Risk and Privacy Implications of Consumer Payment Innovation in the Connected Age
Commentary

Sarah Jane Hughes

Mobile payments present both new—and very traditional—challenges. In this paper, I address these challenges through a series of questions that, if I were designing a new payment method or if I were choosing among several to use, I would want to consider. Before I present these questions, however, I would like to offer three general observations.

The first is that payments providers' innovations are removing them, in whole or part, from traditional regulatory regimes. Finding new "spaces" in which to create new products and services to make payments faster, easier and possibly less costly, is a good thing. Leaving established regulatory regimes, however, carries a cost to providers and their partners: to the extent that consumers and perhaps merchants who take payments are uncertain of the rights and responsibilities they will have under new payment products, adoption of new products may be slower than it otherwise might be.

The second is, to the extent that one of these new providers experiences a major incident—whether a cyber-attack or merely a criminal intrusion into their system—and the public learns about it or individual consumers or merchants suffer losses as a result, concerns about what happens to consumers using the same or similar products are likely to arise. If we were to experience multiple incidents across multiple providers, as the cyber-events of 2010 and 2011 with payments processors and cloud computing services evidence may happen, consumers may race back toward the regulated forms of payments they already know, such as debit and credit cards swiped physically at merchants and ATMs, or checks.

My third observation is linked to the first. Despite the fact that the providers and the technology undergirding mobile payments are moving away from established regulatory regimes, a system in which only contracts govern payments (or in which significant issues are not governed even by contract provisions) imposes new costs on the participants in payments—the consumer or other end users, the

merchants or middlemen, the providers of payments bridges such as credit and debit interchanges or nonbank mobile payments providers, and the holders of funds being transferred, whether depositary institutions or not. Thus, in considering how to frame a new payment product from a business perspective, we must anticipate the types of problems the payment product and the participants in the overall progress of a payment transaction may have and deal with them—or decide not to do so and figure it out later if something goes wrong. The wait-until-later approach is more likely to impose unexpected costs than not. Someone in the payment transaction will absorb these external costs. It is highly desirable, in terms of encouraging adoption, for the risks of errors, fraud, and criminal events to be allocated in advance of the events. This is what payments law and payments contracts do.[1] In addition, the change-in-terms model currently operating in Internet-based transactions—in which the provider unilaterally makes changes and the changes go into effect the nanosecond they are posted on the provider's website—won't work in mobile payments. Payors and payees need to know precisely what will happen to the payment instruction and payment receipt they are about to engage in. Any uncertainty of how a particular payment will operate will cause a delay in adoption or an abandonment of one mobile payment provider's products for another provider's product that operates on a more stable contract platform.

My analysis starts with the premise that every payment system—in the United States, at least—presents similar challenges that need to be addressed. Some of these challenges depend on the channel being used for the payment, whether checks, debit, credit, wire transfers, ACH, or mobile. Some of these do not. The fact that the payment system arises outside an established regulatory system is significant because it means that users, applying their experiences from other payments systems they have used, are likely to be surprised. These challenges need to be addressed in the system design and contracts and to be expressed clearly upfront: they cannot be left behind for later consideration. As noted above, an important side observation here is that the model for changes in terms on the Internet —where the provider makes occasional unilateral changes and the changes go into immediate effect following their posting—will not work in the mobile payments arena because users need to know in advance what rules govern the payments they are about to make.

For this presentation, I focused on three clusters of basic issues, which I have presented as a series of questions without much additional exposition.

Issues Relating to Payment Execution and Consumer Protection

As at the advent of e-commerce when proponents argued it should not be "regulated" for fear of stifling innovation,[2] we are hearing the same calls now with new payments products. I would argue that payments are payments and that certain basic issues require attention in contracts between provider and user, among providers and other participants facilitating the payment, and, as appropriate, between providers and government—but, in the latter case, for somewhat different reasons I describe in

greater detail below. But, more importantly, I would argue that most of the issues in fact are closely related to issues in traditional payments law.[3]

The basic questions I recommend that designers of mobile payment products and prospective users consider pertain to most types of payments being executed in the United States without regard to the "channel"—depositary or nondepositary—being used as the provider of the payment services involved. As most of these questions will be familiar to professionals in the broader payments industry, I do not offer detailed explanations of them or the differences that may exist between or among payment systems in this paper.[4]

1. If funds are deposited with the payment system, are those funds protected—by deposit insurance, state money-transmitter bonds, or not at all—so that the depositor is guaranteed completion of a payment instruction or redemption of the credits reflecting the deposit?

2. Are there limits—as there were with traditional savings accounts—on how and when the depositor may redeem the credits they have with the payment system provider?

3. Are sufficient authentication methods in place to deter unauthorized or altered payments? Or the redirection of validly issued payment instructions to someone other than the beneficiary originally specified?

4. How quickly does the specified beneficiary receive the payment?[5] Are likely delays in sending or crediting disclosed at the time the consumer "sends" the payment instruction?

5. Does the consumer receive a confirmation or other usable record of the payment for later purposes? How quickly does the consumer receive this confirmation or record?[6]

6. When does the discharge of the payment obligation occur? What rules govern if the payment instruction is not executed? Whether by dishonor or system failure or outage?

7. Are damages available for misdirection, failure to complete the payment on a timely basis, or for the lack of proper authentication? Are incidental damages allowed? Are consequential damages—such as late payment charges for delayed payments or as loss-of-bargain damages—available without an express agreement allowing them?

8. What charge(s), if any, will the consumer pay to make a mobile payment? Will charges be per transaction or a periodic fee? How and when will charges be collected? By the provider? By the merchant? Otherwise?

9. What rules govern the ability of the provider to change terms in any contract the provider has with the consumer? How frequently and with what length

and type of notice may providers change the terms of service? What options exist for consumers to opt out of any changes?

10. What rules govern substantive error resolution? Are these rules readily available to the consumer? Are they easy to understand and follow? Do federal or state laws also govern error resolution? What recourse will the consumer have in the event that the error resolution provisions of their contract with the provider or other procedure available does not satisfy the consumer? Access to litigation? Access to arbitration?

11. How long will the consumer have to report errors of amount, authorization, duplication, or misdirection? To whom will the consumer report any suspected error?

12. What contractual or regulatory liability limits protect the consumer in the event of unauthorized payments? What does the consumer have to do to invoke those limits? Is the consumer's opportunity to invoke liability limits time-limited?

13. Beyond immediate confirmation messages or copies of receipts, what type of periodic statement will the consumer receive to allow a review of all payments made via the provider's services during a particular period of time? How much information will the periodic statement, confirmation or copy contain?

14. What are the consequences for the consumer sender of a payment instruction if the payment provider files for bankruptcy protection or is closed by government authorities? What happens if a payments intermediary files for bankruptcy protection?

Consumer Issues that Depend on the Payment Channel Being Used

Different *sources of law* currently govern mobile payments made through direct bank account access and relevant applications (payments that should be referred to as "mobile banking") and payments made through nondepositary providers including, but not limited to, telecommunications companies (payments that should be referred to as "mobile payments").[7] For payments that are made via mobile devices and associated software as the "access devices" for payments from demand deposit accounts,[8] I recommend we use the term "mobile payments" so that the taxonomy of payments in these spheres stays as uniform as possible.

Mobile banking transactions are governed by the federal Electronic Fund Transfer Act[9] as well as by contracts between the bank and its customer. Mobile payment transactions currently are governed by a mix of state laws, including laws governing "money transmission" and "money services,"[10] and by whatever contract provisions govern the telecom-customer relationship. As of May 1, 2012, as I was recreating this paper from the original PowerPoint presentation, the FCC had not adopted any regulations that affect the pure payments portion of the relationship—even though it has other spectrum regulations and the like in effect.[11]

The types of questions that affect the telecom-customer relationship and the nontelecom provider-customer relationship may offer different avenues or needs for regulation. For example, one can imagine that near-field mobile payments may present issues different from more remote payments that function with special "apps."

The disparity between the regulation of mobile payments made via access devices directly between the sender's demand account to a merchant, and those that use processing intermediaries including telecom and other nondepositary providers to handle such payments is likely to remain until Congress acts.

Issues Pertaining to Privacy, Data Security, and Government Access

Mobile payments are likely to involve no fewer participants or individual data streams—and probably more of each. This much seems likely: the greater the number of hands through which a mobile payment instruction must pass, the greater the risks to privacy, data security, and, frankly, to government access.

I recommend that providers, users and potential regulators consider the following questions:

1. How does the payment provider protect the integrity of the payment information in transit and in storage, of the consumer's identity and the transaction data?
2. Is the provider's channel subject to federal or state privacy laws, or both?
3. Is the provider's channel subject to federal data safeguards and disposal laws and regulations, or to state data security laws?[12]
4. How may the channel affect government access to the payment and consumer information embedded in the payment instruction/message?
5. Will the consumer sender be able to recover damages (actual, consequential, or incidental) suffered? Will damages related to identity theft, if any, be recoverable? On what standard? Even in an arbitral forum?
6. Will providers recognize a duty to notify consumers in the event of an interruption the timely execution of a payment or in the event of a cyber-event affecting the data about consumer payment transactions executed by or through this provider or processor that is in addition to any statutory duty to notify the provider may have?

Data Storage and Retrieval Issues

This subset of issues covers very important questions. The duration and location of storage will affect significantly access to payments instructions in litigation and otherwise.

1. How long and where (physically or in the cloud) will records of transmitted payment instructions be stored? Which government agencies, federal or state,

regulate record retention for payment instructions and the accompanying deposit, sender and beneficiary information?[13]

2. How long may the consumer sender have access to these records? (Certain online banking records are available only for 72 days.)

3. How much does/will the provider charge the consumer sender for "copies" of records the consumer sender may need later to prove that the consumer made the payment?

Some Concluding Observations

In this presentation I outlined the types of issues that arise in payments generally and identified those that have particular pertinence to mobile payments. I do not intend to call for a particular form of regulation of nondepositary provided mobile payments. Rather, the purpose of this presentation is to inform those preparing to offer mobile payments products, consumers interested in using them, and governments that regulate payments for a range of purposes about the types of payments issues that mobile payments present with particular emphasis on new risks and new types of exposure of payments instructions to risks relating to data security, government access, and transaction execution.

My greatest concerns have little to do with reliable providers, depositary-based or not. Rather, they relate to the functional equivalents of the "wildcat" banks that were sprinkled over the Midwest in the 19th century and whose obligations were based on so little capital that holders of their notes and script often were unable to access the funds that the instruments evidenced.[14] To the extent that rogue providers enter this space and cause losses to consumers, merchants, and others in the payments processing systems, or that cyber-criminals infiltrate and siphon off funds intended for others, consumer and merchant adoption of mobile payments may slow. Whether slower adoption is a collective good or not, is a question for another day.

Endnotes

[1]System rules may lessen this risk, but they do not entirely resolve it for two reasons. First, consumers tend to be ill-informed about system rules so they may not realize that the rules can help them resolve issues. Second, system rules often only apply to entities that subscribe to the system, such as with ECCHO, even if they often benefit consumers indirectly. In the absence of a provision such as Uniform Commercial Code §4-103, which incorporates Federal Reserve regulations and operating circulars and local clearing house rules as if all participants had expressly agreed to be bound by them, in payments transactions to which the UCC's Article 4 does not apply, this provision is only available by analogy.

[2]For a recent example of this type of argument and the concerns it engenders in other providers, I note that brick-and-mortar business owners in Indiana, including the Simon Mall Group, forced a deal under which the warehouse operations in the state will pay sales taxes by arguing that leaving Amazon.com free of the tax created an unlevel playing field between e-commerce and brick-and-mortar operations. "Indiana reaches online sales tax deal with Amazon.com," *Indianapolis Business Journal*, Jan. 9, 2012, *http://www.ibj.com/indiana-reaches-online-sales-tax-deal-with-amazoncom/PARAMS/article/31851 (reporting that Amazon.com will start paying Internet sales tax in 2014).*

[3]In this connection I urge readers to read the invaluable article by the ABA Task Force on Stored-Value Cards titled "A Commercial Lawyer's Take on the Electronic Purse: An Analysis of Commercial Law Issues Associated with Stored-Value Cards and Electronic Money," 52 *The Business Lawyer*, 653 (1997).

[4]I intend to consider these issues more fully in another paper in the near future.

[5]The paper presented by Bruce J. Summers, Ph.D., on March 30, 2012, at this conference titled "Facilitating Consumer Payment Innovation through Changes in Clearing and Settlement," which introduces fascinating (and possibly also fraught) prospects of real-time settlement of payments made on mobile devices, a paper that everyone interested in mobile payments should read. I would observe for the purposes of my paper that, although a boon to merchants and other direct counterparties of the person issuing the payment instruction, real-time settlement has the prospect to attract criminals to the mobile payments arena, those interested in taking the money and running.

[6]One of the best authentication and verification features of many mobile payments products is the sender's receipt of a prompt confirmation of the transaction. Arguably, confirmation received on the mobile device will provide more lasting, and far more secure, records for the sender. Their only deficit relates to issues about how the confirmations will be used later to prove payments when the sender and payee are not in the same locations at the time questions about the payment may arise.

[7]For this crisp distinction between "mobile banking" and "mobile payments," I am indebted to Philip Keitel of the Federal Reserve Bank of Philadelphia whose

essay titled "Contactless Consumer Payments: A Review of Rules, Laws, and Regulations That Apply to Over-the-Air Communication of Consumers' Payment Information" will appear in the forthcoming anthology of essays about Radio Frequency Devices and Other Near-Field Communications that I am co-editing for the American Bar Association.

[8]The Electronic Fund Transfer Act defines the term "accepted card or other means of access" as "a card, code, or other means of access to a consumer's account for the purpose of initiating electronic fund transfers when the person to whom such card or other means of access was issued has requested and received or has signed or has used, or authorized another to use, such card or other means of access for the purpose of transferring money between accounts or obtaining money, property, labor, or services" 15 U.S.C. §1693a(1) (2010). The term "account" is defined as "a demand deposit, savings deposit, or other asset account (other than an occasional or incidental credit balance in an open end credit plan as defined in section 103(i) of this Act), as described in regulations of the Board, established primarily for personal, family, or household purposes, but such term does not include an account held by a financial institution pursuant to a bona fide trust agreement" 15 U.S.C. §1963a(2). I also note that the term "electronic fund transfer" includes electronic payments initiated through "telephonic instruments" or "computer or magnetic tape" so long as the transaction orders, instructs or otherwise authorizes a financial institution to debit or credit an account 15 U.S.C. 1693a(6).

[9]15 U.S.C. §§1693-1693r (2010), Pub. L.90-321,92 Stat. 3728 (Nov. 10, 1978).

[10]A few states, such as Montana and South Carolina, have no laws or regulations governing money transmission or money services. For a complete listing of state statutes governing money transmission and money services, see *www.ncsl.org*.

[11]For a discussion of spectrum regulations affecting near-field communications, see Gregg P. Skall's essay titled "RFID Frequency Issues" in the forthcoming anthology of essays from the American Bar Association. Mr. Skall is a partner in the firm of Womble Carlyle Sandridge & Rice PLLC in Washington, D.C. He can be reached at 202-857-4441 or gskall@wcsr.com.

[12]At the federal level, only "financial institutions" as defined in the Right to Financial Privacy Act of 1978, 12 U.S.C. §3402 (2010), Pub. L. 95-630, 92 Stat. 3697 (Nov. 10, 1978) are covered by the Act and only when the government agency making the request is an agency of the federal government. The definition of "financial institution" was last amended by the Intelligence Authorization Act for Fiscal Year 2004, Pub. L. 108-177 (Dec. 13, 2003), incorporating every provider designated as a "financial entity" for purposes of the Bank Secrecy Act, 31 U.S.C. §5312(a)(2) (2010). Telecommunications providers are not "financial institutions" or "financial entities" for these purposes at this point.

[13]Depositary institutions are required to maintain records of payment and deposit transactions for a period of seven years. Telecomm providers are not yet

subject to similar requirements, and mobile payments providers who fall into neither category seem to have no record maintenance requirements except as the providers themselves may decide to have.

[14]For a history of wildcat banking, see Gerald P. Dwyer Jr., "Wildcat Banking, Banking Panics, and Free Banking in the United States," Federal Reserve Bank of Atlanta, *Economic Review* 1 (December 1996), available at *http://www.frbatlanta.org/filelegacydocs/acfce.pdf*.