

FTC Recommends Stronger Safeguards for Mobile Payments

Karen H Bromberg, Partner

With the use of mobile payments by consumers reaching “fever pitch”, the FTC has released a new report entitled, *“Paper, Plastic... or Mobile? An FTC Workshop on Mobile Payments,”* discussing how companies can develop mobile payment products and services with adequate financial, security, and privacy protections. Acknowledging that mobile payment solutions offer many potential benefits, the report highlights three principal areas of concern for consumers and companies interested in mobile payment services: dispute resolution, data security, and privacy.

The report’s first concern focuses on how users of mobile payments can resolve disputes in the case of fraudulent payments or unauthorized charges. Noting that mobile payment platforms allow consumers to choose among several different funding sources for payment, each with varying levels of protection and dispute resolution procedures, the report states that consumers may not understand their rights and protections associated with each funding mechanism and therefore encourages companies to develop clear policies on how consumers can resolve such fraudulent and unauthorized charge disputes and clearly convey these policies to consumers. The report also highlights the growing problem of mobile “cramming,” which occurs when third parties place unauthorized charges onto consumers’ mobile phone bills. Rather than rely on consumers to identify unauthorized charges, the report urges industry members (mobile carriers, billing aggregators, and payment processors) to take proactive measures to prevent fraudulent charges from appearing in the first place.

The second key concern addressed in the report is the security of consumers’ financial data. Although technological advances in the mobile payment marketplace offer increased data security for financial information, the report encourages industry-wide adoption of strong measures to ensure security throughout the mobile payment process. While most mobile payment technologies provide end-to-end data encryption, it recommends dynamic data authentication where a unique set of payment information is generated for each transaction. The possibilities for encryption listed in the report cover everything from the authentication of data during the transaction to the secure storage of information on a mobile device.

Finally, cautioning that the use of mobile payments raise “significant privacy concerns,” the report urges companies in the mobile payment sphere to practice “privacy by design,” incorporating strong privacy practices, consumer choice, and transparency into their products from the outset and at every stage of product development. This is of particular concern in the mobile context where “the ability to store and transmit precise geolocation information facilitate unprecedented levels of data collection” and not only potentially gives third parties access to a much larger cache of personal information stored on the consumer’s mobile device, but gives it to a broader spectrum of players not contemplated in traditional

payment systems such as “operating system manufacturers, hardware manufacturers, mobile phone carriers, application developers, and coupon and loyalty program administrators”. These concerns illustrate the heightened need for companies to implement reasonable data collection and security practices.

Although the report’s recommendations are not official guidelines or regulations, they are strong evidence that the FTC is concerned about potential problems in this area. In the absence of official guidelines, companies may be well served by treating the FTC’s recommendations as a model for best practices and a preview of possible future regulation.

About the Author

Ms. Bromberg is the head of the firm’s Intellectual Property and Licensing Group. She handles all aspects of intellectual property, Internet, and technology law, including license agreements, technology transfer and vendor agreements, joint development and co-branding agreements, privacy policies, website terms of service, and management of IP litigation (including patent, trademark, copyright, and trade secret litigation). She was named as a New York *Super Lawyer* for Intellectual Property in 2010, 2011, and 2012.

About Cohen & Gresser

Recently named to *The National Law Journal’s* 2013 “Midsize Hot List,” Cohen & Gresser is a 2013 *Chambers USA*-ranked law firm with offices in New York and Seoul. We represent clients in complex litigation and corporate transactions throughout the world. Founded in 2002, the firm has grown to over fifty lawyers in four practice groups: Litigation and Arbitration; Corporate Law; Intellectual Property and Licensing; and White Collar Defense, Regulatory Enforcement and Internal Investigations. Our attorneys are graduates of the nation’s best law schools and have exceptional credentials. We are committed to providing the efficiency and personal service of a boutique firm and the superb quality and attention to detail that are hallmarks of the top firms where we received our training.

NEW YORK | SEOUL

www.cohengresser.com

info@cohengresser.com

PH: +1 212 957 7600

This information may constitute attorney advertising in certain jurisdictions