United States of America
Federal Trade Commission

Mobile Payments: Putting Your Money Where Your Mouth Is

Remarks of Maureen K. Ohlhausen[1]
Commissioner, Federal Trade Commission

Mobile Payments Day
Hosted by ETA, MAG and FCBA
September 30, 2014

I. Introduction

Thank you to the Electronics Transactions Association, the Federal Communications Bar Association, and the Merchant Advisory Group for having me here today to talk about mobile payments. A quick disclaimer: I speak today only for myself, not for the Federal Trade Commission generally or for any of my fellow Commissioners.

II. The Promise of Mobile Payments

Mobile communication has been one of the most transformative technologies in our lifetime. Mobile phones in particular have changed how we talk to each other, how we record important events, and how we work and play. Now, you can use your mobile phone to pay for things, which is why I've titled this talk "Putting Your Money Where Your Mouth Is." This change is really exciting. It's exciting because mobile payments offer the potential for dramatically increased convenience, security, and consumer choice for everyone with a mobile phone, as well as new competitive choices for business, both large and small.

[1] The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any other Commissioner.

I am particularly excited about how mobile payments technology brings payments and financial services to the unbanked or underbanked. A great case study in the power of mobile payments to reach the unbanked is Kenya. According to a 2010 World Bank report, only 19% of the population of Kenya has a formal bank account.[2] Yet at that time, 40% of the adult population used a SMS-based mobile payment system call M-PESA to pay bills, purchase goods, and transfer money to other individuals.[3] M-PESA has continued to grow in popularity. Kenya was an early leader in this space, but isn't alone. At the end of 2013, nine countries had more mobile payment accounts than bank accounts.[4] I commend the mobile industry for its leadership in this area: GSMA's Mobile Money for the Unbanked programme has played a key role in supporting the deployment of mobile payments in developing countries.[5]

Mobile payments are also transforming small businesses. Mobile technology has dramatically decreased barriers to accepting debit or credit cards. To choose an example very close to home for me, every Thursday afternoon, the Penn Quarter Farmer's Market takes over 8th street, just a block from the FTC headquarters. I have yet to find a vendor there that doesn't take Square, the seemingly ubiquitous white tile that turns a smartphone into a card-swipe cash register. If you've recently been to a farmer's market, a food truck, or a craft fair, I'm sure you've noticed something similar. By opening payment systems to individuals and small companies, Square and similar products make small dollar person-to-person transactions more

---

[2] Ignacio Mas *et al.*, *Mobile Payments go Viral: M-PESA in Kenya*, THE WORLD BANK, 2 n.5, (Mar. 2010), *available at* http://siteresources.worldbank.org/AFRICAEXT/Resources/258643-1271798012256/M-PESA_Kenya.pdf.

[3] *Id.* at 1.

[4] Claire Penicaud & Arunjay Katakam, *State of the Industry 2013 Mobile Financial Services for the Unbanked*, GSMA, 3, *available at* http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/02/SOTIR_2013.pdf.

[5] GSMA, *Mobile Money for the Unbanked*, http://www.gsma.com/mobilefordevelopment/programmes/mobile-money-for-the-unbanked (*last visited* Sept. 29, 2014).

convenient. Square also offers back office services such as invoicing and analytics, further expanding competitive offerings to individuals and small business.

Finally, mobile payments hold the potential to improve the security of payments. Mobile devices with payment features can require a payer to confirm his or her identity in a user-friendly way: the swipe of a thumb or a memorized gesture. Mobile payments can also encrypt data and use special algorithms to perform the equivalent of creating a new, one-time credit card number for every transaction, reducing the possibility that a merchant data breach might result in the theft of consumer payment information.

III. FTC Work in this Area

The FTC has been active in the mobile services area at least since our 2000 workshop on mobile technologies and has actively followed mobile payment technology as it has developed. I personally have long had a keen interest in seeing this new area thrive.

In March 2013 we released a report that highlighted the key findings and issues from a 2012 workshop on mobile payments.[6] The workshop and the subsequent report took a very broad view of mobile payments, including payments made through Near Field Communications, mobile apps, online checkout wallets, and mobile carrier billing. The report found significant potential benefits to consumers, including convenience, lower transactions costs, competition among payment systems, and providing underserved communities with greater access to alternative payment systems and financial services. The report also raised three primary areas of concern: dispute resolution, data security, and privacy. More recently, the FTC responded to the Consumer Financial Protection Bureau's request for information on the use of mobile financial

[6] Fed. Trade Comm'n, *Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments*, (Mar. 2013), *available at* http://www ftc.gov/sites/default/files/documents/reports/paper-plastic-or-mobile-ftc-workshop-mobile-payments/p0124908_mobile_payments_workshop_report_02-28-13.pdf.

services by consumers and the potential of such services for improving the financial lives of economically vulnerable consumers. The FTC's comments touched on many of the same themes as the 2013 mobile payments report, with updates to cover topics such as our mobile cramming enforcement actions and the Data Brokers Report we issued earlier this year.

IV. Mobile Payment Topics

With that overview of FTC activity, I'd now like to dive a bit deeper into three topics related to mobile payments that I find particularly important and timely: mobile cramming, in-app purchases, and data security.

A. Mobile Cramming

Mobile carrier billing – the ability to charge a good or service directly to a mobile phone account – is one of the most widely distributed forms of mobile billing and one of the earliest forms of mobile payments. Through a number of mechanisms, a consumer may pay a third party vendor, and that charge will appear on the consumer's phone bill. Carriers retain a percentage of the billed amount and send the remainder to the third party provider. This technique offers benefits to a wide range of people, given the high penetration of the necessary hardware (a mobile phone) across all segments of society. This form of payment can be particularly useful for consumers who do not have credit cards. Thus, it may be especially beneficial for unbanked and under banked consumers. Mobile carrier billing also has made it easy for consumers donate funds to charitable or political causes using text messages, with the charge placed on their mobile phone account.

However, fraud in this area has been a significant problem for consumers. In particular, the FTC is very concerned with a practice called "mobile cramming," which is the placing of unauthorized third party charges on mobile phone accounts. Mobile crammers sign up

consumers for Premium SMS "subscriptions" without the consumers' knowledge. Such services generally consist of ringtones or text messages containing trivia or horoscopes and typically cost $9.99 per month. Unfortunately, mobile crammers have defrauded consumers of hundreds of millions of dollars' using such charges.

For more than 15 years, the FTC has prosecuted cramming schemes on landline phones, bringing more than 30 enforcement actions under Section 5 of the FTC Act and providing tens of millions of dollars in restitution to consumers. As cramming has become a problem in mobile services, we have focused our attention there. As noted earlier, the FTC discussed mobile cramming in its mobile payments report. We followed up with a workshop on mobile cramming, and issued a related report just this past July.[7] Also this July, the FTC testified before Congress about mobile cramming, emphasizing our diligence in this area.[8] Most importantly, the FTC has actively enforced the law to shut down mobile crammers. Since the spring of 2013, the FTC has brought five cases against merchants, resulting in over $160 million dollars in monetary judgments.[9] And in July, the Commission filed its first mobile cramming action against a telecommunications company for allegedly deceptively concealing third-party cramming charges on billing statements and for allegedly failing to ensure that consumers had consented to such

[7] Fed. Trade Comm'n, *Mobile Cramming: An FTC Staff Report*, (July 2014), *available at* http://www.ftc.gov/system/files/documents/reports/mobile-cramming-federal-trade-commission-staff-report-july-2014/140728mobilecramming.pdf.

[8] *See* Prepared Statement of the Federal Trade Commission on "Cramming on Wireless Phone Bills: A Review of Consumer Protection Practices and Gaps," before the Senate Committee on Commerce, Science, and Transportation, July 30, 2014, *available at* http://www ftc.gov/public-statements/2014/07/prepared-statement-federal-trade-commission-cramming-wireless-phone-bills.

[9] To date, defendants have stipulated to final judgments, partially suspended based on inability to pay, totaling more than $160 million. *See FTC v. Wise Media, LLC*, No. 1:13-cv-1234-WSD (N.D. Ga. 2013); *FTC v. Jesta Digital, LLC*, No. 1:13-cv-01272 (D.D.C. 2103); *FTC v. Tatto, Inc.*, No. 2:13-cv-08912-DSF-FFM (C.D. Cal. 2013). *See also FTC v. Acquinity Interactive, LLC*, No. 14-60166-CIV (S.D. Fla.) (amended complaint filed June 16, 2014); *FTC v. MDK Media, Inc.*, No. 2:14-cv-05099-JFW-SH (C.D. Cal.) (complaint filed July 3, 2014).

charges despite clear indications of fraud.[10] We continue to pursue aggressive enforcement in this area.

I have long been concerned that fraudulent activity in this area, if unchecked, could discredit mobile carrier billing and mobile payments in general. As the major carriers begin to phase out the most frequently abused system, Premium SMS, I hope that consumer fraud in this area will continue to decline. The FTC will continue to watch this issue very closely.

B. In-App Purchases

Let's shift gears to a newer technology: in-app purchases. Although in-app purchases aren't always considered "mobile payments," they really are. Using in-app purchases, smartphone users can buy additional content, functionality, or other features within an app. The consumer's payment typically flows through the app store company – Apple, for example – to the app developer. Because the users need only share their payment information with the app store company, not with each third party app developer, this payment model is convenient and more secure.

As you probably know, the FTC has recently brought several cases about in-app purchases. Our recent cases against the Apple, Amazon, and Google app stores center on a failure to follow a fundamental consumer protection principle: before being charged, consumers must know what amount they are going to be charged and what action triggers that charge. These cases continue a long history of FTC enforcement against companies that charge consumers without authorization, in violation of that fundamental principal. Each of the companies received tens of thousands of complaints related to unauthorized in-app charges by children. Children spent hundreds, and in some cases, thousands of dollars on in-app purchases

[10] *See* Press Release, *FCC Investigates Cramming Complaints Against T-Mobile* (July 1, 2014), *available at* http://www.fcc.gov/document/fcc-investigates-cramming-complaints-against-t-mobile.

on their parents' devices without the informed consent of the parents. Accordingly, our consent orders with Google and Apple (the Amazon case is in litigation) require the companies to adhere to that the fundamental consumer protection principle. Specifically, the orders set a performance standard requiring the companies to, once per device, explain how in-app purchasing works on that device and get express informed consent to that approach from the account holder.

I believe the in-app purchases marketplace will continue to thrive in part because better practices will help restore and maintain consumer confidence in the app marketplace. The lesson of these cases for mobile payments more broadly is that any new technology must still comply with time-honored consumer protection principles.

C. Data Security

Turning now to data security. As smartphones grow more useful, we've placed more personal information in their care. Mobile payments technology continues this trend of trusting our devices to hold sensitive information about us. This trend increases the importance of securing this data on the mobile platform.

At the FTC, the touchstone of our data security enforcement is reasonableness: a company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities. Using this approach, the Commission challenges practices that are unreasonable in light of the full range of circumstances. We don't impose strict liability for a breach. In fact, we close between two and a half to three breach investigations for every one we pursue through a complaint. Also, I believe that our cases have focused on practices that are clearly unreasonable, such as maintaining

financial information in easily accessible unencrypted computer files or failing to change the default passwords on company networking hardware.

Using this approach, we have brought some cases related to data security in the mobile payments area. Most recently, we settled a case with Fandango, a popular movie ticket-purchasing app. There, the app developer overrode the default use of a SSL certificate validation process that helps verify that consumer communications are secure. As a result, the app insecurely transmitted payment and other information of millions of consumers.

Mobile payment technology actually offers the potential for increased data security for financial transactions. To me this is one of the most exciting things about mobile payment technology: it enables end-to-end encryption throughout the entire payment chain, making transactions more secure than, for example, the swipe-and-sign credit card systems used in most retail outlets today. Mobile payments could increase not only the security of mobile platforms, but also the security of our payment systems overall. Given recent headlines about data breaches at major retailers, this is very welcome news.

Mobile payments also appear poised to increase consumer control over their own information. Mobile payments make it possible to pay a merchant electronically without providing identifying information about oneself. The just-introduced Apple Pay system reportedly functions this way, supplying the merchant with only a one-time transaction-specific number – no name, no credit card number - that the merchant uses to get paid. This kind of system combines the convenience of credit and debit cards with the security and privacy of cash.

V. Conclusion

Famous aviator and author Antoine de Saint Exupery, once said, “As for the future, your task is not to foresee it, but to enable it.” I am very excited about the recent developments in

mobile payments and I cannot wait to see what the future will bring in this area. Rather than predicting that future, however, my goal is to ensure that the FTC can help promote innovation, in part by ensuring that consumers who embrace these advances can continue to rely on fundamental protections for their pocketbooks and their private information.

I'd be glad to take questions on these issues at this time.