Client Alert

March 13, 2013

FTC Releases Report on Improving Consumer Protections in Mobile Payments; Recommends Financial, Privacy and Data Security Protections

By Obrea O. Poindexter, D. Reed Freeman, Jr. and Matthew W. Janiga

On March 8, 2013 the Federal Trade Commission ("FTC") released a Report on mobile payments that serves to follow up on the FTC's April 2012 workshop on mobile payments, as well as to lay the groundwork for the application of Section 5 of the FTC Act to new participants that operate in the mobile payments space, such as telecommunications and Internet search companies.

Specifically, the Report explores three consumer protection concerns that were identified by panelists at the FTC's mobile payments workshop: (1) dispute resolution; (2) data security; and (3) privacy. Each of these sections contains suggestions on how mobile payment industry participants can update their current practices, and sheds light on developing FTC expectations under Section 5 of the FTC Act and corresponding enforcement risk. Key findings and recommendations from the Report include:

- The FTC's support of uniform dispute resolution processes across all mobile payment funding methods;
- FTC suggested practices for mobile carrier billing, including permitting consumers to block all third-party charges on their accounts and creating enhanced dispute resolution practices;
- FTC recommendations to secure sensitive financial information used in processing mobile payments, including a reminder to comply with current federal and state requirements; and
- A renewed call for the adoption of the FTC's consumer privacy protection framework.

FTC WANTS UNIFORMITY IN CREDIT CARD, DEBIT CARD, GPR PREPAID CARD AND MOBILE CARRIER BILLING DISPUTE RESOLUTION

The Report highlights the FTC's interest in monitoring how the mobile payments industry resolves customer disputes related to fraudulent payments and unauthorized charges, particularly where the payment source underlying the mobile transaction lacks a robust dispute resolution framework. In doing so, the Report provides an overview of the statutory protections that limit liability for credit cardholders and debit cardholders, and contrasts these protections against the non-existent federal statutory liability frameworks for general-purpose reloadable ("GPR") prepaid cards and other prepaid instruments and mobile carrier billing.

As the Consumer Financial Protection Bureau ("CFPB") has jurisdiction to impose regulatory requirements relating to GPR prepaid cards and other prepaid instruments, the Report primarily reiterates the FTC's support for creating a uniform federal framework for all mobile payment devices that addresses liability limits, disclosure requirements for fees and expiration dates, formal error resolution procedures and authorization standards for recurring payments. The FTC noted

that during 2012, the CFPB collected information about the GPR prepaid market through an advance notice of proposed rulemaking, and expressed the belief that the CFPB's proceeding could have a significant impact for consumers using GPR prepaid cards and other prepaid instruments to fund mobile payments.

FTC SUGGESTED PRACTICES FOR MOBILE CARRIER BILLING DISPUTE RESOLUTION

The FTC's jurisdiction extends to telecommunications providers that are not engaged in common carrier activities, meaning the FTC has the authority to address practices related to mobile carrier billing, which is viewed as another funding method for mobile payments. The FTC has recently focused a fair amount of attention on carrier billing, as it believes that use of carrier billing has resulted in an increase in the "cramming" of fraudulent and unauthorized charges to consumer accounts. As a result, the section of the Report on mobile carrier billing includes suggestions on how the industry could modify its carrier billing dispute resolution practices to avoid regulatory concerns.

Specifically, with regard to preventing cramming, the FTC believes that (1) consumers should be able to block all third-party charges on their mobile accounts, including the ability to block charges on accounts operated by minors; (2) mobile carriers should clearly and prominently inform consumers about third-party charges and how to block them; and (3) mobile carriers should adopt clear and consistent processes that allow consumers to dispute suspicious charges placed on their accounts.

The Report goes on to suggest that mobile carriers should standardize their disclosure and dispute resolution practices. The Report further suggests that mobile carriers voluntarily align their dispute resolution practices to match those that are statutorily required of credit card issuers by the Truth in Lending Act, including allowing consumers to delay payment for charges that are disputed in good faith.

The Report also recommends industry participants make operational adjustments to reduce cramming, such as having mobile carriers, billing aggregators and payment processors that are involved in carrier billing "conduct meaningful upfront vetting" of entities that are allowed to bill to consumer accounts in order to verify which are legitimate third-party merchants. Such a recommendation, if formalized as a requirement, could effectively require carriers and processors to obtain, identify and conduct due diligence on third parties before allowing them to place charges. The FTC is in the process of organizing a roundtable on mobile carrier billing for May of 2013.

POTENTIAL TO IMPROVE SAFEGUARDS ON CONSUMER INFORMATION

The section of the Report on consumer data security suggests ways that sensitive financial data can be kept secure throughout the entire mobile payment transaction, regardless of how many parties are involved. Specifically, the FTC suggests that mobile payment participants look to adopt dynamic data authentication, which would generate unique payment information for each transaction and thereby eliminate the potential that fraudulently obtained financial information might be used for subsequent unauthorized transactions.

The Report also implies that a duty to ensure the security of information may ultimately fall on mobile payment providers, as the Report suggests mobile payment providers encourage all of the companies they incorporate into their payments chain to adopt increased data security measures. The FTC also reminds industry participants that they may already be subject to data security requirements under federal and state law, such as the FTC Safeguards Rule. This section of the Report is especially important because the FTC's standard for data security is based on reasonableness under the circumstances, and the FTC staff has gone out of its way here to indicate to the market what it considers to be

"reasonable." The FTC staff will now deem the industry as being on notice of this expectation.

PRIVACY CONSIDERATIONS IN MOBILE PAYMENTS

The FTC has long been a proponent of increased consumer privacy protections, and the Report continues this advocacy by urging mobile payment industry participants to adopt the recommendations set forth in the FTC's March 2012 report, *Protecting Consumer Privacy in an Era of Rapid Change*. "Privacy by design" is one of the recommended practices, and means that industry participants should examine and address privacy concerns at every stage of a product's development. The FTC also recommends that industry participants provide simplified and appropriate choices for consumers about data collected and used during mobile payments transactions, such as allowing consumers to prevent the sharing of information that is not relevant for a mobile payment transaction.

The FTC further recommends industry participants provide as much upfront transparency as possible about their data practices in order to increase consumer trust. In this regard, the Report directs industry participants to review the FTC's February 2013 report, *Mobile Privacy Disclosures: Building Trust Through Transparency*.

The FTC concludes its Report by noting that it will continue to monitor the mobile payments industry to ensure consumers are provided with appropriate financial, security and privacy protections. In the regard, the Report offers suggestions of how the industry may voluntarily address regulators' developing concerns, as well as a roadmap of potential future regulations that could bring uniformity in how banks, payment processors, and Internet search and telecommunications companies operate in the mobile payments space.

Contact:

Obrea O. Poindexter
(202) 887-8741
opoindexter@mofo.com

D. Reed Freeman, Jr.
(202) 887-6948
rfreeman@mofo.com

Matthew W. Janiga
(202) 887-6955
mjaniga@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life sciences companies. We've been included on *The American Lawyer*'s A-List for nine straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.