

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



\_\_\_\_\_)  
In the Matter of )  
)  
LabMD, Inc., )  
a corporation, )  
Respondent. )  
)  
\_\_\_\_\_)

**PUBLIC**  
Docket No. 9357

**COMPLAINT COUNSEL’S OPPOSITION TO RESPONDENT’S MOTION *IN LIMINE* TO EXCLUDE EXPERT TESTIMONY OF RICK KAM**

The Court should deny Respondent’s Motion *In Limine* to exclude the testimony of Complaint Counsel’s expert witness Rick Kam. Mr. Kam possesses the necessary experience and specialized knowledge to provide expert testimony on the risk of consumer injury—particularly as it relates to medical identity theft—and he reliably applies his analysis to the facts of this case.

**BACKGROUND**

Complaint Counsel retained Mr. Kam to provide expert testimony on the likelihood of consumer harm because of his extensive experience in the areas of identity theft, medical identity theft, and consumer privacy. Complaint Counsel identified Mr. Kam as an expert on February 3, 2014 (**Exhibit A**) and provided Mr. Kam’s expert report on March 18, 2014 (**Exhibit B**). Mr. Kam’s report addresses the likely consumer harms resulting from unauthorized disclosure of sensitive information, with a focus on consumer harms related to disclosure of sensitive health information. Ex. B at 11-12, 15-16, 19-21.

Mr. Kam is a Certified Information Privacy Professional (CIPP/US) with the International Association of Privacy Professionals (IAPP) whose work focuses on mitigating harms resulting from medical identity theft. Ex. B at 25-26. He is President and Co-Founder of ID Experts, a firm that has managed hundreds of data breach incidents. *Id.* at 3. ID Experts has helped clients protect millions of consumers from breach-related harms, and it has restored the identities of thousands of identity theft victims. *Id.* It assists consumers affected by breaches in remediating the consequences of identity theft. *Id.* at 10-11. Mr. Kam presents and publishes regularly on medical identity theft and identity theft to industry groups and the public. *Id.* at 26-32.

Mr. Kam's report provides his expert opinion on the risk of injury to consumers caused by LabMD's unauthorized disclosure of sensitive personal information. *Id.* at 8. Complaint Counsel asked Mr. Kam to assume that LabMD failed to provide reasonable and appropriate security for consumers' personal information maintained on its computer networks. *Id.* at 5. Complaint Counsel did not request—and Mr. Kam did not provide—an opinion on the reasonableness of LabMD's data security. *See id.* Instead, Mr. Kam applied his experience and relevant research, including survey findings, reports, and case studies, to the facts of the case. Ex. B at 10-13, 15-20; Ex. C at 39-41, 91-93, 152-53.<sup>1</sup> Mr. Kam used the following four factors as the framework for his analysis: (1) the nature and extent of the sensitive personal information involved; (2) the unauthorized person to whom the disclosure was made; (3) whether the sensitive personal information was actually acquired or viewed; and (4) the extent to which the risk to the information has been mitigated. Ex. B at 17-18. These factors are based on Mr.

---

<sup>1</sup> Deposition Transcript of Rick Kam (Apr. 15, 2014) (**Exhibit C**).

Kam's experience, his literature review, and other materials cited in his report. Ex. B at 17-19, 22-23, 33-38; Ex. C at 71-73.

Mr. Kam's report considers the risk of harm caused by LabMD's failure "to provide reasonable and appropriate security" for the personal information of consumers maintained on its computer networks. Compl. ¶¶ 10, 22; Ex. B at 23. Mr. Kam's report also evaluates the risk of harm to consumers from the unauthorized disclosure of the LabMD file containing the sensitive personal information of approximately 9,300 consumers that was shared to a public peer-to-peer ("P2P") network [REDACTED] ("P2P Insurance Aging File"). *Id.* ¶¶ 10(g), 17-20; Boback Tr. 9-10; Ex. B at 18-22.<sup>2</sup> Finally, Mr. Kam's report evaluates the risk of harm to consumers caused by the LabMD files with personal information of over 600 consumers ("Sacramento Documents") that were found in the hands of identity thieves in October 2012 by the Sacramento Police Department. *Id.* ¶ 21; Ex. B at 21-23. Mr. Kam concludes that (1) consumers cannot know about certain unauthorized disclosures; (2) use of a consumer's Social Security number by people with different names may indicate identity theft; and (3) LabMD's security failures are likely to cause substantial harm, including medical identity theft. Ex. B at 8, 17-24.

### ARGUMENT

Respondent's Motion should be denied because Mr. Kam is a qualified expert in identity theft and medical identity theft, and his opinions concerning the likelihood of consumer harm resulting from LabMD's failure to provide reasonable and appropriate security are based on

---

<sup>2</sup> Deposition Transcript of Robert Boback (Nov. 21, 2013) (**Exhibit D**).

reliable methodology applied to the facts of this case. The Court can best consider Respondent's arguments concerning the evidentiary value of Mr. Kam's testimony at the close of the hearing.

Motions *in limine* should succeed in excluding evidence "only when the evidence is clearly inadmissible on all potential grounds." *In re Daniel Chapter One*, 2009 FTC LEXIS 85 at \*19 (Apr. 20, 2009). "When ruling on the admissibility of expert opinions, courts traditionally consider whether the expert is qualified in the relevant field and examine the methodology the expert used in reaching the conclusions at issue." *In re Basic Research*, 2006 FTC LEXIS 5 at \*11-12 (Jan. 10, 2006) (citing *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993) and *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 153-54 (1999)). See also Fed. R. Evid. 702. While *Daubert* and Rule 702 acknowledge the gatekeeping role of the judge, this function "to prevent expert testimony from unduly confusing or misleading a jury[] has little application in a bench trial." *In re McWane*, 2012 FTC LEXIS 142, at \*8 (Aug. 16, 2012). Vigorous cross-examination of the expert, alongside presentation of contrary evidence and a careful weighing of the burden of proof is the better approach for challenging expert testimony under *Daubert* in a bench trial. See *In re Basic Research*, 2006 FTC LEXIS 5, at \*9 (Jan. 10, 2006).

**I. MR. KAM IS A QUALIFIED EXPERT ON IDENTITY THEFT AND MEDICAL IDENTITY THEFT**

Mr. Kam is qualified as an expert on identity theft and medical identity theft. An expert may be qualified by "knowledge, skill, experience, training, or education." Fed. R. Evid. 702. "In certain fields, experience is the predominant, if not sole, basis for a great deal of reliable expert testimony." Fed. R. Evid. 702 advisory committee's note. See also, e.g., *United States v. Jones*, 107 F.3d 1147 (6th Cir. 1997) (upholding admission of testimony of handwriting examiner with years of practical experience); *Kumho*, 526 U.S. at 156 ("[N]o one denies that an

expert might draw a conclusion from a set of observations based on extensive and specialized experience.”).

Contrary to LabMD’s assertions, Mr. Kam is qualified to provide expert testimony on the harms consumers are likely to suffer due to LabMD’s failure to provide reasonable and appropriate security for consumers’ personal information. Mr. Kam is a CIPP with more than ten years of experience in identity theft victim restoration. Ex. B at 3, 5. Mr. Kam’s work experience has focused on the harms stemming from disclosure of sensitive medical information. *Id.* at 3. He currently chairs a network of privacy professionals who focus on developing best practices to protect sensitive medical information, and is a founding member of the Medical Identity Fraud Alliance. *Id.* at 25-26. Mr. Kam’s firm, ID Experts, has managed hundreds of data breach incidents, protecting millions of affected consumers and restoring the identities of thousands of identity theft victims. *Id.* at 3. Mr. Kam has responded to unauthorized disclosures as part of ID Experts’ incident response team. *Id.* 3-4, 25. Mr. Kam has been published extensively regarding identity theft and medical identity theft, is a frequent speaker on these issues, and leads and participates in several data privacy groups. *Id.* at 25-32.

## **II. MR. KAM’S EXPERT ANALYSIS IS RELIABLE**

Respondent wrongly argues that Mr. Kam’s methodology is unreliable because it is not “generally accepted” and has not been “peer reviewed” or “verified by testing.” Resp. Mot. at 3-4. These *Daubert* factors are not the only means to assess the reliability of an expert’s methodology; courts may consider other factors relevant to the expert’s field. *See Daubert*, 509 U.S. at 593; *Kumho*, 526 U.S. at 150-51. Depending on the nature of the case and the issue in dispute, reliability considerations may focus upon personal knowledge or experience of an expert. *See Kumho*, 526 U.S. at 150; Fed. R. Evid. 702 advisory committee’s note (noting when

an expert relies “primarily on experience, then the witness must explain how that experience leads to the conclusion reached, why that experience is a sufficient basis for the opinion, and how that experience is reliably applied to the facts”); *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec.*, 691 F. Supp. 2d 448, 473 (2010) (applying advisory committee note’s standard for experience qualifying an expert).

Mr. Kam’s analysis of the risk of consumer injury is based on his extensive experience working in the field of identity theft victim restoration, as well as his knowledge of relevant literature concerning identity theft, medical identity theft, and consumer privacy. Ex. B at 10-11, 13-15, 33-36; Ex. C at 36-37, 44-46, 72-73. Mr. Kam based his analysis on four factors: (1) the nature and extent of the sensitive personal information, (2) the party to whom the unauthorized disclosure was made, (3) whether the sensitive information was actually acquired or viewed, and (4) the extent to which the risk to the information has been mitigated and other materials cited in his report. Ex. B at 17-18. He derived this framework from his work with clients, which he outlined throughout the report, as well as his literature review. Ex. B at 10, 13-15, 33-36; Ex. C at 36-37, 44-46, 72-73.

Mr. Kam’s analysis is a fact-dependent inquiry, and the application of his analysis to this case is informed by his work experience. Ex. C at 72-73. Mr. Kam’s judgment in assessing how each unauthorized disclosure or security failure creates particular risks is informed by years of experience in responding to unauthorized disclosures. Ex. B at 3, 13-14. Mr. Kam explains in detail how he applied his experience to the facts of the LabMD unauthorized disclosures and security failures, how his experience led to his opinions on the likelihood of harm resulting from LabMD’s disclosures of sensitive personal information, and why his experience provides sufficient bases for those opinions. *See* Ex. B at 10-12, 18-19, 21-23; Section III *infra*.

**III. MR. KAM'S ANALYSIS IS SUFFICIENTLY APPLIED TO THE FACTS OF THIS CASE**

Mr. Kam's analysis is sufficiently connected to the facts of this case. A qualified expert may offer expert testimony when the testimony is based on sufficient facts, and the expert reliably applies principles and methods to the facts of the case. Fed. R. Evid. 702. Mr. Kam reliably applied his expertise to the facts of this case and his testimony should therefore be considered by this Court.

Mr. Kam reviewed numerous documents provided to him by Complaint Counsel and applied his analysis to the facts of this case, including the P2P Insurance Aging File and deposition testimony. Ex. B at 6-8. In his analysis of the disclosure of the P2P Insurance Aging File (the "P2P Disclosure"), Mr. Kam considered Mr. Boback's *entire* deposition, including [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Mr. Kam's analysis of harm from the P2P Disclosure also considered the volume and sensitivity of the information contained within the P2P Insurance Aging File. Ex. B at 18. His opinion of the reputational harm that may result from the P2P Disclosure is rooted in a detailed analysis of the disclosed CPT codes. *Id.* at 6, 18, 21, 39-48. Mr. Kam's calculation of the financial harms in out-of-pocket costs and other injuries consumers will likely suffer due to the P2P Disclosure is also based on the specific types and amount of data included in the P2P Insurance Aging File. *Id.* at 19-20. Mr. Kam applied the findings of the Ponemon Institute's 2013 Survey on Medical Identity Theft to aid his analysis of the likely risk of harm faced by the

9,300 consumers whose information was disclosed by LabMD in the P2P Disclosure. *Id.* at 19; Ex. C at 106.

Mr. Kam's opinion regarding the harm likely to result from disclosure of the Sacramento Documents is likewise specific to the information contained in the Sacramento Documents. Ex. B at 23. Mr. Kam considered the Sacramento Documents, investigation, pleas entered by the identity thieves, and usage of the relevant SSNs, and offered his opinion on the harm that can result based on his knowledge of unauthorized disclosures and identity crimes. *Id.* at 22-23; Ex. C. at 154-55. Mr. Kam identified consumers whose information was in the Sacramento Documents and had more than one name associated with an SSN, indicating identity theft may have occurred. Ex. B at 23; Ex. C at 151-55.

Finally, Mr. Kam's opinion regarding consumer harms likely to result from LabMD's failure to provide reasonable and appropriate security to the personally identifiable information stored on its network is sufficiently informed by the facts in this case. LabMD is an entity that stores a high volume of sensitive consumer information, including health information. *See* Ex. B at 23. In consideration of these facts, Mr. Kam opines that LabMD's security failures create an elevated risk of unauthorized disclosure, and therefore are likely to cause harm to consumers in the form of identity crimes. *Id.*

#### **IV. RESPONDENT'S BIAS ARGUMENT IS MERITLESS**

Respondent's suggestion that Mr. Kam's opinions are biased because Mr. Kam has a professional association with Dr. Larry Ponemon, a member of Tiversa's advisory board, is meritless. *See* Mot. at 9. Mr. Kam testified that he has no relationship with Tiversa and that he has not spoken to Mr. Boback about this case. Ex. C at 112, 175. Furthermore, any question as to the existence of bias "goes to the weight, not the admissibility of the testimony, and should be

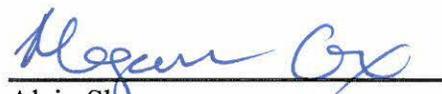
brought out on cross-examination.”” *Grant Thornton v. FDIC*, 297 F. Supp. 2d 880, 884 n.3 (S.D. W. Va. 2004) (quoting *United States v. Kelly*, 6 F. Supp. 2d 1168, 1183 (D. Kan. 1998); see also *In re Foster-Milburn Co.*, 51 F.T.C. 369, 374 (1954) (“[M]atters in reference to bias or interest on the part of expert witnesses relate to the weight and credibility of their testimony rather than their eligibility to testify in the first instance.”))

**CONCLUSION**

For the foregoing reasons, the Court should deny Respondent’s Motion to Exclude the Expert Testimony of Rick Kam.

Dated: May 1, 2014

Respectfully submitted,



Alain Sheer  
Laura Riposo VanDruff  
Megan Cox  
Margaret Lassack  
Ryan Mehm  
John Krebs  
Jarad Brown  
Federal Trade Commission  
600 Pennsylvania Ave., NW  
Room NJ-8100  
Washington, DC 20580  
Telephone: (202) 326-2282 – Cox  
Facsimile: (202) 326-3062  
Electronic mail: mcox1@ftc.gov

*Complaint Counsel*

CERTIFICATE OF SERVICE

I hereby certify that on May 1, 2014, I filed the foregoing document with the Office of the Secretary:

Donald S. Clark  
Secretary  
Federal Trade Commission  
600 Pennsylvania Avenue, NW, Room H-113  
Washington, DC 20580

I also certify that I caused a copy of the foregoing document to be delivered *via* electronic mail and by hand to:

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

I further certify that I caused a copy of the foregoing document to be served *via* electronic mail to:

Michael Pepson  
Lorinda Harris  
Hallee Morgan  
Robyn Burrows  
Kent Huntington  
Daniel Epstein  
Patrick Massari  
Cause of Action  
1919 Pennsylvania Avenue, NW, Suite 650  
Washington, DC 20006  
michael.pepson@causeofaction.org  
lorinda.harris@causeofaction.org  
hallee.morgan@causeofaction.org  
robyn.burrows@causeofaction.org  
kent.huntington@causeofaction.org  
daniel.epstein@causeofaction.org  
patrick.massari@causeofaction.org

Reed Rubinstein  
William A. Sherman, II  
Sunni Harris  
Dinsmore & Shohl, LLP  
801 Pennsylvania Avenue, NW, Suite 610

PUBLIC

Washington, DC 20004  
reed.rubinstein@dinsmore.com  
william.sherman@dinsmore.com  
sunni.harris@dinsmore.com  
*Counsel for Respondent LabMD, Inc.*

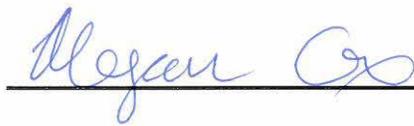
May 1, 2014

By:   
Megan Cox  
Federal Trade Commission  
Bureau of Consumer Protection

**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.

May 1, 2014

By: 

Megan Cox  
Federal Trade Commission  
Bureau of Consumer Protection

# Exhibit A

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

	)	
In the Matter of	)	
	)	
LabMD, Inc.,	)	Docket No. 9357
a corporation,	)	
Respondent.	)	
	)	
	)	

**COMPLAINT COUNSEL’S EXPERT WITNESS LIST**

Pursuant to Rule 3.31A of the Federal Trade Commission’s Rules of Practice, 16 C.F.R. § 3.31A, and the Court’s October 22, 2013 and September 25, 2013 Scheduling Orders, and without waiving its right to identify rebuttal expert(s) at a later date in compliance with the October 22, 2013 Revised Scheduling Order, Complaint Counsel identifies the following individuals as the experts who Complaint Counsel may call in its case in chief or in rebuttal:

**Raquel Hill, PhD**

Professor Hill is a Visiting Scholar at Harvard University’s School of Engineering and Applied Science, Center for Research on Computation and Society. She is also an Associate Professor at Indiana University, School of Informatics and Computing. Professor Hill’s research focuses on trust and security for distributed computing environments and privacy of medical related data. She received both her Bachelor of Science and Master of Science in Computer Science from the Georgia Institute of Technology. She received her PhD in Computer Science

from Harvard University in 2002. A copy of her *curriculum vitae* is attached, and it includes a list of her publications and presentations within the last ten years.

Professor Hill has not testified as an expert at trial or at deposition within the last four years.

**Rick Kam, CIPP/US**

Mr. Kam is a Certified Information Privacy Professional, and he is President and Co-Founder of ID Experts, a company providing services that address the organizational risks associated with sensitive personal data. ID Experts has managed hundreds of data breach incidents and protects millions of individuals. It serves leading healthcare providers, insurance organizations, universities, and government agencies, and it is endorsed by the American Hospital Association. Mr. Kam serves in leadership roles of organizations addressing identity theft, medical identity theft, and data breach risk and remediation, and he presents regularly at conferences regarding these and other subjects. A copy of his *curriculum vitae* is attached, and it includes a list of his publications within the last ten years.

Mr. Kam has not testified as an expert at trial or at deposition within the last four years.

**James Van Dyke**

Mr. Van Dyke is the Founder and President of Javelin Strategy & Research (“Javelin”). Among other services, Javelin produces an annual study of identity theft in the United States. Under Mr. Van Dyke’s leadership, Javelin’s study provides a comprehensive analysis of identity fraud in the United States, which is used extensively by industry and other stakeholders. Mr. Van Dyke presents regularly to thought leaders on issues relating to identity theft and security.

A copy of Mr. Van Dyke's biography is attached, and appended to it is a list of Mr. Van Dyke's publications within the last ten years.

Mr. Van Dyke has not testified as an expert at trial or at deposition within the last four years.

Dated: February 3, 2014

Respectfully submitted,

/s/ Margaret L. Lassack

Alain Sheer

Laura Riposo VanDruff

Megan Cox

Margaret Lassack

Ryan Mehm

John Krebs

Jarad Brown

Complaint Counsel

Federal Trade Commission

600 Pennsylvania Avenue NW

Room NJ-8100

Washington, DC 20580

Telephone: (202) 326-3713 (Lassack)

Facsimile: (202) 326-3026

Electronic mail: mlassack@ftc.gov

**CERTIFICATE OF SERVICE**

I hereby certify that on February 3, 2014, I delivered *via* electronic mail a copy of Complaint Counsel's Expert Witness List to:

Michael Pepson  
Lorinda Harris  
Hallee Morgan  
Kent Huntington  
Robyn Burrows  
Cause of Action  
1919 Pennsylvania Avenue, NW, Suite 650  
Washington, DC 20006  
michael.pepson@causeofaction.org  
lorinda.harris@causeofaction.org  
hallee.morgan@causeofaction.org  
kent.huntington@causeofaction.org  
robyn.burrows@causeofaction.org

Reed Rubinstein  
William A. Sherman, II  
Sunni Harris  
Dinsmore & Shohl, LLP  
801 Pennsylvania Avenue, NW, Suite 610  
Washington, DC 20004  
reed.rubinstein@dinsmore.com  
william.sherman@dinsmore.com  
sunni.harris@dinsmore.com  
*Counsel for Respondent LabMD, Inc.*

February 3, 2014

By: /s/ Margaret L. Lassack  
Margaret Lassack  
Federal Trade Commission  
Bureau of Consumer Protection

Home Address: School of Informatics and  
734 E. Moss Creek Computing  
Drive Indiana University  
Bloomington, IN 47401 Bloomington, IN 47405  
Phone(217)369-0105 Phone (812) 856-5807  
hill raquel@gmail.com E-mail  
[ralhill@indiana.edu](mailto:ralhill@indiana.edu)  
[www.cs.indiana.edu/~ralhill](http://www.cs.indiana.edu/~ralhill)

# Raquel Hill

---

## Education

University of Illinois Urbana, IL

**August 2003- July 2005 Post Doctoral Research Associate**

Harvard University Cambridge, MA

**November 2002 PhD Computer Science**

- Dissertation: Sticky QoS: A Scalable Framework for Resource Reservations.
- Advisor: H.T. Kung

Georgia Institute of Technology Atlanta, GA

**March 1993 MS Computer Science**

**June 1991 BS Computer Science with Honors**

## Professional Experience

**Harvard University, Cambridge, MA, Visiting Scholar, School of Engineering and Applied Science, Center for Research on Computation and Society, 9/2013 – 5/2014**

**Indiana University, Bloomington, Indiana, Associate Professor, School of Informatics and Computing, 6/2012 –Present**

**Indiana University, Bloomington, Indiana, Assistant Professor, School of Informatics and Computing, 08-2005 – 6/2012**

**Indiana University, Bloomington, Indiana, Research Fellow, Kinsey Institute, 12/2010 – Present**

**Jackson State University, Jackson, Mississippi, Adjunct Professor, Department of Computer Science, 2010- Present**

**University of Illinois, Urbana, Illinois, Post-Doctoral Research Associate, Joint Appointment with Department of Computer Science and NCSA, 08/2003 – 07/2005**

**Georgia Institute of Technology Atlanta, GA, Lecturer, within the School Electrical and Computer Engineering, 11/2002 – 08/2003**

**Professional Experience**

**Harvard University**, Cambridge, MA, **Research Assistant** 09/1998 – 09/2002

**IBM Research** , Hawthorne, NY, **Intern**, Summer 1999

**Digital Equipment Corporation**, Cambridge, MA, **Intern**, Summer 1997

**Nortel Networks** , RTP, NC, **Member of Scientific Staff**, 08/1993 – 08/1996

**Hayes MicroComputer Products**, Atlanta, GA, **Coop Student**, 03/1993-07/1993

**Cray Research**, Eagan, MA, **Intern**, Summer 1992

**Cray Research**, Chippewa Falls, WI, **Intern**, Summer 1991

**IBM Corporation**, Atlanta, GA, **Co-op Student**, 06/1987-9/1990

**Grants**

**IBM Corporation, Equipment Grant – Cryptographic Co-processors**

Equipment Value: \$75,000.00      Date: 9/01/05 – Present

**CACR: Privacy Enhanced Online Human Subjects Data Collection**

Total Award Amount: \$49,999.99      Date: 07/01/09 – 12/31/10

Role: PI      Source of Support: IU

**TC: Large: Collaborative Research: Anonymizing Textual Data and Its Impact on Utility**

Total Award: \$568,895      Date: 9/01/10 – 8/31/14

Role: PI      Source of Support: NSF

**FRSP: Childhood Obesity Studies with Secure Cloud Computing**

Total Award: \$36,500      Date: 9/1/11 – 12/31/13

Role: PI

**Publications**

R. Hill, M. Hansen, E. Janssen, S.A. Sanders, J. R. Heiman, L. Xiong, Evaluating Utility: Towards an Understanding of Sharing Differentially Private Behavioral Science Data, Submitted to the *Journal of Biomedical Informatics* (Under Review).

Raquel Hill, Michael Hansen, Veer Singh, “Quantifying and Classifying Covert Channels on Android”, *Journal of Mobile Networks and Applications*, Springer US. DOI. 10.1007/s11036-013-0482-7, (November 2013).

## Publications

D. Hassan, R. Hill, "A Language-based Security Approach for Securing Map-Reduce Computations in the Cloud", To appear in the *Proceedings of the 6<sup>th</sup> IEEE/ACM International Conference on Utility and Cloud Computing*, December 9-12, 2013, Dresden, Germany.

R. Hill, M. Hansen, E. Janssen, S.A. Sanders, J.R. Heiman, L. Xiong, "An Empirical Analysis of a Differentially Private Social Science Dataset" In the *Proceedings of PETools: Workshop on Privacy Enhancing Tools, Held in Conjunction with the Privacy Enhancing Tools Symposium*, July 9, 2013, Bloomington, IN.

M. Hansen, R. Hill, S. Wimberly, Detecting Covert Communications on Android. In the *Proceedings of the 37<sup>th</sup> IEEE Conference on Local Computer Networks (LCN 2012)*, October 22-25, 2012, Clearwater, Florida.

A. C. Solomon, R. Hill, E. Janssen, S. Sanders, J. Heiman, Uniqueness and How it Impacts Privacy in Health-Related Social Science Datasets, In the *Proceedings of the ACM International Health Informatics Symposium (IHI 2012)*, January 28-30, 2012, Miami Florida.

J. Harris, R. Hill, Static Trust: A Practical Framework for Trusted Networked Devices, In the *Proceedings of 44<sup>th</sup> Hawaii International Conference on System Sciences, Information Security and Cyber Crime Track*, (Kauai, HI, 2011), 10 pages, CDROM, IEEE Computer Society.

Al-Muhtadi, Raquel Hill and Sumayah AIRwais "Access Control using Threshold Cryptography for Ubiquitous Computing Environments". *Journal of King Saud University Computer and Information Sciences*, No. 2, Vol. 23, (July 2011).

R. Hill, J. Al-Muhtadi, W. Byrd, An Access Control Architecture for Distributing Trust in Pervasive Computing Environments, at the *6<sup>th</sup> IEEE/IFIP Symposium on Trusted Computing and Communications (TrustCom)*, In the *Proceedings of 8<sup>th</sup> IEEE/IFIP Conference on Embedded and Ubiquitous Computing*, (Hong Kong, China, 2010), 695-702.

J. Harris, R. Hill, Building a Trusted Image for Embedded Communications Systems, In the *Proceedings of 6th Annual Cyber Security and Information Intelligence Workshop*, (Oakridge, TN, 2010), ACM, NY, 65:4.

L. Wang, R. Hill, Trust Model for Open Resource Control Architecture, at *3<sup>rd</sup> IEEE International Symposium on Trust, Security and Privacy for Emerging Applications*, In the *Proceedings of 10<sup>th</sup> IEEE International Conference on Computer and Information Technology*, (Bradford, UK, 2010) 817-823.

## Publications

Gilbert, J.E., MacDonald, J., Hill, R., Sanders, D., Mkpong-Ruffin, I., Cross, E.V., Rouse, K., McClendon, J., & Rogers, G. (2009) Prime III: Defense-in-Depth Approach to Electronic Voting. In the *Journal of Information Security and Privacy*, 2009

J. Al-Muhtadi, R. Hill, R. Campbell, D. Mickunas, Context and Location-Aware Encryption for Pervasive Computing Environments, In *Proceedings of the 4<sup>th</sup> IEEE Conference on Security in Pervasive Computing and Communications Workshops*, (Pisa, Italy, 2006), 283-289.

R. Hill, S. Myagmar, R. Campbell, Threat Analysis of GNU Software Radio, In the *Proceedings of the 6<sup>th</sup> World Wireless Congress*, (San Francisco, CA, 2005).

A. Lee, J. Boyer, C. Drexelius, P. Naldurg, R. Hill, R. Campbell, Supporting Dynamically Changing Authorizations in Pervasive Communication Systems, In the *Proceedings of the 2<sup>nd</sup> International Conference on Security in Pervasive Computing*, (Boppard, Germany, 2005), 134-150.

R. Hill, G. Sampemane, A. Ranganathan, R. Campbell, Towards a Framework for Automatically Satisfying Security Requirements, In the *Proceedings of Workshop on Specification and Automated Processing of Security Requirements in conjunction with the 19<sup>th</sup> IEEE International Conference on Automated Software Engineering*, (Linz Austria, 2004), 179-191.

R. Hill, J. Al-Muhtadi, R. Campbell, A. Kapadia, P. Naldurg, A. Ranganathan, A Middleware Architecture for Securing Ubiquitous Computing Cyber Infrastructures, *5th ACM/IFIP/USENIX International Middleware Conference*, October 2004, in *IEEE Distributed Systems Online*, 5,9 (September 2004), 1-.

R. Hill, H.T. Kung, A Diff-Serv enhanced Admission Control Scheme, In *Proceedings IEEE Global Telecommunications Conference*, (San Antonio, TX, 2001), 2549-2555.

## Refereed Abstracts

A. C. Solomon, R. Hill, E. Janssen, S. Sanders, Privacy and De-Identification in High Dimensional Social Science Data Sets, in the *Proceedings of the 32<sup>nd</sup> Annual IEEE Symposium on Security and Privacy*, Oakland, California, May 22-25, 2011.

R. Hill, J. Camp, Communicating Risk within the GENI Infrastructure, *Workshop on GENI and Security*, University California, Davis, January 22-23, 2009.

R. Hill, J. Wang, K. Nahrstedt, Towards a Framework for Quantifying Non-Functional Requirements, *Grace Hopper Celebration of Women in Computing*, October 2004.

- Refereed Abstracts** J. Al-Muhtadi, R. Hill, R. Campbell, A Privacy Preserving Overlay for Active Spaces, *UbiComp Privacy Workshop in conjunction with the Sixth International Conference on Ubiquitous Computing*, Nottingham, England, September 2004.
- Posters** R. Hill, A.C. Solomon, E. Janssen, S. Sanders, J. Heiman, Privacy and Uniqueness in High Dimensional Social Science and Sex Research Datasets, Presented at the 37<sup>th</sup> Annual Meeting of the International Academy of Sex Research, August 10-13, 2011, Los Angeles, California.
- C. Boston, R. Hill, L. Moore, The Feasibility of Designing a Secure System to Prevent Surgical Errors Using RFID Technology, *in the Proceedings of the CAARMS 15*, Houston, Texas, June 23-26, 2009.
- S. Camara, R. Hill, L. Moore, Understanding How RFID Technology Impacts Patient Privacy, *in the Proceedings of the CAARMS 15*, Houston, Texas, June 23-26, 2009.
- R. Johnson, R. Hill, L. Moore, Evaluating and Mitigating the Security Vulnerabilities of RFID Technology, *in the Proceedings of the CAARMS 15*, Houston, Texas, June 23-26, 2009.
- R. Hill, J. Wang, K. Nahrstedt, Quantifying Non-Functional Requirements: A Process Oriented Approach, *in the Proceedings of the 12th IEEE International Requirements Engineering Conference*, Kyoto, Japan, September 2004.
- Technical Reports** R. Hill, J. Al-Muhtadi, Building a Trusted Location Service for Pervasive Computing Environments, Technical Report, TR646, Computer Science, Indiana University, 2007.
- Dissertation** R. Hill, Sticky QoS: A Scalable Framework for Resource Reservations, Doctoral Dissertation in Computer Science, Harvard University Division of Engineering and Applied Sciences, November 2002.
- Symposiums** “Protecting Privacy in Sex Research: Challenges and solutions offered by new technologies and recommendations for the collection, protection and the sharing of multi-dimensional data”, **Speakers:** Raquel Hill, School of Informatics and Computing, Indiana University, Ulf-Dietrich Reips, iScience, University of Deusto, Bilbao, Spain, Stephanie Sanders, Gender Studies, Indiana University, The 38<sup>th</sup> Annual Meeting of the International Academy of Sex Research, July 8-12, 2012, Lisbon, Portugal
- Invited Talks** “Understanding the Risk of Re-Identification in Behavioral Science Data”, Technology in Government Topics in Privacy Seminar, Data Privacy Lab, Harvard University, Cambridge, MA, November 4, 2013.

## Invited Talks

“Evaluating the Utility of a Differentially Private Behavioral Science Dataset”, Center for Research on Computation and Society (CRCS), Harvard University, Cambridge, MA, October 2, 2013.

“Balancing the Interests in Developing and Sharing Behavioral Science Data”, Workshop on Integrating Approaches to Privacy Across the Research Lifecycle, Harvard University, Cambridge, MA, September 24-25, 2013.

“Kinsey Goes Digital”, Kinsey Institute’s Board of Trustees Meeting, Indiana University, Bloomington, IN, May 20, 2011.

“Integrity-Based Trust for Networked Communications Systems”, Center for Applied Cyber-security Research, Indiana University, Bloomington, IN, December 2, 2010.

“From Kinsey to Anonymization: Approaches to Preserving the Privacy of Survey Participants”, Department of Mathematics and Computer Science, Emory University, Atlanta, GA, November 19, 2010; Indiana University, Bloomington, IN, November 12, 2010.

“PlugNPlay Trust for Embedded Communications Systems”, Purdue University, CERIAS, October 14, 2009; The Symposium on Computing at Minority Institutions, April 8-10, 2010, Jackson State University, Jackson MS.

“Characterizing Trustworthy Behavior of Email Servers”, CAARMS 2009, Rice University, June 23-26, 2009; The Symposium on Computing at Minority Institutions, April 8-10, 2010, Jackson State University, Jackson MS.

“Hardware Enabled Access Control for Electronic Voting Systems”, Rose Hulman, January 6, 2009; Jackson State University, February 26, 2009

“Hardware-enabled Access Control for the Prime III Voting System”, Auburn University, June 16, 2008

“Understanding the Behaviors of Malicious Users of Pervasive Computing Environments”, ARO/FSTC Workshop on Insider Attacks and Cyber Security, June 11-12, 2007, Arlington, Virginia.

“Trusting Your Security”, Second Annual Network Security Workshop, Lehigh University, May 15-16, 2006

“Establishing a Trusted Computing Base for Software Defined Radio”, Information Security Institute, Johns Hopkins University, February 2005, Baltimore, Maryland.

**Invited Talks**

“Towards a Framework for Automatically Satisfying Security Requirements”, Department of Computer Science, Queens University, October 2004, Kingston, Ontario, Canada.

“Overlay QoS”, Department of Computer Science, Auburn University, February 2004, Auburn, Alabama.

“Distributed Admissions Control for Sticky QoS”, *Ninth Annual Conference for African-American Researchers in the Mathematical Sciences*, June 2003, West LaFayette, Indiana.

“Distributed Admissions Control for Sticky QoS”. *Sixth Informs Telecommunications Conference*, March, 2002, Boca Raton, Florida.

Former Congressman Lee Hamilton, Professor Fred Cate, and Professor Raquel Hill, “Security and Privacy in a Cyberwar World: A conversation about Edward Snowden, the NSA and the outlook for reform”, *Indiana Statewide IT Conference*, Indiana University, Bloomington, IN October, 29, 2013

**Panels**

R. Hill, “Building Trusting Systems: Trusting Your Security”, *Workshop on Useable Security, co-located with 11<sup>th</sup> Conference on Financial Cryptography and Data Security*, February 2007, Lowlands, Scarborough, Trinidad/Tobago.

R. Hill, R. Campbell, “Understanding, Managing and Securing Ubiquitous Computing Environments”, *Grace Hopper Celebration of Women in Computing*, October 2004, Chicago, Illinois.

C. Lester, R. Hill, M. Spencer, “Making Waves: Navigating the Transition from Graduate Student to Faculty Member”, *Grace Hopper: Celebration of Women in Computing*, San Diego, California, Oct. 4-6, 2006.

**Teaching**

University	Course	Semesters Taught
Indiana University	I230 Analytical Foundations of Security	Spring 2006, Fall 2007-2011
	CSCI P438 Introduction to Computer Networks	Fall 2009,2010,2012
	CSCI H343 Data Structures (Honors)	Fall 2011,2012
	CSCI B649 Trusted Computing	Spring 2006-2011
	CSCI B649 Data Protection	Spring 2013
Georgia Institute of Technology	ECE 2030 Introduction to Computer Engineering	Spring 2003, Summer 2003

**Professional  
Activities**

**Member of Technical Program Committee**

- IEEE International Conference on Information Technology (ITCC) 2005, Pervasive Computing Track
- IEEE International Conference on Communications 2006: Network Security and Information Assurance Symposium
- Indiana Women in Computing Conference February 2006
- Workshop on Security, Privacy and Trust for Pervasive Computing Applications, September 2006, 2007, 2008, 2009, 2010
- Middleware Support for Pervasive Computing Workshop (PERWARE) at the 4<sup>th</sup> Conference on Pervasive Computing and Communications, March 2007, 2008, 2009
- IEEE International Conference on Computer Communications and Networks, (ICCCN'06), Network Security and Dependability Track, October 2006; (ICCCN'07), Pervasive Computing and Mobile Networking Track, August 2007.
- IFIP Sixth International Conference on Networking (Networking 2007, 2008),
- Fourth International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, March 17-20, 2008 (Tridentcom 2008)
- First International ICST Conference on Mobile Wireless Middleware, Operating Systems and Applications, February 13-15, 2008, (Mobileware 2008, 2009,2010)

**Member of Review Panel**

- **National Science Foundation**
- **Department of Energy**

**References Available Upon Request**



## Rick Kam CV

Date Updated: 1-30-2014

- **Title:** president and co-founder, ID Experts

- **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.

- **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). ID Experts has 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.

- **Affiliations and Organizations**

Mr. Kam and ID Experts are advocates for privacy; active contributors to legislation; and members of the following organizations:

- Chair of PHI Protection Network (PPN), an interactive network of solution providers focused on expediting the adoption of PHI best practices (2012 - current)
- Chair of the Santa Fe Group Vendor Council ID Management Working Group, which published *Victim's Rights: Fighting Identity Crime on the Front Lines*, February 2009 (2007 - 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 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)
- 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)

- Research Planning Committee for the University of Texas Center for Applied Identity Management Research, which focuses on identity management and identity theft risk mitigation best practices. (2009 - current)
- 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 - current)
- Member of Healthcare Information and Management Systems Society (HIMSS), a global, member-based non-profit focused on the betterment of healthcare information technology. (2010 - current)
- 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-current)
- Founding member of Medical Identity Fraud Alliance (MIFA), an assemblage of corporate members in the fight against medical identity fraud. (2013 - current)
- **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 (scheduled)  
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*

▪ **Education**

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

▪ **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**

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**

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 07, 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 Pollock, *IAPP*, October 23, 2012  
[https://www.privacyassociation.org/publications/2012\\_11\\_01\\_the\\_healthcare\\_privacy\\_balance](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**

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**



American National Standards Institute (ANSI)/Internet Security Alliance (ISA), 2008  
[http://www.ansi.org/meetings\\_events/events/cyber\\_risk09.aspx?menuid=8](http://www.ansi.org/meetings_events/events/cyber_risk09.aspx?menuid=8)

➤ **Regulatory/Compliance**

**Privacy and Security Compliance Wish List 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>

## **Biography- James Van Dyke**

James Van Dyke is Founder and President of Javelin Strategy & Research. Javelin provides strategic insights into customer-transactions, serving the largest financial institutions, government agencies, payments brands, merchants and other service providers. Javelin's independent and unique insights result from expert analysis of over 300,000 proprietary research end-points on the three dimensions of customers, providers, and the transactions ecosystem. Mr. Van Dyke is known for numerous new discoveries that have resulted from his company's research on customer-related security, fraud, payments, and electronic financial services.

Areas of particular expertise include consumer behavior, security technologies, personal financial services and payments, and the future of identity management capabilities. Under his leadership, Javelin engages with its clients through three service offerings, including membership-based research subscriptions, custom research projects and strategic consulting.

Javelin's team of statisticians and industry analysts are known for producing the most rigorous annual, nationally-representative victim study of identity crimes in the United States, which builds on methodologies first used by the Federal Trade Commission. This annual study provides detailed, comprehensive analysis of identity fraud in the United States in order to help consumers and businesses better understand the effectiveness of methods used for fraud prevention, detection and resolution.

Mr. Van Dyke has made countless public presentations including testimony before the U.S. House of Representatives on the future of secure personal financial management; to several Federal Reserve Bank gatherings on identity fraud, payments and security; to the Federal Reserve Board of Governors on the impact of security issues on electronic commerce growth; to the RSA Security Conference attendees (the industry's largest such event) on several aspects of data security and recommended solutions; and to several gatherings of banking executives on security, payments and financial services best practices. As a public commentator Mr. Van Dyke's viewpoints now reach over 30 million individuals each year through print and broadcast media around the globe.

Prior to founding Javelin, Mr. Van Dyke was Research Director at Jupiter Media Metrix with focus on security; payments and financial services sectors; Senior Research Analyst at the Internet Research Group; Product Director at Harbinger Corporation with focus on encryption and data movement systems; Product Manager at Harland Systems with focus on financial services and electronic payments technologies; Product Manager at Hewlett Packard; and a variety of positions in employee development, product management and customer deployment at a pre-Web electronic commerce provider.

Mr. Van Dyke received a Master's degree from Golden Gate University and Bachelor of Science from San Jose State University. He is an avid bicyclist and active advocate of 'green' initiatives for businesses, as well as in his personal life. Mr. Van Dyke and his family reside in the San Francisco Bay Area.

***Biometrics in Banking and Payments: Versatile Voice Faces an Apple-Led Fingerprint Revolution***  
Javelin Strategy & Research, Jan 2014

***Social Media Payment: Redefining Shopping for a New Era***  
Javelin Strategy & Research, Jan 2014

***Ten Trends for Financial Services in 2014: Big Data, Big Clouds, Big Mobile, Big Brother***  
Javelin Strategy & Research, Jan 2014

***9<sup>th</sup> Annual Credit Card Issuers' Identity Safety Scorecard***  
Javelin Strategy & Research, Dec 2013

***Mobile Banking Vendor Scorecard***  
Javelin Strategy & Research, Dec 2013

***Financial Alerts Forecast 2013***  
Javelin Strategy & Research, Dec 2013

***Payment Card Data Security Report***  
Javelin Strategy & Research, Dec 2013

***Identity Protection Services Scorecard***  
Javelin Strategy & Research, Dec 2013

***Mobile Banking FI Scorecard***  
Javelin Strategy & Research, Dec 2013

***How Mobile Can Open the Door to \$2.1 Trillion in Bill Payments***  
Javelin Strategy & Research, Dec 2013

***2013 Gang of Five Apple Google Amazon Facebook and PayPal eBay***  
Javelin Strategy & Research, Dec 2013

***Account-to-Account and Person-to-Person Money Transfers in 2013***  
Javelin Strategy & Research, Dec 2013

***Mobile Wallet Game Changers***  
Javelin Strategy & Research, Dec 2013

***2013 ONLINE BANKING AND BILL-PAYMENT FORECAST: 29 Million Holdouts Primed for FI Bill Pay***  
Javelin Strategy & Research, Dec 2013

***INTERNATIONAL REMITTANCE TRANSFERS: How to Tap \$2.1B in Cross-Border Revenue***  
Javelin Strategy & Research, 2013

**VIRTUAL CURRENCIES 2013: Crossing to the Physical Chasm**

*Javelin Strategy & Research, 2013*

**HOW TO UPGRADE ONLINE AND MOBILE ACCOUNT OPENING FOR AN OMNICHANNEL ERA: 2013**

*Javelin Strategy & Research, 2013*

**LEVERAGING AN OMNICHANNEL APPROACH TO DRIVE \$1.5B IN MOBILE BANKING COST SAVINGS**

*Javelin Strategy & Research, 2013*

**ONLINE AND MOBILE RETAIL PAYMENTS AUTHENTICATION: Preventing Fraud in the Age of Data Breaches and Malware**

*Javelin Strategy & Research, 2013*

**2013 DATA BREACH FRAUD IMPACT REPORT: Mitigating a Rapidly Emerging Driver of Fraud**

*Javelin Strategy & Research, 2013*

**CHECKING VS. PREPAID: Threat or Opportunity?**

*Javelin Strategy & Research, 2013*

**MOBILE POS (POINT OF SALE) BUSINESS AND MARKET IMPACT 2013: Emerging Technologies Expand Reach with Lower Cost, Disruptive Services**

*Javelin Strategy & Research, 2013*

**2013 RETAIL POINT OF SALE (POS) UPDATE AND FORECAST: Mobile and Prepaid Opens New POSSibilities**

*Javelin Strategy & Research, 2013*

**REAL-TIME PAYMENTS 2013: Struggling Toward Revolutionary Change**

*Javelin Strategy & Research, 2013*

**2013 BANKING IDENTITY SAFETY SCORECARD: Changing Tactics in the Face of Growing Account Takeover and New Account Fraud**

*Javelin Strategy & Research, 2013*

**HOW TO BUILD BETTER ONLINE AND MOBILE BILL-PAY FOR THE UNDERBANKED**

*Javelin Strategy & Research, 2013*

**21ST-CENTURY PFM FOR A MASS AUDIENCE: How to Build Everyday Online and Mobile PFM**

*Javelin Strategy & Research, 2013*

**2013 IDENTITY FRAUD REPORT: Data Breaches Becoming a Treasure Trove for Fraudsters**

*Javelin Strategy & Research, 2013*

**MOBILE IMAGING: Going beyond Mobile Remote Deposit Capture to Bridge the Consumer Transaction Gap**

*Javelin Strategy & Research, 2013*

**A TALE OF TWO GEN Ys: On the Road to Long-Term Banking Profitability**

*Javelin Strategy & Research, Jan 2013*

**MOBILE SECURITY—PAYMENTS: \$20B Market at Risk Due to Inadequate Consumer Mobile Device Security**

*Javelin Strategy & Research, 2012*

**10 TRENDS FOR FINANCIAL SERVICES IN 2013: Forging a New Frontier for Banking, Payments, Mobile and Security**

*Javelin Strategy & Research, 2012*

**MOBILE, PFM, AND REWARDS: The ACCESS™ Value Paradigm**

*Javelin Strategy & Research, 2012*

**2012 MOBILE BANKING, SMARTPHONE, AND TABLET FORECAST: Mobile Banking Gains 10 Million Users as Smartphone and Tablet Adoption Soars**

*Javelin Strategy & Research, 2012*

**5TH ANNUAL ONLINE RETAIL PAYMENTS FORECAST 2012–2017: Mobile and Alternative Payments Are Changing the Game**

*Javelin Strategy & Research, 2012*

**2012 MOBILE BANKING FINANCIAL INSTITUTION SCORECARD: Three Keys to Mobile Money Movement Success**

*Javelin Strategy & Research, 2012*

**BANKING AUTHENTICATION AND THE FFIEC: Business Customers Crave Biometrics**

*Javelin Strategy & Research, 2012*

**ROAD MAP TO ALERTS 3.0: A New Channel Emerges for Interactive Finance**

*Javelin Strategy & Research, 2012*

**EMV: Moving Toward Ubiquity**

*Javelin Strategy & Research, 2012*

**2012 IDENTITY PROTECTION SERVICES SCORECARD: How to Deliver Customer and Market Value in a Regulated \$4B Market**

*Javelin Strategy & Research, 2012*

**MOBILE PAYMENTS HIT \$20 BILLION IN 2012: Tablets Are Key to a Successful Retail Strategy**  
*Javelin Strategy & Research, 2012*

**HOW TO CONVERT 22 MILLION AMERICANS TO FI BILL PAY**  
*Javelin Strategy & Research, 2012*

**BATTLE FOR CONTROL OF THE MOBILE WALLET: Sorting Out Players, Technologies and Strategies to Win**  
*Javelin Strategy & Research, 2012*

**2012 ONLINE BANKING AND BILL-PAYMENT FORECAST: How to Boost Profitability When Facing Flat-Lining Adoption**  
*Javelin Strategy & Research, 2012*

**ACCOUNT-TO-ACCOUNT AND PERSON-TO-PERSON TRANSFERS: Emerging Players Pose Threat to PayPal**  
*Javelin Strategy & Research, 2012*

**VIRTUAL CURRENCIES: A Global Gamble**  
*Javelin Strategy & Research, 2012*

**QR CODES: HOW APPLE PASSBOOK CHANGES THE MERCHANT EQUATION Best Practices for Mobile Marketing and Mobile Payments**  
*Javelin Strategy & Research, 2012*

**2012 IDENTITY FRAUD FOR SMALL BUSINESS OWNERS: Paypal and Alternative Payments Poised to Change SMBO Payment Landscape**  
*Javelin Strategy & Research, 2012*

**BANK SWITCHING IN 2012: Giant Banks Remain Highly Vulnerable as Customers Weigh Fees and Convenience**  
*Javelin Strategy & Research, 2012*

**REACHING UNDERBANKED AND UNBANKED CONSUMERS IN 2012: Strategies for Connecting with Mobile Financial Services**  
*Javelin Strategy & Research, 2012*

**8TH ANNUAL CARD ISSUERS' SAFETY SCORECARD: Proliferation of Alerts Lead to Quicker Detection Time and Lower Fraud Costs**  
*Javelin Strategy & Research, 2012*

**RETAIL POINT OF SALE FORECAST 2012-2017: Cash is No Longer King; Cards and Mobile Payments Likely to Rise**  
*Javelin Strategy & Research, 2012*

***CUSTOMER-DRIVEN ARCHITECTURE™ 2012: A Blueprint for a Digital Financial Lifestyle That Leads to Greater Paper Suppression***

*Javelin Strategy & Research, 2012*

***2012 ANTIVIRUS AND BROWSER SECURITY REPORT: How to Profit by Engaging the Gen Y Consumer Today***

*Javelin Strategy & Research, 2012*

***2012 TABLET AND BANKING REPORT: Strategic Approach to a Mobile Game Changer***

*Javelin Strategy & Research, 2012*

***PREPAID CARDS AND PRODUCTS IN 2012: Enabling Financial Access for Underbanked and Gen Y Consumers***

*Javelin Strategy & Research, 2012*

***BILL-PAY INNOVATORS (PART 1): What Challengers Must Do To Reshape How Americans Pay Bills***

*Javelin Strategy & Research, 2012*

***BILL-PAY INNOVATORS (PART 2): Players to Watch — From Bill.com to Zumbox***

*Javelin Strategy & Research, 2012*

***The Gang of Four (and Possibly Five) - Apple, Google, Facebook and Amazon - and Paypal***

*Javelin Strategy & Research, 2012*

***COPING WITH REGULATION: The Necessity of Bank Fees***

*Javelin Strategy & Research, 2012*

***2012 IDENTITY FRAUD REPORT: Social Media and Mobile forming the new Fraud Frontier***

*Javelin Strategy & Research, 2012*

***Banking and Social Media, Easy to Say Hard to Do***

*Javelin Strategy & Research, 2011*

***Evolution in Consumer Payments Behavior***

*Javelin Strategy & Research, 2011*

***Mobile Banking, Smartphone and Tablet Forecast 2011-2016***

*Javelin Strategy & Research, 2011*

***10 Trends That Will Transform Banking, Payments, Mobility and Security in 2012***

*Javelin Strategy & Research, 2011*

**5th Annual Mobile Security Report**  
*Javelin Strategy & Research, 2011*

**Personal Finance Management 2011**  
*Javelin Strategy & Research, 2011*

**4th Annual Online Retail Payments Forecast 2011-2016**  
*Javelin Strategy & Research, 2011*

**7th Annual Banking Identity Safety Scorecard**  
*Javelin Strategy & Research, 2011*

**2011 Mobile Banking Financial Institution Scorecard**  
*Javelin Strategy & Research, 2011*

**2011 Online Account Opening**  
*Javelin Strategy & Research, 2011*

**2011 Online Retail Payments Scorecard**  
*Javelin Strategy & Research, 2011*

**2011 – 2012 Mobile Banking Vendor Scorecard**  
*Javelin Strategy & Research, 2011*

**7th Annual Authentication Report**  
*Javelin Strategy & Research, 2011*

**9th Annual Online Banking and Bill Pay Forecast**  
*Javelin Strategy & Research, 2011*

**Fifth Annual ID Protection Services Scorecard**  
*Javelin Strategy & Research, 2011*

**The Durbin Amendment**  
*Javelin Strategy & Research, 2011*

**How to Attract and Keep High-Value ‘Moneyhawks’**  
*Javelin Strategy & Research, 2011*

**Smartphone Banking Security**  
*Javelin Strategy & Research, 2011*

**Evolving Rewards Strategies**  
*Javelin Strategy & Research, 2011*

**Second Annual Antivirus, Browser, and Mobile Security Report**  
Javelin Strategy & Research, 2011

**Seventh Annual Card Issuers' Safety Scorecard**  
Javelin Strategy & Research, 2011

**Virtual Currency and Social Network Payments – The New Gold Rush**  
Javelin Strategy & Research, 2011

**Data Mining and Predictive Analytics for Financial Institutions**  
Javelin Strategy & Research, 2011

**2011 Mobile Remote Deposit Capture**  
Javelin Strategy & Research, 2011

**2011 Small Business Owners (SMBO) Identity Fraud Report**  
Javelin Strategy & Research, 2011

**2011 Prepaid Cards and Products**  
Javelin Strategy & Research, 2011

**2011 Contactless Near Field Communication (NFC) Mobile Payments**  
Javelin Strategy & Research, 2011

**Interactive Financial Alerts 2011**  
Javelin Strategy & Research, 2011

**2011 Mobile Marketing and Advertising**  
Javelin Strategy & Research, 2011

**Gen Y**  
Javelin Strategy & Research, 2011

**2011 Point-to-Point Encryption, Tokenization and Virtual Terminals**  
Javelin Strategy & Research, 2011

**Javelin Early Take on Tablets**  
Javelin Strategy & Research, 2011

**Payments Regulation and Consumer Expectations**  
Javelin Strategy & Research, 2011

***Envisioning an App Store Inside Online Banking***

*Javelin Strategy & Research, 2011*

***2011 Identity Fraud Survey Report***

*Javelin Strategy & Research, 2011*

***2011 Expedited Payments Overview and Forecast***

*Javelin Strategy & Research, 2011*

***Mobile Wallets***

*Javelin Strategy & Research, 2011*

***10 Trends That Will Transform Banking, Payments and Security in 2011***

*Javelin Strategy & Research, 2010*

***Keeping up with the Android***

*Javelin Strategy & Research, 2010*

***2010 Online Retail Payments Update and Forecast***

*Javelin Strategy & Research, 2010*

***2010 Personal Financial Management Competitive Analysis (Part 2)***

*Javelin Strategy & Research, 2010*

***2010 Banking Identity Safety Scorecard***

*Javelin Strategy & Research, 2010*

***E-Commerce Platform Review***

*Javelin Strategy & Research, 2010*

***2010 Authentication Report***

*Javelin Strategy & Research, 2010*

***Personal Finance Management (Part 1)***

*Javelin Strategy & Research, 2010*

***Person-to-Person Mobile Money Transfers***

*Javelin Strategy & Research, 2010*

***Online and Mobile Device Identification***

*Javelin Strategy & Research, 2010*

***Online Alternative Payments***

*Javelin Strategy & Research, 2010*

**2010 Online Banking and Bill Payment Forecast**

*Javelin Strategy & Research, 2010*

**2010 Mobile Banking and Smartphone Forecast**

*Javelin Strategy & Research, 2010*

**2010 Annual Identity Protection Services Scorecard**

*Javelin Strategy & Research, 2010*

**Payment Card Issuer Strategies 2010**

*Javelin Strategy & Research, 2010*

**2010 Mobile Banking Scorecard**

*Javelin Strategy & Research, 2010*

**Financial Regulatory Reform 2010**

*Javelin Strategy & Research, 2010*

**Reg E and Overdrafts**

*Javelin Strategy & Research, 2010*

**Strategic Guide to Same-Day ACH**

*Javelin Strategy & Research, 2010*

**Antivirus and Browser Security Vendors 2010**

*Javelin Strategy & Research, 2010*

**2010 New Account Onboarding**

*Javelin Strategy & Research, 2010*

**2010 Mobile Banking Vendor Analysis**

*Javelin Strategy & Research, 2010*

**Durbin Interchange Amendment**

*Javelin Strategy & Research, 2010*

**2010 Mobile Banking Behaviors**

*Javelin Strategy & Research, 2010*

**2010 Data Breach Prevention and Response**

*Javelin Strategy & Research, 2010*

**2010 Online Account Opening Consumer Analysis and Vendor Ranking**

*Javelin Strategy & Research, 2010*

**2010 Mobile Payments — Crossing the Chasm**

*Javelin Strategy & Research, 2010*

**Sixth Annual Card Issuer's Safety Scorecard**

*Javelin Strategy & Research, 2010*

**Engaging the Underbanked and Unbanked in the U.S.**

*Javelin Strategy & Research, 2010*

**Mobile Remote Deposit Capture**

*Javelin Strategy & Research, 2010*

**ATM and PIN Fraud**

*Javelin Strategy & Research, 2010*

**2010 Prepaid and Gift Card Market**

*Javelin Strategy & Research, 2010*

**Social Media and Banking**

*Javelin Strategy & Research, 2010*

**2010 Mobile Marketing and Advertising**

*Javelin Strategy & Research, 2010*

**Financial Alerts 2010**

*Javelin Strategy & Research, 2010*

**Online Retail Payments Forecast**

*Javelin Strategy & Research, 2010*

**2010 Identity Fraud Survey**

*Javelin Strategy & Research, 2010*

**End- to- End Encryption Tokenization EMV**

*Javelin Strategy & Research, 2010*

**Green Billing 2010**

*Javelin Strategy & Research, 2010*

**10 Trends 2010**

*Javelin Strategy & Research, 2010*

**Multi Channel A2A and P2P Forecast**

*Javelin Strategy & Research, 2009*

**Web Application Security OWASP**

*Javelin Strategy & Research, 2009*

**US Online Channel Security**

*Javelin Strategy & Research, 2009*

**2009 Banking Identity Safety Scorecard**

*Javelin Strategy & Research, 2009*

**2009 Financial Alerts Forecast**

*Javelin Strategy & Research, 2009*

**Data Breach Notifications**

*Javelin Strategy & Research, 2009*

**2009 Javelin Mobile-Banking Scorecard**

*Javelin Strategy & Research, 2009*

**2009 Expedited Payments Forecast**

*Javelin Strategy & Research, 2009*

**Multi-Channel Authentication Via Mobile Banking**

*Javelin Strategy & Research, 2009*

**Personal Finance Management Tools**

*Javelin Strategy & Research, 2009*

**Contactless Mobile Payments Ecosystem**

*Javelin Strategy & Research, 2009*

**2009 Mobile-Banking and Smartphone Forecast**

*Javelin Strategy & Research, 2009*

**UnderBanked Business Banking Segmentation**

*Javelin Strategy & Research, 2009*

**2009 Online Banking and Bill Payment Forecast**

*Javelin Strategy & Research, 2009*

**Mobile Person to Person Payments**

*Javelin Strategy & Research, 2009*

**Understanding Consumer Willingness to Fight Fraud**

*Javelin Strategy & Research, 2009*

**Fifth Annual Card Issuers' Identity Safety Scorecard**

*Javelin Strategy & Research, 2009*

**How PCI Compliant Companies Can Be Breached**

*Javelin Strategy & Research, 2009*

**Alternative Payments Vendor Success**

*Javelin Strategy & Research, 2009*

**Personal Finance Management Beyond PFM Lite**

*Javelin Strategy & Research, 2009*

**The Customer-Driven Architecture**

*Javelin Strategy & Research, 2009*

**Identity Protection Services Scorecard**

*Javelin Strategy & Research, 2009*

**OTS Unfair Credit Card Practices**

*Javelin Strategy & Research, 2009*

**Online Account Opening**

*Javelin Strategy & Research, 2009*

**The Importance of Consumer Trust on FI Profitability Final**

*Javelin Strategy & Research, 2009*

**Health Information Breach**

*Javelin Strategy & Research, 2009*

**Credit Card Spending Declines Brochure.pub**

*Javelin Strategy & Research, 2009*

**Profiling Severely Injured Fraud Victims**

*Javelin Strategy & Research, 2009*

**Gen Y Security**

*Javelin Strategy & Research, 2009*

**Gen Y Mobile Banking**

*Javelin Strategy & Research, 2009*

**Marketing to Gen Y**

*Javelin Strategy & Research, 2009*

**Gen Y Online Banking and Bill Pay**

*Javelin Strategy & Research, 2009*

**Gen Y Acquisition Strategies**

*Javelin Strategy & Research, 2009*

**Mobile Wallet Applications**

*Javelin Strategy & Research, 2009*

**Identity Fraud Survey Report**

*Javelin Strategy & Research, 2009*

**Prepaid Product Evolution**

*Javelin Strategy & Research, 2008*

**10 Trends That Will Shape Financial Services in 2009**

*Javelin Strategy & Research, 2008*

**2008 Mobile Banking Security Standards**

*Javelin Strategy & Research, 2008*

**2008 Banking Identity Safety Scorecard**

*Javelin Strategy & Research, 2008*

**2008 Online Banking and Bill Payment Forecast**

*Javelin Strategy & Research, 2008*

**Online Retail Payments Forecast**

*Javelin Strategy & Research, 2008*

**Online Storage Vaults**

*Javelin Strategy & Research, 2008*

**Data Breaches**

*Javelin Strategy & Research, 2008*

**Mobile-Banking Consumer Behaviors**

*Javelin Strategy & Research, 2008*

**2008 Financial Alerts Forecast**

*Javelin Strategy & Research, 2008*

**2008 Expedited Payments Forecast**

*Javelin Strategy & Research, 2008*

**High Gasoline Prices and Inflation**

*Javelin Strategy & Research, 2008*

**Mobile Banking Vendor Analysis**

*Javelin Strategy & Research, 2008*

**Consumer Authentication for Retail Banking**

*Javelin Strategy & Research, 2008*

**Credit Card Issuer Profitability in a Difficult Economy**

*Javelin Strategy & Research, 2008*

**Credit Card Customer Satisfaction**

*Javelin Strategy & Research,*

**Mobile Marketing — Targeted, Timely, and Two-way**

*Javelin Strategy & Research, 2008*

**The Four E's of Green Banking**

*Javelin Strategy & Research, 2008*

**2008 US Mobile Banking Benchmark Study**

*Javelin Strategy & Research, 2008*

**2008 Identity Fraud Forecast**

*Javelin Strategy & Research, 2008*

**Contactless Strategy and Forecast**

*Javelin Strategy & Research, 2008*

**2008 Card Issuers' Identity Safety Scorecard**

*Javelin Strategy & Research, 2008*

**Mobile Person-to-Person Payments and Transfers**

*Javelin Strategy & Research, 2008*

**Online Banking Behavior Segmentation**

*Javelin Strategy & Research, 2008*

**2008 Identity Fraud Survey Report**

*Javelin Strategy & Research, 2008*

**2008 ID Survey Report Excerpts for Card Issuers**

*Javelin Strategy & Research, 2008*

**Mobile Channel Usage Forecast**

*Javelin Strategy & Research, 2008*

**Credit Card Acquisition and Account Management**

*Javelin Strategy & Research, 2008*

**Identity Fraud Protection Services**

*Javelin Strategy & Research, 2007*

**Generation Y Payments Behaviors and Attitudes**

*Javelin Strategy & Research, 2007*

**Person-to-Person Lending**

*Javelin Strategy & Research, 2007*

**The Future of Federated Identity**

*Javelin Strategy & Research, 2007*

**Online Payments Forecast**

*Javelin Strategy & Research, 2007*

**Online Account Opening Adoption Forecast**

*Javelin Strategy & Research, 2007*

**Securing the Enterprise**

*Javelin Strategy & Research, 2007*

**Generation Y Banking Behaviors and Attitudes**

*Javelin Strategy & Research, 2007*

**Financial Institution Blogs**

*Javelin Strategy & Research, 2007*

**2007 Card Issuer Identity Safety Scorecard**  
*Javelin Strategy & Research, 2007*

**2007 Online Banking and Bill Payment**  
*Javelin Strategy & Research, 2007*

**Mobile Payments Forecast**  
*Javelin Strategy & Research, 2007*

**Online Banking Personal Financial Management**  
*Javelin Strategy & Research, 2007*

**Payments Interchange**  
*Javelin Strategy & Research, 2007*

**Mobile Banking Security**  
*Javelin Strategy & Research, 2007*

**Mobile Banking – Getting It Right This Time**  
*Javelin Strategy & Research, 2007*

**Data Breaches & Buyer Behavior**  
*Javelin Strategy & Research, 2007*

**New Account Onboarding Communication**  
*Javelin Strategy & Research, 2007*

**Telephone Banking Authentication**  
*Javelin Strategy & Research, 2007*

**Expedited Bill Payments Forecast**  
*Javelin Strategy & Research, 2007*

**Email Marketing & Online Communication**  
*Javelin Strategy & Research, 2007*

**ATM Functionality Enhancements**  
*Javelin Strategy & Research, 2007*

**'07 ID Fraud Survey Report**  
*Javelin Strategy & Research, 2007*

**Authentication for Online Brokerages**  
*Javelin Strategy & Research, 2006*

**Consumer Info & Financial Safety Products**

*Javelin Strategy & Research, 2006*

**Debit Rewards Programs**

*Javelin Strategy & Research, 2006*

**Contactless Technology**

*Javelin Strategy & Research, 2006*

**Reaching Underbanked Latinos**

*Javelin Strategy & Research, 2006*

**Interactive Financial Messaging**

*Javelin Strategy & Research, 2006*

**Mitigating New Account Fraud**

*Javelin Strategy & Research, 2006*

**Beyond FFIEC Compliance**

*Javelin Strategy & Research, 2006*

**Health Savings Accounts**

*Javelin Strategy & Research, 2006*

**'06 Banking Safety Scorecard**

*Javelin Strategy & Research, 2006*

**Credit Monitoring Services**

*Javelin Strategy & Research, 2006*

**Data Breaches & Identity Fraud**

*Javelin Strategy & Research, 2006*

**Debit Versus Credit**

*Javelin Strategy & Research, 2006*

**Consumer Security Preferences**

*Javelin Strategy & Research, 2006*

**Securing Consumer PCs**

*Javelin Strategy & Research, 2006*

**Online Bill Viewing and Payment**  
Javelin Strategy & Research, 2006

**Consumer Adoption of Alerts Doubles**  
Javelin Strategy & Research, 2006

**Online Loan Application**  
Javelin Strategy & Research, 2006

**President Bush ID Fraud Report**  
Javelin Strategy & Research, 2006

**Consumer Credit Card Preferences**  
Javelin Strategy & Research, 2006

**'06 Issuer Safety Scorecard**  
Javelin Strategy & Research, 2006

**The Demographics of ID Fraud**  
Javelin Strategy & Research, 2006

**Merchant Contactless Report**  
Javelin Strategy & Research, 2006

**The New Data Security Paradigm**  
Javelin Strategy & Research, 2006

**Alternative Payments Online**  
Javelin Strategy & Research, 2006

**'06 ID Fraud Survey Report**  
Javelin Strategy & Research, 2006

**Electronic Bill Presentment**  
Javelin Strategy & Research, 2006

**'05 Online Banking Safety Scorecard**  
Javelin Strategy & Research, 2006

**Security Services**  
Javelin Strategy & Research, 2005

**Strong Authentication**  
Javelin Strategy & Research, 2005

**Fighting New Account Fraud**

*Javelin Strategy & Research, 2005*

**Bill and Statement Delivery**

*Javelin Strategy & Research, 2005*

**Online Account Security**

*Javelin Strategy & Research, 2005*

**Online Banking in the Face of Fraud**

*Javelin Strategy & Research, 2005*

**Online Banker Demographics**

*Javelin Strategy & Research, 2005*

**Phishing: Awareness & Behavior**

*Javelin Strategy & Research, 2005*

**'05 Issuer Safety Scorecard**

*Javelin Strategy & Research, 2005*

**e-Bill Payment Timing**

*Javelin Strategy & Research, 2005*

**Credit Monitoring & ID Fraud Insurance**

*Javelin Strategy & Research, 2005*

**'05 ID Fraud Survey Report**

*Javelin Strategy & Research, 2005*

**Bill Payment and Presentment**

*Javelin Strategy & Research, 2004*

**'04 ID Fraud Safety Scorecard**

*Javelin Strategy & Research, 2004*

**Alerts**

*Javelin Strategy & Research, 2004*

**Check Electronification**

*Javelin Strategy & Research, 2004*

**'03-'04 Finance Household Update**  
*Javelin Strategy & Research, 2004*

**Least Cost Routing**  
*Javelin Strategy & Research, 2004*

**Online Account Management**  
*Javelin Strategy & Research, 2004*

# Exhibit B

**REPORT OF RICK KAM, CIPP/US**

**IN THE MATTER OF LABMD**

**FTC COMPLAINT #1023099, DOCKET #9357**

**MARCH 18, 2014**

## Table of Contents

<b>TABLE OF CONTENTS</b> .....	<b>2</b>
<b>EXECUTIVE SUMMARY</b> .....	<b>3</b>
<b>INTRODUCTION</b> .....	<b>3</b>
<b>II. SUMMARY OF THE FTC’S REQUEST FOR EXPERT OPINION</b> .....	<b>5</b>
<b>III. SUMMARY OF CONCLUSIONS</b> .....	<b>8</b>
<b>IV. IDENTITY CRIME: AN OVERVIEW</b> .....	<b>10</b>
<b>V. IMPACT OF IDENTITY CRIMES ON VICTIMS</b> .....	<b>13</b>
<b>VI. ANALYSIS OF RISK OF HARM FROM LABMD’S FAILURE TO PROTECT CONSUMER DATA</b> .....	<b>17</b>
<b>APPENDIX A: CV</b> .....	<b>25</b>
<b>APPENDIX B: LITERATURE REVIEW</b> .....	<b>33</b>
<b>APPENDIX C: STATE BREACH NOTIFICATION LAWS IN EFFECT BEFORE MAY 2008</b> .....	<b>37</b>
<b>APPENDIX D: LIST OF CPT CODES</b> .....	<b>39</b>

## 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<sup>1</sup> 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.

---

<sup>1</sup>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 (insuranceaging\_6.05.071.pdf):** 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:
  - o First and last names, and middle initials
  - o Dates of birth
  - o Nine-digit Social Security numbers (SSNs)
  - o Health insurance provider numbers, names, addresses, and phone numbers
  - o Current Procedural Terminology (CPT) Codes: Uniform set of codes defined by the American Medical Association to describe medical, surgical, and diagnostic services.
  - o 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 this file was found on peer-to-peer networks. He indicated that at four of the IP addresses on which Tiversa found the 1,718-page P2P Insurance Aging file, Tiversa also found unrelated sensitive consumer information that could be used to commit identity theft, including passwords, tax returns, account numbers, and Social Security numbers.
- 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 prostate cancer, herpes, hepatitis, HIV, and testosterone levels.

## 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.<sup>2</sup>

## 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

---

<sup>2</sup> *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.<sup>3</sup>

### **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.<sup>4</sup> 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).

---

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

<sup>4</sup> 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](http://www.utica.edu/academic/institutes/ecii/publications/media/cimip_id_theft_study_oct_22_noon.pdf).

<b>Table 1: Motivating Factors for Committing Identity Theft or Fraud</b>		
<b>Motive</b>	<b>Number</b>	<b>Percentage</b>
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.<sup>5</sup> Tax identity theft typically prevents victims from being able to successfully file their tax returns and obtain refunds.<sup>6</sup> The delay can extend, in some cases, as long as six months.<sup>7</sup> 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.

---

<sup>5</sup> "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>.

<sup>6</sup> "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>.

<sup>7</sup> 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.<sup>8</sup> 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.<sup>9</sup>

## 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."<sup>10</sup>

Another problem is health insurance. The Ponemon survey found that 39 percent of medical identity theft victims lost their healthcare coverage.<sup>11</sup> 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.<sup>12</sup> 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.

---

<sup>8</sup> Ponemon Institute 2013 Survey on Medical Identity Theft, p. 5.

<sup>9</sup> Ponemon Institute 2013 Survey on Medical Identity Theft, p. 5.

<sup>10</sup> Ponemon 2013 Survey on Medical Identity Theft, p. 12.

<sup>11</sup> Ponemon 2013 Survey on Medical Identity Theft, p. 10.

<sup>12</sup> The Facts about the Medical Information Bureau (MIB). From [http://www.mib.com/facts\\_about\\_mib.html](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,<sup>13</sup> Table 2 below illustrates the health risks to victims of medical identity theft:

<b>Table 2. Other Harms from Medical Identity Theft</b>	<b>Ponemon Percentage of Medical Identity Victims</b>
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.<sup>14</sup>

---

<sup>13</sup> Ponemon 2013 Survey on Medical Identity Theft, p. 8.

<sup>14</sup> “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.<sup>15</sup>

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:

---

<sup>15</sup> 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. Approximately 9,300 consumers' sensitive data was found in a LabMD document available on a P2P network on February 5, 2008, in clear text, 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 the P2P Insurance Aging file was found at four IP address along with unrelated sensitive consumer information that could be used to commit identity theft. Boback also testified sensitive consumer information in the P2P file could be available to anyone who had access to the peer-to-peer network. He also stated that law enforcement had apprehended someone suspected of identity theft or fraud using one of the IP addresses.

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, the P2P Insurance Aging file was first found on the peer-to-peer network on February 5, 2008, at IP address 68.107.85.250. It was found again on November 5, 2008, at IP address 173.16.83.112; again on April 7, 2011, at IP address 201.194.118.82; and yet again on June 9th in 2011, at IP address 90.215.200.56. Boback also said Tiversa searched for the file in preparation for his testimony on November 21, 2013, and still found the file available on the P2P network. 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.<sup>16</sup> 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.<sup>17</sup>

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.

---

<sup>16</sup> Ponemon 2013 Survey on Medical Identity Theft, p. 2.

<sup>17</sup> 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.<sup>18</sup>

**Table 3. Projected Number of Victims Suffering “Other Harms” from Medical Identity Theft**

<b>“Other Harms” from Medical Identity Theft</b>	<b>Ponemon % of Medical Identity Victims</b>	<b>Projected Number of Victims**</b>
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.”*

---

<sup>18</sup> 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. Several of the CPT codes indicate tests for the presence of prostate cancer, testosterone levels, or STDs—specifically HIV, hepatitis, and herpes.

- There were 3,195 instances of CPT code 84153; 548 instances of CPT code 84154; and 109 instances of CPT code G0103. These CPT codes describe tests for “prostate specific antigen”—an indication of possible prostate cancer. More than 3,000 consumers had these CPT codes linked to their name.
- There were 134 instances of CPT code 84402 and 435 instances of CPT code 84403, which test for testosterone levels. Testosterone results can be used to evaluate men for testicular dysfunction. In men, low levels of testosterone may cause reduced fertility or lack of libido. More than 400 consumers had these CPT codes linked to their name.
- Nineteen (19) consumers had one or more of the following CPT codes, indicating tests for herpes: 86694, 86695, and 86696.
- Six consumers (6) had one or more of these CPT codes, indicating tests for hepatitis B or C: 86705 and/or 86706.
- There were 13 instances of CPT code 86689, which indicates a test for HIV.

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 that she could not confirm that the identity thieves used this data to commit identity fraud, the fact that known identity thieves acquired this information increases the possibility that the crime occurred. 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 LabMD notified the consumers listed on the Day Sheets on March 27, 2013. 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.<sup>19</sup>

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

---

<sup>19</sup> “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, approximately 12 percent of the consumers notified enrolled in credit monitoring. 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.<sup>20</sup>

---

<sup>20</sup> 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

A handwritten signature in black ink, appearing to be 'RM', written in a cursive style.

---

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](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](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	<a href="https://www.javelinstrategy.com/brochure/314">https://www.javelinstrategy.com/brochure/314</a>	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	<a href="http://norse-corp.com/HealthcareReport2014.html">http://norse-corp.com/HealthcareReport2014.html</a>	Barbara Filkins, sponsored by Norse	Discusses the vulnerabilities of the healthcare industry to cyberthreats.
Dec. 2013	Identity Theft and Your Social Security Number	<a href="http://www.socialsecurity.gov/pubs/EN-05-10064.pdf">http://www.socialsecurity.gov/pubs/EN-05-10064.pdf</a>	Social Security Administration	Consumer tips on protecting against SSN-related identity theft.

Dec. 2013	Victims of Identity Theft, 2012	<a href="http://www.bjs.gov/content/pub/pdf/vit12.pdf">http://www.bjs.gov/content/pub/pdf/vit12.pdf</a>	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	<a href="http://www.treasury.gov/tigta/press/press_tigta-2013-40.htm">http://www.treasury.gov/tigta/press/press_tigta-2013-40.htm</a>	Treasury Inspector General for Tax Administration	Press release
Oct. 2013	First Aid for Medical Identity Theft: Tips for Consumers	<a href="https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis_16_med_id_theft.pdf">https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis_16_med_id_theft.pdf</a>	Calif. Dept. of Justice	Consumer information on medical identity theft.
Oct. 2013	Medical Identity Theft: Recommendations for the Age of Electronic Medical Records	<a href="https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/medical_id_theft_recommend.pdf">https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/medical_id_theft_recommend.pdf</a>	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	<a href="http://www.treasury.gov/tigta/auditreports/2013reports/201340122fr.html">http://www.treasury.gov/tigta/auditreports/2013reports/201340122fr.html</a>	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	<a href="http://medidfraud.org/2013-survey-on-medical-identity-theft/">http://medidfraud.org/2013-survey-on-medical-identity-theft/</a>	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	<a href="http://www.verizonenterprise.com/DBIR/2013/">http://www.verizonenterprise.com/DBIR/2013/</a>	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	<a href="http://www.irs.gov/uac/Newsroom/Tips-for-Taxpayers-Victims-about-Identity-Theft-and-Tax&gt;Returns">http://www.irs.gov/uac/Newsroom/Tips-for-Taxpayers-Victims-about-Identity-Theft-and-Tax&gt;Returns</a>	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	<a href="https://www.javelinstrategy.com/brochure/276">https://www.javelinstrategy.com/brochure/276</a>	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	<a href="http://www.emc.com/collateral/white-papers/h12105-cybercrime-healthcare-industry-rsa-wp.pdf">http://www.emc.com/collateral/white-papers/h12105-cybercrime-healthcare-industry-rsa-wp.pdf</a>	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	<a href="https://www.himss.org/files/HIMSSorg/content/files/CreatingATrustedEnvironmentReducingtheThreatofMedicalIdentifyTheftFINA.pdf">https://www.himss.org/files/HIMSSorg/content/files/CreatingATrustedEnvironmentReducingtheThreatofMedicalIdentifyTheftFINA.pdf</a>	HIMSS Privacy and Security Task Force, Kroll-sponsored	Evaluates risk and mitigation strategies for protecting PHI.
March 2012	The Financial Impact of Breached PHI	<a href="http://webstore.ansi.org/phi/">http://webstore.ansi.org/phi/</a>	Workgroups	ANSI whitepaper on the financial impact of breached protected health information.
Oct. 2009	IDSP Workshop Report: Measuring Identity Theft	<a href="http://webstore.ansi.org/identitytheft/#Measuring">http://webstore.ansi.org/identitytheft/#Measuring</a>	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	<a href="http://www.healthit.gov/sites/default/files/medidtheftreport011509_0.pdf">http://www.healthit.gov/sites/default/files/medidtheftreport011509_0.pdf</a>	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	<a href="http://blogs.wsj.com/health/2008/11/07/express-scripts-data-breach-leads-to-extortion-attempt/">http://blogs.wsj.com/health/2008/11/07/express-scripts-data-breach-leads-to-extortion-attempt/</a>	Sarah Rubenstein, Wall Street Journal Health Blog	Article describing two extortion attempts involving patient information.

Oct. 2008	Medical Identity Theft Environmental Scan	<a href="http://www.healthit.gov/sites/default/files/hhs_onc_medid_theft_envscan_101008_final_cover_note_0.pdf">http://www.healthit.gov/sites/default/files/hhs_onc_medid_theft_envscan_101008_final_cover_note_0.pdf</a>	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	<a href="http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf">http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf</a>	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	<a href="http://www.utica.edu/academic/institutes/ecii/publications/media/cimip_id_theft_study_oct_22_noon.pdf">http://www.utica.edu/academic/institutes/ecii/publications/media/cimip_id_theft_study_oct_22_noon.pdf</a>	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	<a href="http://www.worldprivacyforum.org/2006/05/report-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/</a>	Pam Dixon	Report on impact of medical identity theft including cases.
July 2005	Identity Theft Literature Review	<a href="https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf">https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf</a>	Newman and McNally	Identity theft literature review funded by the Department of Justice.
Ongoing	The Facts about MIB	<a href="http://www.mib.com/facts_about_mib.html">http://www.mib.com/facts_about_mib.html</a>	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

CPT	Description of CPT	Instances in 1,718 File	Coding Notes
36415	Collection of Venous blood by venipuncture	372	Routine blood draw
80048	Basic Metabolic Panel	262	A basic metabolic panel with total calcium includes the following tests: total calcium (82310), carbon dioxide (82374), chloride (82435), creatinine (82565), glucose (82947), potassium (84132), sodium (84295), and urea nitrogen (BUN) (84520). The blood specimen is obtained by venipuncture. See the specific codes for additional information about the listed tests.
80053	Comprehensive Metabolic Panel	278	A comprehensive metabolic panel includes the following tests: albumin (82040), total bilirubin (82247), total calcium (82310), carbon dioxide (bicarbonate) (82374), chloride (82435), creatinine (82565), glucose (82947), alkaline phosphatase (84075), potassium (84132), total protein (84155), sodium (84295), alanine amino transferase (ALT) (SGPT) (84460), aspartate amino transferase (AST) (SGOT) (84450), and urea nitrogen (BUN) (84520). Blood specimen is obtained by venipuncture. See the specific codes for additional information about the listed tests
80061	Lipid Panel	87	Lipid panel This panel must include the following: Cholesterol, serum, total (82465) Lipoprotein, direct measurement, high density cholesterol (HDL cholesterol) (83718) Triglycerides (84478)
80069	Renal Function	61	A renal function panel includes the following tests: albumin (82040), total calcium (82310), carbon dioxide (bicarbonate) (82374), chloride (82435), creatinine (82565), glucose (82947), inorganic phosphorus (phosphate) (84100), potassium (84132), sodium (84295), and urea nitrogen (BUN) (84520).
80076	Hepatic function panel	61	A hepatic function panel includes the following tests: albumin (82040), total bilirubin (82247), direct bilirubin (82248), alkaline phosphatase (84075), protein, total (84155), alanine amino transferase (ALT) (SGPT) (84460), and aspartate amino transferase (AST) (SGOT) (84450). Blood specimen is obtained by venipuncture. See the specific codes for additional information about the listed tests.
82105	Alpha-fetoprotein (AFP); serum	28	This test may be abbreviated as AFP. It may also be referred to as fetal alpha globulin. While this test is most often associated with pregnancy, it is also used to diagnose a variety of other conditions. During pregnancy, the test is normally performed between the 16th and 18th week of gestation. If levels are abnormal, it may be repeated approximately one week after the first test. Analysis is normally performed by radioimmunoassay (RIA).
82140	Ammonia	43	This test may be requested as NH <sub>3</sub> . Elevated levels may indicate that the liver is not able to detoxify ammonia from the blood due to severe liver disease. A number of methods are used including enzymatic, resin enzymatic, and ion-selective electrode (ISE).
82310	Calcium, total	48	This test may be abbreviated Ca. Blood is obtained by venipuncture or heel stick. Specimen is obtained in the morning and a fasting sample is preferable. Postural changes and venous stasis may provide misleading results. Accurate diagnosis may require obtaining additional specimens on subsequent days. Method is spectrophotometry or atomic absorption spectroscopy (AAS). The test may be used to assess thyroid and parathyroid function
82330	Calcium; ionized	2	This test may also be referred to as free calcium. It may be abbreviated iCa, Ca <sup>++</sup> or Ca <sup>+2</sup> . Ionized or free calcium refers to calcium that is not bound to proteins in the blood. It is the metabolically active portion of the calcium in the blood. Blood is obtained by venipuncture and collected anaerobically. Method is by ion-selective electrode (ISE). The test may be used to assess thyroid and parathyroid function.
82340	Calcium, urine quantitative, time specimen	69	This test may be abbreviated Ca urine, Ca <sup>++</sup> or Ca <sup>+2</sup> . A 24-hour urine specimen is generally required. The patient flushes the first urine of the day and discards it. All voided urine for the next 24 hours is collected and refrigerated. Method is spectrophotometry or atomic absorption spectrometry (AAS).
82347	Carbon dioxide (bicarbonate)	3	This test may be requested as CO <sub>2</sub> , HCO <sub>3</sub> , or bicarbonate. Bicarbonate (carbon dioxide) is an indicator of electrolyte and acid-base status (alkalosis, acidosis). It is elevated in metabolic alkalosis, compensated respiratory acidosis, and hypokalemia. It is decreased in metabolic acidosis, compensated respiratory alkalosis, and in diabetic ketoacidosis. Blood specimen is normally obtained by arterial puncture, but venipuncture may also be used. Bicarbonate is usually calculated using the Henderson-Hasselbalch equation (HCO <sub>3</sub> = Total CO <sub>2</sub> - H <sub>2</sub> CO <sub>3</sub> ). However, it can also be determined by titration.

82369	Calculus, infrared spectroscopy	170	This test may be requested as $\text{CO}_2$ , $\text{HCO}_3$ , or bicarbonate. Bicarbonate (carbon dioxide) is an indicator of electrolyte and acid-base status (alkalosis, acidosis). It is elevated in metabolic alkalosis, compensated respiratory acidosis, and hypokalemia. It is decreased in metabolic acidosis, compensated respiratory alkalosis, and in diabetic ketoacidosis. Blood specimen is normally obtained by arterial puncture, but venipuncture may also be used. Bicarbonate is usually calculated using the Henderson-Hasselbalch equation ( $\text{HCO}_3 = \text{Total } \text{CO}_2 - \text{H}_2\text{CO}_3$ ). However, it can also be determined by titration.
82378	Carcinoembryonic antigen	4	This test may be abbreviated as CEA. While CEA occurs normally in the gastrointestinal tract, it may be elevated for certain benign and malignant neoplasms and other diseases. CEA is used primarily to monitor patients with colorectal cancer and to a lesser extent advanced breast cancer. Method is immunofluorescence, enzyme immunoassay (EIA), and radioimmunoassay (RIA).
82384	Catecholamines fractionated	1	Catecholamines are biogenic amines that include epinephrine, norepinephrine, and dopamine. This test is used to diagnose hypertension caused by increased levels of catecholamines secreted by specific types of tumors. Preferred method is high performance liquid chromatography (HPLC), but radioimmunoassay (RIA) or radiochemical assay may also be used. Code 82384 reports fractionated catecholamines and quantifies total epinephrine, norepinephrine, and dopamine separately. Most assays measure only free catecholamines, but some measure both free and conjugated types.
82435	Chloride; blood	1	This test may be requested as Cl, blood. Chloride is a salt of hydrochloric acid and is important in maintaining electrolyte balance. Methods include colorimetry, coulometry, and ion-selective electrode (ISE).
82436	Chloride; urine	74	This test may be requested as Cl, urine. Chloride is important in maintaining proper electrolyte balance. A 24-hour urine test is preferred, but shorter timed collections and random specimens may also be used. If a timed specimen is used, the patient flushes the first urine of the day and discards it. All voided urine for the next 24 hours (or shorter time increment) is collected and refrigerated. Methods include colorimetry, coulometry, and ion-selective electrode (ISE).
82465	Cholesterol, serum or whole blood, total	6	Cholesterol level is a risk indicator for atherosclerosis and myocardial infarction. Blood specimen is obtained by venipuncture. Method is enzymatic. This test reports total cholesterol in serum or whole blood.
82507	Citrate	65	Citrate determinations in urine are useful in evaluating nephrolithiasis. A 24-hour urine specimen is required. The patient flushes the first urine of the day and discards it. All voided urine for the next 24 hours is collected and refrigerated. Citrate may be measured using enzymatic/spectrophotometric methods or chromatography.
82565	Creatinine; blood	219	Serum creatinine is the most common laboratory test for evaluating renal function. Method is enzymatic or colorimetry.
82570	Creatinine; other source	69	Urine creatinine levels are not normally used to evaluate disease processes except as part of a creatinine clearance test, but they are a good indicator of the adequacy of timed urine specimens. Amniotic fluid creatinine is used to evaluate fetal maturity. For amniotic fluid specimen, a separately reportable amniocentesis is performed. Method is enzymatic, Jaffe reaction, or manual.
82607	Cyanocobalamin	4	This test may be requested as antipernicious anemia factor, true cyanocobalamin, or Vitamin B12. It is essential for red blood cell maturation and for gastrointestinal and neurologic health. Decreased levels may be indicative of certain anemias. Method is chemiluminescence, competitive protein binding (CPB) radioassay, or radioimmunoassay (RIA).
82615	Cystine and homocystine. Irome. Qualitative	26	Cystine and homocystine are amino acids indicative of disease when found in the urine. Method is ion exchange chromatography or spectrophotometry
82627	Dehydroepiandrosterone-sulfate (DHEA-S)	9	This test may be requested as DHEA-S or DHEAS. Serum DHEA-S levels may be used to evaluate hirsutism. Elevations may be indicative of ovarian or adrenal disorders, neoplasm of the adrenal cortex, Cushing's disease, or ectopic ACTH-producing neoplasm. Decreased levels in amniotic fluid may be indicative of anencephaly. For amniotic fluid specimen, an amniocentesis is performed. Method is typically radioimmunoassay (RIA).

82670	Estradiol	13	This test may be requested as unconjugated estradiol (E2). Estradiol is derived from ovaries, testes, and the placenta and is the most active endogenous estrogen. Method is radioimmunoassay (RIA).
82672	Estrogens; total	3	This test may be requested as total estrogen in serum or urine. Because the serum assay does not measure estriol levels, urine assay is perhaps more commonly ordered. Estrogens are the female sex hormones and include estradiol, estrone, and estriol. Method is spectroscopy or fluorometry
82746	Folic acid; serum	4	This test may be requested as serum folate. This test is used to detect folic acid deficiency. Folic acid is a B vitamin necessary for normal red blood cell production. It is stored in the body as folates. Folic acid deficiency results in a form of megaloblastic anemia. Method is competitive binding protein (CPB) radioimmunoassay, chemiluminescence, or microbiological assay.
82947	Glucose; quantatie, blood	4	This test may be requested as a fasting blood sugar (FBS). This quantitative test is used to evaluate disorders of carbohydrate metabolism. The patient has ordinarily fasted for eight hours. Method is enzymatic.
83001	Gonadotropin; follicle stimulating hormone	73	This test may be requested as FSH or follitropin. FSH is a gonadotropic hormone produced by the pituitary gland. It stimulates growth and maturation of the ovarian follicle in females and promotes spermatogenesis in males. This test may be requested in an infertility work-up. Method is immunoassay.
83002	Gonadotropin; luteinizing hormone (LH)	63	This test may be requested as LH, lutropin, or interstitial cell-stimulating hormone (ICSH). LH is a gonadotropic hormone secreted by the pituitary gland. LH required for ovulation in females and stimulates testosterone production in males. LH may be ordered as part of an infertility work-up. Method is immunoassay.
83036	Glycosylated (A1C)	32	These tests may also be known as HbA1C. A blood specimen is collected. Glycosylated hemoglobin levels reflect the average level of glucose in the blood over a three-month period. Methods may include high-performance liquid chromatography and ion exchange chromatography (83036) or FDA approved home monitoring device (83037).
83519	Immunoassay for analyte other than infectious agent antibody or infectious agent antigen; quantitative, by radioimmunoassay (eg, RIA)	42	Immunoassay uses highly specific antigen to antibody binding to identify specific chemical substances. This code reports measurement (quantitative analysis) using radioimmunoassay (RIA) technique for identifying analytes (chemical substances) that are not specifically identified elsewhere, excluding infectious agent antibody or infectious agent antigen.
83540	Iron	1	This test may be requested as Fe. Iron is an essential constituent of hemoglobin, which is present in foods and absorbed through the small bowel (duodenum and jejunum). Method is colorimetry or atomic absorption spectrophotometry. This test is often used in combination with other tests to evaluate anemia, acute leukemia, lead poisoning, acute hepatitis, and vitamin B6 deficiency. It is also used to evaluate iron poisoning caused by accidental overdose (children) or excessive use of supplements.
83550	Iron binding capacity	1	This test may be abbreviated as TIBC. Iron is an essential constituent of hemoglobin, which is present in foods and absorbed through the small bowel (duodenum and jejunum). Method is colorimetry or atomic absorption spectrophotometry. TIBC measures the total amount of iron capable of binding to the protein transferrin. This test is often used in combination with other tests to evaluate anemia, various neoplasms, acute hepatitis and other liver disease, hemochromatosis, thalassemia, and renal disease.
83615	Lactate dehydrogenase	3	This test may also be ordered as LD or LDH. The test is a measure of LD or LDH, which is found in many body tissues, particularly the heart, liver, red blood cells, and kidneys. Methods used are lactate to pyruvate or pyruvate to lactate. This test may be ordered for a wide variety of disorders, including renal diseases and congestive heart failure.
83735	Magnesium	70	Magnesium, abbreviated Mg, is an inorganic cation essential for many physiochemical processes. It is an enzyme activator found in body fluids and cells. Magnesium depletion is clinically associated with weakness and neuromuscular disorders including cardiac arrhythmias and seizures. IV therapy, malabsorption, dialysis, pregnancy, toxicity and conditions such as hyperparathyroidism and hyperaldosteronism deplete magnesium. Specimen types and methods of testing vary. Colorimetry or spectrophotometry are methods frequently used.
83835	Metanephrines	1	The test is performed to determine metanephrine or normetanephrine concentrations. The specimen is urine collected over a 24-hour period. Method is high performance liquid chromatography (HPLC). Metanephrine or normetanephrine concentrations may be associated with neuroendocrine tumors or even associated with intense physical activity, life threatening illness and drug interferences.

83935	Osmolality; urine	23	The test is performed to determine metanephrine or normetanephrine concentrations. The specimen is urine collected over a 24-hour period. Method is high performance liquid chromatography (HPLC). Metanephrine or normetanephrine concentrations may be associated with neuroendocrine tumors or even associated with intense physical activity, life threatening illness and drug interferences.
83945	Oxalate	68	This test is also known as oxalic acid. Urine collection is over a 24-hour period, or a first morning. The specimen may be taken as an estimate of daily output. Methods of testing may include colorimetry and high performance liquid chromatography. The test may be performed to determine patients at risk of forming oxalate calculi (stones), which are common in the urinary tract.
83970	Parathormone (parathyroid hormone)	29	This test may also be ordered as a PTH or parathyrin. The specimen is post-fasting serum requiring special handling. Methods may include immunochemiluminometric assay (ICMA), radioimmunoassay (RIA), and immunoradiometric assay (IRMA). Testing determines the PTH levels and may be used to differentiate between primary or secondary causes of parathyroid disorders
83986	pH; body fluid, not otherwise specified	72	This test may also be called fecal pH, pleural fluid pH, or thoracentesis pH. The specimen for pleural fluid is by thoracentesis; for stool, fresh random sample; for urine, random sample; or ascitic fluid by paracentesis, etc. Methods may include a pH meter for pleural fluid; aqueous stool suspension with pH paper for stool; dipstick double indicator principal or pH meter for urine. The test may be ordered to differentiate among numerous diagnoses, depending on the sample taken and the method used.
84066	Phosphatase, acid; prostatic	5	This test may also be known as PAP and prostatic phosphatase. The specimen is post-fasting serum. Methods may include radioimmunoassay (RIA), enzyme monophosphate, alpha naphthylphosphate, and titrate inhibition. This test may be used to stage prostate cancer, to diagnose metastatic prostate adenocarcinoma and to monitor treatment of those diagnosed with prostatic carcinoma.
84100	Phosphorus inorganic ( phosphate)	5	This test may be ordered as PO4. Methods may include phosphomolybdate-colorimetric and modified molybdate-enzymatic, and colorimetric. The testing may be performed to measure high or low levels of phosphorus to determine a variety of differential diagnoses. Potassium supplements increase phosphate levels. Also, phosphate levels may increase during the last trimester of pregnancy.
84105	Phosphorus inorganic (phosphate); urine	72	This test is performed to identify the calcium/phosphorus balance. High values may be associated with primary hyperparathyroidism, vitamin D deficiency, and renal tubular acidosis; low values may be due to hypoparathyroidism, pseudohypoparathyroidism, and vitamin D toxicity. The test may also be used for nephrolithiasis assessment.
84132	Potassium; serum, plasma or whole blood	3	This test may be requested as K or K+. Potassium is the major electrolyte found in intracellular fluids. Potassium influences skeletal and cardiac muscle activity. Very small fluctuations outside the normal range may cause significant health risk, including muscle weakness and cardiac arrhythmias. Blood specimen is serum, plasma, or whole blood. Methods include atomic absorption spectrometry (AAS), ion-selective electrode (ISE), and flame emission spectroscopy (FES).
84133	Potassium; serum, plasma or whole blood; urine	73	This test may be ordered as urine K+. The specimen is collected by the patient over a 24-hour period or is random urine sample. Methods may include flame emission photometry and ion-selective electrode (ISE). The test may be ordered to determine elevated levels for the differential diagnoses of chronic renal failure, renal tubular acidosis, and for diuretic therapy.
84144	Progesterone	7	This test is performed to determine corpus luteum function, confirm ovulation, and to diagnose incompetent luteal phase and insufficient progesterone production, which may be the cause of habitual abortions. The specimen is serum. Methods may include radioimmunoassay (RIA) and direct time-resolved fluorescence immunoassay.
84146	Prolactin	83	Prolactin is a hormone secreted by the anterior pituitary gland. This test may be performed for the differential diagnoses of prolactinemia, galactorrhea (lactation disorder), pituitary adenomas, pituitary prolactinoma, and other pituitary tumors. The specimen is post-fasting serum. Methods may include immunoassay and radioimmunoassay (RIA).
84153	Prostate specific antigen (PSA); completed (direct measurement); total	3564	The specimen is serum. Methods may include radioimmunoassay (RIA) and monoclonal two-site immunoradiometric assay. These tests may be performed to determine the presence of cancer of the prostate, benign prostatic hypertrophy (BPH), prostatitis, post prostatectomy to detect residual cancer, and to monitor therapy. There are several forms of PSA present in serum. PSA may be complexed with the protease inhibitor alpha-1 antichymotrypsin (PSA-ACT). Complexed PSA is the most measurable form. PSA is also found in a free form. Free PSA is not complexed to a protease inhibitor. Higher levels of free PSA are more often associated with benign conditions of the prostate than with prostate cancer. Total PSA measures both complexed and free levels to provide a total amount present in the serum. A percentage of each form is sometimes calculated to distinguish benign from malignant conditions. Code 84152 reports complexed PSA; 84153 is for total serum PSA; 84154 is for free (not complexed) PSA.
84154	Prostate specific antigen (PSA); completed (direct measurement); free	584	The specimen is serum. Methods may include radioimmunoassay (RIA) and monoclonal two-site immunoradiometric assay. These tests may be performed to determine the presence of cancer of the prostate, benign prostatic hypertrophy (BPH), prostatitis, post prostatectomy to detect residual cancer, and to monitor therapy. There are several forms of PSA present in serum. PSA may be complexed with the protease inhibitor alpha-1 antichymotrypsin (PSA-ACT). Complexed PSA is the most measurable form. PSA is also found in a free form. Free PSA is not complexed to a protease inhibitor. Higher levels of free PSA are more often associated with benign conditions of the prostate than with prostate cancer. Total PSA measures both complexed and free levels to provide a total amount present in the serum. A percentage of each form is sometimes calculated to distinguish benign from malignant conditions. Code 84152 reports complexed PSA; 84153 is for total serum PSA; 84154 is for free (not complexed) PSA.
84260	Serotonin	1	This test may also be called 5-HT or 5-Hydroxytryptamine. The specimen is whole blood or serum or spinal fluid. A separately reportable lumbar puncture is performed to collect cerebrospinal fluid (CSF). Methods may include fluorometry, radioimmunoassay (RIA), and gas or liquid chromatography spinal puncture to obtain specimen is reported separately, see 62270. This test may be performed to diagnose carcinoid syndrome and severe depression.
84295	Sodium; serum, plasma or whole blood	8	Sodium is an electrolyte found in extracellular fluid. Blood specimen for serum, plasma, or whole blood sodium (Na) in 84295 is obtained by venipuncture. Methods include atomic absorption spectrometry (AAS), flame emission photometry, and ion-selective electrode (ISE). The specimen for urine Na in 84300 is collected over a 24-hour period or by random urine sample. Methods may include flame emission photometry and ISE. This test is used to identify increased (hypernatremia) and decreased (hyponatremia) levels of sodium due to various conditions or disease states. Report 84302 for a sodium level test done on another source of specimen other than blood serum or urine.

84300	Sodium; serum, plasma or whole blood; urine	71	Sodium is an electrolyte found in extracellular fluid. Blood specimen for serum, plasma, or whole blood sodium (Na) in 84295 is obtained by venipuncture. Methods include atomic absorption spectrometry (AAS), flame emission photometry, and ion-selective electrode (ISE). The specimen for urine Na in 84300 is collected over a 24-hour period or by random urine sample. Methods may include flame emission photometry and ISE. This test is used to identify increased (hypernatremia) and decreased (hyponatremia) levels of sodium due to various conditions or disease states. Report 84302 for a sodium level test done on another source of specimen other than blood serum or urine.
84382	Sulfate, urine	42	This test may be ordered to determine kidney stone risk and in the investigation of sulfur metabolism studies. Sulfates may be measured for the diagnosis of metachromatic leukodystrophy (sulfatide lipidosis), an inherited lipid metabolism that results in the accumulation of metachromatic lipids in the tissues of the central nervous system, leading to paralysis and often death in early adolescence. The specimen is a random or timed urine collection. Method is spectrophotometry.
84402	Testosterone; free	146	These tests may be used to evaluate testosterone levels. Testosterone is an androgenic hormone responsible for, among other biological activities, secondary male characteristics in women. Increased testosterone levels in women may be linked to a variety of conditions, including hirsutism. Code 84403 reports total testosterone, which includes both protein bound and free testosterone. Code 84402 reports testosterone as a free unbound protein. This test may be ordered to assist in diagnosis of hypogonadism, hypopituitarism, and Klinefelter's syndrome, among other disorders. The specimen is serum. Method may be by radioimmunoassay (RIA) and immunoassay (non-isotopic).
84403	Testosterone; total	486	These tests may be used to evaluate testosterone levels. Testosterone is an androgenic hormone responsible for, among other biological activities, secondary male characteristics in women. Increased testosterone levels in women may be linked to a variety of conditions, including hirsutism. Code 84403 reports total testosterone, which includes both protein bound and free testosterone. Code 84402 reports testosterone as a free unbound protein. This test may be ordered to assist in diagnosis of hypogonadism, hypopituitarism, and Klinefelter's syndrome, among other disorders. The specimen is serum. Method may be by radioimmunoassay (RIA) and immunoassay (non-isotopic).
84436	Thyroxine; total	2	This test may be ordered as a T4. The specimen is serum. Methods may include radioimmunoassay (RIA), enzyme-linked immunosorbent assay (ELISA), fluorescence polarization immunoassay (FPIA), and chemiluminescence assay (CIA). The test is performed to determine thyroid function as screening test; total thyroxine makes up approximately 99 percent of the thyroid hormone.
84439	Thyroxine; free	11	This test may be ordered as a FT4, free T4, FTI or FT4 index. The specimen is serum, requiring special handling. Methods may include radioimmunoassay and equilibrium dialysis for reference method. Free thyroxine is a minimal amount of the total T4 level (approximately one percent). This test is not influenced by thyroid-binding abnormalities and perhaps correlates more closely with the true hormonal status. It may be effective in the diagnosis of hyperthyroidism and hypothyroidism.
84443	Thyroid stimulating hormone (TSH)	23	TSH is produced in the pituitary gland and stimulates the secretion of thyrotropin (T3) and thyroxine (T4); these secretory products monitor TSH. The specimen is serum, requiring special handling. Heel stick or umbilical cord sample is drawn from newborns and may be collected on a special paper. Methods may include radioimmunoassay (RIA), sandwich immunoradiometric assay (IRMA), fluorometric enzyme immunoassay with use of monoclonal antibodies, or microparticle enzyme immunoassay on IMx (MEIA). This test may be performed to determine thyroid function, to differentiate from various types of hypothyroidism (e.g., primary, and pituitary/hypothalamic), or to diagnose hyperthyroidism. The test may be ordered to evaluate therapy in patients receiving hypothyroid treatment, and to detect congenital hypothyroidism
84479	Thyroid hormone (T3 or T4) uptake or thyroid hormone binding ratio	2	This test may be requested as T3 uptake and T4 uptake or THBR. The specimen is serum. Method is chemiluminescent immunoassay
84480	Triiodothyronine T3; total (TT-3)	4	This test may be ordered as a T3 (RIA) or total T3. The specimen is serum. Methods may include radioimmunoassay (RIA), immunochemiluminometric assay, and fluorometric immunoassay. Abnormal results may be diseases and disorders related to the thyroid.
84520	Urea nitrogen; quantitative	147	This test may be requested as blood urea nitrogen (BUN). Urea is an end product of protein metabolism. BUN may be requested to evaluate dehydration or renal function. Blood specimen is serum or plasma. Method is colorimetry, enzymatic, or rate conductivity. This test measures (quantitates) the amount of urea in the blood.
84540	Urea nitrogen; urea	42	This test may provide useful information regarding carbohydrate metabolism (diabetes), kidney function, and acid-base balance, in addition to dietary protein. Urea is a measure of protein breakdown in the body. Urine urea excretion can be measured to obtain a ratio between the plasma (blood) urea and the urine urea; this ratio is an indicator of kidney function. Urine collection over a 24-hour period. Methods may include enzymatic assay, colorimetry, and conductometric.
84550	Uric acid; blood	56	This test may be requested as urate. Uric acid may be ordered to evaluate gout, renal function and a number of other disorders. Blood specimen is serum or plasma. Method is enzymatic or high performance liquid chromatography (HPLC).
84560	Uric acid; other source	68	Uric acid is also known as urate. Methods may include high performance liquid chromatography, uricase, and phosphotungstate. The test may be ordered to determine the possible occurrence of calculus formation, evaluate uric acid in gout, and to identify genetic defects and some malignancies in body fluids other than blood.
84585	Vanillylmandelic acid (VMA), urine	1	This test is also called 3-methoxy-4-hydroxymandelic acid test, and also as VMA. Urine collection is over a 24-hour period and requires special handling. Methods may include colorimetry, spectrophotometry, gas chromatography, and high performance liquid chromatography (HPLC). The test may be performed to evaluate hypertensive states and to diagnose certain tumors and to monitor the efficacy of treatment modalities.
84702	Gonadotropin, chorionic (hCG); quantitative	39	This test may be ordered as hCG or as a serum pregnancy test. The specimen is serum. Method may be radioimmunoassay (RIA), two-site immunoradiometric assay (IRMA), two-site enzyme-linked immunosorbent assay (ELISA), and radioreceptor assay (RRA). This test is quantitative and measures the amount of hCG present, a determinate of pregnancy and certain tumors.
85014	Blood count; hematocrit	7	This test may be ordered as a hematocrit, Hmt, or Hct. The specimen is whole blood. Method is automated cell counter. The hematocrit or volume of packed red cells (VPRC) in the blood sample is calculated by multiplying the red blood cell count or RBC times the mean corpuscular volume or MCV.
85018	blood count; hemoglobin	1	This test may be ordered as hemoglobin, Hgb, or hemoglobin concentration. The specimen is whole blood. Method is usually automated cell counter but a manual method is seen in labs with a limited test menu and blood bank drawing stations. Hemoglobin is an index of the oxygen-carrying capacity of the blood.
85025	Blood count; automated differential WBC count; completed (CBC), automated	79	This test may be ordered as a complete automated blood count (CBC). The specimen is whole blood. Method is automated cell counter. This code includes the measurement of erythrocytes (red blood cells or RBC), leukocytes (white blood cells or WBC), hemoglobin, hematocrit (volume of packed red blood cells or VPRC), platelet or thrombocyte count, and indices (mean corpuscular hemoglobin or MCH, mean corpuscular hemoglobin concentration or MCHC, mean corpuscular volume or MCV, and red cell distribution width or RDW). Code 85025 includes an automated differential of the white blood cells or "diff" in which the following leukocytes are differentiated: neutrophils or granulocytes, lymphocytes, monocytes, eosinophils, and basophils. Report 85027 if the complete CBC, or automated blood count, is done without the differential WBC count

85027	Blood count; completed (CBC), automated	37	This test may be ordered as a complete automated blood count (CBC). The specimen is whole blood. Method is automated cell counter. This code includes the measurement of erythrocytes (red blood cells or RBC), leukocytes (white blood cells or WBC), hemoglobin, hematocrit (volume of packed red blood cells or VPRC), platelet or thrombocyte count, and indices (mean corpuscular hemoglobin or MCH, mean corpuscular hemoglobin concentration or MCHC, mean corpuscular volume or MCV, and red cell distribution width or RDW). Code 85025 includes an automated differential of the white blood cells or "diff" in which the following leukocytes are differentiated: neutrophils or granulocytes, lymphocytes, monocytes, eosinophils, and basophils. Report 85027 if the complete CBC, or automated blood count, is done without the differential WBC count.
85652	Sedimentation rate, erythrocyte; automated	1	This test may be ordered as a Zeta sedimentation rate or as a Zeta sed rate. Specimen is whole blood. Method is centrifugation; this is an automated test. This test is a non-specific screening test for a number of diseases including anemia, disorders of protein production such as multiple myeloma, and other conditions that alter the size and/or shape of red cells or erythrocytes. This test may also be used to screen diseases that cause an increase or decrease in the amount of protein in the plasma or liquid portion of the blood.
85660	Sickling or RBC, reduction	1	This test may be ordered as a sickle cell metabisulfite test, a sickle cell reduction test, an erythrocyte (RBC) sickling test, or as an RBC reduction sickle cell test. Specimen is whole blood. The method is manual. Whole blood is mixed with a reducing agent that causes erythrocytes that contain abnormal amounts of hemoglobin S to sickle or change their shape to an elongated 'sickle' cell. The solution is examined microscopically and the numbers of sickle cells are reported as a percentage of normal erythrocytes or RBCs.
86301	Immunossay for tumor antigen, quantitative; CA 19-9	1	This test may also be requested as carbohydrate antigen 19-9. The specimen is serum. Method is immunoassay. Quantitative analysis for CA 19-9 is used primarily as a marker for pancreatic cancer. It identifies recurrence and monitors patients. It is also used to monitor gastrointestinal, head/neck, and gynecological cancer. It may identify recurrence of stomach, colorectal, liver, gallbladder, and urothelial malignancies.
86592	Syphilis test, non-treponemal antibody; qualitative	11	This nontreponemal (screening) antibody test is commonly ordered as RPR (rapid plasma reagin), STS (serologic test for syphilis), VDRL (venereal disease research laboratory), or ART (automated reagin test). It may also be ordered as standard test for syphilis. The specimen is serum. The test is commonly used to provide a diagnosis (screening test) for syphilis. The method is by nontreponemal rapid plasma reagin (RPR)-particle agglutination test. More recently, it is being performed by automated methodology, such as enzyme-linked immunosorbent assay (ELISA).
86631	Antibody; Chlamydia	1	This test may be ordered as chlamydia psittaci or LVG titer. The specimen is serum or finger stick in adults, or heel stick in infants. Methods are complement fixation (CF), enzyme-linked immunosorbent assay (ELISA), and immunofluorescent antibody (IFA). This test may be used to determine exposure to chlamydia, though the test should not be used as a specific type. Chlamydomonas is a genus of algae that can cause nongonococcal urethritis, among other infections.
86632	Antibody; Chlamydia, IgM	1	This test may be ordered as chlamydia IgM titer. The specimen is serum or finger stick in adults, or heel stick in infants. Complement fixation (CF), enzyme-linked immunosorbent assay (ELISA), and immunofluorescent antibody (IFA) are methods commonly used to determine previous exposure to chlamydia or a current infection. Chlamydomonas is a genus of algae that can cause nongonococcal urethritis, among other infections.
86689	HTLV or HIV antibody, confirmatory test	13	This test is commonly ordered as HTLV or HIV by Western blot. The specimen is serum. This test may be performed as a confirmation of a positive test for human T cell leukemia II virus or human immunodeficiency virus (HIV), often by a previous enzyme-linked immunoassay (ELISA).
86694	Antibody; herpes simplex, non-specific type	6	These tests may be ordered as HSV antibody titer, HSV titer, herpes simplex antibody titer, or HSV IgG/IgM. The specimen is serum or finger stick in adults, or heel stick in infants. A number of methodologies have been employed, such as complement fixation (CF), enzyme linked immunosorbent assay (ELISA), indirect fluorescent antibody (IFA), enzyme immunoassay, and latex agglutination. This test has been used as a serologic method to detect previous or recent exposure to herpes simplex. To report non-specific type testing, see 86694; testing for type 1, see 86695; testing for type 2, see 86696.
86695	Antibody; herpes simplex, type 1	20	These tests may be ordered as HSV antibody titer, HSV titer, herpes simplex antibody titer, or HSV IgG/IgM. The specimen is serum or finger stick in adults, or heel stick in infants. A number of methodologies have been employed, such as complement fixation (CF), enzyme linked immunosorbent assay (ELISA), indirect fluorescent antibody (IFA), enzyme immunoassay, and latex agglutination. This test has been used as a serologic method to detect previous or recent exposure to herpes simplex. To report non-specific type testing, see 86694; testing for type 1, see 86695; testing for type 2, see 86696.
86696	Antibody; herpes simplex, type 2	19	These tests may be ordered as HSV antibody titer, HSV titer, herpes simplex antibody titer, or HSV IgG/IgM. The specimen is serum or finger stick in adults, or heel stick in infants. A number of methodologies have been employed, such as complement fixation (CF), enzyme linked immunosorbent assay (ELISA), indirect fluorescent antibody (IFA), enzyme immunoassay, and latex agglutination. This test has been used as a serologic method to detect previous or recent exposure to herpes simplex. To report non-specific type testing, see 86694; testing for type 1, see 86695; testing for type 2, see 86696.

86701	Antibody; HIV-1	2	This test may be ordered as an HIV-1 serological test, an HIV-1 antibody, or by an internal code. HIV is a retrovirus and the causative agent of acquired immunodeficiency syndrome (AIDS). Specimen is serum. Numerous kits are now available that use a variety of viral proteins and serumsynthetic peptides as antigens. Methodology is enzyme immunoassay (EIA), enzyme-linked immunosorbent assay (ELISA), radioimmunoprecipitation assay (RIPA), or indirect fluorescent antibody (IFA). A negative test does not guarantee negative status and the test is often repeated several times.
86704	Hepatitis B core antibody; total	6	This test may be ordered as hepatitis Bc Ab (HBcAb), total. It may also be ordered as HBcAb, anti-HBc, HBVc Ab, anti-HBVc. This test identifies Hepatitis B core total antibodies (IgG and IgM), which are markers available to identify individuals with acute, chronic, or past infection of hepatitis B. The presence of high-titered IgM specific HBcAb is always indicative of an acute infection. The presence of IgG may indicate acute or chronic infection. Blood specimen is serum. Methods include radioimmunoassay (RIA) and enzyme-linked immunosorbent assay (ELISA).
86705	Hepatitis B core antibody; IgM antibody	1	This test may be ordered as hepatitis Bc Ab (HBcAb), IgM. It may also be ordered as HBcAb, anti-HBc, HBVc Ab, anti-HBVc. This test identifies Hepatitis B core IgM antibodies, the presence of which always indicates an acute infection. Blood specimen is serum. Methods include radioimmunoassay (RIA) and enzyme-linked immunosorbent assay (ELISA).
86706	Hepatitis B surface antibody	5	This test may be requested as Hepatitis B surface antibody (HBsAb), Hepatitis Bs Ab, HBV surface antibody, or anti-HBs. The presence of HBsAb is indicative of a previous resolved infection or vaccination against hepatitis B. Blood specimen is serum. Methods include radioimmunoassay (RIA), enzyme immunoassay (EIA), immunoradiometric assay (IRMA), and immunoenzymatic assay (IEMA).
86708	Hepatitis A antibody; total	4	This test may be ordered as Hepatitis A Antibody (HAAb), HAV antibody, anti-Hep A or anti-HAV total (IgG and IgM). The presence of HAV IgG antibody may indicate acute infection or previous resolved infection, while IgM antibody always indicates acute infectious disease. Blood specimen is serum. Methods include radioimmunoassay (RIA), enzyme immunoassay (EIA), immunoradiometric assay (IRMA), immunoenzymatic assay (IEMA), and microparticle enzyme immunoassay (MEIA).
86709	Hepatitis A antibody; IgM antibody	3	This test may be ordered as Hepatitis A Antibody (Haas), HAV IgM antibody, anti-Hep A IgM, or anti-HAV IgM. The presence of IgM antibody indicates acute infectious disease. Blood specimen is serum. Methods include radioimmunoassay (RIA), enzyme immunoassay (EIA), immunoradiometric assay (IRMA), immunoenzymatic assay (IEMA), and microparticle enzyme immunoassay (MEIA).
86803	Hepatitis C antibody	4	This test may be ordered as hepatitis C antibody titers. It may also be ordered as anti-hepatitis C titers, HCV Ab titers, and anti-HCV titers. This test is normally used for an initial hepatitis C screen. Positive or unequivocal tests are repeated using different techniques that are reported separately. Blood specimen is serum. Methods may include enzyme-linked immunosorbent assay (ELISA) or enzyme immunoassay (EIA).
86850	Antibody screen, ABC, each serum technique	1	This test may be ordered as an RBC antibody detection. The test is a screen for particular antibodies to red cell antigens that may present problems during a blood transfusion or childbirth. Blood specimen is whole blood. The test may be performed using tubes, microtiter plates, or gel cards. Another method is agglutination.
87015	Concentration (any type), for infectious agents	2	Concentration may also be referred to as thick smear preparation. The source samples are treated to concentrate the presence of suspect organisms, usually through sedimentation or flotation. There are two common methods of concentration for ova and parasite exams: formalin concentration and zinc sulfate flotation. The most common concentration methods for AFB stains or cultures are the N-acetyl-L cysteine method, cytocentrifugation, and the Zephiran-trisodium phosphate method. Do not report 87015 in conjunction with 87177.
87070	Culture, bacterial; any other source except urine, blood or stool, earovi, with isolation and presuptive identification of isolates	9	Common names for this test are numerous and may include routine culture, aerobic culture, or, using a body or source site, may be referred to as vaginal culture, cerebral spinal fluid culture, etc. Presumptive identification of aerobic pathogens or microorganisms in the sample is by means of identifying colony morphology. The test includes gram staining and subculturing to selective media for the detection of bacterial growth. There are several automated systems that detect the presence of bacteria using colorimetric, radiometric, or spectrophotometric means. The purpose of this culture test is to detect the presence of any or multiple aerobic bacteria from a body source or site, except urine, blood, or stool samples, and to identify the micro-organism(s), but not to the specific level of genus or species requiring additional testing, such as slide cultures. The collection and transport of specimen is varied and specimen dependent. Report 87071 when the identified aerobic isolate(s) is quantified in growth numbers.
87075	Culture. Bacterial; any source, except blood, anaerobic with isolation and presuptive identification or isolates	5	The most common name for this procedure is anaerobic culture. Presumptive identification of anaerobic pathogens or microorganisms in the sample is by means of identifying colony morphology. The test includes gram staining and subculturing to selective media for the detection of bacterial growth. There are several automated systems that detect the presence of bacteria using colorimetric, radiometric, or spectrophotometric means. The purpose of this culture test is to detect the presence of any or multiple anaerobic bacteria from any body source or site, except blood, and to identify the micro-organism(s), but not to the specific level of genus or species requiring additional testing, such as slide cultures. Tissues, fluids, and aspirations, except blood samples, are collected in anaerobic vials or with anaerobic transport swabs and transported immediately. Anaerobic bacteria are sensitive to oxygen and cold.
87077	Culture, bacterial; aerobic isolate, additional methods required for definitive identification, each isolate	233	This code reports definitive anaerobic (87076) or aerobic (87077) organism identification of an already-isolated anaerobic or aerobic bacterium. The pathogen has already been presumptively identified, but additional testing is required to identify the specific genus or species. The additional definitive testing methods include biochemical panels and slide cultures. Studies using chromatography, molecular probes, or specific immunological techniques may be employed for definitive testing, but are not included in this code and are reported separately.

87086	Culture; bacterial; quantitative colony count, urine	2370	These codes report the performance of a urine bacterial culture with a calibrated inoculating device so that a colony count accurately correlates with the number of organisms in the urine. In 87088, isolation and presumptive identification of bacteria recovered from the sample is done by means of identifying colony morphology, subculturing organisms to selective media and the performance of a gram stain or other simple test to identify bacteria to the genus level. There are several automated systems that detect the presence of bacteria using colorimetric, radiometric, or spectrophotometric means. In 87086, quantified colony count numbers within the urine sample are measured.
87088	Culture, bacterial; with isolation and presumptive identification of each isolate,	881	These codes report the performance of a urine bacterial culture with a calibrated inoculating device so that a colony count accurately correlates with the number of organisms in the urine. In 87088, isolation and presumptive identification of bacteria recovered from the sample is done by means of identifying colony morphology, subculturing organisms to selective media and the performance of a gram stain or other simple test to identify bacteria to the genus level. There are several automated systems that detect the presence of bacteria using colorimetric, radiometric, or spectrophotometric means. In 87086, quantified colony count numbers within the urine sample are measured.
87116	Culture, tubercle or other acid-fast bacilli (eg, TB, AFB, mycobacterial) any source	2	Common names include AFB culture, TB culture, mycobacterium culture, and acid-fast culture. Collection methods are source dependent. The methodology is by culture for the isolation and presumptive identification of mycobacterium. An acid-fast smear should be done at the time the specimen is cultured. Media for isolation should include both solid and liquid types.
87147	Culture, typing, immunofluorescent method, each antiserum; immunologic method, other than immunofluorescence	20	This test is used for more specifically identifying cultured specimens using an immunologic method other than immunofluorescence. For example, agglutination technique may be used to more specifically identify Salmonella usually to a group level since there are more than 2,000 serovar of Salmonella. The different species have been grouped by common antigens and are tested with polyvalent antisera and reported by group (e.g., Salmonella Group D).
87177	Ova and parasites, direct smears, concentration and identification	1	Common names for this procedure are ova and parasite exam, or O & P. Stool is collected in a clean, leak-proof container (when processed within one hour) or the specimen is added to formalin or fixative (both available in commercial kits). The methodology of an ova and parasite exam for stools includes a direct smear, and smear of concentrated material, such as formalin concentration technique or zinc flotation method. Identification is by observing parasites with the aid of a microscope. Do not report 87177 in conjunction with 87015.
87184	Susceptibility studies, antimicrobial agent; disk method, per plate	1	This is commonly called a Kirby-Bauer or Bauer-Kirby sensitivity test. It is a sensitivity test to determine the susceptibility of a bacterium to an antibiotic. The methodology is disk diffusion and results are reported as sensitive, intermediate, or resistant. As many as 12 antibiotic disks may be used per plate and the procedure is billed per plate not per antibiotic disk.
87186	Susceptibility studies, antimicrobial agent; microdilution or agar dilution (minimum inhibitory concentration [MIC] or breakpoint), each multi-antimicrobial, per plate	8	This procedure may be called an MIC, or a sensitivity test. It is a sensitivity test to determine the susceptibility of a bacterium to an antibiotic. The methodology is microtiter dilution (several commercial panels use this method). Results are given as a minimum inhibitory concentration (MIC) with an interpretation of sensitive, intermediate, or resistant. The antibiotics on commercial plates are numerous, but predetermined. The procedure is charged by plate not by antibiotic.
87205	Smear, primary source with interpretation; gram or Giemsa stain for bacteria, fungi or cell types	8	Any smear done on a primary source (e.g., sputum, CSF, etc.) to identify bacteria, fungi, and cell types. An interpretation of findings is provided. Bacteria, fungi, WBCs, and epithelial cells may be estimated in quantity with an interpretation as to the possibility of contamination by normal flora. A gram stain may be the most commonly performed smear of this type.
87340	Infectious agent antigen detection by enzyme immunoassay technique; hepatitis B surface antigen	5	This test may be requested as HBsAg by enzyme immunoassay (EIA). Hepatitis B is a retrovirus that can cause persistent infection leading to cirrhosis and hepatocellular carcinoma. HBsAg is a lipoprotein that coats the surface of the hepatitis B virus. Blood specimen is serum.
87490	Infectious agent detection by nucleic acid; Chlamydia trachomatis, direct probe technique	1	This test may be requested as Chlamydia trachomatis or C. trachomatis by direct DNA probe. C. trachomatis is a frequently occurring sexually transmitted disease. It may cause nonspecific urethritis or pelvic inflammatory disease (PID), although it is frequently asymptomatic in women. Another serotype also causes conjunctivitis. The specimen is treated to isolate the DNA using direct probe.
87491	Infectious agent detection by nucleic acid; Chlamydia trachomatis, amplified probe technique	28	This test may be requested as Chlamydia trachomatis or C. trachomatis by direct DNA probe. C. trachomatis is a frequently occurring sexually transmitted disease. It may cause nonspecific urethritis or pelvic inflammatory disease (PID), although it is frequently asymptomatic in women. Another serotype also causes conjunctivitis. The specimen is treated to isolate the DNA using direct probe.
87590	Infectious agent detection by nucleic acid; Neisseria gonorrhoeae, direct probe technique	1	This test may be requested as gonorrhea direct DNA probe, gonorrhea molecular probe assay, or DNA detection of gonorrhea. Neisseria gonorrhoea is one of the most common sexually transmitted infections. Molecular (nucleic acid probe) techniques offer rapid, accurate identification of Neisseria gonorrhoea. While a cervical or urethral swab is preferred, molecular techniques are sensitive enough to detect the organism in urine also. Neisseria gonorrhoea can be detected by DNA, RNA, or rRNA probes.
87591	Infectious agent detection by nucleic acid; Neisseria gonorrhoeae, amplified probe technique	28	This test may be requested as gonorrhea amplified DNA probe, gonorrhea molecular probe assay, or DNA detection of gonorrhea. Neisseria gonorrhoea is one of the most common sexually transmitted infections. Molecular (nucleic acid probe) techniques offer rapid, accurate identification of Neisseria gonorrhoea. While a cervical or urethral swab is preferred, molecular techniques are sensitive enough to detect the organism in urine also. Neisseria gonorrhoea can be detected by DNA or rRNA probes. Amplification can be performed using a number of techniques. Polymerase chain reaction (PCR) and ligase chain reaction (LCR) detect gonorrhea DNA. An assay is also available which detects gonorrhea ribosomal RNA (rRNA).
88108	Cytopathology, concentration technique, smears and interpretation	1195	Cytopathology, concentration technique, (e.g., Saccomanno, cytocentrifugation, and cytopsins) may be done on many different types of specimen samples like bronchial, cervicovaginal, and conjunctival brushings, nipple discharge, sputum, and gastrointestinal epithelial cell specimens. Cellular smear preparations (cervicovaginal, conjunctival, bronchial brushings, nipple discharge) are immediately fixed in 95 percent ethanol or pap fixative to eliminate drying. GI, urologic, and sputum samples are collected with a Saccomanno fixative added. Following preparation, the sample is centrifuged to yield a pellet at the bottom of the tube and overlying supernatant. The clear fluid supernatant is decanted completely and the pellet is used to make direct smears of the concentrated sample for cytopathology and cell counts. Cytocentrifugation, cytopsins, smears and interpretations are then performed.
88162	Cytopathology, smears, any other source; extended studies involving over 5 slides and/or multiple stains	87	Specimen collection is by separately reportable percutaneous needle biopsy. Methods include microscopy examination of smears or a centrifuge specimen. These codes report the pathology examination portion of the procedure only. Code 88160 reports screening and interpretation only. Code 88161 reports preparation, screening and interpretation. Code 88162 reports an extended study involving more than five slides and/or multiple stains.

88271	Molecular cytogenetics; DNA probe, each (eg. FISH)	1	Molecular cytogenetics represents relatively new techniques capable of detecting changes in chromosomes that cannot be detected by traditional microscopic techniques. This code reports the use of a DNA probe to identify chromosomal abnormalities. Fluorescent in situ hybridization (FISH) is one type of DNA probe. It allows chromosomes and genes to be analyzed simultaneously. In situ hybridization involves treating native double-stranded DNA to render it single-stranded. The strand is incubated to allow the strand to recognize complementary bases and to reform as a double-strand (hybridization). When a strand is radioactively marked, it is the "probe." The specificity to which the hybridization takes place is analyzed.
88302	Level II - Surgical pathology, gross and microscopic examination Appendix, incidental Fallopian tube, sterilization Fingers/toes, amputation, traumatic Fore skin, newborn Hernia sac, any location Hydrocele sac Nerve Skin, plastic repair Sympathetic ganglion Testis, castration Vaginal mucosa, incidental Vas deferens, sterilization	94	This examination may be ordered as a gross and microscopic pathology exam or a gross and microscopic tissue exam. The exam may not be specifically ordered ahead of time; rather, the tissue is harvested in the course of a surgery and sent for routine lab evaluation. Tissue is submitted in a container labeled with the tissue source, preoperative diagnosis, and patient identification information. Specimens from separate sites must be submitted in separate containers, each labeled with the tissue source. This procedure is used to describe examination of tissues presumed normal. It includes both a gross and microscopic examination with the microscopic exam mainly to confirm the tissue is free of disease. Examples of its use might include tissues from a fallopian tube or vas deferens performed in the course of sterilization procedures, newborn foreskin following circumcision, hernia sac, hydrocele sac, etc.
88305	Level IV - Surgical pathology, gross and microscopic examination Abortion - spontaneous/missed Artery, biopsy Bone marrow, biopsy Bone exostosis Brain/meninges, other than for tumor resection Breast, biopsy, not requiring microscopic evaluation of surgical margins Breast, reduction mammoplasty Bronchus, biopsy Cell block, any source Cervix, biopsy Colon, biopsy Duodenum, biopsy Endocervix, curettings/biopsy Endometrium, curettings/biopsy Esophagus, biopsy Extremity, amputation, traumatic Fallopian tube, biopsy Fallopian tube, ectopic pregnancy Femoral head, fracture Fingers/toes, amputation, non-traumatic Gingiva/oral mucosa, biopsy Heart valve Joint, resection Kidney, biopsy Larynx, biopsy Leiomyoma(s), uterine myomectomy - without uterus Lip, biopsy/wedge resection Lung, transbronchial biopsy Lymph node, biopsy Muscle, biopsy Nasal mucosa, biopsy Nasopharynx/oropharynx, biopsy Nerve, biopsy Odontogenic/dental cyst Omentum, biopsy Ovary with or without tube, non-neoplastic Ovary, biopsy/wedge resection Parathyroid gland Peritoneum, biopsy Pituitary tumor Placenta, other than third trimester Pleura/pericardium - biopsy/tissue Polyp, cervical/endometrial Polyp, colorectal Polyp, stomach/small intestine Prostate, needle biopsy Prostate, TUR Salivary gland, biopsy Sinus, paranasal biopsy Skin, other than cyst/tag/debridement/plastic repair Small intestine, biopsy Soft tissue, other than tumor/mass/lipoma/debridement Spleen Stomach, biopsy Synovium Testis, other than tumor/biopsy/castration Thyroglossal duct/brachial cleft cyst Tongue, biopsy Tonsil, biopsy Trachea, biopsy Ureter, biopsy Urethra, biopsy Urinary bladder, biopsy Uterus, with or without tubes and ovaries, for prolapse Vagina, biopsy Vulva/labia, biopsy	1573	These examinations would be ordered as a gross and microscopic pathology exam or a gross and microscopic tissue exam. Tissue is submitted in a container labeled with the tissue source, preoperative diagnosis, and patient identification information. Specimens from separate sites must be submitted in separate containers, each labeled with the tissue source. Codes 88304-88309 describe levels of service for specimens requiring additional levels of work due to a presumed presence of disease. Code 88304 describes the lowest level of complexity for diseased or abnormal tissue with each subsequent code (88305, 88307, and 88309) describing in ascending order higher levels of complexity and physician work. Specific types of disease and tissue sites are listed for each code in the CPT(r) description.
88307	Level V - Surgical pathology, gross and microscopic examination Adrenal, resection Bone - biopsy/curettings Bone fragment(s), pathologic fracture Brain, biopsy Brain/meninges, tumor resection Breast, excision of lesion, requiring microscopic evaluation of surgical margins Breast, mastectomy - partial/simple Cervix, conization Colon, segmental resection, other than for tumor Extremity, amputation, non-traumatic Eye, enucleation Kidney, partial/total nephrectomy Larynx, partial/total resection Liver, biopsy - needle/wedge Liver, partial resection Lung, wedge biopsy Lymph nodes, regional resection Mediastinum, mass Myocardium, biopsy Odontogenic tumor Ovary with or without tube, neoplastic Pancreas, biopsy Placenta, third trimester Prostate, except radical resection Salivary gland Sentinel lymph node Small intestine, resection, other than for tumor Soft tissue mass (except lipoma) - biopsy/simple excision Stomach - subtotal/total resection, other than for tumor Testis, biopsy Thymus, tumor Thyroid, total/lobe Ureter, resection Urinary bladder, TUR Uterus, with or without tubes and ovaries, other than neoplastic/prolapse	1	These examinations would be ordered as a gross and microscopic pathology exam or a gross and microscopic tissue exam. Tissue is submitted in a container labeled with the tissue source, preoperative diagnosis, and patient identification information. Specimens from separate sites must be submitted in separate containers, each labeled with the tissue source. Codes 88304-88309 describe levels of service for specimens requiring additional levels of work due to a presumed presence of disease. Code 88304 describes the lowest level of complexity for diseased or abnormal tissue with each subsequent code (88305, 88307, and 88309) describing in ascending order higher levels of complexity and physician work. Specific types of disease and tissue sites are listed for each code in the CPT(r) description.
88321	Consultation and report on referral slides prepared elsewhere	18	A pathology consultation involves an opinion or advice on the presence or absence of diseased or abnormal tissue provided at the request of another physician. These three codes report consultations and written interpretations on slide or material referred from another facility or source. Code 88321 reports a consultation and written report on slide prepared by another source; 88323 reports a consultation and written report on material referred from another source requiring routine preparation of slides by the consultant; and 88325 reports a comprehensive consultation with review of records, evaluation of specimens requiring more complex slide preparation, and a written report.

88342	Immunohistochemistry or immunocytochemistry, each separately identifiable antibody per block, cytologic preparation, or hematologic smear; first separately identifiable antibody per slide	226	This immunohistochemistry procedure is also referred to as immunostain or peroxidase-antiperoxidase (PAP). It is a technique used to identify specific antigens found in tumor cells. It is used primarily for the diagnosis of poorly differentiated neoplasms. There are several methods of performing immunocytochemistry tests; however, all involve treating the specimen with a tumor specific antibody, incubation, and subsequent washing of the specimen to remove unbound antibody and counterstaining with secondary antibodies to determine the antibody location. The specimen is examined for positive and negative responses. Multiple immunostains are normally performed on each specimen to more specifically identify the suspect neoplasm by providing known positive and negative responses specific to that neoplasm. Report 88342 for the first antibody identified and 88343 for each additional antibody identified on the same slide.
88367	Morphometric analysis, in situ hybridization (quantitative or semi-quantitative) each probe; using computer assisted technology	247	Morphometric analysis may also be referred to as histomorphometry. A quantitative or semiquantitative analysis is done with in situ hybridization. In situ hybridization involves isolating and detecting specific nucleotide (mRNA) sequences within morphologically preserved cells and tissues by hybridizing a complementary nucleic acid strand, called a probe, to the sequence of interest within the prepared cells. The cells of interest may be snap frozen and fixed in paraformaldehyde, spun out of suspension onto glass slides and fixed with methanol, or formalin fixed embedded in paraffin. The probe is first labeled with an easily detectable substance, such as a radioactive isotope, before hybridization. Types of probes used are oligonucleotides, single-stranded DNA, double-stranded DNA, and RNA, or riboprobes. The labeled probe strand is added to the prepared cells. The pairing or bonding (hybridization) that occurs between the complementary sequences of nucleotide bases in the probe to the specific mRNA sequences allows the expression of the type of sequence being detected to be seen on the target gene. Analysis is done to determine the organization, structure, form and composition within the morphologically preserved cells being studied, either manually in 88668 or using computer-assisted technology in 88367. These codes are reported once for each type of probe used.
88368	Morphometric analysis, in situ hybridization (quantitative or semi-quantitative) each probe; manual	2	Morphometric analysis may also be referred to as histomorphometry. A quantitative or semiquantitative analysis is done with in situ hybridization. In situ hybridization involves isolating and detecting specific nucleotide (mRNA) sequences within morphologically preserved cells and tissues by hybridizing a complementary nucleic acid strand, called a probe, to the sequence of interest within the prepared cells. The cells of interest may be snap frozen and fixed in paraformaldehyde, spun out of suspension onto glass slides and fixed with methanol, or formalin fixed embedded in paraffin. The probe is first labeled with an easily detectable substance, such as a radioactive isotope, before hybridization. Types of probes used are oligonucleotides, single-stranded DNA, double-stranded DNA, and RNA, or riboprobes. The labeled probe strand is added to the prepared cells. The pairing or bonding (hybridization) that occurs between the complementary sequences of nucleotide bases in the probe to the specific mRNA sequences allows the expression of the type of sequence being detected to be seen on the target gene. Analysis is done to determine the organization, structure, form and composition within the morphologically preserved cells being studied, either manually in 88668 or using computer-assisted technology in 88367. These codes are reported once for each type of probe used.
G0103	Prostate cancer screening; prostate specific antigen test (PSA)	112	This code reports a total prostate specific antigen (PSA) test for cancer screening. The specimen collection is by venipuncture. Methods may include radioimmunoassay (RIA) and monoclonal two-site immunoradiometric assay. There are several forms of PSA present in serum. PSA may be complexed with the protease inhibitor alpha-1 antichymotrypsin (PSA-ACT) or found in a free form. Higher levels of free PSA are more often associated with benign conditions than with cancer. Total PSA measures both complexed and free levels to provide a total amount present in the serum. A percentage of each form is sometimes calculated to help distinguish benign from malignant conditions.

# Exhibit C

# Transcript of the Testimony of **Richard L. Kam**

**Date:** April 15, 2014

**Case:** In Re: LabMD, Inc.

NON-PUBLIC - DO NOT DISCLOSE



Ace-Federal Reporters, Inc.  
Phone: 202-347-3700  
Fax: 202-737-3638  
Email: [info@acefederal.com](mailto:info@acefederal.com)  
Internet: [www.acefederal.com](http://www.acefederal.com)

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

UNITED STATES OF AMERICA

BEFORE THE FEDERAL TRADE COMMISSION

- - - - -x

In the Matter of :  
LabMD, Inc. : Docket No. 9357  
A corporation :

- - - - -x

CONFIDENTIAL - DO NOT DISCLOSE

DEPOSITION OF RICHARD L. KAM

Washington, DC  
Tuesday, April 15, 2014

REPORTED BY:  
DONALD R. THACKER

Page 34

1 36 percent of respondents say it took nearly a year  
 2 or more working with their healthcare provider or  
 3 insurers to resolve the crime, and 48 percent say  
 4 the crime is still not resolved. Citation 10,  
 5 bottom of the page, Ponemon Institute 2013 on  
 6 Medical Identity Theft, page 12.  
 7 Q Thank you, anywhere else in the report?  
 8 A Same page, 15, Another problem is health  
 9 insurance. The Ponemon survey found that 39 percent  
 10 of medical identity theft victims lost their  
 11 healthcare coverage, Citation 11, Ponemon  
 12 2013 Survey on Medical Identity Theft, page 10.  
 13 Q Anywhere else?  
 14 A Page 17, under subheading Consumers  
 15 Ability to Avoid Possible Harms.  
 16 Q In the middle of the page?  
 17 A In the middle of the page, second  
 18 paragraph from the end, Javelin Research finds that  
 19 almost one in three data breach victims in 2013 fell  
 20 victim to identity fraud in the same year. Citation  
 21 15, Javelin 2014 Identity Fraud Report, page 8.  
 22 Q And that's where we started off so we  
 23 circled back find of.  
 24 A Yes.  
 25 Q Do you recall back when we were talking

Page 35

1 about page 11 and we were talking about that  
 2 particular area of testimony or other report;  
 3 correct?  
 4 A On page 11?  
 5 Q I'm sorry -- right, the same report but we  
 6 are now on 17, you are referring to the same report,  
 7 the same figure?  
 8 A Yes.  
 9 Q Is that the nearly one in three data  
 10 breach victims 30.5 percent, that nearly one third;  
 11 correct?  
 12 A The words I use, Javelin Research finds  
 13 that almost one in three data breach victims, almost  
 14 one in three.  
 15 Q Right. Is there anywhere else in your  
 16 report you look to for your use of averages and  
 17 aggregates?  
 18 A In the appendices I referred to several  
 19 projects that I worked on where we have used various  
 20 research studies averages and other things.  
 21 Q Is there a particular page you are looking  
 22 at right now just for a general --  
 23 A Sure, page four, heading Affiliations and  
 24 Organizations, white papers as listed on that page.  
 25 Q Prior to the break you also indicated that

Page 36

1 you have developed an approach over the years, do  
 2 you remember when you testified to that?  
 3 A Yes.  
 4 Q Can you explain to me what the approach  
 5 that you have developed over the years is?  
 6 A I'll point you to it in my report.  
 7 Q Okay, is it contained in your report?  
 8 A It is.  
 9 Q Okay. What part of your report expresses  
 10 the approach that you have developed over the years?  
 11 A It starts on page 17, under the heading  
 12 Consumers Ability to Avoid Possible Harms, last  
 13 paragraph, starting with, For my analysis I used the  
 14 following four factors to examine the likely risk of  
 15 harm to consumers from the unauthorized disclosure  
 16 of their sensitive personal information.  
 17 And then on page 18 I go on to describe  
 18 those four factors.  
 19 Q And they are listed there 1, 2, 3, 4 on  
 20 page 18?  
 21 A Yes.  
 22 Q Is your approach that you have developed  
 23 over the years expressed anywhere else in your  
 24 report or is that the primary expression of your  
 25 method or approach?

Page 37

1 A It is one of the elements of my approach.  
 2 Q These four factors are one of the  
 3 elements?  
 4 A Yes.  
 5 Q What are the other factors or elements?  
 6 Let's clarify that, I'm sorry, how would you use, in  
 7 your own words, would you call them elements or  
 8 factors, I don't want to put words in your mouth?  
 9 A Yeah, these are four factors I use to  
 10 assess the likely risk of harm to consumers whose  
 11 information has been disclosed in a non-authorized  
 12 disclosure.  
 13 Q And for your approach are there other  
 14 elements? You have termed these four as a part of  
 15 your approach, are there other elements to your  
 16 approach that you have developed over the years?  
 17 A Pieces of the process.  
 18 Q I'm sorry, what does that mean?  
 19 A Okay. The way the report is organized I  
 20 started by describing the likely harms consumers may  
 21 experience based on disclosure of their sensitive  
 22 personal information, specifically medical identity  
 23 theft. I then use the four factors to assess the  
 24 risk of harm, and then I use the various, the  
 25 specific research that's cited in my report to

1 estimate the likely harms to consumers in the form  
 2 of out-of-pocket costs and other harms.  
 3 Q And the other elements?  
 4 A Can you be more precise?  
 5 Q For your analysis you have identified the  
 6 likely harms and you used the four factors, then you  
 7 used -- I think you said specific research or --  
 8 A Specific research.  
 9 Q Specific research to estimate the likely  
 10 harms?  
 11 A Specific medical identity theft to  
 12 estimate the likely harms.  
 13 Q So I got three there, three pieces of the  
 14 process, is that fair to say, is there another piece  
 15 to the process?  
 16 A I would call it more my experience working  
 17 on similar situations.  
 18 Q Is there a similar situation to LabMD  
 19 disclosures in your mind?  
 20 A Every data breach is different.  
 21 Q Are there any that are similar that are  
 22 very close, closely tailored to the LabMD alleged  
 23 disclosures that come to mind?  
 24 A Every breach is different.  
 25 Q Do you view this case as unique to its own

1 facts; is that fair to say?  
 2 A Yes.  
 3 Q I'm going to circle back to page 11, the  
 4 2014 Identity Fraud Report by Javelin Strategy &  
 5 Research, you were talking about that brief  
 6 paragraph below the bulleted items; do you see that  
 7 paragraph according to the 2014 identity fraud  
 8 report?  
 9 A Yes.  
 10 Q How does the figure expressed here, the  
 11 30.5 percent, apply to the LabMD case specifically,  
 12 or does it in your mind?  
 13 A Can you be more specific?  
 14 Q Is that figure relevant to this case, and  
 15 if it is, in what way?  
 16 A The Javelin Strategy & Research figure is  
 17 relevant to the case, however, it's outside of the  
 18 scope of the request that the Federal Trade  
 19 Commission asked me to look into, because it talks  
 20 to identity fraud. I'm specifically looking at in  
 21 my report medical identity theft.  
 22 Q Is that there for informational purposes  
 23 then? Let me rephrase that, did you apply that  
 24 figure, the 30.5 percent to the specific facts of  
 25 the LabMD disclosure in your forming your analysis

1 as expressed in your report?  
 2 A No.  
 3 Q In forming your opinions could you compare  
 4 any of LabMD specific facts and circumstances to  
 5 those in the study you cite here to the determine  
 6 how the study fit the case? I guess you're saying  
 7 the study doesn't fit the case; is that what you are  
 8 saying?  
 9 A You will have to be more clear. Direct me  
 10 to what you are referring to, please.  
 11 Q The 30 percent figure?  
 12 A On page 11?  
 13 Q Yes.  
 14 A 30.5 percent, Javelin Research.  
 15 Q Yes, in forming your opinion could you  
 16 compare any of LabMD's specific facts and  
 17 circumstances to those in the study cited here to  
 18 determine how it might fit this case?  
 19 A I need you to be more precise.  
 20 Q If I'm understanding you correctly, you  
 21 didn't apply this figure to the specific factors of  
 22 the LabMD case; is that correct?  
 23 A Yes.  
 24 Q In your review of the specific facts of  
 25 the LabMD matter is there any evidence that nearly

1 one in three of the patients whose data was  
 2 allegedly exposed in the LabMD documents fell victim  
 3 to identity theft?  
 4 A Will you rephrase that.  
 5 (The reporter read the record as requested.)  
 6 THE WITNESS: I was asked by the  
 7 Commission to specifically look at the likely  
 8 injuries to consumers, specifically around medical  
 9 identity theft.  
 10 Q So it's fair to say then you didn't come  
 11 to any conclusion with respect to whether their  
 12 data was -- strike that.  
 13 You didn't come to my conclusions that the  
 14 specific victims fell victim to identity theft in  
 15 coming to your opinion as directed by the FTC?  
 16 A No.  
 17 Q Is there any proof that any of the  
 18 patients whose data was allegedly exposed in the  
 19 Sacramento incident fell victim to identity theft as  
 20 a result of that exposure to that incident?  
 21 A I wasn't asked to provide an opinion on  
 22 that.  
 23 Q That's not part of your opinion?  
 24 A No.  
 25 Q That's fair to say?

1 A No.  
 2 Q It is not part of your opinion?  
 3 A It is not part of my opinion.  
 4 MS. MEHM: Kent, could I ask you to take a  
 5 very short break, maybe about five minutes.  
 6 MS. RIPOSO VAN DRUFF: I think it will  
 7 expedite some questions if you will allow us to  
 8 confer. I don't think we need more than a couple  
 9 minutes. Okay.  
 10 (10:35 a.m. -- recess -- 10:43 a.m.)  
 11 BY MR. HUNTINGTON:  
 12 Q Let's go back on the record. Okay, we  
 13 just took a break for about five minutes or so.  
 14 Mr. Kam, is there something, do you need to correct  
 15 your testimony from something you stated earlier  
 16 today, did something come up over the break that  
 17 causes you to clarify your testimony?  
 18 A I would like to clarify my answer to the  
 19 last question.  
 20 (The reporter read the record as requested.)  
 21 THE WITNESS: I would like to clarify my  
 22 answer to the last question relative to potential  
 23 victims of identity theft. If you turn to page 23  
 24 of my report, heading Use of Social Security numbers  
 25 and day sheets, I did provide and respond to the

1 request from the Federal Trade Commission to review  
 2 their analysis of the 600, approximately 600 Social  
 3 Security numbers that were listed in the day report,  
 4 finding that there were several that had multiple  
 5 names associated with the same Social Security  
 6 number, indicating the potential for identity theft.  
 7 BY MR. HUNTINGTON:  
 8 Q So you did that in response to the request  
 9 of the FTC?  
 10 A Yes.  
 11 Q My question is, whether you determined any  
 12 causality with respect to victims following identity  
 13 theft, you did not; correct?  
 14 A I was asked to estimate the likelihood.  
 15 Q So your opinion is confined to likelihood,  
 16 is that fair to say, likelihood of harm?  
 17 A Likelihood of harm, risk of harm.  
 18 Q Likelihood of risk of harm?  
 19 A Yes.  
 20 Q Could you turn to page 17 of your expert  
 21 report. Earlier today you pointed to this section I  
 22 believe which starts halfway down the page,  
 23 Consumers' Ability to Avoid Possible Harms, and do  
 24 you see that, Mr. Kam?  
 25 A Yes.

1 Q Do you remember earlier today you pointed  
 2 to this section just briefly with respect to the  
 3 four factors?  
 4 A Yes.  
 5 Q It says in the bottom line, bottom  
 6 paragraph there, that quote, "For my analysis I used  
 7 the following four factors to examine the likely  
 8 risk of harm to consumers from the unauthorized  
 9 disclosure of their sensitive personal information."  
 10 Did I read that correct correctly?  
 11 A Yes.  
 12 Q Do you see on the next page on page 18  
 13 where it lists the four factors that we were talking  
 14 about earlier today; do you see that?  
 15 A Uh-huh, yes.  
 16 Q How did you determine in your analysis, in  
 17 the analysis which you have developed through your  
 18 experience, how did you determine what four  
 19 factors to use in analyzing the likelihood of harm  
 20 to consumers from the unauthorized of their  
 21 sensitive personal medical information?  
 22 A Based on my experience working with  
 23 clients who have experienced an unauthorized  
 24 disclosure of sensitive personal information.  
 25 Q So the four factors are developed totally

1 based on your experience; is that fair to say?  
 2 A Experience, yes.  
 3 Q Just so we can be clear, in developing the  
 4 four factors, did you consult any specific reports  
 5 or scholarly works in developing those four factors  
 6 as your analytic method?  
 7 A Can you be more precise?  
 8 Q So in developing -- you have got four  
 9 factors; is that fair to say?  
 10 A Yes.  
 11 Q So in developing those, I want to carve  
 12 out your experience, but in developing those four  
 13 factors did you consult any specific reports or  
 14 scholarly works to come to use these four factors  
 15 for your analytic method?  
 16 A These four factors were developed over the  
 17 course of seven or eight years working with our  
 18 clients, and their counsel.  
 19 Q Would you point to a specific timeframe  
 20 for those seven to eight years?  
 21 A 2005 to date.  
 22 Q So we are talking about nine years, I  
 23 guess?  
 24 A Well, I'm kind of -- let me count them,  
 25 yes.

1 Q Did you write any specific reports or  
 2 scholarly works with respect to these four factors?  
 3 A When we work with clients there is work  
 4 product under nondisclosure where our discussions  
 5 with their counsel and their response teams revolves  
 6 around discussion of these four factors.  
 7 Q So those works would have been developed  
 8 by counsel and you together; is that fair to say?  
 9 A Yes.  
 10 Q Apart from those types of written  
 11 documents did you draft any published reports or  
 12 scholarly works with respect to those four factors?  
 13 A No.  
 14 Q So it's fair to say that the documents we  
 15 are talking about are not written documents that  
 16 have been subjected to a peer review; correct?  
 17 A They are under nondisclosure agreements.  
 18 Q But they are not published -- so they are  
 19 not publicly issued; is that fair to say?  
 20 A Yes.  
 21 Q They are under a confidentiality order of  
 22 the court, perhaps?  
 23 A Confidentiality agreements of  
 24 nondisclosure; correct.  
 25 Q So they are written under a nondisclosure

1 agreement, not necessarily a court litigation-type  
 2 thing?  
 3 A Yes.  
 4 Q Have you issued -- if you already  
 5 testified to this, I apologize, but have you issued  
 6 an expert report in another litigation?  
 7 A No.  
 8 Q Have you worked as a consultant in any  
 9 other litigation?  
 10 A No.  
 11 Q When I say consulting, consulting expert  
 12 who has to testify is what I'm getting at, have you  
 13 worked as a consulting expert in any other  
 14 litigation?  
 15 A Can you be more precise?  
 16 Q Well, let's say you are a testifying  
 17 expert in this case; do you understand that?  
 18 A Yes.  
 19 Q In some cases there are people of learned  
 20 expertise who don't testify; do you follow what I'm  
 21 saying?  
 22 A Can you give me an example?  
 23 Q Well, they might perform support to  
 24 attorneys that are working in the case but they  
 25 never testify; do you follow?

1 A Give me an example.  
 2 Q That's an example, say in this case, say  
 3 the FTC has a consulting expert that they need to  
 4 help them because they are not experienced in the  
 5 field that you may be or you may not be, but they  
 6 are lawyers, they are not identity theft  
 7 experienced, let's say; are you following me?  
 8 A Yes, so far.  
 9 Q So say they had somebody who worked with  
 10 them that they could probably pay at a lower rate  
 11 than you to testify; do you follow?  
 12 A So far, yes.  
 13 Q Do you in your experience -- strike that.  
 14 In your experience have you worked as a  
 15 consulting expert to support litigation where you  
 16 did not testify?  
 17 A No.  
 18 Q In the matters where you have performed  
 19 services under confidentiality agreements I can  
 20 understand that you wouldn't be able to comment  
 21 about them; is that fair to say?  
 22 A Yes.  
 23 Q Are there other matters that you have  
 24 worked that are not subject to a nondisclosure  
 25 agreement that you can tell me about?

1 A In what context?  
 2 Q That you used, that you are basing your  
 3 four factor test?  
 4 A No.  
 5 Q In developing your four factor test that  
 6 is expressed on page 18 of your expert report, for  
 7 these four factors did you rely on any statistical  
 8 analysis in developing these four factors?  
 9 A No.  
 10 Q Apart from your personal experience did  
 11 you use any data in developing these four factors,  
 12 any specific data?  
 13 A No, it was based on my experience over the  
 14 11 -- nine years we calculated.  
 15 Q Do you give equal weight to each of the  
 16 four factors?  
 17 A No.  
 18 Q Which factors do you give greater weight  
 19 to in applying the four factors?  
 20 A It depends on the breach.  
 21 Q With respect to the alleged LabMD data  
 22 breaches involved in this case, the P2P disclosure,  
 23 alleged disclosure, and the Sacramento incident or  
 24 the Sacramento disclosure, with respect to those two  
 25 alleged breaches do you give heightened weight to, I

1 analysis on that one statement; correct?  
 2 A That's correct. Can I add one piece?  
 3 Q Sure, go ahead, absolutely.  
 4 A The second and third risk factors as  
 5 listed on page 19, I indicated there were four IP  
 6 addresses, where there was unrelated sensitive  
 7 consumer information that could be used to commit  
 8 identity theft. So in conjunction with the fact  
 9 that one of those IP addresses may have been  
 10 associated with an identity theft event or fraud was  
 11 one of the elements that went into my analysis of  
 12 the second and third factors.  
 13 Q All right, are you looking at the fourth  
 14 factor right now in testifying?  
 15 A No.  
 16 Q I'm sorry, I guess I'm not following you.  
 17 A I'm sorry.  
 18 Q When I saw you said the four factors I  
 19 immediately let town the page --  
 20 A Could you go back to the top of page 19,  
 21 your question earlier asks what I considered in my  
 22 analysis of the second and third factors.  
 23 Q Uh-huh, yes.  
 24 A And it includes the fact that four IP  
 25 addresses were found with unrelated sensitive

1 consumer information that could be used to commit  
 2 identity theft. In addition to the fact that as  
 3 Robert Boback testified, one may have been used  
 4 based on the arrest of the identify thief.  
 5 Q Okay, I think I'm following you now. So  
 6 right there you were pointing to the second full  
 7 sentence on -- second full sentence in paragraph one  
 8 on page 19, when you say, quote "In his testimony,  
 9 Boback said that the P2P insurance aging file was  
 10 found at four IP addresses along with unrelated  
 11 sensitive consumer information that could have could  
 12 be used to commit identity theft; that's what you  
 13 are pointing to right now; correct?  
 14 A Yes.  
 15 Q So that's in other parts of the deposition  
 16 where he talks about the four places; correct?  
 17 A That's correct.  
 18 Q So what you are doing is you are pointing  
 19 to other parts of the deposition for those --  
 20 A To help identify my analysis.  
 21 Q -- to assist in that analysis?  
 22 A Yes.  
 23 Q And my wrap up question is, you are still  
 24 talking about the universe of the deposition of  
 25 Mr. Boback, you didn't go external to Mr. Boback's

1 deposition to another --  
 2 A No.  
 3 Q -- another deposition; correct?  
 4 A Correct.  
 5 Q Okay. I would like to turn your attention  
 6 to the second full paragraph on page 19. So I'll  
 7 try to do this one, save your --  
 8 A Before you go there?  
 9 Q Sure.  
 10 A You were asking me about the four factors  
 11 that I had used to analyze the risk of harm and we  
 12 didn't talk about the fourth factor, which is in my  
 13 report.  
 14 Q We didn't talk about the fourth factor?  
 15 A No.  
 16 Q Well, we are going to get there, we are  
 17 going to talk about that now; okay?  
 18 A Perfect.  
 19 Q And I'm trying to go through all four,  
 20 thanks for --  
 21 A I'm just trying to stay on the thread.  
 22 Q Exactly. Under the heading of page 18  
 23 heading starts Analysis of P2P Disclosure I want to  
 24 draw your attention to the fourth risk factor as  
 25 it's written out on page 19, the second full

1 paragraph; do you see that paragraph?  
 2 A You need to help me, can you point me to  
 3 that?  
 4 Q Point you to the second full paragraph on  
 5 page 19.  
 6 A The fourth risk factor?  
 7 Q Yes, the paragraph that starts with the  
 8 fourth risk factor?  
 9 A Yes.  
 10 Q Do you see that in front of you?  
 11 A Yes.  
 12 Q On page 19 you also wrote in your expert  
 13 report that quote "The fourth risk factor is the  
 14 extent to which the risk of the consumers' personal  
 15 information has been mitigated. According to  
 16 Boback's testimony the P2P insurance aging file was  
 17 first found on the peer-to-peer network on  
 18 February 5, 2008, at IP address 68.107.85.250. It  
 19 was found again on November 5, 2008, at IP address  
 20 173.16.83.112; again on April 7, 2011, at IP address  
 21 201.194.118.82; and yet again on June 8th --"  
 22 A 9th.  
 23 Q I'm sorry, thank you, "on June 9th in 2011  
 24 at IP address 90.215.200.56. Boback also said that  
 25 Tiversa searched for the file in preparation for his

1 testimony on November 21, 2013, and still found the  
2 file available on the P2P network. LabMD did not  
3 mitigate the risk of identity crimes created by this  
4 unauthorized disclosure by notifying consumers. In  
5 my experience a significant number of these  
6 consumers had or could still fall victim to identity  
7 crimes since they have no way of independently  
8 knowing that LabMD disclosed their information  
9 without authorization for almost six years --" I'm  
10 sorry, "almost six years ago. This unauthorized  
11 exposure puts the affected consumers at a  
12 significantly higher risk of identity than the  
13 general public." Did I read that fairly, maybe not  
14 exactly correctly, but did I read that fairly?

15 A To clarify the last sentence reads, this  
16 unauthorized disclosure puts the affected consumers  
17 at a significantly higher risk of identity crimes  
18 than the general public.

19 Q Do you want to correct anything else I  
20 said just so we have it clear for the record?

21 A No.

22 Q Did you rely on any other evidence for  
23 your analysis of the four risk factors apart from  
24 Mr. Boback's testimony?

25 A Any evidence?

1 Q So for the specific point of your analysis  
2 of the fourth risk factor what I'm trying to draw  
3 your attention to, are you relying on something else  
4 in this case apart from Mr. Boback for your  
5 understanding, for your basis of saying that it was  
6 out there and available?

7 A No.

8 Q Just so we can clarify this before we go  
9 off the record, it's a pretty good point to break,  
10 it's about ten of noon right now, are you aware of  
11 any other evidence besides the Boback deposition of  
12 what IP addresses the insurance aging file was  
13 allegedly available on in the P2P network?

14 A Can you rephrase that?

15 Q Is there any other evidence that you  
16 looked at besides the Boback deposition of what --  
17 which says, what IP addresses the insurance aging  
18 file was allegedly available on a P2P network?

19 A Not that I can recall at this time.

20 Q And if you -- you can talk about it over  
21 lunch, but I just want to make sure that you are not  
22 pointing to some other document to get those IP  
23 addresses to nail down your fourth risk factor, if  
24 you are relying on something else I want to know it  
25 today just so we are on the same page, but in my

1 Q Any evidence or deposition testimony, did  
2 you rely on any other evidence for your analysis of  
3 the four risk factors?

4 A Other than Boback's testimony?

5 Q Yes.

6 A Yes.

7 Q What would that be?

8 A Federal Trade Commission documents.

9 Q What Federal Trade Commission documents,  
10 apart from the Boback deposition, indicated to you  
11 that the insurance aging file was available on a P2P  
12 network?

13 A When assessing the fourth risk factor I  
14 looked at where this information was, as Robert  
15 Boback testified, as well as what information was  
16 disclosed and how long it has been disclosed in  
17 order to provide a high risk assessment, risk of  
18 high, for this particular factor.

19 Q Okay, I think I'm tracking your answer.  
20 What I want to focus in on is your understanding of  
21 that file being available, so just for the specific  
22 point that the P2P disclosure for the 1718 files; do  
23 you understand what I'm saying, the insurance aging  
24 report?

25 A Yes.

1 reviewing the case and looking at your report it  
2 seems to me that just comes from the Boback  
3 deposition, so if you want to clarify after the  
4 break that's fine, but sitting here right now you  
5 are not aware of something else other than the  
6 Boback deposition that gave you the four ideas about  
7 risk?

8 A Not that I recall at this time.

9 Q And will you try to clarify that one  
10 before the end of the day if there is something  
11 else?

12 A Yes.

13 MR. HUNTINGTON: Let's take a break.  
14 (Whereupon, at 11:52 a m., the deposition  
15 was recessed, to be reconvened at 1:00 p m. this  
16 same day.)

17  
18  
19  
20  
21  
22  
23  
24  
25

1 AFTERNOON SESSION (1:07 p m.)  
 2 Whereupon,  
 3 RICHARD L. KAM  
 4 resumed the stand and, having been previously duly  
 5 sworn, was examined and testified further as  
 6 follows:  
 7 EXAMINATION (Resumed)  
 8 MR. HUNTINGTON: Let's go back on the  
 9 record.  
 10 MS. MEHM: Could we just note for the  
 11 record that we are resuming at approximately  
 12 1:08 p m. Eastern.  
 13 MR. HUNTINGTON: Before we went off the  
 14 record and during the morning we noted that the  
 15 court reporter might need some breaks, I'm going to  
 16 ask the court reporter specifically, if you need to  
 17 a take a break, just let me know. I understand you  
 18 have been diagnosed with pneumonia; correct?  
 19 THE REPORTER: Yes, thank you.  
 20 BY MR. HUNTINGTON:  
 21 Q I'm going to pull your expert report out  
 22 again, Mr. Kam, and draw your attention to page 19.  
 23 Before we went off the record for lunch we were  
 24 talking about the fourth risk factor; correct?  
 25 A Yes.

1 Q In that second full paragraph that starts,  
 2 the fourth risk factor is the extent to which the  
 3 risk of consumers' personal information has been  
 4 mitigated, you wrote that; right?  
 5 A Yes.  
 6 Q You see where I am in the report?  
 7 A Yes.  
 8 Q If you move down through the paragraph  
 9 through the IP addresses we were talking about, the  
 10 sentence that starts with LabMD and then the next  
 11 sentence starts, in my experience?  
 12 A Yes, I see that.  
 13 Q Okay. It says in my experience a  
 14 significant number of these consumers have or could  
 15 still fall victim to identity crimes; do you see  
 16 that, Mr. Kam?  
 17 A Yes.  
 18 Q Did you rely on any other source or method  
 19 of analysis besides consulting your experience in  
 20 writing that statement in your expert report?  
 21 A Can you rephrase that to make sure I  
 22 understand it.  
 23 (The reporter read the record as requested.)  
 24 BY MR. HUNTINGTON:  
 25 Q Where I said that statement I was keyed in

1 on quote, "In my experience, significant number of  
 2 these consumers have or could fall victim to  
 3 identity crimes," just focusing in on that quote of  
 4 yours, close quote after crimes, did you rely on any  
 5 other source or method of analysis besides  
 6 consulting your experience to draft that statement?  
 7 A To be clear, my experience is made up of  
 8 the work that I do at ID Experts over the nine  
 9 years, it includes the other experts that I work  
 10 with in the data breach response and victim  
 11 restoration arena over the last nine or ten years,  
 12 it includes the literature that exists and review of  
 13 that information, it includes the courses that I  
 14 take to maintain a Certified Information Privacy  
 15 Professional certification every year, it includes  
 16 the breadth of my experience over the -- a wide  
 17 range of educational and work experiences.  
 18 Q Given that as your definition of  
 19 experience, is there anything else that you are  
 20 relying on to make that statement?  
 21 A Not that I can recall at this time.  
 22 Q Are there any specific pieces of  
 23 literature that you are pointing to to make that  
 24 statement sitting here right now; do you think?  
 25 A If you review the literature review as

1 well as some of the white papers that I've had an  
 2 opportunity the work on, if you include those that  
 3 would probably extend and cover most of the things  
 4 that I brought to the table today.  
 5 Q Is there anything else that you can  
 6 identify, I mean that's in your expert report;  
 7 right?  
 8 A All of these things, yes.  
 9 Q Other than what is provided in your expert  
 10 report?  
 11 A No, like others, I read the newspaper, I  
 12 receive updates on various topics related to  
 13 privacy.  
 14 Q Are you done?  
 15 A Yes.  
 16 Q All right. In your experience might  
 17 people change their names over time?  
 18 A Yes.  
 19 Q Might people change addresses over time?  
 20 A Yes.  
 21 Q Might people change insurance providers or  
 22 plans over time?  
 23 A Yes.  
 24 Q Might people change financial institutions  
 25 over time?

1 to?

2 BY MR. HUNTINGTON:

3 Q Can you answer?

4 A I would ask that you be specific about

5 which piece of -- which breach we are talking about.

6 Q Start with the P2P, is there any proof

7 that even one fraudulent account has been opened as

8 a result of the alleged P2P breach?

9 A I was asked to estimate the likely injury

10 to consumers by the Commission, as I stated earlier.

11 Q And you only did what you were asked to;

12 right?

13 A Yes.

14 Q For your report purposes?

15 A Yes.

16 Q So if we can take apart from your report

17 purposes, have you been told that there exists proof

18 that even one account has been opened as a result of

19 the P2P breach by the FTC?

20 A I only did as the FTC asked because to

21 estimate the likely injuries based on the facts that

22 I was presented with.

23 Q But that's not my question, I asked you if

24 they had told you that there exists proof that one

25 fraudulent has been opened as a result of the P2P

1 breach?

2 A I don't recall them telling me, no.

3 Q And I asked the same question with respect

4 to the Sacramento incident, is there any proof that

5 even one fraudulent account has been opened as a

6 result of the Sacramento incident?

7 A I don't recall them telling me if there

8 were.

9 Q Let's take like three-minutes.

10 (1:47 p.m. -- recess -- 1:56 p.m.)

11 BY MR. HUNTINGTON:

12 Q We can go back on the record. Mr. Kam,

13 before we took a break we were talking about, a

14 couple steps back we were talking about page 19, I

15 would like to turn your attention to page 19 of your

16 expert report.

17 A Yes.

18 Q Under the heading quote "Harm from the P2P

19 disclosure," close quote, and the subheading

20 Estimated Financial Out-of-Pocket Cost to Victims of

21 Medical Identity Theft, we were talking a little bit

22 about this paragraph before we took a break;

23 correct?

24 A Yes.

25 Q It says there that quote, "According to

1 the findings of the 2013 survey on medical identity

2 theft by Ponemon Institute 0.0082 is the estimated

3 base rate for medical identity theft in the U.S.

4 This represents the proportion of consumers who

5 indicated that they were medical identity victims as

6 drawn from a representative panel of 5000 adult aged

7 U.S. consumers.

8 "Therefore, 9300 breached records times

9 0.0082 equals 76, the estimated number of victims

10 for medical identity theft"; did I read that

11 correctly?

12 A Yes.

13 Q In this calculation the 76, the number 76

14 there on page 19 as the product, I guess that is,

15 product of your calculation, is that a calculation

16 specific for LabMD, 76?

17 A Yes.

18 Q That's your estimated number for LabMD for

19 the --

20 A For the P2P disclosure.

21 Q For the P2P, not the Sacramento but for

22 the P2P disclosure?

23 A Yes, by my analysis, yes.

24 Q The next paragraph down the paragraph goes

25 on to say, below the calculation it goes on to say

1 that quote "The Ponemon study also found that

2 36 percent of victims of medical identity theft paid

3 an average of \$18,660 as out-of-pocket costs"; did I

4 read that correctly?

5 A Yes.

6 Q On page 19 it goes on to state that --

7 starts out on page 20, it says, "Therefore: 9300

8 breach victims times 0.0082 base rate times .36, I

9 should say 0.36, equals 27 potential victims who

10 would have to pay the average of \$18,660 in

11 out-of-pocket costs, consumers' out-of-pocket costs

12 would exceed \$500,000"; did I read that correctly?

13 A Yes.

14 Q So this report is a result of your careful

15 consideration of your expertise in the subject area;

16 right, based on your experience?

17 A And the material from the Federal Trade

18 Commission.

19 Q The documents they gave you?

20 A The documents as well as --

21 Q The deposition and the information on

22 pages six to eight of this expert report; correct?

23 A That's correct. You forgot the literature

24 review.

25 Q Okay, and that are in the expert report;

Page 106

1 networks. These estimates should be viewed as a  
2 floor versus universe of potential harms that could  
3 befall the 10,000 affected consumers.  
4 Q Okay. I want to circle back to your  
5 calculations.  
6 A Where are you referring to?  
7 Q Page 19, the multiplication includes the  
8 base rate, the base rate for the general U.S.  
9 population; right?  
10 A It was derived based on the U.S.  
11 population based on the Ponemon methodology.  
12 Q But it has no significant with respect to  
13 the LabMD documents?  
14 A Other than it would estimate the likely  
15 number of potential medical identity theft victims  
16 given a U.S. population.  
17 Q That's the number that's found in the  
18 entire U.S. population, the rate of people in  
19 Washington, D.C. is not any different than the rate  
20 that you have expressed here as to being  
21 LabMD-specific; correct?  
22 MS. MEHM: Counsel, am I hearing a  
23 question there?  
24 THE WITNESS: Can you be more precise?  
25 BY MR. HUNTINGTON:

Page 107

1 Q You are giving me a number for the LabMD  
2 alleged data breach. You are estimating 76;  
3 correct?  
4 A Yes.  
5 Q That's the general U.S. population; right,  
6 that's not the LabMD, there is no calculation that  
7 differs from the general of the rate of the  
8 population of the United States and Atlanta, and  
9 Sacramento, and Texas; correct, that's the general  
10 U.S. rate, one and the same, it's not tied with the  
11 LabMD case in any way, shape, or form; is it?  
12 A It is a rate that I used to apply an  
13 estimate based on the best research available.  
14 Q You have given me the U.S. base rate as an  
15 estimate based on the U.S. base rate for medical  
16 identity fraud; right?  
17 A Yes.  
18 Q You have not given me anything that is new  
19 or different with respect to this case, this case  
20 being the LabMD matter, for alleged breach?  
21 A Be more precise, I'm not giving you  
22 anything, what does that mean?  
23 Q Anything. You have just given me the  
24 general population rate for medical identity fraud;  
25 correct?

Page 108

1 A Yes, I have. Isn't the LabMD patient in  
2 the U.S.?  
3 Q Correct. So you are just, you have  
4 described a number to this, being specifically  
5 tailored to this case, when all you have done is  
6 given me the general population rate; correct?  
7 A I used the best information available to  
8 create an estimate of likely injury based on 9300  
9 consumers being affected by medical identity theft.  
10 Q So your opinion is that the number of the  
11 patients whose identity was allegedly exposed in the  
12 LabMD document who have quote/unquote "likely been  
13 harmed" and the amount of the projected injury,  
14 that's exactly equal to the number and amount that  
15 you would expect to see in the U.S. adult  
16 population; correct?  
17 A Yes.  
18 Q Can you demonstrate for me in any way,  
19 shape, or form that more than 90, I'm sorry, that  
20 more than 76 of the 9300 of the patients whose data  
21 was allegedly exposed in the LabMD document, the P2P  
22 number, the P2P document, can you demonstrate that  
23 any of them have been actual victims of identity  
24 theft since the disclosure?  
25 A I was asked by the Commission to do an

Page 109

1 assessment of the likely injury of medical identity  
2 theft. I used the Ponemon Institute survey  
3 specifically on medical identity theft to establish  
4 a base rate, we which equals 76 consumers.  
5 Q So it's fair to say that I'm going to  
6 expect at trial that you are not going to attempt to  
7 demonstrate the actual or provide -- strike that.  
8 At the trial of this matter you are not  
9 going to try to demonstrate that more than 76 of the  
10 9300 of the patients whose data was allegedly  
11 exposed in the LabMD P2P document have been actual  
12 victims of identity theft since the alleged  
13 disclosure; correct?  
14 A Medical identity theft.  
15 Q Correct.  
16 A And for clarification, this specific  
17 calculation looks at the estimated number of medical  
18 identity theft victims and the potential of  
19 out-of-pocket financial costs.  
20 Q But you are not going to be testifying to  
21 the actual victims of identity theft since the date  
22 of disclosure; correct?  
23 A No.  
24 Q Would there be a way for you to  
25 demonstrate that more than 76 of the 9300 folks

Page 110

1 whose data was allegedly exposed in the LabMD P2P  
2 document have been actually victims of identity  
3 theft since this disclosure?  
4 A The Commission didn't ask me to reach out  
5 to the individuals who were affected by the P2P  
6 disclosure.  
7 Q And you didn't do that; correct?  
8 A No.  
9 Q And you don't expect to do that before the  
10 trial in this matter; correct?  
11 A No.  
12 Q That's not part of your expert opinion;  
13 correct?  
14 A Yes.  
15 Q Would you just flip back to the front page  
16 of the report itself, the Ponemon report, again, if  
17 you would just testify for the record what the title  
18 of the report is?  
19 A It is the 2013 survey On Medical Identity  
20 Theft.  
21 Q Do you know what year it uses for its data  
22 set?  
23 A 2013.  
24 Q Are you aware of the year of the alleged  
25 P2P incident by LabMD.

Page 111

1 A Yes.  
2 Q What year was that?  
3 A The first discovery was February 5th,  
4 2008. There were multiple discoveries after that,  
5 including up to the point where Robert Boback  
6 testified that he had done a search for the P2P  
7 disclosure file, and found it also in 2013 before  
8 his testimony.  
9 Q And we talked about that this morning;  
10 right, that's the Boback testimony where he finds it  
11 in multiple places, at least four times in 2008;  
12 correct?  
13 A 2008, 2011, 2013 most recent version.  
14 Q My question is more to the initial  
15 incident, as best we know from the testimony in this  
16 case, 2008; correct?  
17 A The initial disclosure --  
18 Q Alleged?  
19 A -- alleged disclosure based on the facts  
20 that I was presented with was February 5th, 2008,  
21 but the data as I mentioned earlier is still  
22 available on P2P networks to this day according to  
23 Robert Boback.  
24 Q As best you know from reviewing his  
25 deposition testimony; correct?

Page 112

1 A Those were the facts I was presented with,  
2 yes.  
3 Q Have you spoken to Mr. Boback with respect  
4 to this --  
5 A No.  
6 Q -- this case, you haven't spoken with him?  
7 A Correct.  
8 Q So you based your calculations on the  
9 Ponemon survey; correct?  
10 A Yes.  
11 Q And so you believe the Ponemon survey to  
12 be accurate; correct?  
13 A I believe it to be reliable.  
14 Q You believe it to be accurate?  
15 A Reliable.  
16 Q So you are not so certain that it's  
17 accurate, you believe it's reliable?  
18 A It's the best information available and I  
19 believe it to be reliable.  
20 Q But you don't know if it's accurate or  
21 not?  
22 A I believe it to be reliable.  
23 Q If you would turn to page five of the  
24 Ponemon survey. If you would turn to page five, it  
25 says quote, "The number of medical identity theft

Page 113

1 victims increased, Table 1c shows that the number of  
2 new cases over the past year is estimated at  
3 313,000. This estimated increase in the base rate  
4 of --  
5 A I'm sorry, where are you reading, from the  
6 Ponemon study, that's where you are --  
7 Q Yes, I'm sorry, go back to page five, my  
8 apologies, the second full paragraph, see how it  
9 starts with a paragraph, there is table 1b, and then  
10 there is another paragraph in between the two  
11 tables?  
12 A Yes.  
13 Q That's where I'm reading; okay?  
14 A Yes.  
15 Q So let me start again. If you turn to  
16 page five in that paragraph, it says quote "The  
17 number of medical identity theft victims increased.  
18 Table 1c shows that the number of new cases over the  
19 past year is estimated at 313,000. This estimated  
20 increase in the base rate of identity theft victims  
21 climbed from .0068 to .0082 which represents a  
22 19 percent increase over one year. Did I read that  
23 correctly?  
24 A Yes.  
25 Q Okay. Looking at the table beneath this

Page 150

1 Q In preparing for your deposition today did  
2 you review the deposition of Eric Garcia?  
3 A Eric Garcia, the name is not familiar to  
4 me.  
5 Q If you would turn to page 22 of your  
6 expert report, sir?  
7 A Yes.  
8 Q I'm going to skip ahead to page 23. On  
9 page 23 you discuss the 600 some odd Social Security  
10 numbers of the patients whose data was allegedly  
11 exposed in Sacramento; correct?  
12 A Are you referring to the second paragraph?  
13 Q Yes.  
14 A Yes.  
15 Q With respect to that paragraph you just  
16 pointed to under the heading use of SSNs and day  
17 sheets have you -- strike that, how can you be sure  
18 you have eliminated all of the name changes that are  
19 relevant to this matter?  
20 A So the process started with an analysis of  
21 the Federal Trade Commission's report, reviewing all  
22 of the names contained in the document, which  
23 numbered approximately 600 in total, and I spent  
24 several hours reviewing that document to identify  
25 misspellings, typos, potential name changes because

Page 151

1 of marriage.  
2 Q You personally worked through the  
3 document?  
4 A Yes.  
5 Q Are you, to the best of your ability,  
6 certain that you evaluated all of the name changes?  
7 A To the best of my ability, yes.  
8 Q Based on your experience?  
9 A Yes.  
10 Q Did you analyze any evidence of the  
11 likelihood that two names using the same SSN is due  
12 to identity theft?  
13 A Yes.  
14 Q What did you do?  
15 A I evaluated all of the names in the da  
16 sheets and looked at those that had multiple uses,  
17 and based on whether there were different names,  
18 dates of birth, genders, addresses, did my best to  
19 determine whether or not I felt they may be at risk  
20 of identity theft.  
21 Q Once you had eliminated or made your  
22 eliminations from that set, are you saying that you  
23 can say for certain for causation purposes that the  
24 multiple names using the same Social Security number  
25 is due to identity theft?

Page 152

1 A I estimate the likelihood that  
2 approximately 100 individuals whose Social Security  
3 numbers have multiple people associated with them  
4 could be victims of identity theft.  
5 Q They could be but you don't know  
6 definitely; correct?  
7 A Yes.  
8 Q Did you analyze any evidence of what the  
9 base rate is among the general population for the  
10 likelihood of two names using the same SSNs and  
11 compare that to the rate among the patients whose  
12 data was allegedly exposed in the Sacramento?  
13 A Do you want to repeat the question,  
14 please.  
15 (The reporter read the record as requested.)  
16 THE WITNESS: Yes.  
17 BY MR. HUNTINGTON:  
18 Q How did you do that?  
19 A I looked at two sources to compare with  
20 what I found in the FTC analysis.  
21 Q What were those two sources?  
22 A One of the sources is indicated in my  
23 literature review, which is the Bureau of Justice  
24 Statistics' recent report on identity theft, which  
25 indicates that 6.7 percent of the population fall

Page 153

1 victim to identity theft or had fallen victim to  
2 identity theft in 2012. And I also considered the  
3 2013 Javelin Research report that I mentioned  
4 earlier in my expert report that indicates that one  
5 in three consumers whose Social Security numbers  
6 have been compromised by a breach fell victim to  
7 medical -- or to identity theft in 2013.  
8 Q Is that calculation performed here in the  
9 area of your report that provides information with  
10 respect to the alleged Sacramento incident?  
11 A No.  
12 Q Why not?  
13 A When I looked at the information that  
14 would be useful to determine whether there is a  
15 possibility that the consumers that were identified  
16 in the 40 LabMD day sheets might be victims of  
17 identity fraud I used my analysis of the Federal  
18 Trade Commission report as the basis for my opinion,  
19 as -- which is on page 23.  
20 Q And what on page 23 is your expressed  
21 opinion on that topic, if you could point that out?  
22 A Starting with the paragraph the Federal  
23 Trade Commission analysis of the approximately 600  
24 Social Security numbers using the clear database  
25 reveal that 314 Social Security numbers had multiple

Page 154

1 names listed. I eliminated those that were due to  
2 misspellings, name changes and typos, leaving  
3 approximately 100 Social Security numbers that  
4 appear to have been used by people with different  
5 names.  
6 More than one individual using the same  
7 Social Security number is an indicator that identity  
8 thieves may have used this information to commit  
9 identity theft.  
10 Q And you just read that first paragraph  
11 under that heading use of SSNs and day sheets;  
12 correct?  
13 A Yes.  
14 Q I think I'm asking you something a little  
15 bit different, what I would like to know is whether  
16 you ever determined what the base rate is of the  
17 general population for having two names associated  
18 with the same SSN?  
19 A Are you being specific to identity theft?  
20 Q Yes.  
21 A No.  
22 Q Without adjusting for the base rate how  
23 can you know whether the number of patients whose  
24 data was allegedly exposed in the Sacramento is  
25 statistically higher than expected?

Page 155

1 A Can you point me where that is referenced?  
2 Q I'm just asking a general question, I'm  
3 looking for an answer, I'm not seeing it in your  
4 report, so I'm just asking you the question, and  
5 perhaps it is in there, perhaps not, perhaps it's  
6 just a bad question, I'm just looking for your  
7 answer. What I'm asking is, without adjusting for  
8 the base rate how can you know whether the number of  
9 patients whose data was allegedly exposed in  
10 Sacramento is statistically significantly higher  
11 than expected?  
12 A The approach that I used was to actually  
13 look at the facts from the case that were provided  
14 by the Federal Trade Commission through this report,  
15 to provide my best estimate of the likely victims of  
16 identity fraud from the Sacramento disclosure.  
17 Q And what is that estimate?  
18 A Approximately 100 individuals.  
19 Q Based on your experience?  
20 A Yes, and the facts that were presented by  
21 the Federal Trade Commission.  
22 Q Do you still have the Ponemon survey  
23 somewhere there in front of you, Mr. Kam?  
24 A Yes.  
25 Q With respect to the Ponemon survey you

Page 156

1 cite to the Ponemon survey throughout your report,  
2 throughout your expert report; correct?  
3 A Yes.  
4 Q You believe it's --  
5 A Besides other reports.  
6 Q True, but I'm just switching back to the  
7 Ponemon survey, it's cited throughout your report in  
8 various places; is that fair to say?  
9 A Yes.  
10 Q Yes?  
11 A Yes.  
12 Q Do you believe it's accurate; is that fair  
13 to say?  
14 A I think I have said I believe it's  
15 reliable.  
16 Q You did say that. So you consider it  
17 reliable; correct?  
18 A Yes.  
19 Q Trustworthy?  
20 A If trustworthy equals reliable, yes.  
21 Q And you rely on it because if I'm  
22 understanding your prior testimony, you believe that  
23 it provides the best data to aid you in your  
24 analysis of the LabMD case; is that fair?  
25 A As one of the reports I relied on, yes.

Page 157

1 Q Page 27 of the Ponemon study, I will read  
2 this for the record, but on the second paragraph  
3 down, paragraph that starts, Many cases, second  
4 paragraph says, Many cases of medical identity theft  
5 reported in this study result from the sharing of  
6 personal identification with family and friends. In  
7 some cases family members take the victim's personal  
8 credentials without consent. Rarely does it occur  
9 from data breaches, malicious insiders and identity  
10 thieves or loss of medical credentials. This  
11 finding that medical identity theft was a family  
12 affair consistent with previous studies conducted by  
13 Ponemon Institute. Did I read that fair fairly and  
14 correctly?  
15 A Yes.  
16 Q Do you agree with that?  
17 A Yes.  
18 Q So a large part of the medical identity  
19 theft is by family members?  
20 A I believe what Ponemon's research found  
21 specifically is that there is a percentage, which we  
22 can turn to the page in a second, that is committed  
23 by family members.  
24 Q Do you know where that page is in the  
25 Ponemon survey?

Page 174

1 A No.  
2 Q What did your sponsorship of the Ponemon  
3 Institute entail financial?  
4 A We provide -- we paid for the development  
5 or the publication of the report.  
6 Q How much did you pay for the publication?  
7 A Which report are you referring to?  
8 Q Well, if you break it out, for each  
9 report?  
10 A Let's see, for patient data privacy  
11 report, roughly \$50,000.  
12 Q And for the other report how much would  
13 that have entailed financially?  
14 A Approximately \$12,500.  
15 Q Approximately \$12,500?  
16 A Yes.  
17 Q What was ID Expert's role in the survey if  
18 there was one, apart from financial support?  
19 A Sponsorship specifically.  
20 Q So you got your name on the report; is  
21 that fair to say?  
22 A Yes.  
23 Q So you got some advertising out of that  
24 sponsorship?  
25 A Yes.

Page 175

1 Q Did you have a personal relationship with  
2 Larry Ponemon?  
3 A What do you mean personal, can you be more  
4 specific?  
5 Q Do you know him personally apart from your  
6 business relationship?  
7 A No.  
8 Q Do you -- I just want to lay foundation,  
9 do you have a business relationship with  
10 Mr. Ponemon?  
11 A In the sponsorship of these two reports,  
12 yes.  
13 Q Are you aware that Larry Ponemon is a  
14 Tiversa board member?  
15 A I recall hearing that somewhere, yes.  
16 Q You don't know that, you just heard that?  
17 A I just heard that.  
18 Q Do you have a relationship, contractual or  
19 otherwise, to Tiversa?  
20 A No.  
21 Q Are you familiar with Mike Daugherty's  
22 book?  
23 A No.  
24 Q When I say Mike Daugherty do you know who  
25 I'm referring to?

Page 176

1 A Yes.  
2 Q The CEO of LabMD?  
3 A Yes.  
4 Q Are you aware of LabMD claims against  
5 Tiversa?  
6 A None of the specifics.  
7 Q Are you aware of them in a general nature?  
8 A Only what I read in the newspaper.  
9 Q What did you read in the newspaper?  
10 A That LabMD is suing or was suing Tiversa.  
11 Q Do you know the basis of those claims  
12 between the two companies, Tiversa and LabMD?  
13 A No.  
14 Q What is your relationship, contractual or  
15 otherwise, to Javelin Strategies and Research.  
16 A I purchased two of their reports.  
17 Q Do you remember how much those reports  
18 cost?  
19 A To the best of my recollection I believe  
20 the 2013 Javelin Research report was \$3500, and the  
21 Javelin 2012 report was \$3,000.  
22 Q 3000? Do you have any other relationship  
23 with Javelin Strategy and Research other than buying  
24 those two reports?  
25 A No.

Page 177

1 Q What is your relationship, contractual or  
2 otherwise to the Federal Trade Commission?  
3 A I was engaged to provide an expert report.  
4 Q Do you have any other business  
5 relationship with the FTC apart from your retention  
6 as expert in this case?  
7 A No.  
8 Q Are any internal or external studies  
9 sponsored by ID Experts funded in part or whole with  
10 FTC grants?  
11 A No.  
12 Q Do you have an understanding as to how you  
13 were selected as an expert witness by the FTC?  
14 A They saw me present at one of their  
15 conferences.  
16 Q Which conference was that?  
17 A It was May 7th, 2013, on senior identity  
18 theft.  
19 Q And who did you meet with at that  
20 conference?  
21 A Megan Cox.  
22 Q Anyone else?  
23 A Not that I recall at this time.  
24 Q With respect to your retention as an  
25 expert for the LabMD matter were you recommended by

# Exhibit D

**In the Matter of:**

LabMD, Inc.

*November 21, 2013*

*Robert J. Boback*

**Condensed Transcript with Word Index**



**For The Record, Inc.**

**(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555**

