Paper, Plastic... or Mobile?

An FTC Workshop on Mobile Payments

FTC Staff Report | March 2013

This report is available online at
www.ftc.gov/os/2013/03/130306mobilereport.pdf.
The online version of this report contains live hyperlinks.

Contents

Introduction[1]

For years, there has been growing anticipation about the use of mobile payments as a regular way for consumers to pay for goods and services. Recently, this anticipation has reached a fever pitch. For instance, one survey of 1000 financial services, technology, telecommunications, and retail executives revealed that 83 percent of those executives believed that mobile payments would "achieve widespread mainstream consumer adoption" by 2015.[2] As a result, it is no surprise that in just the past year, several of the country's largest and most well known companies – including Google, Intuit, AT&T, Verizon, T-Mobile, Visa, Mastercard, and Verifone – have entered or increased their presence in the mobile payments market. Smaller start-ups such as Dwolla, LevelUp, and Boku also are vying for a seat at the table.

As the nation's consumer protection agency, the Federal Trade Commission ("FTC") is committed to staying abreast of technologies that affect consumers to ensure that consumer protections keep pace with these technologies. Towards that end, the FTC has actively addressed developments in mobile technology through workshops, policy initiatives, and enforcement actions. In 2000, the FTC held its first workshop to examine emerging mobile technologies and the issues they raised for consumers.[3] Since then, it has held workshops on the applications and implications of Radio Frequency Identification ("RFID") technology,[4] the

1. This report was prepared by staff of FTC's Division of Financial Practices, including Duane Pozza, Patricia Poss, and former staff member James Chen. They received substantial assistance from Carrie Gelula of the Division of Consumer and Business Education and Stacy Feuer of the FTC's Office of International Affairs.
2. *See* Jason Ankeny, *Financial Execs Survey: Mobile Payments Going Mainstream by 2015*, FierceMobileContent.com, July 13, 2011, *available at* http://www.fiercemobilecontent.com/story/financial-execs-survey-mobile-payments-going-mainstream-2015/2011-07-13.
3. *See* FTC Workshop, *The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues* (Dec. 11-12, 2000), staff report and transcript *available at* http://www.ftc.gov/bcp/workshops/wireless/index.shtml.
4. *See* FTC Workshop, *Radio Frequency Identification: Applications and Implications for Consumers* (June 21, 2004), staff report and transcript *available at* http://www.ftc.gov/bcp/workshops/rfid/index.shtm; FTC Workshop, *Transatlantic RFID Workshop on Consumer Privacy and Data Security* (Sept. 23, 2008), *available at* http://ftc.gov/bcp/workshops/transatlantic/index.shtml.

role of mobile commerce,[5] the emergence of contactless payment systems,[6] and advertising and privacy disclosures in mobile environments.[7]

In addition to workshops, the FTC has brought law enforcement actions relating to mobile technology issues, including a number of actions against mobile application ("app") developers.[8] The agency also obtained settlements with large players in the mobile marketplace such as Google and Facebook, requiring them to implement comprehensive privacy programs for all of their internet and mobile services.[9] The FTC has further issued policy reports, including a report setting forth a privacy framework that would govern players in the mobile ecosystem,[10] and two staff reports highlighting the lack of meaningful privacy disclosures associated with mobile apps directed at children.[11] The FTC also has developed and disseminated consumer and business education on mobile apps.[12]

The FTC's interest in mobile payments stems from its mandate to protect consumers in the commercial marketplace, as well as its broad jurisdiction over many of the companies that participate in the mobile payments ecosystem. 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

5. *See* FTC Workshop, *Protecting Consumers in the Next Tech-ade* (Nov. 6-7, 2006), staff report, and transcript *available at* http://www.ftc.gov/bcp/workshops/techade/what.html.
6. *See* FTC Workshop, *Pay on the Go: Consumers & Contactless Payment* (July 24, 2008), transcript *available at* http://www.ftc.gov/bcp/workshops/payonthego/index.shtml.
7. *See* FTC Workshop, *In Short: Advertising and Privacy Disclosures in a Digital World* (May 30, 2012), transcript *available at* http://www.ftc.gov/bcp/workshops/inshort/index.shtml.
8. A list of FTC mobile technology matters can be found at http://ftc.gov/opa/reporter /mobile/index.shtml.
9. *See, e.g.*, *In re Google, Inc.,* File No. 102 3136, Docket No. C-4336 (Oct. 13, 2011) (consent order), *available at* http://ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf; *In re Facebook, Inc.,* File No. 092 3184 (Nov. 29, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.
10. *See* FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers* (Mar. 2012), *available at* http://ftc.gov/os/2012 /03/120326privacyreport.pdf.
11. *See* FTC Staff Report, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (Dec. 2012), *available at* http://www.ftc.gov/opa/2012/12/kidsapp.shtm; FTC Staff Report, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), *available at* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.
12. *See, e.g.*, FTC, *Understanding Mobile Apps* (June 2011), *available at* http://www.onguardonline.gov/articles/0018-understanding-mobile-apps; FTC, *Marketing Your Mobile App: Get It Right from the Start,* (Aug. 2012), *available at* http://business.ftc.gov/documents/bus81-marketing-your-mobile-app.

companies, and retailers and other merchants.[13] The FTC has jurisdiction over all of these entities.[14] The FTC's jurisdiction also extends to telecommunications providers when they are not engaged in common carrier activities. Thus, mobile phone operators engaging in payment functions such as mobile carrier billing[15] are under FTC jurisdiction. Additionally, the FTC enforces provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act that regulate interchange fees involving entities such as card networks, state-chartered credit unions, and other entities not regulated by the Federal Reserve. The FTC further shares joint enforcement jurisdiction with the Consumer Financial Protection Bureau over non-depository providers of financial products or services, such as payment processors.[16]

A study issued last year by the Board of Governors of the Federal Reserve System, entitled *Consumers and Mobile Financial Services*, examined the growth of mobile banking and mobile payments.[17] The Federal Reserve found that 87% of the United States population owns a mobile phone, 44% of which are smartphones. Only about 12% of mobile phone owners had made a mobile payment in the past 12 months, and the most common use of mobile payments was to make an online bill payment (47% of mobile payment users). Concerns about the security of the technology were the primary reason given for not using mobile payments (42%). However, there appears to be significant interest among mobile phone users in expanding how they use mobile technology to access financial services. The Federal Reserve found that even among mobile phone users who do not currently use mobile

13. As stated at the workshop, compared to traditional payment systems, mobile payments can involve a significantly larger number of players. *See* FTC Workshop, *Paper, Plastic . . . or Mobile? An FTC Workshop on Mobile Payments* (Apr. 26, 2012) [hereinafter FTC Workshop], A. Levitin, Georgetown University Law Center, session 1 transcript, at 29. A webcast of the workshop, session transcripts and other related material are available at http://www.ftc.gov/bcp/workshops/mobilepayments/. References to the workshop transcript identify the speaker, the session number, and the transcript page.
14. The FTC's jurisdiction reaches any person, partnership or corporation that affects commerce, except for limited exclusions such as depository institutions. *See* 15 U.S.C. § 45(a)(2). State governments also have broad jurisdiction over companies in the mobile payments ecosystem. For instance, the California Public Utilities Commission established a rule providing the right to reverse unauthorized charges billed to prepaid or postpaid mobile phone accounts. *See* Cal. Pub. Util. Comm'n, Order Instituting Rulemaking on the Commission's Own Motion to Establish Consumer Rights and Consumer Protection Rules Applicable to All Telecommunications Utilities (Oct. 28, 2010), *available at* http://docs.cpuc.ca.gov/PUBLISHED/FINAL_DECISION/125959.htm.
15. "Mobile carrier billing" is a payment method whereby a consumer pays for a good or service from a third party by placing the charge on his or her mobile phone bill, and the mobile carrier bills the charge and collects payment from the consumer. This kind of third-party billing service is not a common carrier service.
16. *See* 12 U.S.C. § 5581(b)(5)(c).
17. *See* Board of Governors of the Federal Reserve System, *Consumers and Mobile Financial Services*, (Mar. 2012), *available at* http://www.federalreserve.gov/econresdata/mobile-device-report-201203.pdf.

banking, 28% report that they will definitely or probably use mobile banking at some point. Further, the underbanked make comparatively heavy use of both mobile banking and mobile payments, with 29% having used mobile banking and 17% having used mobile payments in the past 12 months.

To learn more about the mobile payments industry and its effects on consumers, the FTC convened a workshop on April 26, 2012. For purposes of the workshop and this report, staff took a very broad view of mobile payments and included technologies and products in which a payment is made using a mobile device, such as payments made through Near Field Communication ("NFC") technologies, mobile apps, online checkout wallets, and mobile carrier billing.[18] The workshop began with an overview of the innovative products and services being developed and the potential changes coming for consumers and merchants.[19] The first panel explored the emerging options for consumers using mobile payments. Panelists spoke about the potential benefits that mobile payments offer. For consumers, mobile payments can be an easy and convenient way to pay for goods and services, get discounts through mobile coupons, and earn or use loyalty points.[20] Mobile payments also may provide under-served communities with greater access to alternative payment systems.[21] For merchants, mobile payments may lead to lower transaction costs by allowing a consumer to utilize funding options other than a credit or debit card.[22] Mobile payments may also spur competition among payment methods, benefitting consumers and merchants alike.

While mobile payments offer many potential benefits to consumers, they also raise consumer protection concerns. Panelists identified three primary areas where concerns are likely to arise with the increasing use of mobile payments: dispute resolution, data security, and privacy. This report discusses these topics and highlights those areas where staff believes continued monitoring and attention are warranted. In the end, it is clear that building a

---

18. NFC is a type of wireless communications technology that can be used to effect a payment where two devices, such as a smartphone and reader, communicate through short range radio waves. Mobile apps refer to software programs that run on mobile devices. Online wallets are programs or services that allow a consumer to store payment information such as credit card account numbers and shipping addresses in a central online location. See footnote 15 and text below for a discussion of mobile carrier billing. These technologies and products are not necessarily mutually exclusive. For instance Google Wallet is an online wallet that can be accessed through a mobile app. When using Google Wallet for a transaction at a physical store, it utilizes NFC technology to process the transaction.
19. *See* FTC Workshop, C. Coye Benson, Glenbrook Partners, session 1 transcript, at 4-16.
20. *See* FTC Workshop, K. Enright, Google, session 1 transcript, at 20.
21. *See* FTC Workshop, L. Saunders, National Consumer Law Center, session 1 transcript, at 43-44.
22. *See* FTC Workshop, J. Valentine, SCVNGR/LevelUp, session 1 transcript, at 28.

framework for mobile payments that keeps the consumer experience in mind will go a long way towards developing consumer trust and widespread adoption of these new products and services.

The Legal Landscape and Resolution of Disputes in Mobile Payment Systems

One of the most significant concerns for users of mobile payments is how to resolve disputes in the case of fraudulent payments or unauthorized charges. Depending on the payment source used to fund the mobile payment (*e.g.*, credit card versus prepaid card versus mobile carrier billing), consumers may or may not have statutory protections regarding unauthorized charges. The second workshop panel looked at the protections afforded to consumers using mobile payment systems and discussed some of the confusion caused by their differing protections. The panel also touched on some of the special concerns that have developed with regard to payments made through a consumer's mobile phone account.

Mobile payment services typically function by linking to one or more payment sources. Many mobile payment platforms allow consumers to choose among several different funding sources for payment, such as a credit card, debit card, bank account, or mobile phone account. For instance, a particular payment application on a smartphone may be linked to a credit card so that the credit card is charged when the consumer pays using that application. During the workshop, FTC staff presented observations about these various funding sources based upon an examination of the websites of 19 U.S. mobile payment service providers.[23] Staff found that 15 of 19 providers allowed consumers to fund their mobile payments via credit or debit cards, 7 of 19 allowed funding by bank account debit, 4 of 19 allowed billing to a mobile carrier account, and 7 of 19 allowed multiple funding sources.[24]

Mobile payment users may not recognize that their protections against fraudulent or unauthorized transactions can vary greatly depending on the underlying funding source. Generally, credit cards provide the strongest level of statutory protection, capping liability for unauthorized use at $50.[25] If a mobile payment is linked to a bank debit card, a consumer's

23. *See* FTC Workshop, M. Mohapatra, FTC, and A. Schlossberg, FTC, session 2 transcript, at 1-2.
24. *See* FTC Workshop, M. Mohapatra, FTC, and A. Schlossberg, FTC, *A Snapshot of Select Mobile Payment Providers' Disclosures: FTC Staff's Preliminary Observations*, slide 5, *available at* http://ftc.gov/bcp/workshops/mobilepayments/.
25. *See* 12 C.F.R. § 1026.12.

liability for unauthorized transfers is limited to $50 if reported within two business days, and up to $500 for charges reported after two business days.[26] However, if consumers do not report unauthorized debit transactions on their bank account within 60 days after their periodic statement is mailed to them, they can face unlimited liability, whether or not the charges result from a lost or stolen card or another electronic transfer.[27]

Other types of funding mechanisms, however, do not have the same statutory protections as credit cards and debit cards. 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. At the workshop, one consumer group advocated for the extension of the additional federal protections afforded to credit and debit cards to these financial products, specifically pointing out the inequitable situation caused when these cards are used as payment vehicles for mobile payments.[28] Certainly, the inconsistency in protections complicates the landscape for consumers who may not understand the differences between these funding sources.

The Consumer Financial Protection Bureau ("CFPB") is currently examining the extension of protections to general purpose reloadable cards ("GPR"), which are expanding in usage and are one of the ways that mobile payments are funded.[29] FTC staff filed a comment in the CFPB's review, supporting protections for consumers of these cards and supporting the CFPB's efforts to obtain information about the costs and benefits of extending legal protections to these products. The comment discussed, in particular, four protections that currently apply to other types of payment cards: 1) liability limits, 2) disclosure requirements for fees and expiration dates, 3) error resolution procedures, and 4) authorization standards for recurrent payments. The FTC staff comment noted the relevance of these issues for mobile payments because students and the underbanked are among the greatest users of general purpose reloadable cards; more than 91% of underbanked consumers have mobile phones; and mobile

26. *See* 12 C.F.R. § 1005.6.

27. *See id*.

28. *See* FTC Workshop, M. Jun, Consumers Union, session 2 transcript, at 10-11; Consumers Union, *Mobile Pay or Mobile Mess: Closing the Gap Between Mobile Payment Systems and Consumer Protections,* at 8-11, 15 (June 2011), *available at* http://www.consumersunion.org/pdf/Mobile-Pay-or-Mobile-Mess.pdf (recommending that the rights afforded to consumers using credit card and debit cards to fund mobile payments be extended to consumers using pre-paid or gift cards as well as those billing items to post-paid and pre-paid wireless telephone accounts).

29. Electronic Fund Transfers (Regulation E) ANPR, 77 Fed. Reg. 30923 (May 24, 2012).

service providers have encouraged their customers to use general purpose cards as a payment method.[30] The CFPB's proceeding could have significant implications for consumers using reloadable payment cards to fund mobile payments.

Some companies have filled in gaps in the statutory protections by contractually promising consumers protections in the event that there is a dispute about a payment. For instance, staff's research of the websites of 19 current U.S. mobile payment providers revealed that three of the seven companies that allowed funding from stored value cards voluntarily provided additional protection that limited their customers' liability for fraudulent or unauthorized charges to $50.[31] While staff applauds companies that are voluntarily providing these protections, staff notes that because the protections are voluntary, such protections are not consistent, and companies that provide them could withdraw or modify them at their discretion.

Consumers should understand their rights and protections when choosing whether to pay using a mobile device, what mobile payment service to use, and what funding mechanism to use. To assist consumers in making these choices, companies should develop clear policies regarding fraudulent and unauthorized charges and clearly convey these policies to consumers. In the end, to the extent consumers need additional protections, policymakers will need to consider the benefits of providing consistent protections across mobile payments, and weigh these benefits against the costs of implementation.

Special Concerns Regarding Mobile Carrier Billing

As mentioned above, one potential mobile payment funding option is the ability to charge payments directly to a mobile phone bill, known as "mobile carrier billing." A growing number of third parties have entered into agreements with carriers to place charges on mobile

30. *See* Comment of the Staff of the FTC Bureau of Consumer Protection in Consumer Financial Protection Bureau, Docket No. CFPB-2012-0019 (July 23, 2012), at 3-7, *available at* http://www.ftc.gov/os/2012/07/120730cfpbstaffcomment.pdf. Extending legal protections to these products, however, also may impose costs on consumers. Issuers of GPR cards who do not screen potential customers may incur higher marginal costs in developing new systems to prevent fraudulent and unauthorized transactions to comply with a regulation. Moreover, if issuers of GPR cards are legally responsible for the difference between the costs of a fraudulent or unauthorized transaction and the legal limit of liability, they may seek to recoup these costs through increases in the costs of the cards such as the fees they charge to consumers. *See id.* at 4-5.

31. *See* FTC Workshop, M. Mohapatra, FTC, session 2 transcript, at 3.

phone bills.[32] However, there are no federal statutory protections governing consumer disputes about fraudulent or unauthorized charges placed on mobile carrier bills. As with prepaid cards, consumers must rely on the terms of their mobile carrier agreements or those companies' good will when these disputes arise.

The mobile carrier billing platform raises a unique challenge with regard to third parties placing fraudulent charges onto consumers' mobile carrier bills. This practice was first identified in connection with the landline billing platform and is generally known as "cramming." In a recent comment to the Federal Communications Commission ("FCC"), the FTC noted that crammed charges on mobile phone bills are a significant problem that appears to be on the rise.[33] This development should cause concern for all stakeholders in the mobile payments marketplace because it threatens to undermine mobile carrier billing as a legitimate and trusted payment option.[34]

As the Commission stated in its comment to the FCC, consumers should receive basic protections against such crammed charges on their mobile bills. First, consumers should have the ability to block *all* third-party charges on their mobile accounts, including the ability to block third-party charges on individual accounts operated by minors in the household, in order to ensure that cramming does not occur.[35] Second, mobile carriers should clearly and prominently inform their customers that third-party charges may be placed on customers' accounts and explain how to block such charges at the time that accounts are established and when they are renewed.[36] Third, mobile carriers should establish a clear and consistent process for customers to dispute suspicious charges placed on their account and obtain reimbursement.[37]

---

32. For example, Google allows Android app purchases to be charged to a customer's mobile phone bill in many cases. *See* Google, "Purchasing Android apps via Carrier Billing," *available at* http://support.google.com/googleplay/bin/answer.py?hl=en&answer=167794&topic =1046 718&ctx=topic.

33. *See* Reply Comment of the Federal Trade Commission in Federal Communications Commission CG Docket No. 11-116 (July 20, 2012), at 5-7 ("FTC Reply Comment"), *available at* http://www.ftc.gov/os/2012/07/120723crammingcomment.pdf.

34. Indeed, panelists at the workshop acknowledged issues with cramming on this payment platform. *See* FTC Workshop, M. Niejadlik, Boku, session 2 transcript, at 25; *see also* M. Crowe, Federal Reserve Bank of Boston, session 2 transcript, at 26-27.

35. *See* FTC Reply Comment at 12.

36. *Id.*

37. *Id.* This should preferably be done through establishing a single point of contact (in order to enable so-called "one and done" resolution).

The comment stated that such measures should be mandated by law or regulation to ensure that consumers have baseline protections.[38]

Other potential approaches have been suggested in various contexts. Some of these approaches focus on enhancing disclosures and facilitating disputes. For example, while improved disclosures may not be sufficient alone to fully address mobile cramming, mobile carriers could standardize and prominently highlight billing descriptions of third-party charges, in a format that makes clear why the consumer is being billed for a third-party charge, the provider or merchant that placed the charge, and the good or service being provided.[39] Mobile carriers could also consider notifying consumers of any recurring charges on their mobile phone bills (such as subscriptions) in advance of each such charge and provide the opportunity to cancel the subscription before the charge is imposed.[40]

In addition, mobile carriers could consider contractually requiring aggregators and other third parties to maintain sufficient and accessible records of consumers' authorizations of individual charges, in order to allow disputes to be efficiently resolved.[41] They also could continue to standardize their consumer dispute policies to more closely align with statutory protections accorded in the context of credit cards or debit cards.[42] Further, mobile carriers could allow consumers to delay payment for good faith charge disputes, without the possibility

38. *Id.*

39. Mobile carriers are currently subject to some FCC regulation regarding billing for third-party services. *See* 47 C.F.R. §§ 64.2400, 64.2401. To date, the FCC has not applied certain other landline billing requirements, such as placement of third-party charges in a separate bill section, to mobile carriers. *See In re Empowering Consumers to Prevent and Detect Billing for Unauthorized Charges ("Cramming")*, Report and Order and Further Notice of Proposed Rulemaking, CG Docket No. 11-116 (FCC), ¶¶ 46-48 (Apr. 27, 2012).

40. For example, the CTIA has issued guidelines for Premium SMS charges – in which a consumer opts in to a third-party charge after receiving a text message (SMS) to his or her handset – that require users to be notified of recurring premium charges and provided with an opportunity to opt out at least 24 hours before renewal charges are incurred. *See* CTIA, "CSC Monitoring Compliance Handbook,"(May 8, 2012), *available at* http://www.wmcglobal.com/images /CTIA playbook.pdf.

41. Mobile aggregators are companies that facilitate the connection between mobile carriers and providers of goods or services, including by routing SMS messages confirming transactions to or from mobile networks. A list of aggregators that are connected and approved to send SMS messages by at least one U.S. mobile carrier is available at http://www.usshortcodes.com/csc_aggregators.html.

42. *See, e.g.*, Consumers Union, "How Top Wireless Carriers Compare On Consumer Protections For Mobile Payments," *available at* http://defendyourdollars.org/document/how_top_wireless_carriers_compare_on_consumer_protections_for_mobile_payments (Dec. 13, 2011) (surveying policies of four major mobile carriers at the end of 2011).

that their mobile phone service will be cut off or they will receive an adverse credit report, until the dispute is resolved.[43]

Others urge industry members to take more proactive measures to prevent fraudulent charges from appearing on bills in the first place. To combat cramming effectively, it is not sufficient to rely on consumers to identify unauthorized charges, particularly since many consumers do not know that third parties can place charges on their mobile bills, and that the third parties can do so even if the consumer provides no credit card or other payment information.[44] Rather, an effective strategy requires participation by all entities involved in third-party billing – including mobile carriers, billing aggregators, and payment processors, which generally receive a portion of the third-party charges billed to a mobile account.[45]

Accordingly, these entities could conduct meaningful upfront vetting to ensure that only legitimate third-party merchants are able to place charges.[46] They could monitor refund or chargeback percentages for content providers or other merchants placing the charges, and take steps to bar fraudulent actors from placing further charges rather than continuing to do business with them.[47] They also could affirmatively monitor content providers' marketing

43. In California, the California Public Utilities Commission mandates that while a consumer dispute over a third-party charge on a mobile bill is pending, the consumer shall not be required to pay the disputed charge or any associated late charges or penalties, the charge may not be sent to collection, and no adverse credit report may be made based on non-payment of that charge. *See* California Public Utilities Commission, Revised General Order 168, Part 4, § 7, *available at* http://docs.cpuc.ca.gov/PUBLISHED/GENERAL_ORDER/138818.htm.

44. *See, e.g., In re Empowering Consumers to Prevent and Detect Billing for Unauthorized Charges ("Cramming")*, Report and Order and Further Notice of Proposed Rulemaking, CG Docket No. 11-116 (FCC), ¶¶ 22, 60 (Apr. 27, 2012) (noting evidence that consumers are often unaware that third-party charges can appear on landline numbers bills).

45. *See, e.g.*, Comment of CTIA – The Wireless Association in Federal Communications Commission, CG Docket No. 11-116 (June 25, 2012), at 5-6 (describing some contractual financial arrangements in this market).

46. As one example of a troubling practice that could be detected through a reasonable vetting process, one company that was recently enjoined for mobile cramming had used multiple corporate entities, which were registered across the country to addresses that were actually UPS stores. *See Cellco Partnership v. Hope*, Order and Preliminary Injunction, No. CV 11-0432-PHX-DOC (D. Ariz. May 11, 2011), at 3-4.

47. The California Public Utilities Commission currently requires wireless providers to submit reports of refunds by third-party service providers that place charges on wireless bills, as well as suspensions or terminations of those service providers. *See supra* n. 43 at § 11. There may be a need for further reporting and disclosure of such providers to ensure that suspended or terminated providers do not remain active billing via other wireless providers.

campaigns for compliance with industry marketing guidelines for mobile carrier billing and for signs of fraudulent activity.[48]

Given the range of potential approaches to addressing fraudulent charges on the mobile carrier platform, FTC staff is in the process of organizing a separate roundtable on this issue in May. Staff will invite stakeholders to address the efficacy of current efforts to stop mobile cramming, the need for new approaches (whether voluntary, regulatory, or statutory), and to consider the costs and benefits associated with any new approaches. Participants may consider the potential solutions outlined above, in addition to others that may be proposed. In light of the widespread fraudulent activity that has occurred with landline phone billing,[49] it is important for all stakeholders to act expeditiously to combat the growing problem of mobile cramming.

Consumer Data Security in Mobile Payments

Another key concern for consumers when making mobile payments is whether or not their sensitive financial information can be stolen or intercepted. As noted above, a Federal Reserve study reported that 42% of consumers were concerned about data security, and this concern was the most cited reason why consumers have not used mobile payments.[50] Specifically, consumers were concerned about hackers gaining access to their phone remotely, or someone intercepting payment information or other data.[51] Given that a major impediment to consumers' adoption of mobile payment technologies is the perceived lack of security, the incentives for industry to get security right should be strong. Nevertheless, although the technology to provide enhanced security in the mobile payments market is available, it is not clear that all companies in this market are employing it.

Technological advances in the mobile payment marketplace offer the potential for increased data security for financial information. A number of workshop panelists described how, under the traditional payment system, financial data is often transmitted or stored in an

48. The industry has promulgated certain voluntary guidelines, including the CTIA's "CSC Monitoring Compliance Handbook" for mobile billing, *see* http://www.wmcglobal.com/images/CTIA_playbook.pdf (May 8, 2012), and the Mobile Marketing Association's U.S. Consumer Best Practices for Messaging, *see* http://www.mmaglobal.com /uploads/Consumer -Best-Practices.pdf (Oct. 16, 2012).

49. *See* Comment of the Federal Trade Commission in Federal Communications Commission CG Docket No. 11-116 (Oct. 24, 2011), at 2-4, *available at* http://www.ftc.gov/os/2011/12/111227crammingcomment.pdf.

50. *See* Board of Governors of the Fed. Reserve System, *Consumers and Mobile Financial Services*, (Mar. 2012) at 13.

51. *Id*. at 53.

unencrypted form at some point during the payment process.[52] By contrast, mobile payment technology allows for encryption throughout the entire payment chain, which is often referred to as "end-to-end encryption."[53] Additionally, under the traditional payment system, financial information on a card's magnetic stripe that is transmitted from a merchant to a bank consists of the same information sent each time a consumer makes a payment. Thus, if this information is intercepted, it can be used repeatedly for subsequent, unauthorized transactions.[54] Mobile payments, however, can utilize dynamic data authentication, whereby a unique set of payment information is generated for each transaction. Accordingly, even if the data is intercepted, it cannot be used for a subsequent transaction.[55] In the mobile context, payment information also can be stored on a secure element that is separate from the rest of a phone's memory, preventing hackers who access a phone operating system from compromising sensitive financial information.[56]

Mobile payment providers should increase data security as sensitive financial information moves through the payment channel, and encourage adoption of strong security measures by all companies in the mobile payments chain. Consumers may be harmed when less responsible companies use insecure methods to collect and store payment information. Further, the reputation of the industry as a whole may suffer if consumers believe lax security practices are the norm. Many federal and state laws also impose data security requirements on businesses that collect and use financial information and other sensitive data.[57]

There are practical steps consumers themselves can take to secure their sensitive financial information in the mobile payments marketplace. Most simply, if consumers are using payment apps on their phones, they can set password protection for unlocking their phone.[58] Consumers also can often set a second password for any payment apps. Further, consumers

---

52. *See, e.g.*, FTC Workshop, P. Rasori, Verifone Systems, Inc., session 3 transcript, at 10; B. Milne, Dwolla, session 3 transcript, at 12.
53. *See* FTC Workshop, P. Rasori, Verifone Systems, Inc., session 3 transcript, at 10.
54. *See* FTC Workshop, B. Greene, Visa, Inc., session 3 transcript, at 12.
55. *Id*.
56. *Id*. at 26.
57. *See, e.g*. FTC Safeguards Rule, 16 C.F.R. § 314.1 *et*. *seq*. (requiring financial institutions to implement reasonable security for financial information); Cal. Civ. Code § 1798.81.5 (requiring businesses that own, license or maintain personal information about California residents to maintain reasonable data security procedures and practices). The FTC Act also prohibits unfair or deceptive practices, including such practices as they relate to privacy and data security. For information about FTC enforcement actions in the data security area, see http://business.ftc.gov/privacy-and-security.
58. *See* FTC Workshop, M. Niejadlik, Boku, session 2 transcript, at 14.

should be informed that if a phone with mobile payment apps is stolen, they can contact their mobile carrier immediately and have the phone and all payment apps disabled.[59] Education can play an important role in alerting consumers to these protective measures.[60] FTC staff encourages all stakeholders to raise consumer awareness about the security of mobile payments and the steps consumers can take to protect themselves.

Privacy

Panelists at the FTC's workshop also discussed privacy issues. Indeed, the use of mobile payments raises significant privacy concerns, due to both the high number of companies involved in the mobile payments ecosystem and the large amount of data being collected.[61] In addition to the banks, merchants, and payment card networks present in traditional payment systems, mobile payments often involve new actors such as operating system manufacturers, hardware manufacturers, mobile phone carriers, application developers, and coupon and loyalty program administrators.[62] When a consumer makes a mobile payment, any or all of these parties may have access to more detailed data about a consumer and the consumer's purchasing habits as compared to data collected when making a traditional payment.[63]

For example, when a consumer pays using a credit or debit card during a traditional point of sale purchase, the merchant typically has detailed data about the products the consumer purchased, but does not have the consumer's contact information.[64] Conversely, the financial institution that issued the card has a consumer's contact information and the name of the merchant where the consumer shopped, but generally does not have information about specific purchases.[65] Mobile payments can allow multiple players within the mobile payments ecosystem to gather and consolidate personal and purchase data in a way that was not possible under the traditional payments regime. Such consolidation may provide benefits to consumers, such as helping merchants offer products or services that a consumer is more likely to want.[66]

---

59. *See* FTC Workshop, S.J. Hughes, Maurer School of Law, Indiana University, session 3 transcript, at 20.
60. *Id*. at 17.
61. *See* FTC Workshop, H. Geiger, Center for Democracy & Technology, session 4 transcript, at 3-4.
62. *See* FTC Workshop, J. Anderson, Mastercard, session 1 transcript, at 37.
63. *See* FTC Workshop, H. Geiger, Center for Democracy & Technology, session 4 transcript, at 4.
64. *See id*. at 4-5.
65. *Id*.
66. *See* FTC Workshop, M. Duncan, National Retail Federation, session 4 transcript, at 3.

This collection of data may also help reduce the incidence of fraud.[67] However, these data practices also raise significant privacy issues.

In the FTC's report, *Protecting Consumer Privacy in an Era of Rapid Change* ("Privacy Report"),[68] the Commission set forth a series of recommendations for protecting consumer privacy. At its core, the Privacy Report urged companies to adopt three basic practices: (1) "privacy by design," (2) simplified choice for businesses and consumers, and (3) greater transparency. These principles apply to companies in the mobile payments marketplace, and many of the topics addressed in the Privacy Report also were discussed during the workshop.

"Privacy by design" means that companies should consider and address privacy at every stage of product development. Thus, a company should provide reasonable security for consumer data, and should limit data collection to that which is consistent with the context of a consumer's interaction with that company.[69] In the mobile context, unique features of a mobile phone, such as the ability to store and transmit precise geolocation information, facilitate unprecedented levels of data collection. This only heightens the need for companies to implement reasonable data collection and security practices.[70]

Panelists also noted that companies should provide appropriate choices to consumers about data collection and use related to mobile payments. For example, some said that companies should consider giving consumers the choice to restrict disclosure of information that is not necessary for completing a payment transaction,[71] or that use of payment data for other purposes or by third parties should not be pre-selected as default options.[72] Other panelists underscored the importance of context in determining whether choice is warranted. For instance, if the collection of data would be obvious from the context of a transaction, such as collecting and using location data to help a consumer find the nearest ATM machine, it may not be reasonable to ask the consumer to read and click through a lengthy privacy disclosure regarding that data collection.[73] Another panelist noted that restrictions on data collection

67. *See* FTC Workshop, M. Spadea, Promontory Financial Group, LLC, session 4 transcript, at 1.
68. *Available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf.
69. *Id*. at 24-27.
70. *See* FTC Workshop, H. Geiger, Center for Democracy & Technology, session 4 transcript, at 4.
71. *See id*. at 10.
72. *See* FTC Workshop, S. Grant, Consumer Federation of America, session 4 transcript, at 20.
73. *See* FTC Workshop, P. Walshe, GSM Association, session 4 transcript, at 12.

or the secondary use of collected data could lead to companies seeking to charge money for previously free products or services.[74]

Finally, companies should develop ways to provide transparency about their data practices in the mobile payments context in order to increase consumer trust in this growing marketplace. As some panelists indicated, when a company provides greater transparency regarding the information it collects, consumers are more likely to trust the company and to use its product.[75] Panelists noted, however, that providing meaningful disclosures in the mobile context is particularly challenging, given the small screens of mobile devices and the many entities involved in the mobile payments ecosystem.[76] How to make effective privacy disclosures on mobile devices was addressed at greater length in a recent FTC workshop and report,[77] and also is being addressed in a multi-stakeholder process sponsored by the U.S. Department of Commerce.[78] Mobile privacy transparency remains an important area of work for the FTC and all stakeholders in the mobile payments marketplace.

International Mobile Payment Issues

The FTC workshop also discussed the use of mobile payment technologies abroad and what the U.S. can learn from other countries' experiences. Mobile payments have developed extensively throughout the world. In some countries, like Kenya and the Philippines, mobile payments primarily take the form of mobile text messaging/SMS[79] for remittances and person-to-person money transfers. In others, like Japan, Korea and some European countries, mobile

74. *See* FTC Workshop, M. Spadea, Promontory Financial Group, LLC, session 4 transcript, at 13.

75. See FTC Workshop, M. Spadea, Promontory Financial Group, LLC, session 4 transcript, at 13 (stating that the key to privacy in the mobile payments context is transparency, and that "if consumers are informed about what is being done with their data … they should be empowered to make … decisions" about which services to use); *see also* FTC Workshop, P. Walshe, GSM Association, and H. Geiger, Center for Democracy & Technology, session 4 transcript, at 12-14 (explaining their reactions to data collection occurring in various mobile payments-related applications when such data collection is explained in a transparent manner).

76. *See* FTC Workshop, L. Saunders, National Consumer Law Center, session 1 transcript, at 36.

77. *See* FTC Workshop, *In Short: Advertising & Privacy Disclosures in a Digital World*, (May 30, 2012), transcript *available at* http://www.ftc.gov/bcp/workshops /inshort/index.shtml; FTC Staff Report, *Mobile Privacy Disclosures: Building Trust Through Transparency,* (Feb. 2013), *available at* http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf.

78. *See* Press Release, National Telecommunications & Information Administration, Department of Commerce, *First Privacy Multistakeholder Meeting: July 12, 2012* (June 15, 2012), *available at* http://www.ntia.doc.gov/other-publication/2012/first-privacy-multistakeholder-meeting-july-12-2012.

79. This refers to the transfer of money through text messages between accounts individuals hold with a mobile phone operator, as opposed to a traditional financial institution such as a bank.

payments deploy SMS and NFC technologies for mass transit and retail applications developed by partnerships between mobile network operators, banks, and governments.

According to a workshop panelist representing the Organization for Economic Co-operation and Development (OECD)'s Committee on Consumer Policy (CCP),[80] the global volume of transactions is growing rapidly and both traditional and non-traditional financial organizations are increasingly processing the transactions.[81] To provide leadership on the consumer protection issues surrounding mobile payments, the CCP established an informal working group on mobile payments that has been looking at many of the concerns discussed at the workshop.[82] The CCP is in the process of preparing policy guidance for governments and stakeholders on issues such as information disclosures for mobile payments, the varying levels of consumer protection among payment providers and payment vehicles, and dispute resolution and redress.

In addition, other governments and international organizations also are exploring common consumer protection concerns across differing markets, business models, and technologies. The European Commission, for example, is looking at similar issues as part of its work on the electronic payments market in Europe,[83] and the International Consumer Protection and Enforcement Network ("ICPEN")[84] is exploring consumer protection enforcement challenges in this area. Making sure consumers are adequately protected as they adopt mobile payments on a global level will be essential to consumer trust and adoption of new and innovative mobile payment systems.

---

80. The OECD is an international organization of 34 market-based democratic countries that fosters international cooperation through standards, agreements, recommendations and guidelines on economic and social issues. The OECD's Committee on Consumer Policy has been exploring consumer issues in the digital economy, and has been working for a number of years to analyze and strengthen consumer protection in online payments. *See* http://www.oecd.org/internet/consumerpolicy/consumersinthedigitaleconomy.htm. In August 2012, the CCP published an analytic "Report on Consumer Protection in Online and Mobile Payments" summarizing mobile payments developments and consumer protection challenges in OECD and non-OECD countries. *See* OECD, "Report on Consumer Protection in Online and Mobile Payments," OECD Digital Economy Papers, No. 204, (2012), *available at* http://dx.doi.org/10.1787/5k9490gwp7f3-en.

81. *See* FTC Workshop, B. Acoca, Organization for Economic Co-operation and Development, session 3, transcript, at 1-5.

82. *Id.*

83. The European Commission is the executive body of the European Union. Last year, the Commission issued a "Green Paper" on the development of secure, transparent, and innovative internet and mobile payment systems in Europe. FTC staff filed a comment in response to the Green Paper highlighting the FTC's mobile work and emerging consumer protection issues. *See* FTC Staff Comments, "Towards an Integrated European Market for Card, Internet and Mobile Payments" (Apr. 10, 2012), *available at* http://www.ftc.gov/os/2012/04/120410ecgreen.pdf.

84. *See* https://icpen.org/.

Conclusion

Without question, mobile payments have the potential to provide significant benefits to consumers and businesses. Industry is experimenting with many technologies, business models, and partnerships that provide consumers with new and exciting products and services. Although the industry is still young, FTC staff encourages those developing mobile payment products and services to create them with financial, security, and privacy protections in mind. 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 new and innovative services.


04
26
5956 3228 4569 678
Jonathan S. Doe