7-10-2012

Developing the Framework for Safe and Efficient Mobile Payments, Hearing before Senate Committee on Banking, Housing, and Urban Affairs, 112th Congress

Sarah Jane Hughes
Indiana University Maurer School of Law, sjhughes@indiana.edu

INDIANA UNIVERSITY
MAURER SCHOOL OF LAW
Bloomington
211 S. Indiana Avenue Bloomington, IN 47405-7001 (812) 855-6318

Prepared Statement

of

Sarah Jane Hughes

Maurer School of Law, Indiana University[1]

for the

Senate Banking Committee

July 10, 2012 Hearing on Mobile Payments

[1] My prepared remarks and any remarks I may make in response to your questions reflect only my own views and do not necessarily reflect the views of the Trustees of Indiana University or the Maurer School of Law.

Mr. Chairman, Ranking Member Shelby, and honorable members of the Committee, I am pleased to be invited to discuss mobile payments generally, and the benefits and risks that mobile payments offer to merchants and other users in the marketplace.

Mobile payments are among the most innovative payments options emerging across the world. They enable person-to-person and person-to-business payments using flip phones and text messaging (SMS) in less developed countries. In the developed states, where banking systems and telecom networks are more regulated, mobile payments are emerging as a handy means of making small-dollar payments in the person-to-person and person-to-business markets. Perhaps even more importantly in the United States, they are enabling the unbanked and under-banked to make payments at lower risk and cost than some of the other payment options they may have.

Sponsors of mobile payments services vary significantly in size, the breadth and scale of the services offered, and the extent of federal or state regulation to which their businesses generally, and their payments services in particular, are subjected. Supervision and enforcement also differ significantly.

Mobile payments providers and developers of special mobile payments applications are attracting significant sums in capital investments, which suggest promising business models.

Nationwide merchants such as Starbucks were early adopters of mobile payments options for their businesses. Paying for a coffee or a snack could be completed before the foam on a specialty drink disappeared. Speedier payments, however, can be associated with business decisions to lower security safeguards – at least in the credit and debit industries.

Other merchants in the United States – including plumbers and participants in farm markets and craft shows, and increasingly non-profit organizations – are beginning to use mobile payments to take payments from their retail customers. These may be small transactions for a pound of field tomatoes, medium-sized transactions for the plumber's house call, or larger payments such as recurring utility, car finance or mortgage payments. But, unlike Starbucks where larger-dollar purchases are probably rare, non-profit organizations can take contributions or sell quantities of tickets that are much larger in dollar terms using mobile payments options. Small-dollar and larger-dollar transactions may present different risks for merchants, consumers, mobile payments providers, and the financial institutions that hold the funds sent or received via mobile payments.

So far, we have not heard much about larger-dollar payments being made for recurring purposes, such as mortgage payments or car finance installments, but there is little to stop that from happening from a technical or legal perspective. For these types of payments, banks have expressed concerns about the security of underlying banking account information in the hands of relatively new entrants to the payments industry.[2]

Your letter of invitation laid out many possible topics for witnesses to cover. I will focus my remarks on benefits and costs to merchants who take or might take mobile payments, and also to the other regulatory and enforcement issues their participation in payments may present. In some cases, the different issues that consumers and merchants have in the marketplace for mobile payments may converge; on others, they may diverge. I have identified five areas in which mobile payments are likely to benefit

---

[2] Statement for the Record from Robert C. Hunter, Deputy General Counsel, The Clearing House Association, L.L.C. to The Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, June 29, 2012 [hereinafter "The Clearing House Association, June 29, 2012 Letter"].

our economy and why they are so attractive to merchants, and five areas in which mobile payments present new concerns that may need to be regulated or harmonized and otherwise may require new enforcement approaches. In creating these lists, I made no assumptions about how regulation will evolve.

Turning first to potential benefits of mobile payments, I have five topics to cover and have provided one or more examples to illustrate the range of issues that may arise.

1. Taking mobile payments is quick and functional.

Mobile payments – whether utilizing existing credit or debit card interchange services or "rails" or the services of telecom or other providers – have the potential to help the owners of small businesses, small non-profit organizations, and farmers and artisans who bring their goods to farmers' markets and craft shows collect payments from their retail customers.

Mobile payments are speedy: they take only a few seconds to process. They operate without expensive and bulky equipment. They do not require a heavy specialty card reader. (The "reader" for Square, for example, is only about an inch square and the connector fits into the plug on the seller's smart phone or tablet.) Small merchants using smart phone apps also can take checks from their retail customers, using a feature called "remote deposit." No doubt, members of the Committee have seen ads from USAA and other financial institutions for remote deposits for the service members, veterans, and their dependents and families who USAA serves.

In addition, mobile payments, as replacements for magnetic-stripe credit and debit cards, may enable merchants in the United States to skip the impending transition from mag-stripe to chip-and-pin cards and the new readers that chip-and-pin technologies require. Mobile readers may be less expensive than chip-and-pin systems.

2. **Taking mobile payments helps small business owners collect smaller sums due from retail customers and may help to expand the economy.**

Two of the leading mobile payments services providers, Square and Intuit, count among their merchant customers thousands of small business operators (such as plumbers) and non-profit organizations (who take mobile payments for tickets sales and for contributions from supporters). The less time these merchants have to spend at tellers' windows or in line for the ATM, the more time they have to help customers, fixing leaking showers or providing services to the community. Thus, mobile payments may help smaller businesses maximize their productivity and add to the economy's health.

Mobile payments also help merchants at farmers' markets and craft fares make sales they otherwise might not – if the consumer involved has to stop and find an ATM machine before completing the purchase.

3. **Taking mobile payments may help merchants deter fraudulent charges at the point of sale.**

At two conferences in which I participated earlier this year, speakers explained in great detail why mobile payments were safer for consumers than payments with traditional plastic credit and debit cards; they paid less attention to whether they would be safer for merchants as well.

Unlike a tangible plastic credit or debit card whose credentialing and verification protocols – the account number, expiration date, customer name, and security code printed on the card itself – remains constant, mobile payments offer a more dynamic set of credentials that includes the mobile device's location at the time of the payment transaction and the ability of the mobile device to generate a unique identifier for every payment transaction. Dynamic credentialing is one feature that will help merchants – and consumers – avoid fraudulent charges.

Some mobile payments providers such as Square offer merchants another credentialing device – a real-time opportunity to match the face of the person offering to make the mobile payment with the face shown on the mobile device, or with the same merchant's record of the face of the person who last used the same mobile device to make a payment. Some consumers won't want merchants to store their photos for later purposes, but many probably won't care.

In addition, the geo-location of using the mobile device for "proximity" payments adds a security layer. Geo-location gives merchants – as well as processors and providers – an extra level of confidence that the mobile device from which the payment instruction or order is emanating is in fact the proper one.[3]

Dynamic credentialing, including facial recognition possibilities and geo-locational information, offers potentially greater safety in payments than the more static tangible plastic cards on which we have relied for the past 35 years or more.

The full-scale dynamic credentialing I have described – without going into detail about the technologies that support it, primarily because they are proprietary technologies in part – may not apply as functionally if the mobile device is being used to make a payment outside of the merchant's own store. Thus, "remote" mobile payments could raise some of the same fraudulent charge issues that merchants currently face in "card-not-present" transactions today in the credit and debit card payment spheres.

We do know that the card industry has created a payment application data security standard ("PA DSS"), much like its relatively successful PCI DSS set of security standards (for payment cards). But PCI DSS is not an ironclad solution to fraud risks from data interception or otherwise, as we learned from the episodes that TJX, Hannaford Brothers, and Global Payments experienced. Each of those companies had

[3] The degree to which counterfeiting of mobile payments technology becomes an issue is yet unknown.

been PCI DSS compliant, but none were the nanosecond following the security breaches they suffered. And, once a retailer or processor falls out of compliance, it must re-prove its security procedures to qualify again.

4. **Taking mobile payments offers merchants opportunities to build customer loyalty through mobile-based rewards programs, geo-locationally based or individually directed advertising, and other information about customers derived from the payment transaction that can be re-used.**

In contrast to traditional tangible plastic credit and debit cards that carry only basic credentialing and payment information, mobile payments offer merchants potential means of communicating with customers that can help merchants build customer loyalty and promote special offers.

5. **Taking mobile payments allows merchants to reach consumers who do not have demand deposit accounts or their equivalents or credit cards.**

With estimates of the number of unbanked adults in the United States upwards of 30 million households [check most recent figure – FTC or FRB March, 2012], merchants who take mobile payments may get customers who otherwise would have to pay in cash.[4] Unbanked consumers, particularly recent immigrants, often have smart phones instead of traditional computers and use smart phones – via mobile payments and mobile banking – to make payments to retailers and creditors.

Unbanked persons' adoption of mobile payments adoption is a means of reducing their dependence on cash and cash equivalents such as money orders, and

[4] Not having to handle cash or checks is a benefit to merchants all of itself in terms of accounting and fraud losses and speeds merchants' ability to get the proceeds of transactions into their bank accounts and forward to suppliers, landlords, and other creditors.

may serve as the basis for reducing their costs of participating in the retail economy and reducing the risks associated with carrying cash.

Now turning to possible risks or costs merchants (and consumers) may experience when taking mobile payments, we will see some overlap between risks present in credit and debit card transactions and risks in mobile payments. New risks also may arise.

6. **Taking mobile payments may not be free from interception risks or from malware applied to the data streams along the path maintained by app providers, intermediary processors, and the ultimate payor (such as the financial institution or telecom) that have affected the credit card industry, and thus may pose security risks similar or additional to those in the current payments marketplace.**

Mobile payments providers emphasize the greater security at the point of sale that mobile payments can provide over credit or debit cards, for the reasons I have mentioned above. What is less discussed is a possibility, if not a probability, that because the payments data and accompanying transaction data potentially move through more hands on their path to the ultimate payor, there is a greater likelihood of data interception (through war-driving interception as the data move from the mobile device to the merchant, and from the mobile device to a processor and then to the payor and then to the merchant – depending on the manner in which the payment is processed) or through malware introduced along the path. More simply put, the more participants in payments processing the greater the number of opportunities for interception or the application of malware.

7. **Taking mobile payments and harvesting more consumer information from these payments transactions places more personally identifiable information in the hands of merchants and the payments system participants downstream from merchants – and imposes on them more extensive, and possibly different data-protection responsibilities than they formerly may have had.**

Among the counter-weights to the benefits merchants may gain from having more information about their customers and targeted, inexpensive means of communication with them about merchants' offers, merchants will find compliance responsibilities they may not have anticipated. The more participants in the mobile payments processing path, the greater the number of potential harvesters and holders of personally identifiable information and purchase histories.

The value of these data harvests features at least as prominently as the shares of available direct income from marketing the software and processing the payments is likely to offer – at least in the United States where payments processing had been become increasingly efficient (as with checks) or already has been regulated by Congress (debit card interchange and some credit card fee limitations).

Some of these participants are not familiar with federal and state privacy protections or with requirements of Gramm-Leach-Bliley's Title V (Privacy) and the federal Safeguards Rule, of the Fair Credit Reporting Act and the federal Disposal Rule, or with the Children's Online Privacy Protection Act ("COPPA")[5] and the COPPA Rule.[6] Some

[5] 15 U.S.C. § 6501-6506 (2010).

[6] 16 C.F.R. Part 312 (2010).

participants will not be covered by either of the first two Acts or rules, but probably are already covered by COPPA and its rule. Having suitable supervision from federal and state regulators and suitable enforcement resources to protect individuals and this nascent industry from bad publicity is an important goal.

The State of New Jersey recently entered into a settlement with a mobile app creator whose target audience was children.[7] The action, brought in the United States District Court for the District of New Jersey, alleged that 24 x 7 Digital, LLC, and its owners Mark Yamashita and Rei Yoshioka, "collected, maintained, and transmitted to a third party, personal information about children" in violation of COPPA and the COPPA Rule. Among the elements of relief to which the defendants agreed was the destruction of the children's personal information – including the information they transmitted – within five days of the entry of the order.

An additional issue with data collected, stored, and transmitted involves its treatment in a future bankruptcy proceeding of the collector, storage operator, and recipients. The Committee may recall the public furor over the fate of children's data in the early days of internet commerce involving an online children's toy store and a company called DoubleClick, and the tussle over whether the children's personal information – as part of the debtor's "customer lists" was eligible to be auctioned for the benefit of the debtor's general creditors.

[7] Chiesa v. 24 x 7 Digital, LLC, et al., Civ. No. 2:12-cv-03402 (Jun. 26, 2012) (consent decree and order for injunction and other relief).

8. **Taking mobile payments does not necessarily relieve merchants of problems with charge-backs for fraudulent charges or other costs associated with data security problems.**

As the Clearing House Association recently explained to the House Committee on Financial Services' Subcommittee on Financial Institutions and Consumer Credit, banks "are usually required to absorb fraud liability and always absorb the cost of re-credentialing [the consumer] regardless of whether they had any connection with the underlying breach that compromised the data."[8]

Another aspect of this issue is that merchants will be dealing with more players in the payment than they may be accustomed to, and this broader array of counter-parties means more contracts to negotiate and monitor. Contracts will assign settlement times, charge back rules, transactional limits, and costs. Providers may reserve the right to change the terms of these agreements frequently, and may or may not tolerate patterns of behavior that are less than fully compliant with the contracts' provisions. Merchants lose eligibility to participate (as happens upon occasion in the credit and debit payments industries) and have little ability to be restored to participation in their new-found payments tools.

[8] The Clearing House Association, Letter of June 29, 2012, *supra* note 2, at 1, 2, 5.

9. **Taking mobile payments does not relieve merchants of responsibility for payment data integrity or for post-payment data security, and, because of the growing number of payments systems participants, may increase time needed to explain payments to customers, increase fraud risks, and also may create new risks for institutions that hold funds and facilitate settlements .**

This heading subsumes two subgroups of issues. The first relates to payment data integrity. Merchants need tools to prevent interference with the data stream so that a payment of $10 remains a payment of $10 as it moves through processing.

The second relates to post-payment data security at merchant's own locations and in their databases. Merchants need to safeguard data while the payment is being processed and for whatever time needed to respond to charge-backs, etc. They also need to dispose of the data properly and safely after it is not needed for any particular purpose or ultimately not needed to comply with applicable records retention requirements imposed by federal or state governments.

Data integrity (safeguards against alteration or replication of the sums the consumer intended to pay and the merchant wanted to receive) is important is all payments transactions. We have relatively elaborate rules for checks, credit and debit cards, and funds transfers (wholesale and retail) to protect data integrity and resolve disputes. For consumer transactions with credit and debit cards, federal law provides error resolution and liability limits.

We also want to provide for post-payment data security. Will the same standards that apply to storage of credit card information post-transaction/ payment apply to mobile payments? Will merchants be required to store personally identifiable information related to the purchase separately from the payment transaction

information? Will all intermediaries who can collect and maintain data be subject to the same obligations – whether from federal or state laws?

10. **Taking mobile payments may – but may not – require merchants to adjust their compliance with federal statutes, regulations, and executive orders pertaining to the deterrence of money laundering or prohibitions against doing business with concerns from designated foreign states or with "specially designated nationals" – individuals who are connected or suspected of being connected with drug or arms trafficking or support of terrorism– for purposes of compliance with the panoply of laws and executive orders enforced by the Department of the Treasury's Office of Foreign Assets Control.**

I have left for last the law enforcement issues on my list. Mobile payments offer a new set of opportunities to money launderers and those who would fund terrorists. Their person-to-person payments capacities and their speed and ease of transport are factors. Their abilities to dis-intermediate payments or to layer payments through multiple sets of hands are significant enticements for money launderers. Of these issues, speedy processing/settlements and disintermediation are the most problematic.

These laws are notoriously hard to enforce and preparing compliance plans for businesses eager to comply is a huge industry for law firms and consulting companies. Merchants hate these compliance responsibilities for their complexity and the effort required to train their rotating staffs.

Payments disintermediation generally, and perhaps the more so for mobile payments, is likely to make it harder for federal agents and local law enforcement to spot problems in local markets. Disintermediation in mobile payments also may hinder enforcement of AML and terrorist-finance control laws and agreements domestically and globally.

Sellers who take mobile payments also may have compliance responsibilities – as will providers and processors – with state safety and soundness registration and examination regimes for money services businesses and with state privacy and data security breach laws.

In closing, I have focused my remarks on domestic transactions and payments in which merchants in the United States and consumers here participate. Cross-border transactions and the payments associated with them raise other issues – issues that add significant dimensions to certain of the issues I have mentioned, with issues pertaining to charge-backs and error-resolution rules at one end of the spectrum, network and device compatibility in the middle, and issues pertaining to taxation and deterrence and identification of money laundering or terrorist support – given the wide array of providers and the technologies or business models they may deploy – at the opposite end.

Banks and consumers are justifiably concerned about broader access to customers' account information and the enticements that these data present to hackers, and even petty thieves. Consumers are justifiably nervous about the security of any personal information they convey to merchants through mobile devices and their geo-locational tracking properties. Consumers are justifiably concerned about who will have access to their personal information and payment account information as it travels, perhaps especially about how much third-party (and government) access there will be to it.

In terms of the future of regulation of mobile payments, we may see self-regulation, the existing mix of state and federal regulation and enforcement – or even some regional compacts such as those that spear-headed interstate banking in the 1980's, additional federal regulation or enforcement, or even a cross-border or multi-national regulation and enforcement scheme. A first task is to determine whether the different

silos of providers – banks and other financial institutions (as defined by various federal laws), telecom providers, mobile app developers, and payments intermediaries who are in none of those industries – should be regulated under a common set of expectations and requirements, or should be regulated according to the role they play in mobile payments.

Thank you again for the opportunity to be with you today. If you have questions about this statement or would like to discuss the issues I have discussed further, please contact me at sjhughes@indiana.edu or call me at 812-855-6318.