



LOEB & LOEB adds Knowledge.

Privacy Law

ALERT

MARCH 2013

FTC Report on Mobile Payments

The Federal Trade Commission issued a report and recommendations for mobile payments called [Paper, Plastic... or Mobile? An FTC Workshop on Mobile Payments](#), which is based on a workshop held by the Commission in 2012 to examine these issues.

The report, while noting that mobile payments can provide innovative and convenient options for consumers, highlights three major areas of potential concern for consumers. The first concern is how consumers can resolve disputes in the case of fraudulent payments or unauthorized charges. Many mobile payment platforms (such as those using Near Field Communications (NFC) technologies, mobile apps and online checkout wallets) allow consumers to choose among several different funding sources for payment, such as a credit card, debit card, bank account or mobile phone account. Consumers may not recognize that their protections against fraudulent or unauthorized transactions can vary greatly depending on the underlying funding source. Generally, credit cards and bank debit cards provide the strongest level of statutory protection (e.g., liability limitations, disclosure requirements for fees and expiration dates, error resolution procedures, and authorization standards for recurring payments); however, other types of funding mechanisms do not have the same statutory protections. For example, there are no federal statutes besides the FTC Act that protect consumers from unauthorized charges if their mobile payment mechanism is linked to a pre-funded account or stored-value card such as a gift card or general purpose reloadable card, also known as a pre-paid debit card. The report reiterated the significance of the Consumer Financial Protection Bureau's [pending proceeding](#) where the issue of whether to extend certain statutory protections to general purpose reloadable cards is under consideration. The FTC filed comments in that proceeding supporting extended protections for consumers of these cards. As such, the report recommends that companies develop clear policies on how consumers can

resolve disputes arising from fraudulent mobile payments or unauthorized charges.

The report also discusses the growing problem of mobile "cramming," which occurs when third parties place unauthorized charges on consumers' mobile phone bills. The Commission explained that it has previously indicated in a comment proceeding before the FCC that consumers should receive basic protections against this practice of mobile cramming by, among other things, giving consumers the ability to block third-party charges on their mobile devices. The report explains, however, that because there are several approaches to addressing fraudulent charges on mobile carrier platforms, there will be an [FTC roundtable](#) in May to discuss this issue.

Second, the report addresses the need for strong data security measures to ensure security throughout the mobile payment process. The report addresses ways sensitive financial information can be kept secure during the mobile payment process, such as through end-to-end encryption (i.e., allowing for encryption throughout the entire payment chain). The report encourages all stakeholders in the mobile payment ecosystem to raise awareness about the security of mobile payments and identify the steps consumers can take to safeguard data on their mobile devices (e.g., by encouraging consumers to set one password to unlock the mobile device and another password to access the payments app on the device).

The third concern is privacy. The FTC explains that the use of mobile payments raises significant privacy concerns, due to both the high number of companies involved in the mobile payment ecosystem and the large amount of data being collected. The Commission reiterates its "privacy by design"

This publication may constitute "Attorney Advertising" under the New York Rules of Professional Conduct and under the law of other jurisdictions.

recommendation (i.e., companies should consider and address privacy at every stage of product development) and urges companies to incorporate strong privacy practices, consumer choice and transparency into their products from the beginning of the design process. The report also notes the privacy issues arising from the consolidation of consumers' personal information in the mobile payment process. Mobile payment providers may have access to more information than a traditional retailer would, such as contact information and a record of a consumer's location.

Mobile payments frequently involve entities such as hardware manufacturers, operating system developers, application developers, data brokers, coupon and loyalty program administrators, payment card networks, advertising companies, and retailers and other merchants. The FTC will continue to monitor mobile payment options and to evaluate whether consumers have adequate protections and the information they need to make informed choices about these services.

Advanced Media and Technology Department

KENNETH A. ADLER	KADLER@LOEB.COM	212.407.4284
ROBERT M. ANDALMAN	RANDALMAN@LOEB.COM	312.464.3168
ALISA C. BERGSTEIN	ABERGSTEIN@LOEB.COM	312.464.3155
IVY KAGAN BIERMAN	IBIERMAN@LOEB.COM	310.282.2327
CHRISTIAN D. CARBONE	CCARBONE@LOEB.COM	212.407.4852
TAMARA CARMICHAEL	TCARMICHAEL@LOEB.COM	212.407.4225
MARC CHAMLIN	MCHAMLIN@LOEB.COM	212.407.4855
MARGARET CHARENDOFF	MCHARENDOFF@LOEB.COM	212.407.4069
CRAIG A. EMANUEL	CEMANUEL@LOEB.COM	310.282.2262
KENNETH R. FLORIN	KFLORIN@LOEB.COM	212.407.4966
DANIEL D. FROHLING	DFROHLING@LOEB.COM	312.464.3122
NOREEN P. GOSSELIN	NGOSSELIN@LOEB.COM	312.464.3179
DAVID W. GRACE	DGRACE@LOEB.COM	310.282.2108
THOMAS A. GUIDA	TGUIDA@LOEB.COM	212.407.4011
NATHAN J. HOLE	NHOLE@LOEB.COM	312.464.3110
MELANIE J. HOWARD	MHOWARD@LOEB.COM	310.282.2143
MICHAEL W. JAHNKE	MJAHNKE@LOEB.COM	212.407.4285
THOMAS P. JIRGAL	TJIRGAL@LOEB.COM	312.464.3150
IEUAN JOLLY	IJOLLY@LOEB.COM	212.407.4810
JULIE E. LAND	JLAND@LOEB.COM	312.464.3161
JESSICA B. LEE	JBLEE@LOEB.COM	212.407.4073
MICHAEL MALLOW	MMALLOW@LOEB.COM	310.282.2287
KATHERINE THERESE MASON	KMASON@LOEB.COM	212.407.4898

This alert is a publication of Loeb & Loeb and is intended to provide information on recent legal developments. This alert does not create or continue an attorney client relationship nor should it be construed as legal advice or an opinion on specific situations.

Circular 230 Disclosure: To ensure compliance with Treasury Department rules governing tax practice, we inform you that any advice contained herein (including any attachments) (1) was not written and is not intended to be used, and cannot be used, for the purpose of avoiding any federal tax penalty that may be imposed on the taxpayer; and (2) may not be used in connection with promoting, marketing or recommending to another person any transaction or matter addressed herein.

© 2013 Loeb & Loeb LLP. All rights reserved.

DOUGLAS N. MASTERS	DMASTERS@LOEB.COM	312.464.3144
NERISSA COYLE MCGINN	NMCGINN@LOEB.COM	312.464.3130
ANNE KENNEDY MCGUIRE	AMCGUIRE@LOEB.COM	212.407.4143
DANIEL G. MURPHY	DMURPHY@LOEB.COM	310.282.2215
BRIAN NIXON	BNIXON@LOEB.COM	202.618.5013
ANGELA PROVENCIO	APROVENCIO@LOEB.COM	312.464.3123
CHRISTINE M. REILLY	CREILLY@LOEB.COM	310.282.2361
KELI M. ROGERS-LOPEZ	KROGERS-LOPEZ@LOEB.COM	310.282.2306
SETH A. ROSE	SROSE@LOEB.COM	312.464.3177
ROBERT MICHAEL SANCHEZ	RSANCHEZ@LOEB.COM	212.407.4173
ALISON POLLOCK SCHWARTZ	ASCHWARTZ@LOEB.COM	312.464.3169
STEVE A. SEMERDJIAN	SSEMERDJIAN@LOEB.COM	212.407.4218
BARRY I. SLOTNICK	BSLOTNICK@LOEB.COM	212.407.4162
REGAN A. SMITH	RASMITH@LOEB.COM	312.464.3137
BRIAN R. SOCOLOW	BSOCOLOW@LOEB.COM	212.407.4872
WALTER STEIMEL, JR.	WSTEIMEL@LOEB.COM	202.618.5015
AKIBA STERN	ASTERN@LOEB.COM	212.407.4235
JAMES D. TAYLOR	JTAYLOR@LOEB.COM	212.407.4895
MICHAEL A. THURMAN	MTHURMAN@LOEB.COM	310.282.2122
JILL WESTMORELAND	JWESTMORELAND@LOEB.COM	212.407.4019
DEBRA A. WHITE	DWHITE@LOEB.COM	212.407.4216
MICHAEL P. ZWEIG	MZWEIG@LOEB.COM	212.407.4960