MasterCard Worldwide
Law Department
2000 Purchase Street
Purchase, NY 10577-2509

tel 1-914-249-2000
www.mastercard.com

MasterCard
Worldwide

June 1, 2009

By Electronic Mail

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex M)
600 Pennsylvania Avenue, NW
Washington, DC 20580

RE: Health Breach Notification Rulemaking, Project No. R911002

To Whom It May Concern:

MasterCard Worldwide ("MasterCard")[1] submits this comment letter in response to the Proposed Rule published by the Federal Trade Commission ("FTC") pertaining to requirements for vendors of personal health records ("PHS vendors") and related entities to notify individuals in connection with certain data breaches ("Proposal"). The Proposal results from a direction to the FTC in the HITECH Act to adopt interim final regulations implementing Section 13407 of the HITECH Act relating to data breach notification. MasterCard appreciates the opportunity to comment on the Proposal.

In General

The scope of this comment letter is relatively narrow. In particular, MasterCard is concerned about the FTC's suggested interpretation of the definition of "individually identifiable health information" under section 1171 of the Social Security Act. This definition is central to the Proposal, and we respectfully request the FTC to review how it interprets this key term.

Individually Identifiable Health Information

A critical term in Section 13407 of the HITECH Act and in the Proposal is "individually identifiable health information." Section 13407 provides that the term has the same meaning provided in Section 1171(6) of the Social Security Act. The text of the Proposal does the same. Under Section 1171(6) of the Social Security Act, "individually identifiable health information" is

[1] MasterCard Worldwide (NYSE: MA) advances global commerce by providing a critical link among financial institutions and millions of businesses, cardholders and merchants worldwide. Through the company's roles as a franchisor, processor and advisor, MasterCard develops and markets secure, convenient and rewarding payment solutions, seamlessly processes more than 16 billion payments each year, and provides industry-leading analysis and consulting services that drive business growth for its banking customers and merchants. With more than one billion cards issued through its family of brands, including MasterCard®, Maestro® and Cirrus®, MasterCard serves consumers and businesses in more than 210 countries and territories, and is a partner to 25,000 of the world's leading financial institutions. With more than 24 million acceptance locations worldwide, no payment card is more widely accepted than MasterCard. For more information go to www.mastercard.com.

any information that: (i) identifies the individual (or there is a reasonable basis to believe that the information can be used to identify the individual); (ii) is "created or received by a health care provider, health plan, employer, or health care clearinghouse;" *and* (iii) "relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual."

We are concerned that the FTC has provided an interpretation of this term that does not appear to comport with the statutory definition. Specifically, in the Supplementary Information, the FTC states that a "database containing names and credit card information, even if no other information was included," would be covered by the Proposal because such information allegedly is "individually identifiable health information." We do not believe this is the correct interpretation of the law. A name and credit card number, by themselves, are certainly not "individually identifiable health information" because such information has no indicia that it is created or received by a health care provider, health plan, employer, or health care clearinghouse. Furthermore, a name and a credit card number, by themselves, have no bearing on the health of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual.

Similarly, even if the credit card information were associated with a PHS vendor's database, the information would still not constitute individually identifiable health information. As noted above, the information must be "*created or received* by a health care provider, health plan, employer, or health care clearinghouse." (Emphasis added.) Payment card information in a PHS vendor's database is received by, and the record itself is created by, the PHS vendor, not a health care provider, health plan, employer, or health care clearinghouse.[2] Such information would therefore not satisfy the requirements to be considered "individually identifiable health information."

For these reasons, MasterCard asks the FTC to specifically reject its proposed interpretation of "individually identifiable health information" in any final rule. If the FTC chooses not to reject

---

[2] The only possible category that could apply to PHR vendors is the first category for health care providers. The term "health care provider" has been defined under the HIPAA regulations to mean "a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business." 45 C.F.R. § 160.103. "Health care" is defined to include, but is not limited to, the following:

- Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
- Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

See id. Because a PHR vendor does not treat patients or sell medical items in accordance with a prescription, but is rather an entity that offers electronic maintenance and access to health records, it cannot be considered a health care provider. We note that the FTC does not argue in the proposed rule that PHR vendors qualify as health care providers. Furthermore, to the extent a PHR vendor is a health care provider, and therefore a HIPAA-covered entity, a breach involving the PHR vendor would not be subject to this Proposal.

this interpretation explicitly, we ask that the FTC omit any reference to credit card information in the final rule and its Supplementary Information. Such an omission would not affect the substance of the FTC's rulemaking, as the reference to credit card information is largely, if not completely, unnecessary given the scope of the Proposal. The scope of the Proposal is generally limited to PHS vendors and their service providers. The most likely circumstance in which a PHS vendor (or its service provider) would possess a name and credit card number would be in connection with the PHS vendor's receipt of payment from a cardholder for the provision of services to the cardholder (*e.g.*, to host a centralized medical record file for the cardholder). As discussed above, the Proposal would not govern a breach involving this type of information.[3] The only possible chance that a name and credit card number would be subject to the Proposal would be if the vendor were in possession of a health care record from a doctor or other provider, such record incidentally included the patient's payment information for services from the provider, and the record were the subject of a breach in the hands of the vendor (or its service provider). A discussion of payment card information in this context is not necessary, especially since the breach of the medical record itself would be subject to the final rule regardless of whether the record included payment card information.

* * * * *

Again, MasterCard appreciates the opportunity to provide comments on the Proposal. If you have any questions regarding our comments, please do not hesitate to call me at (914) 249-5978 or our counsels at Sidley Austin LLP in this matter, Michael F. McEneney at (202) 736-8368 or Karl F. Kaufmann at (202) 736-8133.

Sincerely,

Jodi Golinsky
Vice President
Regulatory and Public Policy Counsel

cc: Michael F. McEneney, Esq.
Karl F. Kaufmann, Esq.

[3] This does not mean that consumers would not necessarily learn of, and be protected from, a breach involving the vendor's information. The ubiquity of state breach notification laws generally ensures that notice would be provided in some manner. Furthermore, card issuers may also notify cardholders in response to a breach. In all circumstances, credit cardholders are protected against unauthorized liability on their credit card accounts, including under MasterCard's Zero Liability Policy and under federal law.