Prepared Statement of

Sarah Jane Hughes

Maurer School of Law, Indiana University

For the Hearing entitled

"The Disrupter Series: Mobile Payments"

Before the

Subcommittee on Commerce, Manufacturing, and Trade

Of the Committee on Energy and Commerce

House of Representatives

United States Congress

December 1, 2015

Mr. Chairman, Ranking Member Schakowsky, Representative Brooks from my home state of Indiana, and other honorable members of the Subcommittee, I am pleased to be invited to discuss mobile payments generally and the benefits and risks that mobile payments offer to merchants and consumers in today's marketplace. It appreciate the opportunity to be on this panel with distinguished representatives of U.S. Samsung Pay, the Merchant Customer Exchange, and my long-time professional acquaintance from the American Bar Association's Cyberspace Law Committee, John Muller of PayPal. This prepared statement and any remarks I may make during the hearing reflect only my personal views and do not necessarily reflect the views of the Trustees of Indiana University, or of the Uniform Law Commission, or of the Faster Payments Task Force operating under the auspices of the Federal Reserve Banks with which I am currently engaged in scholarly and public-service projects.

Mobile payments are among the most innovative and convenient payment options emerging across the world. They enable person-to-person payments globally using flip phones, text messaging and smart phones and in the U.S. are primarily used for person-to-business payments transactions using smart phones and other near-field communications systems. Among the many benefits that mobile payments offer in the U.S. and globally are their ability to provide unbanked and under-banked individuals and businesses to make payments more conveniently and at lower risk and cost than other payment options that maybe available.

Providers of mobile payments services vary significantly in size, the breadth and scale of the services they offer, and the extent of federal and state regulation in the United States that apply to their businesses generally. Their payment services in the United States are subject to differing supervision and consumer protection rules depending on whether the mobile payment device serves as an "access device" to the user's demand deposit account at a financial institution (the functional equivalent of a debit card) or the payment is billed to a wireless provider's monthly invoice to the user.

Mobile payments offer speedier conclusions to person-to-business payments in many cases than can be achieved through other payments options. As I noted when I testified before the Senate Committee on Banking, Housing and Urban Affairs in 2012, using a mobile payment to pay for a specialty coffee drink at Starbucks can be completed before the foam dissolves. This is particularly true because the mobile payment can be completed by the consumer even if the Internet connection the merchant has is offline; the wireless feature of mobile payments travels via the same wireless systems that operate the mobile phone or device.

Interest in speedier payments in the United States has been growing since my last testimony on mobile payments. This interest has prompted changes in the automated clearing house ("ACH") payments system operated under rules adopted by the National Automated Clearing House Association ("NACHA") and by the Clearing House Payments Company to speed up the clearing and settlement of ACH payments. Since 2013, the Federal Reserve Banks have been working on a project to create "faster payments" options for consumers and businesses and invited participants from many sectors to participate in its Faster Payments Task Force. The Task Force has been engaged in 2015 in efforts to frame the utilities, governance, legal structures and efficiency of faster payment solutions for domestic and cross-border transactions. I have been delighted to serve on the Faster Payments and Legal Working Groups created to support in this important effort.

Mobile payments can play important roles in raising individual contributions for disaster recovery, as they did for relief of victims of the Haiti earthquake, and for charitable and "crowdfunding" innovators and community and arts programming. It is conceivable – although I lack data to confirm this – that individuals who play in Daily Fantasy Sports also use mobile payments services and devices.

States and consortiums of state legislators and regulators including the Uniform Law Commission and the Conference of State Bank Supervisors have been watching mobile payments and

considering whether new state laws or regulations are needed to ensure the safe and transparent operation of mobile payments. The Uniform Law Commission, for example, sponsored a study committee on alternative and mobile payments in 2014; I served as the reporter to that study committee, which ultimately decided not to focus on mobile payments at that time. Since then, the ULC is re-considering whether to authorize a more in-depth study of mobile payments services that are not already regulated by state laws or federal legislation such as the Electronic Fund Transfers Act.

The balance of this prepared statement focuses on the issues on which the Chairman requested information and opinion. These are:

- How have mobile payment options disrupted the traditional payments landscape? What hurdles exist for widespread consumer adoption?
- What technologies have improved security for consumers' payment information in the mobile environment?
- What privacy considerations should be examined in the mobile payments ecosystem?
- How has mobile payment technology increased market access for the underbanked and small businesses?

I will respond to each of these questions in turn.

How have mobile payment options disrupted the traditional payments landscape? What hurdles exist for widespread consumer adoption?

The answer to this question is that it is difficult to tell the extent to which mobile payments options have disrupted traditional payments options. Despite the fact that two-third of American adults own smartphones, there is relatively little data about overall use of mobile payments by consumers in the United States. It appears that a much smaller subset of smartphone owners use them to make

mobile payments. One frequently cited reason is that U.S. consumers have numerous other convenient payments options, including credit and debit cards and assorted prepaid cards.

A recent survey of consumer users of new mobile payments options such as ApplePay, Samsung's Android payment product and others is only somewhat more encouraging. The survey executed by Trustev, a company that offers online fraud prevention services to retailers and banks, is described in an October 31, 2015 article in TECH INSIDER.[1] The author reported that:

> Trustev found that only about 1 in 5 people (20.7%) in the US who have an iPhone that works with Apple Pay — the iPhone 6 and newer — have even *tried* Apple Pay.
>
> Of those who have used Apple Pay, 56% report that they only use it once during a typical week, and 15.3% say they "never" use it during the week.
>
> The numbers are even lower for Samsung Pay and Android Pay. (Although the two services are different, Trustev combined them for the survey because Samsung Pay is only available on a small number of Android devices.)
>
> Only 14% of people who have the Samsung Galaxy S5 and S6 have ever used Samsung Pay or Android Pay, according to Trustev. Of those people who have, only 36.17% use it once in the typical week and 38.3% report they "never" use it.
>
> Rurik Bradbury, the chief marketing officer of Trustev, told Tech Insider that he thinks mobile payments haven't caught on because paying with a credit card isn't that difficult.
>
> "It just seems to me that there's not much of a problem Apple Pay fixes," Bradbury said. "Paying with a credit card is very easy. It's a habit everyone has."
>
> Indeed, Trustev also found that more than 82% of survey respondents reported that paying with a credit card in a store is "very easy" or "easy."[2]

The article points out that these products are new. Apple Pay was introduced in September 2014 and the Samsung and Android mobile payments options were introdcued in 2015, with the Samsung product introduced only a month before the survey and Adroid Pay on September 11, 2015.[3]

---

[1] Tim Stenovic, *A new survey shows people aren't really using Apple Pay,* TECH INSIDER (Oct. 31, 2015), http://www.techinsider.io/not-very-many-people-use-mobile-payments-2015-10. The survey included 1,000 respondents who had iPhones and Apple Pay and 1,000 respondents using Samsung Galaxy or other Android smart phones. *Id.*

[2] *Id.*

Other studies suggest a broader use of and satisfaction with mobile payments options. The same article in TECH INSIDER reported:

> Surveys by the Auriemma Consulting Group this year consistently found that 42% of iPhone 6 and 6 Plus owners have used Apple Pay, and that people who use the feature are very satisfied with it.
>
> When reached for comment, a Samsung spokesperson said that when the company beta-tested Samsung Pay in the US, 90% of people who used it said they were most likely to continue using the feature, and 90% reported they were most likely to recommend it to a colleague or friend.
>
> Samsung also said on Wednesday that people in the US who use Samsung Pay are likely to use it again — the company reported an average of eight Samsung Pay transactions per user.[4]

These surveys leave me with a more optimistic impression about future usage of newer mobile payments products, including Apple Pay, Samsung and Android Pay. These are early days, particularly for Samsung and Android Pay. Investors interested in mobile payments technologies should not depart this space based on such early returns, in my opinion. With three new major-branded mobile payments offerings in the past 15 months, it simply may be too soon to tell the extent to which how consumers will adopt which of these mobile options or others that may be available.

The logical, follow-on question to this first question is whether there are hurdles to consumer adoptions of mobile payments products? The answer in my opinion is that there are no legal barriers to broader adoption. But that there may be knowledge barriers to adoption—that is, that consumers do not adopt new payments technologies until they understand how they work, who backs the payment product, and what to do if the consumer has a complaint about the provider's performance or the performance of the merchant that accepted payment via the mobile option. In other words, I am inclined to think that additional consumer education about these products could make consumers more

[3] *Id.*
[4] *Id.*

likely to use them if they had smartphones capable of supporting these new options. This would require work by mobile payments providers to make their products and dispute-resolution procedures as transparent and efficient as possible. This need for information and product differentiation is also present in other emerging payments options being offered in the United States.

I might cite one barrier to greater use of mobile payments that comes from the merchant side – the cost of and training associated with acquiring new "readers" to receive information for contactless payments, etc. I do not have data on how much it costs merchants to acquire a contactless reader or how much training and monitoring of employees it takes to get to smooth and sufficiently speedy use of one to make it worthwhile for merchants. Ms. Deckinger, however, may be able to speak to this issue. But I do recall that costs that merchants had to incur to get early-stage smart-card payments devices from 1995 through to the end of the Mondex and Citi experiments in this country were cited as a reason why the smart-card option was so hard to grow.

What technologies have improved security for consumers' payment information in the mobile environment?

Among the most-cited perceived impediments to wider consumer adoption of mobile payments options is security. I suspect that the data-security breach episodes by major retailers over the past decade have made consumers increasingly concerned about data security, just as they have driven U.S. merchants and financial services providers to increase their attention to ensuring effective security.

Among the most important improvements in the mobile payment ecosystem are the availability of new security features on the phone physically, such as passwords or passcodes set by users, fingerprint-reading functions, and the ability to delete data remotely in the event that the phone is lost or stolen. Multifactor authentication and tokenization are additional options for greater mobile payments security. Multifactor authentication effectively requires the username, password or passcode

(including a fingerprint), and the device or phone itself. The phone's location function allows the authentication process to verify that the phone and consumer are in the same location. This verifies the payment from the outset, but it may not prevent loss of the payment or user data downstream as the payment "instruction" moves towards clearing and settlement. Multifactor authentication also is not used in connection with other features, such as reward programs and customer-relationship management or with remote (device not present) transactions.

The tokenization option of enhancing security permits strong security along the downstream route to clearing and settlement, in rewards programs and in customer-relationship management. Tokenization works only for one-time verification; it prevents linkage of a payment to prior payments by the user or the user's phone or device.

Apart from technological security aids, providers of mobile payments services face federal and state compliance obligations that may encourage them to enhance the security of their systems. The Federal Trade Commission's "Safeguards" Rule, codified at 16 C.F.R. Part 314, mentioned in the Majority Memorandum for this hearing, covers mobile payments providers and downstream processing, clearing and settlement services connected to them. Additionally, the Majority Memorandum noted, the FTC can use its FTC Act Section 5 authority to secure remedies for violations by mobile payments providers that are not banks or communications carriers themselves. However, the recent FTC Administrative Law Judge decision in In the Matter of LabMD, Inc.,[5] Initial Decision (Nov. 13, 2015), casts doubt on the use of Section 5's "unfair and deceptive acts or practices in commerce" authority as a means of redressing

[5] FTC Docket No. 9357. The original administrative complaint was filed on August 28, 2013.

security breaches unless the FTC staff can prove more than theoretical harm to consumers as a result of the breach.[6] The FTC Complaint Counsel filed a Notice of Appeal on November 24, 2015.

As the Majority also noted, about a quarter of the States include financial account, credit and debit card information under their statutory definitions of "personal information." Private actions brought for violations of these State statutory requirements also have encountered problems proving injury to consumers in some courts.

Mobile payments providers and those seeking to enter this ecosystem as providers or processors nevertheless can follow some "best practices" for securing data required to receive, clear and settle payments. I would encourage merchants and others engaged in receipt or processing of mobile payments to use the recent FTC guidance on simple security practices, *Start with Security: A Guide for Business.* [7] The Guide sets forth a ten-step outline of what business can do to enhance the security of customers' information, both personal and financial.

Efforts by federal and state bank regulators also promise to yield stronger security ecosystems for all payments providers. In this connection, I would cite the work by the FFEIC in 2015 on its new Cybersecurity Assessment Tool, led by Valerie Abend of the Office of the Comptroller of the Currency, and the stronger cybersecurity requirements expected from the New York State Department of Financial Institutions, spearheaded by the former Superintendent Benjamin Lawsky. Although the Cybersecurity Assessment Tool and the New York DFS requirements may not affect every provider directly, efforts such as these offer encouragement and guidance options to providers beyond those directly affected.

What privacy consideration should be examined in the mobile payments ecosystem?

[6] Fed. Trade Comm'n., Press Release, *Administrative Law Judge Dismisses FTC Data Security Complaint Against Medical Testing Laboratory LabMD, Inc.* (Nov. 19, 2015), https://www.ftc.gov/news-events/press-releases/2015/11/administrative-law-judge-dismisses-ftc-data-security-complaint.
[7] (Sept. 2015) https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

In my 2012 Senate testimony, I noted that harvesting consumer information from mobile payments transactions places more personally identifiable information and more personal financial information in the hands of merchants and the downstream payment system participants including non-bank payments processors. I have found little evidence of change on this front since July 2012.

Many non-bank payments processors are not regulated by the States or federal regulators to the same degree that depository institutions such as commercial banks and credit unions, or providers operating under State "money transmitter" licenses, such as PayPal, are. However, the 2000 Federal Trade Commission rule implementing Title V (Privacy), Subchapter I of the Gramm-Leach-Bliley Financial Services Modernization Act of 1999, codified at 15 U.S.C. 6801-6809, covers all participants in the provision of consumer financial products and services. 65 Fed. Reg. 33645, 33655, 33655 (explaining the inclusion in the final "Privacy" rule's definition of "financial institution", 16 C.F.R. § 313.2(k), entities engaged in providing data processing and data transmission services in connection with financial products and services provided to consumers, citing Section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. § 1843(k)). The "Privacy" regulations promulgated by other federal financial regulators have similar but not identical coverage. Thus, between the rule written by the FTC in 2000 and now also enforced by the Consumer Financial Protection Bureau, and the rules written by the Comptroller of the Currency, Federal Deposit Insurance Corporation, and Board of Governors of the Federal Reserve System, most of the providers of mobile payments should have a sufficient roadmap on how to handle the personal identifiable information and financial information that they obtain from the processing of payments via mobile devices.

The Committee may be aware that commercial banks have expressed concerns about privacy and security in non-bank payments processing in the past.[8] The potential for a mobile payment provider and the downstream payments participants necessary for clearing and settlement of the payment back to the merchant involved to collect and use information about the customer's spending habits and vendors of choice is and will continue to be substantial. Whenever additional entities handle payment and user information, the risks of capture and improper uses of these data grow. Thus, a multi-party mobile payments downstream network and could create privacy risks in a degree comparable or greater than privacy risks experienced in credit and debit transactions – unless all participants commit to privacy standards and comply with any applicable limitations on re-use and implement and monitor their systems for interceptions by intruders.

It is not clear to me that Congress should enact or require agencies to promulgate additional compliance obligations on merchants or mobile payments providers to ensure privacy at this time. But, I think it is far to point out that consumers will forego payments providers and merchants who do not protect their privacy or guard the systems that process, clearing and settle payments to a sufficient extent. We only have to look at the downturn in business for merchants that suffered data-security breaches over the past few years to observe how quickly consumers can take their business to a different merchant, or in the case of mobile payments usage, to "hang up" on mobile payments in favor of another payment option.

How has mobile payment technology increased market access for underbanked consumers and small businesses?

The success of mobile payments outside the United States, particularly among unbanked and underbanked individuals and businesses in Africa, suggests that mobile payments can benefit

[8] *See, e.g.,* 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.

underbanked persons greatly. In this country, we are seeing the emergence of smartphones as the key connectivity option for less affluent persons and for those who reside and work in rural areas or parts of cities where fewer bank branches operate than they formerly did. Wireless phones have replaced land lines in these populations and also provide their Internet connections. Mobile payments offer attractive options for making payments on a person-to-person ("P2P") or person-to-business ("P2B") basis for those businesses that can accept payments via a mobile option.

Media coverage suggests that home-maintenance and garden-care businesses, house-cleaning services, plumbers, and massage therapists and many more types of small businesses use mobile payments as a preferred payment option. (They also may deposit checks they receive via remote-deposit options on smartphones offered by an increasing number of depository institutions.) These businesses may receive larger-dollar payments via mobile services than those in some retail businesses, but, regardless of the dollar values being paid, using mobile payments can help small businesses grow their revenues and profitability. They offer special opportunities to build customer loyalty through rewards programs and geo-locationally based or directed advertising that some consumers enjoy.

The convenience for small businesses of using mobile payments can be significant. The business owner does not have to worry about keeping track of payments in cash or check, does not have to add trips to make deposits to their daily or weekly scheduled, and has a reliable report of receipts and deposits from the mobile or remote-deposit provider. As I mentioned in my 2012 testimony, taking mobile payments may help businesses of every size deter fraudulent charges at the point of sale – even as credit cards with chips become common in the United States – because of the dynamic credentialing that mobile payments options provide via location information and unique identifiers for each transaction. Square and Apple Pay offer even more unique credentialing options in the forms of matching the face of the consumer making the payment and the photo stored with Square or the fingerprint identifier used by Apple Pay.

Another group of "small businesses" that benefit from mobile payments in the U.S. are farmers and local operators of farm markets, artisans who sell at arts fairs, and small arts organizations. I serve on the board of The Yard, Inc. , a dance colony in Massachusetts, that began using Square for ticket sales and credit-and-debit contributions about four years ago. The convenience for The Yard and for our patrons has been a boon to our earned income and personal contributions, and the manner in which we can use this excellent option also saves us accounting and processing costs that really adds value to The Yard's bottom line.

From the perspective of consumers, mobile payments options offer more secure payments alternatives than cash and lower-cost and more secure means of making payments than postal money orders or commercial money orders. They also enable payments by holders of prepaid cards and payroll cards remotely, which saves time and transportation costs. Thus, market access has already increased for the unbanked and underbanked, but I have found no firm evidence of the current uses of mobile payments among these two traditionally underserved groups. I would expect that as providers such as Apple, Samsung, and Android and others expand their offerings that these groups will benefit further from the use of mobile payments and that the businesses with whom they deal will benefit as well.

Thank you, Mr. Chairman and Representative Schakowsky, for the opportunity to appear before you this morning. I would be pleased to answer questions you may have.