WORLD PRIVACY FORUM

4 Monroe Parkway
Suite K
Lake Oswego, OR 97035

FTC PrivacyCon 2018

Request to Present New Research Regarding Medical Identity Theft

I am pleased to make a request to present new research about medical identity theft. This work updates our understanding of how medical identity theft occurs, where, and what the new vulnerabilities are. This is new research.

I have researched medical identity theft for more than a decade. In 2005, I coined the term "medical identity theft." In 2006, I published the first major report about the issue. I have been doing substantive work refining my early knowledge of this crime, and believe the new research and findings are highly relevant to the FTC's work and are in the public interest. I have published a very small portion of this research in a special issue of Springer-Nature in 2017, with the broader report to come out later this year or early 2018.

I. Contact Information

Pam Dixon Executive Director,
World Privacy Forum

www.worldprivacyforum.org

II. Title and Extended Abstract:

The Modern modus operandi of Medical Identity Theft*: updating benchmarks to include biometric spoofs and complex geographic patterns of the crime*

Medical identity theft is unique in its *modus operandi*, which typically creates alterations to health files as a consequence of the activities of the crime. Due to the health harms that

can result from alterations to medical files, this crime is particularly important to detect and resolve. Today, with just over a decade of clear public discussion of this crime, criminals still typically alter victims' health care records as part of the process of committing the crime. This has not changed. What has changed, however, are other aspects of the *modus operandi* of medical identity theft. These changes have created a new set of risk patterns, and corresponding requirements for updated responses and mitigations. The new patterns are complex, but understandable, and there is much that could be done to combat the newest iterations of this crime. This research documents these shifts and new fact patterns.

To uncover and understand the fact patterns, this research analyzed the legal and geographic patterns of medical identity theft based on FTC FOIA data, DOJ data on healthcare fraud prosecutions, and additional public source data. Additionally, the research included interviews with health care providers, victims, and biometric experts.

In comparing and analyzing these data sets, the research has revealed striking patterns and findings, two of which I would like to highlight here:

- First, medical identity theft has strong geographically-linked patterns. There is a baseline set of consistent geographic patterns, which are readily understandable, and which this research seeks to document. But there are now also substantial "hot spots" for this crime that flare into existence in ways that are unpredictable. This research documents the "flares" of criminal medical identity theft activity over several years.
- Second, in attempting to solve the crime of medical identity theft, as well as attempting to properly identify patients, health care providers have begun to turn to biometric identification systems as a solution to identification and authentication. These systems can, however, become a source of a new and challenging variant of medical identity theft based on biometric spoofing and morphing. This research coins the term "biometric identity theft" to describe the suite of problems that criminals can create by abusing biometric systems operated by health care providers. This is a particularly challenging new wrinkle in the crime.

These findings refine the understanding of modern medical identity theft threat vectors

and point to improvements that can be made to solve for the problems these risks present.

Other available research in the general area of medical identity theft includes commercially sponsored medical identity theft research; commercially sponsored research in this area generally has a focus on economic consequences and other issues such as documenting the size of the problem, and the efficacy of credit report monitoring. This research includes economic analysis and it also includes a broader set of benchmarks, including the new risks, and documentation of geographic patterns of the crime.

This research will be published in late 2017 or early 2018.

III. Publication details of my prior research in this area

A. Springer-Nature, Special Issue on Heath Privacy: June, 2017, peer-reviewed. *A Failure to Do No Harm: India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.* Pam Dixon, Springer Nature, *Health Technology*. DOI 10.1007/s12553-017-0202-6. http://rdcu.be/tsWv. Open Access via Harvard-Based *Technology Science*: https://techscience.org/a/2017082901/. This original research paper is focused on biometric issues, and I include it here because one segment of the research discussed the problems of biometric spoofing and "biometric identity theft" in the health care context.

B. Medical Identity Theft Report: *Medical Identity Theft, The Information Crime that can Kill You*, Pam Dixon, World Privacy Forum, 2006. http://www.worldprivacyforum.org/wp-content/uploads/2007/11/wpf_medicalidtheft2006.pdf

C. NCVHS testimony, first known testimony on medical ID theft: Testimony of Pam Dixon*, Electronic Health Records and the National Health Information Network: Patient Choice, Privacy, and Security in Digitized Environments Before The National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy and Confidentiality*, August 16, 2005. http://www.worldprivacyforum.org/wp-content/uploads/2005/08/pamdixonNCVHStestimonyfinal.pdf.

D. 1 FAQ for Victims of Medical Identity Theft : *FAQ: Medical ID Theft: How to*

Recover if You're A Victim -- And What to Do if You are Worried about Becoming a Victim, Bob Gellman and Pam Dixon, World Privacy Forum, https://www.worldprivacyforum.org/2012/04/faq-victims-of-medical-id- theft/

D. 2 Consumer Tips for Victims of Medical Identity Theft: < https://www.worldprivacyforum.org/2012/04/consumer-tips-medical-id-theft- what-to-do-if-you-are-a-victim/

E. Medical Identity Theft, Mapped by City: https://www.worldprivacyforum.org/2011/08/medicalidentitytheft-map/

IV. Description of Demonstration

I will present and discuss research findings, and as part of that, I will present a sequence of data visualizations showing the growth and regionality of the crime, with an explanations of the regional patterns. I will also present on biometric morphing and spoofing in the health care setting.

V. Conclusion and Funding Sources

Thank you for your consideration of this research. If you would like more information about this research, please do not hesitate to contact us.

This research was funded by a cy pres restitution grant, and this funding is neither tied to nor sponsored by any corporation or business entity. The cy pres was granted to the World Privacy Forum, which is a 501C3 non-profit public interest research group and is the direct funder of this research.

This research has been conducted in the public interest, and will advance the understanding of the crime of medical identity theft. Multiple implications arise from this research, including implications for how to detect, deter, and cure the harms of this crime.

Respectfully submitted,

Pam Dixon
Executive Director,
World Privacy Forum