WORLD **PRIVACY** FORUM

Non-profit, non-partisan public interest research group focused on in-depth research and reports

September 18, 2006

Federal Trade Commission
Office of Comptroller of the Currency
Board of Governors of the Federal Reserve Board
Federal Deposit Insurance Corporation
Office of Thrift Supervision
National Credit Union Administration

Re: Comments of the World Privacy Forum on Proposed Regulations on Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003

FTC Project No. R611019, RIN 3084-AA94
OCC Docket Number 06-07, RIN 1557-AC87
FRB Docket Number R-1255
FDIC RIN 3064-AD00
OTS No.2006-19, RIN 1550-AC04
NCUA Proposed Rule 717

The World Privacy Forum respectfully submits the following comments on the proposed Identity Theft Red Flags Rule pursuant to the joint notice of proposed rulemaking published in the Federal Register July 18 2006, ***Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003***.[1]

The World Privacy Forum is a non-profit, non-partisan public interest research organization.[2] It focuses on in-depth research and analysis of privacy topics, including topics in medical and financial privacy. The Forum has been actively engaged in the area of medical privacy; the Forum has testified before The National Committee on Vital and Health Statistics (NCVHS) on the privacy and confidentiality of electronic health records and the proposed National Health Information Network. In May 2006 the World Privacy Forum published the first major report on

[1] 16 C.F.R. Part 681: Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003: Joint Notice of Proposed Rulemaking, With the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, and the National Credit Union Administration.

[2] <http://www.worldprivacyforum.org>.

medical identity theft.[3] In 2005, the Forum published two reports focused on issues relating to AnnualCreditReport.com.[4]

Summary of Comments:

- Medical identity theft is not adequately recognized in the proposed rule, in fact, it is not recognized at all despite its substantial contribution to problems stemming from identity theft.
- Medical identity theft is not adequately recognized by the health care industry, by federal agencies, or by state agencies. This lack of attention, if continued, could serve to allow the crime to increase and cause pubic health, safety, and financial issues as well as increased financial sector risks.
- The draft Red Flag rule does not identify health care providers as creditors and as users of consumer reports; this needs to be addressed.
- Red Flag principles must apply to those who maintain medical records, however this has not been made explicitly clear in the proposed Red Flag rule.
- The draft rule needs to be specifically integrated with the health privacy rule for enforcement and other purposes.
- There is a need for specific health care-context examples in Appendix A of the draft rule.

I. Medical Identity Theft is not Adequately Recognized by the Health Care Industry or Federal and State Agencies

Medical identity theft is a significant problem and one that is not adequately recognized by the health care industry or by federal and state agencies that have responsibilities for identify theft matters. Medical identity theft is a crime that can cause great harm to its victims. Despite the profound risk it carries, it is the least studied and most poorly documented of the cluster of identity theft crimes.[5] It is also the most difficult to fix after the fact, because victims have limited rights and recourses. Medical identity theft typically leaves a trail of falsified information in medical records that can plague victims' medical and financial lives for years.

Medical identity theft is both an information crime and a health crime. In this crime, a victim's medical identity is stolen or appropriated in some way. Victims' financial life may be impacted, and there may be other complicating factors. Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity – such as a Social Security Number-- without the victim's knowledge or consent to obtain medical services or goods, or when someone uses an individual's identity to obtain money by falsifying claims for medical services and falsifying medical records to support those claims.

---

[3] Pam Dixon, Robert Gellman, *Medical Identity Theft: The Information Crime that Can Kill You,* World Privacy Forum, May 3, 2006. < http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf>.

[4] Pam Dixon, *Call Don't Click Update: Still be smart about ordering Federally mandated free credit reports,* World Privacy Forum, July 14 2005. < http://www.worldprivacyforum.org/pdf/wpfcalldontclickpt2_7142005.pdf> and *Call Don't Click: Why it's smarter to order federally mandated free credit reports via telephone, not the Internet*, World Privacy Forum, February 25, 2005. <http://www.worldprivacyforum.org/pdf/wpf_calldontclick_study_2005.pdf>.

[5] For a description of identity theft crimes and statistics about the incidence of these crimes, see Federal Trade Commission, Identity Theft Survey Report (Sept. 2003). The complete report is available at: <http://www.consumer.gov/idtheft/pdf/synovatereport.pdf>.

Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim's name. Victims of medical identity theft may also experience the now-familiar consequences of financially oriented forms of identity theft.

Research shows that victims of medical identity theft may receive the wrong medical treatment, find their health insurance exhausted, and could become uninsurable for both life and health insurance coverage. They may fail physical exams for employment due to the presence of diseases in their health record that do not belong to them, and they may experience loss of credit or bankruptcy. They may receive dunning notices for treatment they never received, and may not be able to clear their names due to poor understanding and knowledge of this crime. Unambiguous evidence exists that this crime is being committed, and that these harms are already occurring.[6]

Today, victims of medical identity theft are falling through several existing gaps in consumer and medical arenas. The medical world seldom focuses on financial identity theft, with few knowing the complexities of how to help victims with error reporting problems and so on. Financial identity theft experts are seldom experts in the federal health privacy rule known as HIPAA[7] or in the complexities of the medical care treatment and payment systems. The Federal Trade Commission (FTC), which has studied financial identity theft, is not responsible for addressing medical issues. That falls to the Department of Health and Human Services, which has not published focused studies or guidance about medical identity theft in particular. The HHS Office of Inspector General investigates cases of generalized health care fraud and abuse, which may only touch the issue tangentially.

These gaps, which to date have been inadvertent and unintentional, must be closed. Close attention must be paid to the problem of medical identity theft and its victims by Federal and State governments, by the financial sector and by the health care sector, among other stakeholders. A pathway of clear, meaningful and effective recourse, and prevention and detection techniques will include appropriate inclusion of medical identity theft as a Red Flag issue.

Medical identity theft is not as well known as financial identity theft yet. But the lack of knowledge about this issue does not diminish its importance, nor does it diminish the need for specific Red Flag rules specifically addressing medical identity theft.

---

[6] See World Privacy Forum Medical Identity Theft 2006 report pages 6-8; 19-30. See also: United States v. Skodnek, 933 F. Supp. 1108, 1996 U.S. Dist. LEXIS 9788 (D. D. Mass. 1996). See also Comment of L. Weaver in Federal Trade Commission, Identity Theft Victim Assistance Workshop, (Aug. 18, 2000),<http://www.ftc.gov/bcp/workshops/idtheft/comments/weaverlind.htm>. See also Office of Inspector General, Health and Human Service, Criminal Actions (Sept. 2005), <http://oig.hhs.gov/fraud/enforcement/criminal/05/0905.html>.

[7] The Federal health privacy rule was issued by the Department of Health and Human Service under authority granted by the Health Insurance Portability and Accountability Act of 1996. The privacy rules were first issued in 2000 and became effective in 2003. There are also HIPAA rules for security. More information and copies of all the HHS rules and publications can be found at the website of the Office of Civil Rights, which is the HHS agency responsible for enforcement of the HIPAA privacy rule. <http://www.hhs.gov/ocr/hipaa/>.

II. The Draft Rule Does Not Identify Health Care Providers and Creditors and Users of Consumer Reports

It is understandable that the proposed Red Flag rule focuses largely (albeit not exclusively) on financial institutions. However, the problem of identity theft involves institutions that are not part of the financial services industry. Doctors, hospitals, and other health care providers may be both *creditors* and *users of consumer reports* under FACTA. The extent to which all health care providers are aware of their status and obligations as creditors and users of consumer reports is debatable,[8] but it is certainly fair to suggest that awareness is not as high as it is among financial institutions.

To give one example, there is a pattern in medical identity theft crimes where perpetrators change the billing address and the phone numbers on the medical charts of victims. The victim of the crime often only learns of the problem after a bill has gone to collection and a skip trace has been performed. At that point, victims typically receive angry letters from hospitals and other health care providers asking for immediate payment for services rendered in their name. While the health care providers should realize that there may be an identity theft problem, this does not always occur.[9]

This lack of awareness may be a contributor, at least to some extent, to the growing incidence of medical identity theft.

The failure of the draft rule to expressly identify health care providers as both creditors and users of consumer reports exacerbates the lack of policy and practical attention to medical identity theft. It is notable that the words *hospital*, *doctor*, and *medical* do not appear in the draft rule. In other words, the draft rule does nothing to flag its applicability to the health care community or to suggest to health care providers that the rule can apply to them. Even lawyers reading the rule may not easily reach the conclusion that health care providers can be covered.

The failure to mention the rule's applicability to health care overlooks the volume and importance of medical identity theft as a significant subset of identity theft. The World Privacy Forum believes strongly that the issue of medical identity theft needs more policy attention, industry response, and public awareness. Language should be added to the final rule to highlight

---

[8] That health care providers are creditors and users of consumer reports is not in question. It is a common practice for providers to ask how a bill will be paid, especially if there is no insurance. For services like Lasik eye surgery, providing credit is included in some advertisements, so it is therefore integral to the activity, and patients must meet credit checks. (See for example, <http://lasikvision.imswebmktg.com/lasikvision/unique/88011.php?GCID=S15543x031&KEYWORD=lasik%2Blaser%2Beye%2Bsurgery>. The Lasik Vision Institute included offers of credit for "No Money Down, No Interest until 2008, at 22.98 APR for the surgery. Last visited at September 18, 2006. Many more examples of offers of credit combined with Lasik and other procedures exist.)

[9] One specific example of this (among many potential examples) occurred in Birmingham, Alabama. An acquaintance of the victim stole his expired temporary drivers' license and used it to receive emergency medical treatment in his name at several area hospitals. Months later, the victim received a letter from an attorney demanding payment for an anesthesia group. The victim in this case was able to clear his name because an investigative reporter from a TV station helped him break through hospital red tape. The hospital was apparently reluctant to release the medical file to the victim. But the reporter was able to convince the hospital to compare a medical x-ray of the perpetrator's and the victim's right hand – which were markedly different, and thus cleared the victim's name. The victim said his imposter's activities added up to more than $10,000 in medical bills. See "Medical Identity Theft: What's the Deal?" NBC13.com, March 21, 2003. <http://www.nbc13.com/news/2057120/detail.html>.

the rule's applicability to health care providers. This may require no more than a sentence or two in the right place.

It may not be possible or practical for the rule to identity every possible creditor or user, but health care is a particular large percentage of the nation's economy, and a source of a significant, if unknown, percentage of overall identity theft cases. The agencies should be able to spare a few words in the rule to make it crystal clear that health care providers have obligations under the rule. At a minimum, the analysis accompanying the rule should discuss and confirm the rule's applicability to health care providers.

III. Red Flag Principles Must Apply to Those Who Maintain Medical Records

The agencies should expressly discuss medical identity theft as a subset of identity theft in either the rule itself or in the analysis that accompanies the rule. This should only take a few words. It is important that the health care industry be put on notice that it has responsibility to look for cases of medical identity theft and to help consumers who may be victims. The Red Flag principles will apply, albeit with some differences, to those who maintain medical records and not just to those who maintain financial records.

Evidence of medical identity theft may arise from discrepancies in medical records and not just from changes in financial or demographic information. A health care provider who discovers that the blood type recorded in a patient's medical record will not, without more education and awareness, think that the error could be evidence of medical identity theft. The same is also likely to be the case when a doctor's office discovers a change of address in its records that the patient claims not to have made.

It is an important and appropriate step to specifically add health care providers to the Red Flag rule.

IV. The Draft Rule Needs To be Integrated with the Health Privacy Rule

The draft rule needs to be integrated with the requirements of the health privacy rule issued by the Department of Health and Human Services under the authority of the Health Insurance Portability and Accountability Act. The requirement in the draft rule that users must develop and implement policies and procedures for verifying the identity of a consumer for whom it has obtained a consumer report and for whom it received a notice of address discrepency is, in effect, another administrative requirement comparable to those set out in the HIPAA health privacy rule at 45 CFR §164.530.

Those covered entities that use consumer reports likely fall under the FTC's administrative enforcement powers for the Fair Credit Reporting Act (FCRA). However, if the FCRA's requirements are not made a part of the HIPAA privacy rule, even if only by cross reference, then the likelihood of compliance with the draft rule is much reduced.

The same is true for the draft rules requirement that a creditor have a written Identity Theft Prevention Program (Program), with reasonable policies and procedures to address the risk of

identity theft to its customers and the creditor. Compliance by health care institutions will take more than the publication of a final Red Flag rule in the Federal Register. Financial institutions may pay attention to FCRA rules, but health care providers do not.

This may be an example of how different and unrelated privacy regimes create gaps that undermine the effectiveness of privacy protections for individuals. There is a reasonable prospect that those in the Department of Health and Human Services who are responsible for HIPAA are not aware of the draft Red Flag rule or of the FCRA requirements that fall on some covered entities. If the FTC does not take some action to highlight the effect of its Red Flag rule on HIPAA covered entities, then that rule is likely to go unimplemented in significant parts of the health care community. It is important that this problem not be left on the jurisdictional line between two agencies, ignored by both.

Specific suggestions for change include:

- One appropriate response would be to highlight in the draft Red Flag rule the obligations of HIPAA covered entities to comply.

- Another response would be for the FTC to go out of its way to contact the appropriate office at DHHS so that both agencies can work together to formulate a better integration of the two rules.

- The FTC should help DHHS to prepare and post a new FAQ on the Red Flag rule on the HIPAA website.

V. Red Flags in a Health care Context: The Need for Health Care-Context Examples in Appendix A of Draft Rule

The Red Flags in Appendix A of the draft rule need to include some examples likely to arise only in medical situations. Based on the report prepared by the World Privacy Forum,[10] we suggest that these examples be added to Appendix A. The idea is to give health care providers and others a better idea of what constitutes a Red Flag in the medical context.

Suggested Red Flags to be added to Appendix A:

1. Records showing medical treatment that is inconsistent with physical examination or medical history as reported by the patient.
2. Records showing substantial discrepancies in age, race, and other physical descriptions.
3. Questions raised by a patient about an explanation of benefits for services that the patient never received.
4. Dispute of a bill by a patient who is the victim of financial forms of identity theft.

[10] See *supra* note 3.

5. Any formal dispute of services or goods rendered by a provider who is given the specific reason of medical identity theft as the reason for the dispute.
6. Blood type discrepancy.[11]

Currently, patients who are the victims of medical identity theft face difficult challenges in disputing claims and bills that other individuals posing as them have created. It is not unusual for hospitals that have turned victims over to a collections process to refuse to discuss the case with the victim. Meanwhile, collection agencies often refuse to believe the victim or acknowledge the possibility of medical identity theft, even if there is solid and well-documented proof of victimization, or the existence of other documentation that exonerates the victim. Thus, when there is a dispute arising on the credit report due to an uncollected health care provider debt, the victims in these cases often cannot get the disputed claim removed.

VI. Conclusion

While the proposed Red Flag regulations contain some good language for Red Flags in the financial sector, the long term value of the Red Flag regulations will be substantially undermined by ignoring the impact and reality of medical identity theft and its relationship to the financial and the health care sectors. Medical identity theft – the use of identity information for obtaining health care or medical goods or services – is a growing problem, and one that poses public safety and health issues as well as financial issues.

The World Privacy Forum believes strongly that the issue of medical identity theft needs more policy attention, industry response, and public awareness. Health care comprises a particularly large percentage of the nation's economy, and is a source of a significant percentage of overall identity theft cases. For this reason, language should be added to the final Red Flag rule to highlight the rule's applicability to health care providers. This need not involve a large redrafting of the proposed rule; these changes can be incorporated with minimal edits and changes in several sections of the draft rule.

If health care providers and the health care sector in particular are not brought specifically into the proposed Red Flag regulations, then this problem will be allowed to fester and in all probability grow. Solving the problem now is the right thing to do. If it is allowed to become even more entrenched, medical identity theft may become more difficult for consumers and the financial and the health care sector to mitigate and resolve later on.

If the FTC in particular does not take some action to highlight the effect of its Red Flag rule on HIPAA covered entities, then the Red Flag rule is likely to go unimplemented in significant parts of the health care community. It is important that this problem not be left on the jurisdictional line between two agencies.

[11] While blood type discrepancy may occur due to general error, it is also a substantial harbinger of medical identity theft. This as a Red Flag could act to alert individuals to other problems that may exist.

Agencies have the opportunity to address this problem now. Forward progress can and should be made in this area by making the Red Flag rule unambiguously applicable to health care providers. This is an opportunity that must not be overlooked or ignored.

The World Privacy Forum has signed on to broader comments regarding the strictly financial aspects of the proposed Red Flag rules. The issues regarding medical identity theft are important enough that highlighting them in these separately submitted comments was a necessity.

Respectfully submitted,

Pam Dixon
World Privacy Forum
www.worldprivacyforum.org