis. Thus, his testimony is not reliable under *Daubert* because "the methods of th[is] putative expert ha[ve] neither been 'verified by testing, subjected to peer review, nor evaluated for...potential rate of error'...." *Allen v. LTV Steel Co.*, 68 Fed. Appx. 718, 721-22 (7th Cir. 2003).

Most, if not *all*, of Kam's work has been through client-consulting arrangements governed by confidentiality agreements. Exhibit 2, R.K. Dep., 48:23–48:25, 49:2–49:4. *See Daubert*, 509 U.S. at 593-94. The error-rate of his methodology is unknown and untestable due to the confidentiality agreements.

Neither the four-factor methodology nor any work based on it has been peer-reviewed or published. R.K. Dep. 46:10–46:20; *see Daubert*, 509 U.S. at 593-94. Because his methodology has not been accepted in the field and there is no way to evaluate it, FTC cannot demonstrate that Kam's four-factor test is sufficiently reliable under *Daubert*.

B. Kam's Four-Factor Methodology Is Not Based On Any Data.

Kam did not consult any data or literature when he initially developed his four factors. His methodology is not the product of reliable principles and methods, nor is it based on sufficient facts or data. FRE 702; *see Daubert*, 509 U.S. at 597; *Allen*, 68 Fed. Appx. at 721-22. Kam testified that his four factors were based *solely* on his "experience working with clients" of his company.[1] R.K. Dep. 44:16-45:2; R.K. Report, 17-18. In developing the factors, Kam *did not*: (1) employ any statistical analysis, R.K. Dep. 49:5-9; (2) consult any specific reports, *id.* at 45:3-18; (3) consult any specific scholarly works, *id.* 45:3-18; (4) rely upon *any* data other than his generalized "experience," *id.*, 49:13; and (5) could not provide *any* additional basis for the four factors he developed, *id.* at 44:16-45:2. In short, Kam's methodology has no basis in fact or accepted theory, and his testimony, based on his personally-held theories on data privacy, should be excluded.

[1] Mr. Kam stated that his unique, untested four-factor method was developed solely from his (confidential) "experience working with clients." R.K. Dep. 44:16-45:2.

C. Kam's Analysis is Biased.

Kam applied his personally-created four-factor method in the manner most disadvantageous to LabMD in every given circumstance—and could not articulate any consistent methodology for applying it. Kam's testimony demonstrates that Kam's method here was simply to place the heaviest weight on whichever factor disfavored LabMD most by indicating the highest level of risk for any given fact of this case, even if other factors suggested lower risk levels. R.K. Dep. 49:18-20; 52:13-16; 52:17-23. Kam's biased methodology warrants exclusion of his testimony. *See In re Countrywide Fin. Corp. Mortgage-Backed Secs. Litig. v. Countrywide Fin. Corp.*, 2013 U.S. Dist. LEXIS 172367, *61-62 (C.D. Cal. Dec. 2, 2013).

II. Kam's Opinion Of The 1,718 File Is Inadmissible.

A. Kam's Statistical Analysis Is Unreliable.

Kam fundamentally misunderstands the statistical analysis he relied on to form his opinions. In his report, Kam used a base rate for medical identity theft in the entire U.S. adult population that he copied from the Ponemon Institute's 2013 Survey on Medical Identity Theft ("Ponemon Survey"). R.K. Report, 19 (citing Exhibit 3, Ponemon Survey at 2). A base rate is the measure of the relative frequency with which an event occurs within a reference population. *See* Jonathan J. Koehler, *When Do Courts Think Base Rate Statistics Are Relevant?*, 42 JURIMETRICS J. 373, 374 (Summer 2002). Here, Kam just took the Ponemon Study's base rate for the general U.S. population (.0082), and multiplied it by the number of names in the 1,718 file. R.K. Report, 19-20 (citing Ponemon Survey at 2,27,8,10); R.K. Dep. 92:8-23; 95:7-15). In other words, Kam calculated that the likelihood that any given patient in the 1,718 file would experience medical identity theft was *identical* to that of any given adult in the U.S. population.

He admitted he cannot demonstrate that any more of these patients were actual victims of identity theft. *Id.* 108:18-109:23.

Kam also failed to account for changing rates of medical identity theft between 2008 and 2013. The Ponemon Study indicated that between 2012 and 2013 alone the rate of medical identity theft increased by 19%. Ponemon Survey at 5. Yet Kam did not adjust for the decreased likelihood that patients on the 1,718 file would have been victims of medical identity theft during 2008 or subsequent calendar years, compared with 2012. *See* R.K. Report, 19-20.

B. Kam Uncritically Relied On Insufficient Facts About The P2P Incident.

Kam uncritically relied on speculative, vague third-party double-hearsay when assessing risk of harm from the P2P incident. He must base his opinions on sufficient facts, for "[a]n expert's…testimony is inadmissible 'when…based on assumptions which are speculative and…not supported by the record." *Casey v. Geek Squad*, 823 F.Supp. 2d 334, 340-41 (D. Md. 2011)(citation omitted). For the P2P incident, Mr. Kam emphasized his second factor—"the unauthorized person…to whom…disclosure was made." R.K. Report at 18; *see* R.K. Dep. 52:17-53:7. {[redacted]} Kam did not attempt to justify reliance on this double-hearsay but said: "I didn't base my *entire* analysis on that one statement." R.K. Dep., 61:19–

62:12 (emphasis added). His analysis of the P2P incident is solely based on third-party speculation, hence his conclusions are unreliable.

III. Kam's Other Opinions Are Infected With Analytical Errors And Based On Insufficient Facts.

A. Kam's Analysis of the Sacramento Incident Is Unreliable.

Kam's methodology in estimating the likelihood of harm due to the Sacramento incident is unreliable. In analyzing the social security numbers ("SSN"s) included in LabMD's Day Sheets, Kam did not cite to anything other than his "experience" to suggest that SSNs associated with multiple names "is an indicator that identity thieves may have used this information to commit identity theft."[2] R.K. Report, 23; R.K. Dep., 155:12-21.

Kam did not calculate whether the rate for multiple names associated with the SSNs from the Day Sheets was any higher than you might expect to see normally, or what proportion of such SSNs would normally have benign causes. R.K. Report at 23; R.K. Dep. 154:14-21; *see Allen*, 68 Fed. Appx. at 721 (expert testimony unreliable where it did not establish a connection between facts of case and relied-upon reports and did not attempt to account for alternative explanations). The document FTC provided Kam to show double-usage of SSNs did not include dates on which the second name was used, so he could not eliminate SSNs that were being used by multiple people prior to the Sacramento incident. *See* R.K. Dep., 185:5-10. Because Kam provided no meaningful basis for his opinions, they should be excluded.

B. Kam Did Not Rely On Adequate Facts Or Methods In Estimating Consumer Harm From LabMD's General Security For PHI.

[2] Here, Kam also misapprehended facts he materially relied on in forming his conclusions, stating that he believed that [redacted]—the suspects in whose Sacramento house LabMD's Day Sheets were found—had "identity theft charges and convictions prior to the events in Sacramento on October 5, 2012," when in fact they did not. Kam Dep. 147:19-148:2.

Kam conducted essentially no analysis of the risk of harm to consumers from LabMD's general security measures. Where a theory "was not arrived at by use of any 'technique' capable of being evaluated in the scientific community" and the witness does "not apply any particular methodology to arrive at the opinion," it cannot assist the trier of fact. *See Abramson v. Walt Disney World*, 370 F. Supp. 2d 1221, 1224-26 (M.D. Fla. 2005). Kam acknowledged that "organizations that have lower security measures in place have an increased risk of having a data breach." R.K. Dep. 160:7-9. Yet, in "assessing the risk of injury to consumers," he simply "assumed that LabMD failed to provide reasonable and appropriate security...on its computer networks" without considering the relative quality of LabMD's security practices. R.K. Report, 5; R.K. Dep., 165:13-20. Kam's opinion of LabMD's general security practices is thus bald speculation that should be rejected..

IV. Kam Is Not A Qualified Expert In Any Relevant Field.

Kam is not qualified to testify as an expert on the risk of harm to consumers. He is not qualified to give opinions on statistical analysis or medical-information privacy, for he holds no degrees in statistics or mathematics. R.K. Dep., 181:11-16.

Kam's experience consists primarily of work he performed under client-consulting arrangements kept secret by nondisclosure agreements, so there is no way to evaluate whether his experience qualifies him as an expert here. *See id.* 48:23-25, 49:2-4.

Kam has no academic degrees in data-privacy, IT, or medicine. *Id.* 181:5-10; 181:17-182:4. Kam only has a "CIPP" professional certification in data-privacy from the IAPP, which indicates *only* that, according to IAPP, he is versed in U.S. privacy laws and regulations. IAPP, "Certified Information Privacy Professional/United States (CIPP/US)," https://www.privacyassociation.org/certification/cipp_certification_programs (accessed April 22,

2014). Kam's CIPP certificate is not evidence he has a practical understanding of data-security issues.

Because he possesses no relevant academic qualifications and his work experience, shielded by confidentiality agreements, is impossible to evaluate, Kam cannot qualify as an expert under *Daubert*. His testimony should be excluded.

V. Kam's Opinion Is Biased.

Kam has professional entanglements with Larry Ponemon, and, through him, Robert Boback. The most heavily-cited source in Kam's report is the survey conducted by the Ponemon Institute. *See, e.g.,* R.K. Report, 18-21. Though taking no part in the analysis, Kam's company, IDExperts, funded that survey in the amount of $50,000. R.K. Dep. 174:2-11. Ponemon was also on the board of IDExperts. R.K. Dep. 173:2-24.

Kam also relied heavily on Boback's testimony. *See* R.K. Report, 19-20. Until recently, Ponemon was on the advisory boards both of ID Experts and Tiversa. *Id.* 173:2-173:24; Tiversa, "Tiversa Advisory Board," http://www.tiversa.com/about/advisors.html (accessed April 22, 2014). Ponemon is still on Tiversa's board, as Kam is well-aware. *See* R.K. Dep. 175:13-15.

This shows Kam's tilting the scales against LabMD, *see supra* Section I.C, is in Kam's business interest. His bias renders his conclusions unreliable.

CONCLUSION

For the forgoing reasons, Rick Kam's expert testimony should be excluded.

Dated: April 22, 2014

Respectfully submitted,

William A. Sherman, II, Esq.
Dinsmore & Shohl, LLP
801 Pennsylvania Ave., NW
Suite 610
Washington, DC 20004
Phone: (202) 372-9100
Facsimile: (202) 372-9141
william.sherman@dinsmore.com

PUBLIC

[redacted]

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION
OFFICE OF THE ADMINISTRATIVE LAW JUDGES

In the Matter of	)	[redacted]
LabMD, Inc.,	)	**Docket No. 9357**
a corporation,	)	
Respondent.	)	

MEET-AND-CONFER STATEMENT

Pursuant to ALJ Chappell's Scheduling Order, paragraph 4, Counsel for the moving party, Respondent, LabMD, Inc. (LabMD), hereby certifies that Counsel conferred with Complaint Counsel by telephone on April 21, 2014, at 4:30 pm,[1] in a good-faith effort to resolve by agreement the issues regarding LabMD's Motion In Limine To Exclude The Expert Testimony Of Rick Kam, but the parties were unable to reach agreement.

Respectfully submitted,

William A. Sherman, II, Esq.
Dinsmore & Shohl, LLP
801 Pennsylvania Ave., NW Suite 610
Washington, DC 20004
Phone: (202) 372-9100
Facsimile: (202) 372-9141
Email: william.sherman@dinsmore.com

Counsel for Respondent

[1] On the call, for Complaint Counsel: Laura Van Duff, Jarad Brown, and Megan Cox. For LabMD: William Sherman II.

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION
OFFICE OF THE ADMINISTRATIVE LAW JUDGES

In the Matter of	)	
	)	
LabMD, Inc.,	)	DOCKET NO. 9357
a corporation.	)	
	)	
	)	
	)	

[PROPOSED] ORDER ON RESPONDENT LABMD, INC.'S MOTION *IN LIMINE* TO EXCLUDE THE EXPERT TESTIMONY OF RICK KAM

Upon consideration of Respondent LabMD, Inc.'s Motion *In Limine* To Exclude The Expert Testimony Of Rick Kam, and in consideration of the entire Record in this matter, IT IS HEREBY ORDERED that LabMD, Inc.'s Motion to Exclude is GRANTED.

ORDERED:

D. Michael Chappell
Chief Administrative Law Judge

Date:

EXHIBIT

1

Report of Rick Kam, CIPP/US

In the Matter of LabMD

FTC Complaint #1023099, Docket #9357

March 18, 2014

Table of Contents

Executive Summary

Federal Trade Commission staff has retained me as an expert witness in the Commission's administrative litigation against LabMD. Complaint Counsel has asked me to assess the likely risk of injury, particularly from medical identity theft, to consumers caused by the unauthorized disclosure of their sensitive personal information. This document is a statement of my opinions and contains the bases and reasons for my conclusions. It includes the following information:

- Overview of my credentials and qualifications.
- Overview of the impact of identity crimes from the perspective of consumers affected by the unauthorized disclosure of sensitive personal information.
- Analysis of the potential harm[1] and risk of harm from medical identity theft to consumers whose sensitive personal information was disclosed without authorization.

I. Introduction

My name is Rick Kam, president and co-founder of ID Experts, a company specializing in data breach response and identity theft victim restoration. ID Experts is based in Portland, Oregon. Since 2003, leading healthcare, financial, and educational organizations, and state and federal government agencies have relied on ID Experts to help them respond to unauthorized disclosures of sensitive personal information. I have had the opportunity to work on data breach incidents as part of ID Experts' incident response team. ID Experts has managed hundreds of incidents, protecting millions of affected individuals and restoring the identities of thousands of identity theft victims. Within the healthcare industry, I have worked with organizations ranging in size from individual providers and small clinics to large hospital systems and health insurance companies. ID Experts is recognized as an industry leader, protecting consumers from the harms caused by the unauthorized disclosure of their sensitive personal data.

My expertise includes:

- Identifying and remediating the consequences of identity theft and medical identity theft for consumers whose sensitive personal information was compromised.

[1]The term "injury" is from the FTC complaint and is used interchangeably with the term "harm."

- Helping organizations develop policies and solutions to address the growing problem of safeguarding sensitive personal information.

Based on my unique experience at ID Experts, I lead and participate in several cross-industry data-privacy working groups, resulting in the publication of industry white papers. I regularly speak at conferences and on webinars; work with other privacy and security experts to contribute articles, including a monthly guest article in *Government Health IT*; and offer commentary to privacy, breach risk, and information technology (IT) publications.

Affiliations and Organizations

As a privacy professional, I actively work on initiatives that focus on data privacy to protect consumers and their sensitive personal information, and I belong to or have belonged to the following organizations:

- Chair of PHI Protection Network (PPN), an interactive network of privacy professionals focused on expediting the adoption of best practices to protect sensitive personal medical information. (2012 - present)

- Chair of The Santa Fe Group Vendor Council ID Management Working Group, which published *Victims' Rights: Fighting Identity Crime on the Front Lines,* February 2009. This white paper explores trends in identity crimes, the victim's experience, and proposes a victim's "bill of rights." (2008 - 2012)

- Chair of the American National Standards Institute (ANSI) Identity Management Standards Panel "PHI Project," a seminal research effort to measure financial risk and implications of data breach in healthcare, led by the American National Standards Institute (ANSI), via its Identity Theft Prevention and Identity Management Standards Panel (IDSP), in partnership with the Shared Assessments Program and the Internet Security Alliance (ISA). The "PHI Project" produced *The Financial Impact of Breached Protected Health Information*. (2011 - 2012)

- Co-Chair of three other cross-industry working groups that published whitepapers on assessing cyber and data breach risks. The reports include: *IDSP Workshop Report: Measuring Identity Theft*; *The Financial Management of Cyber Risk: An Implementation Framework for CFOs;* and *The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask*. (2007 - 2012)

- Contributor to the Research Planning Committee for the University of Texas Center for Identity, which focuses on identity management and identity theft risk mitigation best

practices. ID Experts provided case studies of identity crimes to an analytical repository of identity threats and counter measures called *Identity Threat Assessment and Prediction* (ITAP). (2009 - present)

- Member of the International Association for Privacy Professionals (IAPP), the most comprehensive, member-based privacy community and resource. I maintain a Certified Information Privacy Professional CIPP/US certification for data privacy. (2010 - present)

- Member of Healthcare Information and Management Systems Society (HIMSS), a global, member-based non-profit focused on the betterment of healthcare information technology. (2010 - present)

- Member of the Health Care Compliance Association, (HCCA), a member-based non-profit that provides training, certification and resources in support of ethics and regulatory compliance in healthcare. (2011- present)

- Founding member of the Medical Identity Fraud Alliance (MIFA), a group of over 40 private and public industry members in the fight against medical identity theft and medical fraud. (2013 - present)

I have attached a copy of my CV, which fully describes my background and qualifications, and includes a list of my publications over the last 10 years (see Appendix A).

Compensation

The FTC has engaged me as an expert witness in support of its complaint against LabMD. The compensation for this work is $350 per hour, and this report and my testimony are based on the experience outlined in this section, a literature review (see Appendix B), and documents I received from the FTC.

II. Summary of the FTC's Request for Expert Opinion

The Federal Trade Commission has asked me to assess the risk of injury to consumers caused by the unauthorized disclosure of their sensitive personal information. For the purposes of my analysis, I have assumed that LabMD failed to provide reasonable and appropriate security for consumers' personal information maintained on its computer networks.

FTC Documents for Analysis

I have based my analysis on my experience as outlined in Section I of this report, a literature review (see Appendix B), and the documents that I received and reviewed from the FTC, which are listed here.

Documents related to the P2P Disclosure

- **P2P Insurance Aging file [redacted]:** This is the 1,718-page file Tiversa discovered on a peer-to-peer (P2P) network that contained consumer data from the LabMD Insurance Aging Report with roughly 9,300 records. The data elements included in this file are:
  - First and last names, and middle initials
  - Dates of birth
  - Nine-digit Social Security numbers (SSNs)
  - Health insurance provider numbers, names, addresses, and phone numbers
  - Current Procedural Terminology (CPT) Codes: Uniform set of codes defined by the American Medical Association to describe medical, surgical, and diagnostic services.
  - Billing dates and amounts

- **Transcript of the deposition of Robert Boback, CEO of Tiversa, dated November 21, 2013, with supporting exhibits.**

- **Transcript of the deposition of Alison Simmons, former LabMD IT employee, dated February 5, 2014, with supporting exhibits.**

- **Transcript of the deposition of Eric Johnson, Dean of the Owen Graduate School of Management at Vanderbilt University, dated February 18, 2014, with supporting exhibits.**

- **Transcript of the deposition of Michael Daugherty, President and CEO of LabMD, dated March 4, 2014.**

Documents related to the Sacramento Disclosure

- **Day Sheets from LabMD (Sacramento LabMD-Documents.pdf):** These are documents the Sacramento Police Department found on October 5, 2012, during an arrest of two individuals who pleaded "no contest" to identity theft charges. The Day Sheets contain approximately 600 records with first and last names, and middle initials; nine-digit Social Security numbers; and billing dates and amounts.

- **Nine (9) personal checks and one (1) money order from patients of LabMD (Sacramento LabMD-Documents.pdf):** The Sacramento Police Department also found these documents on October 5, 2012, during the same arrest. Information on the checks include: first and last names, and middle initials; addresses; bank routing and account numbers; and signatures. There are also handwritten notes with four of the personal checks with what appear to be SSNs, check numbers, and amounts.

- **"Sacramentoresults7" spreadsheet:** It contains an analysis by the FTC of the Social Security numbers found in the Day Sheets. The FTC used the Thomson Reuters CLEAR database for this analysis. This spreadsheet shows multiple instances of SSNs that are being, or have been, used by people with different names, which may indicate that identity thieves used these SSNs.

- **Transcript of the deposition of Detective Karina Jestes, dated December 17, 2013, with supporting exhibits.**

- **Transcript of the deposition of Kevin Wilmer, FTC investigator, dated February 25, 2014.**

- **Transcript of the deposition of Michael Daugherty, President and CEO of LabMD, dated March 4, 2014.**

- **Breach notification letter from LabMD to Peter Cuttino, letter dated March 27, 2013.**

- **Breach notification letter from LabMD to James Hayes, letter dated March 27, 2013.**

- **FTC Consumer Sentinel Network contact records (Norris and Cuttino.pdf).**

- **FTC-LABMD-003914 to 3915:** 3/27/13 letter from LabMD regarding personal information that "may have been compromised."

- **FTC-LABMD-003910 to 3911:** 12/6/13 letter from LabMD regarding credit monitoring.

Other Documents Related to the FTC Investigation

- **2010.02.24 Ellis Letter to the FTC**
- **2010.06.04 Ellis Letter to the FTC**
- **2010.07.16 Ellis Letter to the FTC**
- **2010.08.30 Ellis Letter to the FTC**
- **2011.05.16 Rosenfeld Letter to the FTC**

- **2011.05.31 Rosenfeld Letter to the FTC**
- **2011.07.12 Rosenfeld Email to the FTC**
- **FTC-MID-000012:** 1/6/14 letter regarding LabMD not "accepting new specimens."
- **FTC Complaint in the Matter of LabMD**
- **Protective Order Governing Discovery of Material.pdf**
- **LabMD's Objections to and Responses to Complaint Counsel's Requests for Admission, dated March 3, 2014**
- **LabMD's Responses to Complaint Counsel's Interrogatories and Discovery Requests, dated March 3, 2014**

III. Summary of Conclusions

As consumers, we place trust in the organizations that hold our most sensitive personal information: Social Security numbers, financial data, and our medical history, to name a few. We have confidence that they will protect this information from unauthorized disclosure.

Once a consumer's sensitive personal data is disclosed without authorization, that consumer has no control over who accesses this information, thus becoming vulnerable to identity fraud, identity theft, and medical identity theft. These crimes can damage a consumer's economic well-being and reputation, and even risk his or her health. Medical identity theft can be especially difficult to resolve because it is impossible to make a victim's personal medical history private again.

In Sections V and VI of this report, I provide an overview of the impact of identity crime, with an emphasis on medical identity theft, and illustrate the possible harm to victims of these crimes. Then, based on that information, the FTC-provided documents, the literature review (see Appendix B), and my own expertise and experience, I provide my analysis of the LabMD case, specifically:

- That consumers have no way of knowing about certain unauthorized disclosures of their sensitive personal information, including medical information, thus putting them at risk of possible harms from identity crimes, including medical identity theft.

- That use of a consumer's SSN by other people with different names is an indication that identity thieves may have used the consumer's SSN.

- That LabMD's failure to employ reasonable and appropriate measures to prevent unauthorized access to consumers' personal information is likely to cause substantial harm, including harm stemming from medical identity theft.

Summary of LabMD Analysis

In my opinion, LabMD's failure to provide reasonable and appropriate security for sensitive personal information, including medical information, is likely to cause substantial injury to consumers and puts them at significant risk of identity crimes. The following is a summary of my analysis of likely risks of harm from identity theft and medical identity theft to the approximately 10,000 consumers affected by the P2P and Sacramento disclosures. Apart from these two incidents, I also believe that LabMD's failure to provide reasonable and appropriate security for the more than 750,000 consumers' personal information maintained on its computer networks creates a risk of unauthorized disclosure of this information. These unauthorized disclosures and the failure to provide reasonable and appropriate security are likely to cause substantial harm to these consumers.

P2P Disclosure

- Approximately 9,300 consumers from the May 2008 unauthorized disclosure are at significant risk of harm from identity crimes.

- LabMD did not notify the 9,300 consumers whose personal information was contained in the 1,718-page P2P Insurance Aging file that Tiversa discovered on February 5, 2008. Robert Boback indicated in his testimony on November 21, 2013, that [redacted]

- These 9,300 consumers have had no opportunity to mitigate the risk of harm because LabMD, which has known about the unauthorized disclosure of their personal information since May 2008, has not notified them of this disclosure. Even if LabMD had provided notice, consumers would still remain at risk of harm from identity crimes since this unauthorized disclosure included Social Security numbers and health insurance numbers, which can be used to commit identity crimes over an extended period of time.

- There is a significant risk of reputational damage for 3,000 or more consumers from the unauthorized disclosure of sensitive medical information, specifically diagnostic codes indicating tests for [redacted].

Sacramento Disclosure

The approximately 600 consumers whose personal information was contained in the LabMD documents found in the hands of Sacramento identity thieves are at risk of harm from identity crimes. In March 2013, LabMD notified these consumers about the incident. LabMD's March 2013 notification gave the affected consumers an opportunity to mitigate some risks of harm. However, consumers receiving notification of data breaches are not immune to identity crime, and they remain at risk of harm from identity crimes.

Consumer Harm from Failing to Provide Reasonable and Appropriate Security

There is a risk of harm to consumers when a company fails to protect sensitive personal information. Apart from the P2P and Sacramento incidents, I also believe that LabMD's failure to provide reasonable and appropriate security for all of its consumers' personal information maintained on its computer networks increases the risk of unauthorized disclosure of this information—likely causing substantial harm to these consumers. This harm often takes the form of identity crimes, including identity theft, identity fraud, and medical identity theft.

IV. Identity Crime: An Overview

This section provides a short overview of the different types of identity crimes—identity theft, identity fraud, and medical identity theft.

Definition of Identity Theft and Identity Fraud

Identity theft occurs when someone uses another person's identity without his or her permission. This could include using another person's name, address, date of birth, Social Security number, credit card and banking information, drivers license, or any combination of these types of personal identifiers to impersonate them. Collectively, this type of information is known as personally identifiable information, or PII.

Identity fraud, for purposes of this report, is the unauthorized use of some portion of another person's information to achieve illicit financial gain. This definition is consistent with that used by Javelin Strategy and Research. In my role at ID Experts, I have managed teams working with thousands of identity theft and identity fraud victims, helping them pinpoint the issues identity thieves caused and working to expunge any negative records created by the identity thieves. Identity thieves can use PII to commit numerous crimes, as illustrated by this list of types of theft that teams working under my supervision have helped consumers resolve:

- Using another person's SSN to create credentials such as fake drivers licenses and birth certificates to perpetrate and legitimize identity fraud.
- New accounts for major credit cards, various retail store cards, and mail-order accounts.
- Takeover of legitimate victim accounts resulting in fraudulent purchases, including goods and services.
- New bank accounts, including checking/savings/investment, resulting in several bank accounts reported to collections.
- Check counterfeiting and forgery.
- Fraudulent tax returns causing victims not to receive their refunds or to seem to owe extensive funds.
- Payday loan fraud reported to collections and other agencies.
- New auto financing accounts for multiple vehicle purchases. These vehicles were then not registered, incurring fees to the victim and making it impossible for them to legitimately register their own vehicles, while the thief sold the fraudulently purchased vehicles.
- Fake drivers licenses created to perpetrate and legitimize fraud, further complicating the dispute process.
- Employment fraud, in which an individual fraudulently works in another state and reports the wages, causing the victim to receive tax notices for non-payment and have difficulty filing legitimate tax returns.
- Merchant processing accounts set up under fake businesses to take credit card payments.

According to the *2014 Identity Fraud Report* by Javelin Strategy and Research, nearly one in three data breach victims (30.5%) also fell victim to identity fraud in 2013.[2]

Definition of Medical Identity Theft

Medical identity theft occurs when someone uses another person's medical identity to fraudulently receive medical services, prescription drugs and goods, as well as attempts to fraudulently bill private and public health insurance entities.

A person's medical identity is comprised of a number of personal data elements. The teams I have supervised at ID Experts have worked on hundreds of healthcare data breaches, in which many of the following data elements were affected:

- Name
- Medical record number
- Health insurance number

---

[2] *2014 Identity Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends*, p. 29, February 2014, by Javelin Strategy & Research.

- Other demographics (which may include address, phone number)
- Charge amounts for services
- Social Security number
- Medicare number (which contains a person's nine-digit SSN)
- Date of birth
- Financial account information
- Patient diagnosis [i.e., International Classification of Diseases (ICD), and Current Procedural Terminology Codes (CPT)]

Medical identity theft is a serious problem, affecting an estimated 1.84 million Americans.[3]

Identity Thieves and Identity Fraud

It may take months or years for a consumer to learn that his or her sensitive personal information was disclosed without authorization and misused to commit an identity crime. This is due, in part, to identity criminals committing a wide variety of identity fraud, some of which may be difficult for the consumer to detect. The teams I have managed at ID Experts work with victims who, in many cases, have several identity fraud issues. A number of the victims we have worked with continue to be harmed, since identity thieves will resell their sensitive personal information to other identity thieves, thus perpetuating the harms for years.

In 2007, Utica College did a study using 517 actual identity theft cases investigated by the U.S. Secret Service.[4] The study did not depend on self-reported victim data. The purpose of the study was to understand the nature, perpetrators, and case characteristics of identity crimes. It found the most significant motive for identity thieves to commit identity fraud is for personal financial gain (see Table 1 below).

---

[3] *2013 Survey on Medical Identity Theft*, p. 2, September 2013, by Ponemon Institute. From http://medid-fraud.org/2013-survey-on-medical-identity-theft/.

[4] *Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement*, p. 38, October 2007, by Center for Identity Management and Information Protection, Utica College. From http://www.utica.edu/academic/institutes/ecii/publications/media/cimip_id_theft_study_oct_22_noon.pdf.

Table 1: Motivating Factors for Committing Identity Theft or Fraud		
Motive	Number	Percentage
Use stolen ID to obtain and use credit	228	45.3%
Use stolen ID to procure cash	166	33%
Use stolen ID to conceal actual identity	114	22.7%
Use stolen ID to apply for loans to buy vehicles	105	20.9%
Use stolen ID to manufacture and sell fraudulent IDs	39	7.7%
Use stolen ID to obtain cell phones and services	23	4.6%
Use stolen ID to gain government benefits	19	3.8%
Use stolen ID to procure drugs	11	2.2%

V. Impact of Identity Crimes on Victims

This section highlights the range of harms that can befall victims of the various forms of identity crimes, with an emphasis on medical identity theft. Here are just a few examples of the challenges and frustrations a typical identity crime victim may experience based on my work at ID Experts:

- The victim may have to deal with a dizzying array of businesses and government institutions. It is not uncommon for an identity thief to establish as many as five fraudulent accounts. In healthcare, for example, a visit to the emergency room would result in several bills (i.e. ambulance, lab, emergency room, doctors). Victims would need to contact each of these entities to dispute fraudulent charges and close these accounts. In many cases this entails following up and submitting copies of a police report, ID theft affidavit, proof of residence, and identification. The victim may have to contact the entity several times to ensure his or her accounts are corrected and all negative records created by the identity thieves are expunged.

- Some local police departments won't accept a police report from an identity theft victim. In our experience, we are aware that taking police reports related to identity crimes works against department crime metrics, which may be a disincentive for police to help victims.

- There is no central "medical identity bureau" where a consumer can set up a fraud alert, like they can with the credit bureaus. He or she has no way to notify healthcare providers or payers, or receive consumer alerts, which are part of credit monitoring services. As a result, identity thieves can continue to use a consumer's medical identity to commit identity crimes.

- If criminal acts are committed under a stolen identity, the first news a victim often has of the theft may be when he or she is arrested. The identity thief's arrest record may also show up in background checks of a victim, affecting things such as passing security clearances, receiving a drivers license, and taking advantage of career opportunities.

- If a victim's checkbook is stolen, this usually means closing out the old account, opening a new one, and filing a police report in case merchants were cheated with bad checks. Some financial institutions won't reimburse all fraud losses for checking or savings accounts until they are confirmed as fraudulent, which may impact a consumer's ability to pay his or her bills.

- Identity thieves submitting fraudulent tax returns is another growing problem affecting approximately 1.8 million consumers.[5] Tax identity theft typically prevents victims from being able to successfully file their tax returns and obtain refunds.[6] The delay can extend, in some cases, as long as six months.[7] This delay materially affects victims' cash flow.

- Many hospitals and clinics do not have staff training or internal processes to help victims of identity theft and medical identity theft. Consumers may not get help or a response unless they can get to a manager, such as the organization's chief medical officer or compliance officer.

---

[5] "Detection Has Improved; However, Identity Theft Continues to Result in Billions of Dollars in Potentially Fraudulent Tax Returns," No. 2013-40-122 (Sept. 20, 2013) (public) p. 1, by Treasury Inspector General. From http://www.treasury.gov/tigta/auditreports/2013reports/201340122fr.html.

[6] "Tips for Taxpayers, Victims about Identity Theft and Tax Returns," by Internal Revenue Service, January 2013. From http://www.irs.gov/uac/Newsroom/Tips-for-Taxpayers,-Victims-about-Identity-Theft-and-Tax-Returns.

[7] Ibid.

- The victim of medical identity theft may have the integrity of their electronic health record compromised if the health information of the identity thief has merged with that of the victim. The resulting inaccuracies may cause serious health and safety risks to the victim, such as the wrong blood type or life-threatening drug allergies.

Financial Harm from Medical Identity Theft

The *2013 Survey on Medical Identity Theft* by Ponemon Institute found that 36 percent of medical identity theft victims incurred an average of $18,660 in out-of-pocket expenses.[8] These costs stem from medical identity theft and include: 1) reimbursement to healthcare providers for services received by the identity thief; 2) money spent on identity protection, credit counseling, and legal counsel; and 3) payment for medical services and prescriptions because of a lapse in healthcare coverage.[9]

Other Harms from Medical Identity Theft

In addition to out-of-pocket costs, victims spent a significant amount of time resolving the problems caused by medical identity theft. According to the Ponemon Institute survey, the amount of time it takes to resolve the crime can discourage victims of medical identity theft from even trying to fix the problem. This is due, in part, because healthcare organizations believe they cannot release medical records that include the identity thief's sensitive personal information to a victim of medical identity theft. For those victims who did try, 36 percent of respondents say it took nearly a year or more working with their healthcare providers or insurers to resolve the crime, and 48 percent say "the crime is still not resolved."[10]

Another problem is health insurance. The Ponemon survey found that 39 percent of medical identity theft victims lost their healthcare coverage.[11] Most life and health insurance organizations subscribe to organizations such as the Medical Information Bureau, which is an insurance consumer reporting agency that maintains a database of medical information to help insurers determine risk and insurance rates for individual consumers.[12] A medical identity theft victim who has been diagnosed with and received prescriptions for conditions that are costly to treat, like cancer or HIV, could possibly lose life or health insurance coverage.

---

[8] Ponemon Institute 2013 Survey on Medical Identity Theft, p. 5.

[9] Ponemon Institute 2013 Survey on Medical Identity Theft, p. 5.

[10] Ponemon 2013 Survey on Medical Identity Theft, p. 12.

[11] Ponemon 2013 Survey on Medical Identity Theft, p. 10.

[12] The Facts about the Medical Information Bureau (MIB). From http://www.mib.com/facts_about_mib.html.

The Ponemon survey on medical identity theft breaks down other harms of medical identity theft to victims including serious health-related risks, loss of confidence in their medical care provider, and more. Using statistics from the Ponemon study,[13] Table 2 below illustrates the health risks to victims of medical identity theft:

Table 2. Other Harms from Medical Identity Theft	**Ponemon Percentage of Medical Identity Victims**
Misdiagnosis of Illness*+	15%
Delay in Receiving Medical Treatment*+	14%
Mistreatment of Illness*+	13%
Wrong pharmaceuticals prescribed*+	11%

**Consequences as a result of inaccuracies in health records.*
+ Respondents were permitted two choices for this portion of the survey.

Potential for Reputational Harm from Medical Identity Theft

Reputational harm can occur from the loss of sensitive personal health information. Medical identity theft victims who may have sexually transmitted diseases are particularly sensitive to having their condition disclosed. Consumers diagnosed with cancer may feel similarly stigmatized. There have also been cases of criminals trying to extort money in exchange for not disclosing sensitive information. Two cases were reported in 2008, in which criminals tried to extort money from Express Scripts and Medical Excess LLC, a subsidiary of AIG, in return for not disclosing health records.[14]

---

[13] Ponemon 2013 Survey on Medical Identity Theft, p. 8.

[14] "Express Scripts Data Breach Leads to Extortion Attempt," by Sarah Rubenstein, November 7, 2008, *Wall Street Journal* Health Blog, http://blogs.wsj.com/health/2008/11/07/express-scripts-data-breach-leads-to-extortion-attempt/.

VI. Analysis of Risk of Harm from LabMD's Failure to Protect Consumer Data

In this section, I analyze the risk of harm from medical identity theft to consumers resulting from LabMD's failure to provide reasonable and appropriate security for consumers' personal information maintained on its computer networks. Specifically, I identify the possible harm to the approximately 10,000 consumers known to be affected by LabMD's unauthorized disclosures of sensitive personal information. Given the specific circumstances of this case, in which LabMD's sensitive consumer data was found in the hands of known identity thieves and the fact that this sensitive consumer data was found on P2P networks as recently as November 2013—and may still exist on these networks—these estimates should be viewed as a floor versus universe of potential harms that could befall the 10,000 affected consumers.

I also explain how, irrespective of these two incidents, LabMD's failure to provide reasonable and appropriate security for more than 750,000 consumers' personal information maintained on its computer networks creates a risk of unauthorized disclosure of this information, thus causing a likelihood of substantial harm to consumers.

Consumers' Ability to Avoid Possible Harms

A consumer cannot know about the security practices of every company that collects or maintains his or her personal information. As a result, states have enacted data breach notification laws (see Appendix C for a list of the state data breach notification laws in effect in May 2008). Generally, notifications are intended to alert affected consumers of a breach so that they can take actions to reduce their risk of harm from identity crime. Without notification, consumers have no way of independently knowing about an organization's unauthorized disclosure of their sensitive information.

It should be noted that breach notification doesn't completely eliminate the risk of harm to consumers from identity crimes. The fact that a consumer's sensitive personal information has been disclosed significantly increases the risk of harm—especially if this information is in the possession of criminals. Javelin Research finds that almost one in three data breach victims in 2013 fell victim to identity fraud in the same year.[15]

For my analysis I used the following four factors to examine the likely risk of harm to consumers from the unauthorized disclosure of their sensitive personal information:

---

[15] Javelin 2014 Identity Fraud Report, p. 8.

1. The nature and extent of the sensitive personal information involved, including the types of identifiers and the likelihood of re-identification. In other words, could the disclosed consumer data elements be used to facilitate identity theft, identity fraud, and medical identity theft? Was sensitive personal data part of the unauthorized disclosure (e.g., name, medical records, health insurance number, diagnostic codes)?

2. The unauthorized person who used the protected health information or to whom the disclosure was made. For instance, was this an employee disclosing the information to another employee, which poses a low risk, versus to an unauthorized individual not associated with that entity, be it another consumer, business, identity thief, etc.?

3. Whether the sensitive personal information was actually acquired or viewed. An example: Was the information stored on a secure encrypted device such as a laptop or storage drive, or were they paper health records left on a public bus and viewed by others?

4. The extent to which the risk to the protected health information has been mitigated. For instance: Were copies of sensitive information destroyed during its recovery from unauthorized parties, or is the data still available for others to misuse?

Analysis of the P2P Disclosure (9,300 records)

According to the materials supplied by the FTC, Tiversa alerted LabMD of the unauthorized disclosure of the P2P Insurance Aging file that contained 9,300 consumer records in May 2008. The compromised data included:

- First and last names, and middle initials
- Dates of birth
- Nine-digit Social Security numbers
- Health insurance provider numbers, names, addresses, and phone numbers
- Current Procedural Terminology (CPT) diagnostic codes
- Billing dates and amounts

I analyzed these data elements looking at the first risk factor, specifically the nature and extent of the information disclosed. [redacted] according to Robert Boback's testimony. The disclosure of names with corresponding Social Security numbers, health insurance provider numbers, and CPT diagnostic codes pose a greater risk of various identity crimes.

The second and third risk factors consider to whom the disclosure was made and whether the information was acquired and viewed. In his testimony, Boback said that [redacted] Boback also testified [redacted]. He also stated that [redacted]

The fourth risk factor is the extent to which the risk to a consumer's personal information has been mitigated. According to Boback's testimony, [redacted] Boback also said [redacted] LabMD did not mitigate the risk of identity crimes created by this unauthorized disclosure by notifying consumers. In my experience, a significant number of these consumers have or could still fall victim to identity crimes since they have no way of independently knowing that LabMD disclosed their information without authorization almost 6 years ago. This unauthorized disclosure puts the affected consumers at a significantly higher risk of identity crimes than the general public.

Harm from P2P Disclosure

Estimated Financial Out-of-Pocket Cost to Victims of Medical Identity Theft

According to the findings from the 2013 Survey on Medical Identity Theft by Ponemon Institute, 0.0082 is the estimated base rate for medical identity theft in the U.S.[16] This represents the proportion of consumers who indicated that they were medical identity theft victims, as drawn from a representative panel of 5,000 adult-aged U.S. consumers.[17]

Therefore:

9,300 breached records x 0.0082 = 76, the estimated number of victims for medical identity theft.

The Ponemon study also found that 36 percent of victims of medical identity theft paid an average of $18,660 in out-of-pocket costs.

---

[16] Ponemon 2013 Survey on Medical Identity Theft, p. 2.

[17] Ponemon 2013 Survey on Medical Identity Theft, p. 27.

Therefore:

9,300 breached victims x 0.0082 base rate x 0.36 = 27 potential victims who would have to pay the average of $18,660 in out-of-pocket costs. Consumers' out-of-pocket costs would exceed $500,000.

Estimation of "Other" Injury from Medical Identity Theft

As discussed in Section V, medical identity theft and identity fraud have the potential to cause "substantial injury" to consumers in ways that are not directly related to finances. And as also mentioned above, LabMD's failure to notify the 9,300 individuals whose information is in the P2P Insurance Aging file potentially puts these consumers' health and safety at risk.

Table 3 below estimates the number of these consumers who could experience other kinds of harm.[18]

Table 3. Projected Number of Victims Suffering "Other Harms" from Medical Identity Theft

"Other Harms" from Medical Identity Theft	Ponemon % of Medical Identity Victims	Projected Number of Victims**
Misdiagnosis of Illness*+	15%	11
Delay in Receiving Medical Treatment*+	14%	11
Mistreatment of Illness*+	13%	10
Wrong pharmaceuticals prescribed*+	11%	8
Loss of health insurance coverage	39%	30

**Consequences as a result of inaccuracies in health records.*

+ Respondents were permitted two choices for this portion of the survey.

*** Calculation for number of possible victims is number of medical records (9,300) x 0.0082 Ponemon percentage of medical identity theft victims x Ponemon "% other harm."*

[18] Ponemon 2013 Survey on Medical Identity Theft, pp. 8,10.

Reputational Injury from Medical Identity Theft

In addition to SSNs and health insurance information, some of the most sensitive medical information disclosed by LabMD are the CPT codes indicating various tests that had been performed. (For an analysis of each CPT code included in the 1,718-page P2P Insurance Aging file, please see Appendix D.) The consumers identified in this file had various medical tests performed, as indicated by the CPT codes. [redacted]

[redacted]

Testing for these sensitive medical conditions does not necessarily indicate a diagnosis. However, disclosure of the fact that the tests were performed could cause embarrassment or other negative outcomes, including reputational harm and changes to insurance for these consumers, including life, health, and disability insurance. Once this health data is disclosed, it is impossible to restore the consumers' privacy.

Analysis of Sacramento Disclosure (~600 Records on Day Sheets, 9 Personal Checks, 1 money order)

The Sacramento Police Department discovered sensitive personal information in the possession of known identity thieves, including 40 pages of Day Sheets with approximately 600 records, and nine personal checks and one money order made out to LabMD. The compromised data contained on the LabMD Day Sheets included:

- First and last names, and middle initials
- Nine-digit Social Security numbers

- Billing dates and amounts

The compromised data contained on the nine checks included:

- First and last names, and middle initials
- Address
- Nine-digit Social Security numbers
- Bank routing and account numbers (on checks)
- Amounts
- Signatures
- Handwritten comments that appear to be SSNs, check numbers, and amounts

I analyzed these data elements using the first risk factor: the nature and extent of sensitive personal information disclosed. This incident disclosed sensitive consumer information, specifically names, nine-digit SSNs, and bank routing and account numbers on the nine checks. This sensitive personal information could be used to commit identity theft and identity fraud.

The Sacramento Police Department found 40 pages of LabMD Day Sheets and nine checks during an arrest on October 5, 2012, in the possession of two individuals who pleaded "no contest" to identity theft. While Detective Jestes said in her testimony [redacted] I based this analysis on the second and third risk factors—who had access to and who viewed the data.

The fourth risk factor considers what actions LabMD has taken to reduce the risk of harm to consumers. Michael Daugherty said [redacted]. LabMD mitigated some of the risk of harm for these consumers with notification and tools like credit monitoring. Even though LabMD provided notice, however, there is a strong possibility some of the approximately 600 consumers will still fall victim to identity theft and identity fraud. In particular, the unauthorized disclosure of SSNs creates the opportunity for identity crimes over a long period of time since consumers don't typically change their SSNs after being notified of a breach. Changing an SSN can be a cumbersome process and doesn't necessarily solve all problems. For example, government agencies and private businesses maintain records under consumers' "old" SSNs, and credit reporting companies may use "old" SSNs to identify credit records.[19]

In my experience, unauthorized disclosures of SSNs increases the risk of identity crimes for consumers. Only a small percentage of consumers who receive notification of a breach will call

[19] "Identity Theft and Your Social Security Number," p. 7, by Social Security Administration, December 2013. From http://www.socialsecurity.gov/pubs/EN-05-10064.pdf.

into consumer hotlines. An even smaller percentage will take advantage of free credit monitoring. According to Michael Daugherty's March 4, 2014, testimony [redacted] Since most consumers won't take any actions to protect themselves—opt in to credit monitoring or set a fraud alert—even after knowing they are at elevated risk of identity crimes, they become even more vulnerable to these crimes.

Use of SSNs in Day Sheets

The FTC analysis of the approximately 600 SSNs using the CLEAR database revealed that 314 SSNs had multiple names listed. I eliminated those that were due to misspellings, name changes, and typos, leaving approximately 100 SSNs that appear to have been used by people with different names. More than one individual using the same SSN is an indicator that identity thieves may have used this information to commit identity theft.

The Sacramento Police Department arrested two known identity thieves who had access to LabMD's sensitive personal information, which increases the risk of harm for the approximately 600 consumers affected by the unauthorized disclosure of their sensitive personal information.

Consumer Harm from Failing to Provide Reasonable and Appropriate Security

Setting aside the unauthorized P2P disclosure and the unauthorized Sacramento disclosure, LabMD's failure to provide reasonable and appropriate security for all its consumers' personal information maintained on its computer networks creates an elevated risk of unauthorized disclosure of this information. This elevated risk, in turn, is likely to cause substantial harm to consumers, in the form of the identity crimes I previously discussed (i.e., identity theft, identity fraud, and medical identity theft). These crimes cause a wide range of economic and non-economic harms to consumers.

Cyber criminals are targeting healthcare organizations because of the high value of sensitive medical information. Organizations with inadequate data security programs are vulnerable to unauthorized disclosures of sensitive personal information. A recently published report by the SANS Institute (an organization that provides security training and certification) found that healthcare systems are the target of cyber thieves, increasing the risk of data theft and fraud.[20]

---

[20] *SANS Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon*, p. 4, by Barbara Filkins, sponsored by Norse, February 2014. From http://norse-corp.com/HealthcareReport2014.html.

Submitted by

Rick Kam, President and Co-Founder of ID Experts

Appendix A: CV

Rick Kam CV

Date Updated: 1-30-2014

I. **Title:** President and co-founder, ID Experts

II. Work Experience—Present

Rick Kam, Certified Information Privacy Professional (CIPP/US), is president and co-founder of ID Experts, based in Portland, Oregon. He has extensive experience leading organizations in the development of policies and solutions to address the growing problem of protecting protected health information (PHI) and personally identifiable information (PII), and remediating privacy incidents, identity theft, and medical identity theft.

Mr. Kam leads and participates in several cross-industry data privacy groups, speaks at conferences and webinars, and regularly contributes original articles, including a monthly guest article in *Government Health IT*, and offers commentary to privacy, data breach risk, and IT publications. He is often quoted as a resource in news articles about medical identity theft, privacy and data breach.

III. About ID Experts

Co-founded by Kam in 2003, ID Experts delivers services that address the organizational risks associated with sensitive personal data, specifically protected health information (PHI) and personally identifiable information (PII). The teams that Kam has supervised at ID Experts have managed hundreds of data breach incidents, protects millions of individuals, and serves leading healthcare providers, insurance organizations, universities, and government agencies and is exclusively endorsed by the American Hospital Association.

IV. Affiliations and Organizations

As a privacy professional, I actively work on initiatives that focus on data privacy to protect consumers and their sensitive personal information, and I belong to or have belonged to the following organizations:

- Chair of PHI Protection Network (PPN), an interactive network of privacy professionals focused on expediting the adoption of best practices to protect sensitive personal medical information. (2012 - present)
- Chair of The Santa Fe Group Vendor Council ID Management Working Group, which published *Victims' Rights: Fighting Identity Crime on the Front Lines*, February 2009.

This white paper explores trends in identity crimes, the victim's experience, and proposes a victim's "bill of rights." (2008- 2012)

- Chair of the American National Standards Institute (ANSI) Identity Management Standards Panel "PHI Project," a seminal research effort to measure financial risk and implications of data breach in healthcare, led by the American National Standards Institute (ANSI), via its Identity Theft Prevention and Identity Management Standards Panel (IDSP), in partnership with the Shared Assessments Program and the Internet Security Alliance (ISA). The "PHI Project" produced *The Financial Impact of Breached Protected Health Information*. (2011 - 2012)

- Co-Chair of three other cross-industry working groups that published whitepapers on assessing cyber and data breach risks. The reports include *IDSP Workshop Report: Measuring Identity Theft*; *The Financial Management of Cyber Risk: An Implementation Framework for CFOs*; and *The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask*. (2007 - 2012)

- Contributor to the Research Planning Committee for the University of Texas Center for Identity, which focuses on identity management and identity theft risk mitigation best practices. ID Experts provided case studies of identity crimes to an analytical repository of identity threats and counter measures called *Identity Threat Assessment and Prediction* (ITAP). (2009 - present)

- Member of the International Association for Privacy Professionals (IAPP), the most comprehensive, member-based privacy community and resource. Mr. Kam maintains a Certified Information Privacy Professional CIPP/US certification for data privacy. (2010 - present)

- Member of Healthcare Information and Management Systems Society (HIMSS), a global, member-based non-profit focused on the betterment of healthcare information technology. (2010 - present)

- Member of Health Care Compliance Association (HCCA), a member-based non-profit that provides training, certification and resources in support of ethics and regulatory compliance in healthcare. (2011-present)

- Founding member of the Medical Identity Fraud Alliance (MIFA), a group of over 40 private and public industry members in the fight against medical identity theft and medical fraud. (2013 - present)

V. **Speaking Engagements**

- HCCA 2014 Compliance Institute, March-April, 2014 (scheduled)

Topic: *Evolving Cyber Threats to PHI: How Can We Safeguard Data to Lessen the Frequency and Severity of Data Breaches*

- National HIPAA Summit, February 5-7, 2014
  Topic: *HIPAA Security*

- The National Health Care Anti-Fraud Association (NHCAA) Institute for Health Care Fraud Prevention, 2013 Annual Training Conference, November 2013
  Topic: *Electronic Health Records & Cyber Crime*

- IAPP Practical Privacy Series, October 2013
  Topic: *Vendor and Data Strategy: The CVS Caremark Case Study*

- ID Experts Webinar, September 23, 2013
  Topic: *HIPAA Omnibus Rule Kicks Off*

- Federal Trade Commission Panel, May 2013
  Topic: *Senior Identity Theft: A Problem in This Day and Age*

- HCCA 2013 Compliance Institute, April 2013
  Topic: *Mobile Threats and How Healthcare Can Reduce Risks*

- PHI Protection Network, March 2013
  Topic: *Understanding the Complexities of PHI Privacy and Security: Turning PHI Security Into a Competitive Advantage*

- American Hospital Association Webinar, August, 2012
  Topic: *Data Breach Containment in an Uncontained World: Featuring a Case Study from Henry Ford Hospital*

- ID Experts Webinar, April, 2012
  Topic: *How to Mitigate Risks, Liabilities, & Costs of Data Breach of Health Info by Third Parties*

- PHI Project Webinar, March 2012
  Topic: *The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security*

- ID Experts Webinar, December, 2011
  Topic: *Second Annual Benchmark Survey on Patient Privacy and Data Security*

- ID Experts Webinar, October, 2011
  Topic: *Minimizing Risks of Lawsuits and Fines when Managing a Data Breach Response*

- IAPP Global Privacy Summit, March 2011
  Topic: *Early Preview: Results from ANSI Working Group on Financial Impact of Unauthorized Disclosure of PII & PHI*

- ID Experts Webinar, November, 2010
  Topic: *Ponemon Institute Benchmark Study on Patient Privacy and Data Security*

- ID Experts Webinar, July, 2010
  Topic: *Avoiding Increased Risks and Liabilities Under the Just Released HITECH/HIPAA Rules*

- ID Experts Webinar, May, 2010
  Topic: *Are You Ready for Data Breaches under the New HITECH Act?*

- IAPP Global Privacy Summit, April 2010
  Topic: *Data Breach Risks and the HITECH Act: Best Practices for Risk Assessments, Notification and Compliance*

- Blue Ribbon Panel Discussion, November 2010
  Topic: *HIPAA Security Risk Analysis Do's and Don'ts*

- Blue Ribbon Panel Discussion, August 2010
  Topic: *Chain of Trust: Implications for BAs and Subcontractors*

- HIMSS Analytics Webinar, November 2009
  Topic: *2009 HIMSS Analytics Report: Taking a Pulse on HITECH, Are Hospitals and Associates Ready?*

- Santa Fe Group Panel Discussion Webinar, April 2009
  Topic: *Identity Crime Trends and Victims Bill of Rights*

- Javelin Strategy and Research Webinar, January, 2009
  Topic: *Data Breach Defense 2009: Prevention, Detection and Resolution Strategies to Help Protect Your Bottom Line*

- Association of Certified Fraud Examiners (ACFE), July 2008
  Topic: *Anatomy of a Data Breach Response*

- Federal Office Systems Exposition (FOSE) Conference, April 2008

Topic: *Independent Risk Analysis: Providing Public Agencies a More Effective Solution to Mitigate Risk*

- National Association of Independent Fee Appraisers, November 2005
  Topic: *Identity Theft*

- Arizona Bankers Association & Federal Bureau of Investigation, Financial Institutions Fraud & Security Seminar, September 2005
  Topic: *Avoid the Crisis: Reduce the Chance Your Bank and Customers Will Be Hit*

VI. Education

Kam received his BA in Management and Marketing from the University of Hawaii, Honolulu, HI.

VII. Published Works

Key articles Mr. Kam has authored:

- **Medical Identity Theft**

  5 Not-So-Merry Tales of Healthcare Fraud Dark Side
  By Rick Kam and Christine Arevalo, *Government Health IT*, December 20, 2013
  http://www.govhealthit.com/news/5-not-so-merry-tales-healthcare-fraud-dark-side

  The Surprising Truth About Medical ID Thieves
  By Rick Kam, *Government Health IT*, October 11, 2013
  http://www.govhealthit.com/news/surprising-truth-about-medical-id-thieves-EHR-ACA-privacy-security

  The Growing Threat of Medical Identity Fraud: A Call to Action
  By The Medical Identity Fraud Alliance with Rick Kam as Contributor, July 2013
  http://medidfraud.org/the-growing-threat-of-medical-identity-theft-a-call-to-action/

  8 Ways to Fight Medical ID Theft
  By Rick Kam, *Government Health IT,* June 17, 2013
  http://www.govhealthit.com/news/commentary-8-ways-fight-medical-id-theft

  Victim's Rights: Fighting Identity Crime on the Front Lines
  By The Santa Fe Group with Rick Kam as Chair, February 2009

  http://santa-fe-group.com/wp-content/uploads/2010/07/SFG-Identity-Crime-Bill-of-Rights-Feb09.pdf

- **Protected Health Information (PHI)**

  What is Your PHI worth?
  By Rick Kam, *Government Health IT*, February 21, 2013
  http://www.govhealthit.com/news/what-your-phi-worth

  The Financial Impact of Breached Protected Health Information
  Rick Kam, contributor. Published by the American National Standards Institute (ANSI), via its Identity Theft Protection and Identity Management Standards Panel (IDSP), in partnership with The Santa Fe Group/Shared Assessments Program Healthcare Working Group, and the Internet Security Alliance (ISA), 2012
  http://webstore.ansi.org/phi/

  PHI Protection Network Announced
  By Rick Kam, ID Experts Blog, October 17, 2012
  http://www2.idexpertscorp.com/blog/single/phi-protection-network-announced/

  The Lifecycle of PHI and Mobile Device Insecurity
  By Rick Kam, *Government Health IT*, June 18, 2012
  http://www.govhealthit.com/news/lifecycle-phi-and-mobile-device-insecurity

  Protected Health Information Should Come with a Disclaimer – "Handle with Care"
  By Rick Kam, ID Experts Blog, March 5, 2012
  http://www2.idexpertscorp.com/blog/single/protected-health-information-should-come-with-a-disclaimer-handle-with-care/

  Protecting PHI: An Industry Initiative and Imperative
  By Rick Kam, ID Experts Blog, April 22, 2011
  http://www2.idexpertscorp.com/blog/single/protecting-phi-an-industry-initiative-and-imperative/

  ANSI and Shared Assessments PHI Project Launched
  By Rick Kam, ID Experts Blog, March 23, 2011
  http://www2.idexpertscorp.com/blog/single/ansi-and-shared-assessments-phi-project-launched/

- **Identity Theft**

  IDSP Workshop Report: Measuring Identity Theft
  Rick Kam, contributor. Published by the American National Standards Institute's (ANSI) Identity Theft Prevention and Identity Management Standards Panel (IDSP), 2009

http://webstore.ansi.org/identitytheft/#Measuring

- **Data Breach**

Data Breaches: 10 Years in Review
By Rick Kam, ID Experts Blog, July 10, 2013
http://www2.idexpertscorp.com/blog/single/data-breaches-10-years-in-review/

2013: The Year of the Data Breach: 11 Data Security Tips to Immunize Your Organization
By Rick Kam, ID Experts Blog, January 9, 2013
http://www2.idexpertscorp.com/blog/single/2013-the-year-of-the-data-breach-11-data-security-tips-to-immunize-your-org/

Why Healthcare Data Breaches Are a C-Suite Concern
By Rick Kam and Larry Ponemon, *Forbes*, December 7, 2012
http://www.forbes.com/sites/ciocentral/2012/12/07/why-healthcare-data-breaches-are-a-c-suite-concern/

5 Key Recommendations to Minimize Data Breaches
By Rick Kam, *HITECH Answers*, December 6, 2012
http://www.hitechanswers.net/5-key-recommendations-to-minimize-data-breaches/

New Ponemon Study Reveals "Common-Cold Frequency" of Data Breaches
By Rick Kam, ID Experts Blog, December 5, 2012
http://www2.idexpertscorp.com/blog/single/new-ponemon-study-reveals-common-cold-frequency-of-data-breaches/

Three Top Data Breach Threats
By Rick Kam and Jeremy Henley, *Western Pennsylvania Hospital News*, November 1, 2012
http://www.pageturnpro.com/Western-PA-Hospital-News/41635-Western-PA-Hospital-News,-Issue-10/index.html#22

Reducing the Risk of a Breach of PHI from Mobile Devices
By Rick Kam, *HITECH Answers*, September 26, 2012
http://www.hitechanswers.net/reducing-the-risk-of-a-breach-of-phi-from-mobile-devices/

Healthcare Data Breaches: Handle with Care
By Rick Kam and Jeremy Henley, *Property Casualty 360*, March 20, 2012

http://www.propertycasualty360.com/2012/03/20/healthcare-data-breaches-handle-with-care

What's Driving the Rise in Data Breaches?
By Rick Kam and Jeremy Henley, *Property Casualty 360*, March 14, 2012
http://www.propertycasualty360.com/2012/03/14/whats-driving-the-rise-in-data-breaches

Wi-Fi Networks Leaving Patients Susceptible to Loss of Personal Data
By Rick Kam, ID Experts Blog, July 20, 2011
http://www2.idexpertscorp.com/blog/single/wi-fi-networks-leaving-patients-susceptible-to-loss-of-personal-data/

- **Privacy**

  Google Glass and Other Devices Presenting New Crop of Privacy Risks
  By Rick Kam, *Government Health IT*, August 14, 2013
  http://www.govhealthit.com/news/google-glass-and-other-devices-presenting-new-crop-privacy-risks

  5 Steps to Protect Patient Privacy
  By Rick Kam and Larry Ponemon, *Government Health IT*, December 07, 2012
  http://www.govhealthit.com/news/5-steps-protect-patient-privacy

  Electronic Health Records vs. Patient Privacy: Who Will Win?
  By Rick Kam and Doug Pollack, *IAPP*, October 23, 2012
  https://www.privacyassociation.org/publications/2012_11_01_the_healthcare_privacy_balance

  Is Privacy a Constitutional Right in America?
  By Rick Kam, ID Experts Blog, May 27, 2011
  http://www2.idexpertscorp.com/blog/single/is-privacy-a-constitutional-right-in-america/

- **Cyber Risk/Security**

  4 Steps for Business Associates to Comply with Omnibus HIPAA
  By Rick Kam and Mahmood Sher-Jan, *Government Health IT*, September 20, 2013
  http://www.govhealthit.com/news/4-steps-business-associates-comply-omnibus-hipaa

  3 Ways to Make Data Protection More Patient-Centric
  By Rick Kam, *Government Health IT*, April 9, 2013
  http://www.govhealthit.com/news/3-steps-building-patient-centric-privacy-and-security

The Financial Management of Cyber Risk: An Implementation Framework for CFOs
Rick Kam, contributor. Published by the American National Standards Institute (ANSI)/ Internet Security Alliance (ISA), 2010
http://webstore.ansi.org/cybersecurity.aspx

The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask
Rick Kam, contributor. Published by the American National Standards Institute (ANSI)/ Internet Security Alliance (ISA), 2008

http://www.ansi.org/meetings_events/events/cyber_risk09.aspx?menuid=8

- **Regulatory/Compliance**
  Privacy and Security Compliance Wish List 2014
  By Rick Kam, *Government Health IT,* January 14, 2014
  http://www.govhealthit.com/blog/privacy-and-security-pros-compliance-wish-list-2014

  11 Data Security Tips for a Healthy Organization in 2013
  By Rick Kam, *Government Health IT*, January 08, 2013
  http://www.govhealthit.com/news/11-data-security-tips-healthy-organization-2013

Appendix B: Literature Review

Date	Publication/Title	URL	Author	Description
Feb. 2014	2014 Identity Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends	https://www.javelinstrategy.com/brochure/314	Javelin Strategy & Research	Analysis of fraud trends to help consumers, financial institutions, and businesses prevent, detect, and resolve fraud.
Feb. 2014	SANS Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon	http://norse-corp.com/HealthcareReport2014.html	Barbara Filkins, sponsored by Norse	Discusses the vulnerabilities of the healthcare industry to cyberthreats.
Dec. 2013	Identity Theft and Your Social Security Number	http://www.socialsecurity.gov/pubs/EN-05-10064.pdf	Social Security Administration	Consumer tips on protecting against SSN-related identity theft.

Dec. 2013	Victims of Identity Theft, 2012	http://www.bjs.gov/content/pub/pdf/vit12.pdf	Bureau of Justice Statistics, U.S. Department of Justice	In-depth statistical analysis on identity theft victims in 2012.
Nov. 7, 2013	TIGTA Report: The IRS Needs to Improve Customer Service for Identity Theft Victims	http://www.treasury.gov/tigta/press/press_tigta-2013-40.htm	Treasury Inspector General for Tax Administration	Press release
Oct. 2013	First Aid for Medical Identity Theft: Tips for Consumers	https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis_16_med_id_theft.pdf	Calif. Dept. of Justice	Consumer information on medical identity theft.
Oct. 2013	Medical Identity Theft: Recommendations for the Age of Electronic Medical Records	https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/medical_id_theft_recommend.pdf	Kamala D. Harris, Attorney General, Calif. Dept. of Justice	Recommendations to help prevent, detect, and mitigate the effects of medical identity theft.
Sept. 20, 2013	Detection Has Improved; However, Identity Theft Continues to Result in Billions of Dollars in Potentially Fraudulent Tax Refunds	http://www.treasury.gov/tigta/auditreports/2013reports/201340122fr.html	Treasury Inspector General for Tax Administration	Report to determine whether the IRS has improved its programs and procedures to identify and prevent fraudulent tax refunds resulting from identity theft.
Sept. 2013	2013 Survey on Medical Identity Theft	http://medidfraud.org/2013-survey-on-medical-identity-theft/	Ponemon Institute	Measures the prevalence, extent, and impact of medical identity theft in the United States to consumers and the healthcare industry.
April 2013	2013 Data Breach Investigations Report	http://www.verizonenterprise.com/DBIR/2013/	Verizon	Provides global insights into the nature of data breaches that help organizations better understand the threat and take the necessary steps to protect themselves.
January 2013	Tips for Taxpayers, Victims about Identity Theft and Tax Returns	http://www.irs.gov/uac/Newsroom/Tips-for-Taxpayers,-Victims-about-Identity-Theft-and-Tax-Returns	Internal Revenue Service	Consumer tips for protecting against and remediating tax-related identity theft.

2013	2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters	https://www.javelinstrategy.com/brochure/276	Javelin Strategy and Research	Analyzes fraud trends in the context of a changing technological and regulatory environment in order to inform consumers, financial institutions, and businesses on the most effective means of fraud prevention, detection, and resolution.
2013	Cybercrime and the Healthcare Industry	http://www.emc.com/collateral/white-papers/h12105-cybercrime-healthcare-industry-rsa-wp.pdf	RSA, The Security Division of EMC	Discusses the growing threat of cybercrime to electronic healthcare data.
June 2012	Creating a Trusted Environment: Reducing the Threat of Medical Identity Theft	https://www.himss.org/files/HIMSSorg/content/files/CreatingaTrustedEnvironment_Reducing_the_Threat_of_Medical_Identify_TheftFINAL.pdf	HIMSS Privacy and Security Task Force, Kroll-sponsored	Evaluates risk and mitigation strategies for protecting PHI.
March 2012	The Financial Impact of Breached PHI	http://webstore.ansi.org/phi/	Workgroups	ANSI whitepaper on the financial impact of breached protected health information.
Oct. 2009	IDSP Workshop Report: Measuring Identity Theft	http://webstore.ansi.org/identitytheft/#Measuring	Workgroup #2 of IDSP	Addresses how research companies measure identity crime. Includes a catalog of 166 research projects to date.
Jan. 2009	Medical Identity Theft Final Report	http://www.healthit.gov/sites/default/files/medidtheftreport011509_0.pdf	Booz Allen Hamilton	Recommendations for addressing issues from a "town hall" meeting. Prepared for HHS, and ONC for Health Information Technology.
Nov. 7, 2008	Express Scripts Data Breach Leads to Extortion Attempt	http://blogs.wsj.com/health/2008/11/07/express-scripts-data-breach-leads-to-extortion-attempt/	Sarah Rubenstein, *Wall Street Journal* Health Blog	Article describing two extortion attempts involving patient information.

Oct. 2008	Medical Identity Theft Environmental Scan	http://www.healthit.gov/sites/default/files/hhs_onc_medid_theft_envscan_101008_final_cover_note_0.pdf	Booz Allen Hamilton	Information and insights about medical Identity theft. Prepared for HHS, and ONC for Health Information Technology.
Sept. 2008	The President's Identity Theft Task Force Report	http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf	Identity Theft Task Force	Documents the Task Force's efforts to implement recommendations for fighting identity theft.
October 2007	Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement	http://www.utica.edu/academic/institutes/ecii/publications/media/cimip_id_theft_study_oct_22_noon.pdf	Center for Identity Management and Information Protection, Utica College	Provides empirical evidence on which law enforcement can base enhanced proactive identity theft control and prevention efforts.
May 2006	Medical Identity Theft: The Information Crime that Can Kill You	http://www.worldprivacyforum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you/	Pam Dixon	Report on impact of medical identity theft including cases.
July 2005	Identity Theft Literature Review	https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf	Newman and McNally	Identity theft literature review funded by the Department of Justice.
Ongoing	The Facts about MIB	http://www.mib.com/facts_about_mib.html	Medical Information Bureau	Website describing MIB's purpose—enabling companies to offer affordable life and health insurance to customers.

Appendix C: State Breach Notification Laws in Effect before May 2008

The number of the Breach Notification Laws in effect before May 2008 is 41. The following list includes the effective dates for each state or territory:

In 2003:

- California (July 1)

In 2005 (12):

- Georgia (May 5)
- North Dakota (June 1)
- Delaware (June 28)
- Florida (July 1)
- Tennessee (July 1)
- Washington (July 24)
- Texas (September 1)
- Arkansas (August 12)
- Virgin Islands (October 17)
- North Carolina (December 1)
- Puerto Rico (December 4)
- New York (December 7)

In 2006 (17):

- Connecticut (January 1)
- Louisiana (January 1)
- Minnesota (January 1)
- Nevada (January 1)
- New Jersey (January 1)
- Maine (January 31)
- Ohio (February 17)
- Montana (March 1)
- Rhode Island (March 1)
- Wisconsin (March 31)
- Pennsylvania (June 20)
- Illinois (June 27)
- Idaho (July 1)
- Indiana (July 1)
- Nebraska (July 14)
- Colorado (September 1)
- Arizona (December 31)

In 2007 (10):

- Hawaii (January 1)
- Kansas (January 1)
- New Hampshire (January 1)
- Utah (January 1)
- Vermont (January 1)
- District of Columbia (July 1)
- Wyoming (July 1)
- Michigan (July 2)
- Oregon (October 1)
- Massachusetts (October 31)

In 2008:

- Maryland (January 1)

Appendix D: List of CPT Codes

EXHIBIT

2

Q Do you remember earlier today you pointed to this section just briefly with respect to the four factors?

A Yes.

Q It says in the bottom line, bottom paragraph there, that quote, "For my analysis I used the following four factors to examine the likely risk of harm to consumers from the unauthorized disclosure of their sensitive personal information." Did I read that correct correctly?

A Yes.

Q Do you see on the next page on page 18 where it lists the four factors that we were talking about earlier today; do you see that?

A Uh-huh, yes.

Q How did you determine in your analysis, in the analysis which you have developed through your experience, how did you determine what four factors to use in analyzing the likelihood of harm to consumers from the unauthorized of their sensitive personal medical information?

A Based on my experience working with clients who have experienced an unauthorized disclosure of sensitive personal information.

Q So the four factors are developed totally

based on your experience; is that fair to say?

A Experience, yes.

Q Just so we can be clear, in developing the four factors, did you consult any specific reports or scholarly works in developing those four factors as your analytic method?

A Can you be more precise?

Q So in developing -- you have got four factors; is that fair to say?

A Yes.

Q So in developing those, I want to carve out your experience, but in developing those four factors did you consult any specific reports or scholarly works to come to use these four factors for your analytic method?

A These four factors were developed over the course of seven or eight years working with our clients, and their counsel.

Q Would you point to a specific timeframe for those seven to eight years?

A 2005 to date.

Q So we are talking about nine years, I guess?

A Well, I'm kind of -- let me count them, yes.

Q Did you write any specific reports or scholarly works with respect to these four factors?

A When we work with clients there is work product under nondisclosure where our discussions with their counsel and their response teams revolves around discussion of these four factors.

Q So those works would have been developed by counsel and you together; is that fair to say?

A Yes.

Q Apart from those types of written documents did you draft any published reports or scholarly works with respect to those four factors?

A No.

Q So it's fair to say that the documents we are talking about are not written documents that have been subjected to a peer review; correct?

A They are under nondisclosure agreements.

Q But they are not published -- so they are not publicly issued; is that fair to say?

A Yes.

Q They are under a confidentiality order of the court, perhaps?

A Confidentiality agreements of nondisclosure; correct.

Q So they are written under a nondisclosure

A Give me an example.

Q That's an example, say in this case, say the FTC has a consulting expert that they need to help them because they are not experienced in the field that you may be or you may not be, but they are lawyers, they are not identity theft experienced, let's say; are you following me?

A Yes, so far.

Q So say they had somebody who worked with them that they could probably pay at a lower rate than you to testify; do you follow?

A So far, yes.

Q Do you in your experience -- strike that.

In your experience have you worked as a consulting expert to support litigation where you did not testify?

A No.

Q In the matters where you have performed services under confidentiality agreements I can understand that you wouldn't be able to comment about them; is that fair to say?

A Yes.

Q Are there other matters that you have worked that are not subject to a nondisclosure agreement that you can tell me about?

A In what context?

Q That you used, that you are basing your four factor test?

A No.

Q In developing your four factor test that is expressed on page 18 of your expert report, for these four factors did you rely on any statistical analysis in developing these four factors?

A No.

Q Apart from your personal experience did you use any data in developing these four factors, any specific data?

A No, it was based on my experience over the 11 -- nine years we calculated.

Q Do you give equal weight to each of the four factors?

A No.

Q Which factors do you give greater weight to in applying the four factors?

A It depends on the breach.

Q With respect to the alleged LabMD data breaches involved in this case, the P2P disclosure, alleged disclosure, and the Sacramento incident or the Sacramento disclosure, with respect to those two alleged breaches do you give heightened weight to, I

A -- and specifically on page 18 for the P2P disclosure I identify the elements that are in that disclosure.

Q So you are looking a little bit further down on page 18 under the bulleted item that starts with first and last names and middle initials; is that correct?

A Yes, dates of birth, nine digit Social Security numbers, health insurance provider numbers, names addresses and phone numbers, current procedural terminology, CPT codes, billing dates and amounts.

Q So with respect to the four factors are you weighting the first factor as the heaviest factor for the P2P disclosure or incident?

A It would be a high risk factor.

Q Would that be the number one factor for potential, the weighting of potential harm?

A Rephrase your question one more time so we get it clear.

(The reporter read the record as requested.)

THE WITNESS: It would be one of the high rated factors based on my analysis.

BY MR. HUNTINGTON:

Q The highest of the four?

A Well, there are several high risk factors associated with this particular incident. This is one of the high rated factors.

Q Okay. What would the other factors that would be high rated be?

A The second element, or the second factor to be precise.

Q The unauthorized person who used the protected health information or to whom the disclosure was made?

A Yes.

Q With respect to the P2P incident, who is your understanding of the unauthorized persons who used the protected health information or to whom the disclosure was made; correct?

A Yes.

Q Who is your understanding of who that is with respect to the P2P incident?

A If you turn to page 19 of my analysis, I identify that the second factor and the third risk factor together in that paragraph, [redacted]

Did I read those two sentences fairly, were you following along?

A Yes.

Q Did I read it correctly?

A Fairly close.

[redacted]

A Yes.

Q To the best of your recollection is there anywhere else in this deposition that you relied on for your statement that quote [redacted] close quote?

A Not that I can recall at this time.

Q None that you can recall at this time; correct?

A Yes.

Q If you would, if you later in the day or otherwise, if you can find somewhere else where it becomes apparent to you, if you could tell me today

or communicate through counsel, I would appreciate knowing that. Leaving today so that you understand we are on the same page I just want to make sure that that is what you were relying on when you made that statement, okay?

A Yes.

Q When you were just reading this and when you were developing the expert report I'll draw your attention back to the deposition transcript, [redacted]

[redacted]

A Yes.

Q How do you interpret that word in context with the testimony, the word [redacted], do you connote that to have any specific meaning?

A I couldn't give you a definition, a Webster's definition of it.

Q But I mean that's what you would point to as Webster's; right, to find a definition if you can't give one right now; is that fair?

A That's fair.

[redacted]

Q When you are looking at that testimony that you just read for me, and thanks, again, for doing that, [redacted]?

A No.

Q [redacted]?

A No.

Q [redacted]?

A No.

Q [redacted]?

A No.

Q [redacted]?

A No.

Q What about the testimony leads you to conclude that the answer is accurate enough to base your analysis, your entire analysis of the second and third risk factors of the P2P incident?

A I didn't base my entire analysis on that one statement.

Q But you have predicated part of your

analysis on that one statement; correct?

A That's correct. Can I add one piece?

Q Sure, go ahead, absolutely.

A The second and third risk factors as listed on page 19, [redacted]

Q All right, are you looking at the fourth factor right now in testifying?

A No.

Q I'm sorry, I guess I'm not following you.

A I'm sorry.

Q When I saw you said the four factors I immediately let town the page --

A Could you go back to the top of page 19, your question earlier asks what I considered in my analysis of the second and third factors.

Q Uh-huh, yes.

[redacted]

on quote, "In my experience, significant number of these consumers have or could fall victim to identity crimes," just focusing in on that quote of yours, close quote after crimes, did you rely on any other source or method of analysis besides consulting your experience to draft that statement?

A To be clear, my experience is made up of the work that I do at ID Experts over the nine years, it includes the other experts that I work with in the data breach response and victim restoration arena over the last nine or ten years, it includes the literature that exists and review of that information, it includes the courses that I take to maintain a Certified Information Privacy Professional certification every year, it includes the breadth of my experience over the -- a wide range of educational and work experiences.

Q Given that as your definition of experience, is there anything else that you are relying on to make that statement?

A Not that I can recall at this time.

Q Are there any specific pieces of literature that you are pointing to to make that statement sitting here right now; do you think?

A If you review the literature review as

the findings of the 2013 survey on medical identity theft by Ponemon Institute 0.0082 is the estimated base rate for medical identity theft in the U.S. This represents the proportion of consumers who indicated that they were medical identity victims as drawn from a representative panel of 5000 adult aged U.S. consumers.

"Therefore, 9300 breached records times 0.0082 equals 76, the estimated number of victims for medical identity theft"; did I read that correctly?

A Yes.

Q In this calculation the 76, the number 76 there on page 19 as the product, I guess that is, product of your calculation, is that a calculation specific for LabMD, 76?

A Yes.

Q That's your estimated number for LabMD for the --

A For the P2P disclosure.

Q For the P2P, not the Sacramento but for the P2P disclosure?

A Yes, by my analysis, yes.

Q The next paragraph down the paragraph goes on to say, below the calculation it goes on to say

was approximately 76; correct?

A One correction to your --

Q Sure.

A Victims of medical identity theft versus I identity theft.

Q Okay. So if I were -- let me re-read that. So by your calculation the number of estimated victims of medical identity theft among the 9300 people whose information was included on the documents allegedly available using the P2P network was approximately 76; correct?

A Yes.

Q And that's the best you can do, you are committed to that number; correct?

A Yes.

Q And the number who had to pay out-of-pocket was approximately 27 based on your calculations; is that correct?

A Yes.

Q And their total combined out-of-pocket cost would exceed approximately $500,000?

A Yes.

Q Correct?

A Correct.

Q And in performing these calculations you

A Yes, I have. Isn't the LabMD patient in the U.S.?

Q Correct. So you are just, you have described a number to this, being specifically tailored to this case, when all you have done is given me the general population rate; correct?

A I used the best information available to create an estimate of likely injury based on 9300 consumers being affected by medical identity theft.

Q So your opinion is that the number of the patients whose identity was allegedly exposed in the LabMD document who have quote/unquote "likely been harmed" and the amount of the projected injury, that's exactly equal to the number and amount that you would expect to see in the U.S. adult population; correct?

A Yes.

Q Can you demonstrate for me in any way, shape, or form that more than 90, I'm sorry, that more than 76 of the 9300 of the patients whose data was allegedly exposed in the LabMD document, the P2P number, the P2P document, can you demonstrate that any of them have been actual victims of identity theft since the disclosure?

A I was asked by the Commission to do an

assessment of the likely injury of medical identity theft. I used the Ponemon Institute survey specifically on medical identity theft to establish a base rate, we which equals 76 consumers.

Q So it's fair to say that I'm going to expect at trial that you are not going to attempt to demonstrate the actual or provide -- strike that.

At the trial of this matter you are not going to try to demonstrate that more than 76 of the 9300 of the patients whose data was allegedly exposed in the LabMD P2P document have been actual victims of identity theft since the alleged disclosure; correct?

A Medical identity theft.

Q Correct.

A And for clarification, this specific calculation looks at the estimated number of medical identity theft victims and the potential of out-of-pocket financial costs.

Q But you are not going to be testifying to the actual victims of identity theft since the date of disclosure; correct?

A No.

Q Would there be a way for you to demonstrate that more than 76 of the 9300 folks

names listed. I eliminated those that were due to misspellings, name changes and typos, leaving approximately 100 Social Security numbers that appear to have been used by people with different names.

More than one individual using the same Social Security number is an indicator that identity thieves may have used this information to commit identity theft.

Q And you just read that first paragraph under that heading use of SSNs and day sheets; correct?

A Yes.

Q I think I'm asking you something a little bit different, what I would like to know is whether you ever determined what the base rate is of the general population for having two names associated with the same SSN?

A Are you being specific to identity theft?

Q Yes.

A No.

Q Without adjusting for the base rate how can you know whether the number of patients whose data was allegedly exposed in the Sacramento is statistically higher than expected?

A Can you point me where that is referenced?

Q I'm just asking a general question, I'm looking for an answer, I'm not seeing it in your report, so I'm just asking you the question, and perhaps it is in there, perhaps not, perhaps it's just a bad question, I'm just looking for your answer. What I'm asking is, without adjusting for the base rate how can you know whether the number of patients whose data was allegedly exposed in Sacramento is statistically significantly higher than expected?

A The approach that I used was to actually look at the facts from the case that were provided by the Federal Trade Commission through this report, to provide my best estimate of the likely victims of identity fraud from the Sacramento disclosure.

Q And what is that estimate?

A Approximately 100 individuals.

Q Based on your experience?

A Yes, and the facts that were presented by the Federal Trade Commission.

Q Do you still have the Ponemon survey somewhere there in front of you, Mr. Kam?

A Yes.

Q With respect to the Ponemon survey you

you expect someone with higher quality data security measures than someone with lower quality data security measures to be at equal risk of experiencing a data security breach?

A No.

Q Why would that be?

A Because organizations that have lower security measures in place have an increased risk of having a data breach.

MS. MEHM: Kent, could I suggest that -- we have been going for about 45 minutes, could we have a ten-minute break?

MR. HUNTINGTON: Let's do five.

MS. MEHM: Okay, let's do five.

(4:42 p.m. -- recess -- 4:52 p.m.)

BY MR. HUNTINGTON:

Q Go back on the record. Right before we broke for a few minutes here we were talking about the risk of harm from LabMD general security practices, is that expressed in your expert report, do you recall that discussion in general?

A Just before we went off?

Q Yes.

A Yes.

Q So is it fair to say that the degree, that

security"; does the report say that?

A Yes.

Q And the first sentence beneath it says quote, "Setting aside the unauthorized P2P disclosure and the unauthorized Sacramento disclosure, LabMD's failure to provide reasonable and appropriate security for all its consumers' personal information maintained on its computer network creates an elevated risk of unauthorized disclosure of this information"; did I read that correctly?

A Yes.

Q Can you point me to anywhere in your report where you analyze or evaluate the degree of adequacy of LabMD's specific security practices, policies, procedures, hardware or software?

A No.

Q Why not?

A I wasn't asked to analyze LabMD's security, the adequacy of their security.

Q On page 23 you say that a recently published report by the SANS Institute (an organization that provides security training and certification) found that health care systems are the target of cyber thieves increasing the risk of

A Dr. Ponemon.

Q Dr. Ponemon used to be on the advisory board for ID Experts; is that correct?

A Used to be, yes.

Q Do you remember what timeframe he sat on the advisory board for ID Experts?

A I believe it was for a few months last year.

Q Was he compensated to sit on the advisory board for ID Experts?

A No.

Q Were his travel costs or any other costs reimbursed meetings?

A To advisory board meetings, yes, reimbursed.

Q For hotel costs?

A Yes.

Q Did you say which months he would have served; do you recall?

A I don't recall.

Q Was it more than three months?

A Probably.

Q Was it more than six months?

A It roughly was six months.

Q Was it more than nine months?

A No.

Q What did your sponsorship of the Ponemon Institute entail financial?

A We provide -- we paid for the development or the publication of the report.

Q How much did you pay for the publication?

A Which report are you referring to?

Q Well, if you break it out, for each report?

A Let's see, for patient data privacy report, roughly $50,000.

Q And for the other report how much would that have entailed financially?

A Approximately $12,500.

Q Approximately $12,500?

A Yes.

Q What was ID Expert's role in the survey if there was one, apart from financial support?

A Sponsorship specifically.

Q So you got your name on the report; is that fair to say?

A Yes.

Q So you got some advertising out of that sponsorship?

A Yes.

Q Did you have a personal relationship with Larry Ponemon?

A What do you mean personal, can you be more specific?

Q Do you know him personally apart from your business relationship?

A No.

Q Do you -- I just want to lay foundation, do you have a business relationship with Mr. Ponemon?

A In the sponsorship of these two reports, yes.

Q Are you aware that Larry Ponemon is a Tiversa board member?

A I recall hearing that somewhere, yes.

Q You don't know that, you just heard that?

A I just heard that.

Q Do you have a relationship, contractual or otherwise, to Tiversa?

A No.

Q Are you familiar with Mike Daugherty's book?

A No.

Q When I say Mike Daugherty do you know who I'm referring to?

not going to point to a specific term or page, but just so I have this clear for the record, do you hold any academic degrees in data security.

A No.

Q Do you hold any academic degrees in information technology?

A No.

Q Do you hold any academic degrees in medicine?

A No.

Q Do you hold any academic degrees in statistics?

A No.

Q Do you hold any academic degrees in mathematics?

A No.

Q Where did you receive your undergraduate degree?

A At the University of Hawaii.

Q Hawaii?

A Yes.

Q What was your degree in?

A Management and marketing.

Q Do you have any other degrees apart from that degree you received at the University of

Hawaii?

A Academic degrees?

Q Academic degrees.

A No.

Q Do you hold any professional certifications?

A Yes.

Q What is that professional certification?

A Certified Information Privacy Professional.

Q What institute or group or organization issues that professional certification?

A IEEP.

Q Does it issue other professional certifications?

A Yes.

Q We have called a certain document a couple different things during the course of this case. During Kevin Wilmer's deposition we called it the native file, but I think you also reviewed that file and you called it something else in your report with regard to the alleged incident at Sacramento?

A Yes.

Q Would you just identify what that document is in your expert report?

you have the document there that you would like to show Mr. Kam? You are asking him to talk about a document that he doesn't have in front of him.

BY MR. HUNTINGTON:

Q I'm asking him to provide a response, you can cross-examine him later, I'm asking him without looking at the document, can you tell when the SSN doubling usage occurred?

A Not specifically from the Sacramentoresults of the document. What I can offer is that people who have multiple uses of their Social Security number indicates that they are or possibly will become victims of medical identity crimes.

MR. HUNTINGTON: And counsel, if you would like to show him the document and answer your questions, you are more than free to do so. I'm completed with my questions for today, thank you for your patience.

THE WITNESS: Thank you.

MS. MEHM: So the only thing, I have nothing further other than to the extent that today's testimony involves information designated as confidential, particularly as it relates to Mr. Boback and his deposition transcript, for which

EXHIBIT

3

Ponemon INSTITUTE

2013 Survey on Medical Identity Theft

Presented by Ponemon Institute, September 2013

Part 1: Executive Summary

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

Survey incorporates feedback from key federal agencies

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

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

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

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

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

The following are key findings from the study

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

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

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

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

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

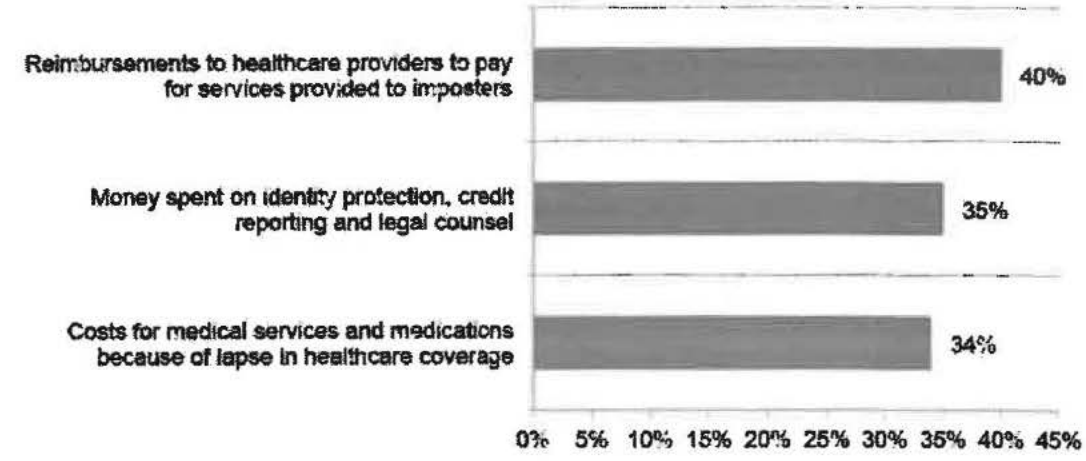
Table 1b. Total costs incurred by medical identity theft victims	Extrapolated Value
Percentage of victims who said they incurred out-of-pocket costs	36%
Number of victims who incurred out-of-pocket costs	661,072
Average out-of-pocket costs incurred by medical identity theft victims	$18,660
Total value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

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

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

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

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

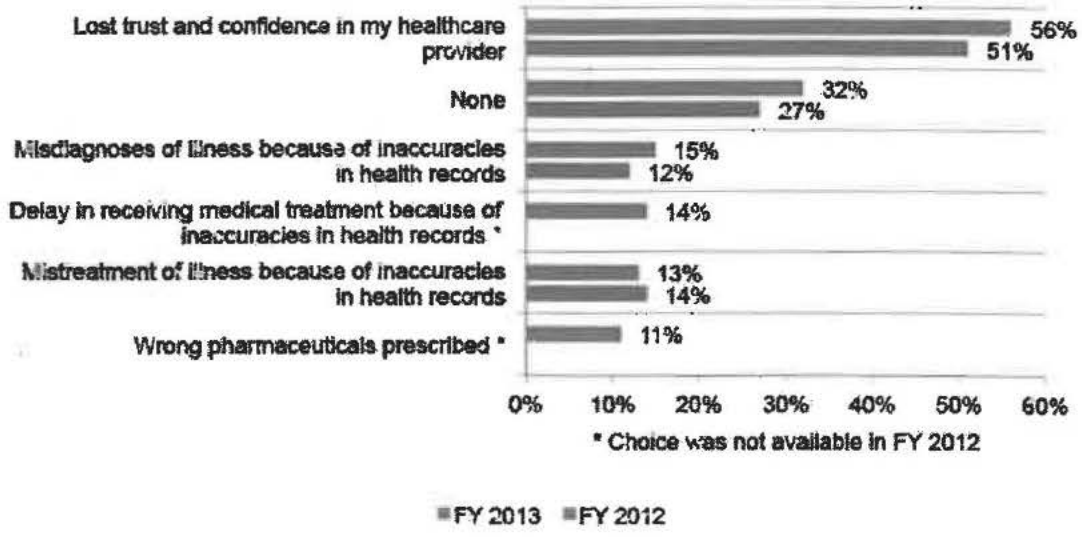


[2]The estimated total economic value shown here cannot be directly compared to last year's total value because the method used to calculate per capita cost changed (e.g., becoming more precise). Assuming this year's per capita cost applied to last year's estimated population would result in a total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

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

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

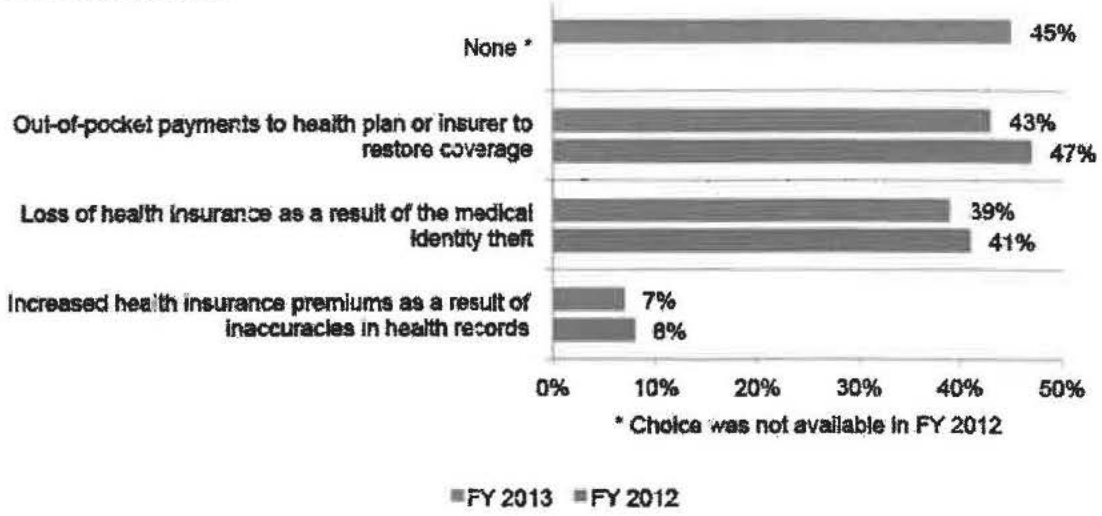
Figure 4. Medical consequences of the medical identity theft incident
Two choices permitted



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

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

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



Part 3: Conclusion: Solving the medical identity theft problem

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

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

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

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

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

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

EXHIBIT

4

CERTIFICATE OF SERVICE

I hereby certify that on April 29, 2014, I filed the foregoing document electronically using the FTC's E-Filing System, which will send notification of such filing to:

Donald S. Clark, Esq.
Secretary
Federal Trade Commission
600 Pennsylvania Ave., NW, Rm. H-113
Washington, DC 20580

I also certify that I delivered via electronic mail a copy of the foregoing document to:

The Honorable D. Michael Chappell
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Ave., NW, Rm. H-110
Washington, DC 20580

I further certify that I delivered via electronic mail a copy of the foregoing document to:

Alain Sheer, Esq.
Laura Riposo VanDruff
Megan Cox
Margaret Lassack
Ryan Mehm
John Krebs
Jarad Brown
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mail Stop NJ-8122
Washington, D.C. 20580

CERTIFICATE FOR ELECTRONIC FILING

I certify that the electronic copy sent to the Secretary of the Commission is a true and correct copy of the paper original and that I possess a paper original of the signed document that is available for review by the parties and the adjudicator.

Dated: April 29, 2014

By: /s/ Hallee K. Morgan
Hallee K. Morgan