Cash, Check or Cell Phone? Protecting Consumers in a Mobile Finance World
February 23, 2010, Washington, DC
Panel Four, Mobile Commerce Challenges: Emerging Consumer Issues

Transcript of a live presentation given at a Federal Reserve Board conference

Harley Geiger:
Thank you all very much for having me. So I'm Harley Geiger, and I'm from the Center for Democracy and Technology, and CDT is a DC-based nonprofit. We're focused on preserving privacy and civil liberties, while enabling companies to innovate and technologies to grow. So, I'm going to be talking about privacy and security.

Why privacy? There are several reasons, of course, and the reason that I'm going to focus on here is that it factors into consumer adoption. The 2007 study from the Helsinki School of Economics found that respondents had been concerned that mobile payment service providers would track their purchases for marketing purposes. Likewise, a 2009 KPMG study found that nearly half of consumers who had not tried mobile payments yet cite privacy and security as the primary reasons. So, mobile payment adoption will increase when consumers have confidence that the method is safe and that their privacy choices will be respected.

So security. And I'm going to talk first about authentication. And here there's cause for optimism, because early contactless cards, as many people I'm sure are aware, were at risk of being skimmed without user authorization. But since mobile phones are essentially small computers, we have the opportunity to build in authentication protocols into the system so that no single transaction goes by without the consumer's notice or consent. There are various ways, of course, to authenticate or authorize a transaction -- PIN numbers, challenge questions, confirmation screens -- and CDT urges providers to integrate these protocols into their systems.

One challenge, though, that authentication is going to face is that authentication may diminish some of the convenience of mobile payments, because mobile payments are supposed to be quick and easy, adding in extra steps may make it less convenient. Still, CDT thinks that users should have control over whether or not authentication is required for each and every transaction. Currently it's not for some small, for example, NFC transactions. However, the risk of fraud does increase without authentication, and it increases without cryptography.

So CDT believes that the entire transaction, from phone to reader, from end to end, should be protected with strong encryption. Here again, there is some cause for optimism in securing a WAP, the wireless application protocol. The first generation of WAP was rather hard to encrypt, but the second generation of WAP makes strong cryptography achievable on mobile phones. So what remains is for providers to adopt it wholesale, and CDT urges them to do so. NFC contactless systems, in particular, are specially deserving of cryptography. They can benefit very strongly from it, because while it is perhaps the easiest mobile payment system to use by just swiping your phone over a reader, it is also

vulnerable to eavesdropping, particularly at a distance, even when the communication range is short, by an unauthorized party wielding an amplifier or an antenna. And this is also particularly so if the NFC system is actively broadcasting a signal, as opposed to being passive. So consumers, we think, ought to have the ability to turn off their NFC signal whenever they want. So, as with authentication, I urge manufacturers and service providers to continue exploring encryption for incorporation into their products.

The mobile phone's small screen size will probably create some difficulties. People have been trained to look for the lock symbol on their websites to ensure that a particular website is secure enough for them to conduct a transaction with their personal information. But there's a question as to whether or not the lock symbol will appear on all mobile browsers. Likewise, people have been trained to spot phishing attempts by seeing if a website is distorted or looks different from that which they're normally used to. But many websites look distorted or different when you look at them on a mobile phone versus a traditional computer. My last point on security is that it's a moving target. Security is a moving target in this area, and mobile payment stakeholders should conduct periodic independent assessments of their operations and those of their affiliates, especially as new challenges inevitably arise to meet the mobile financial services environment.

So I'm going to talk about privacy for a bit. Mobile payment raises several privacy issues, and unfortunately it's clear that mobile payments and mobile banking is going to be another way that technology sort of spreads around consumer information as they go about conducting their routine tasks. So there's a -- one of the biggest questions is whether or not mobile financial services will result in a lot of targeted advertisements. While it remains to be seen whether marketers will -- sorry, whether mobile finance will enable marketers or investigators or other entities to access consumer data to such an extent that consumers need more stringent protection, it's still reasonable to assume that this is going to increase. Service providers are already contemplating this. And we know that most consumers don't want to pay extra for mobile banking. This is encouraging some mobile payment service providers to seek other revenue sources through advertising. But we also know through other studies that many consumers object very strongly to advertisements that are based on their activities. So, mobile payments will generate data in excess of that that we see in traditional credit card transactions, in particular, your NFC number, location data, possibly your purchase data, and your phone number. This may be shuttled to different parties than people are used to.

The consumer data captured during mobile payment transactions can be used in various ways, as I've mentioned already: targeted advertising, location tracking. So let's take near field communication as an example again. NFC is capable of exchanging a wide variety of data, such as business cards, photos, wallpapers, ringtones. So what other data will be transferred with payments? For example, will consumers be divulging their phone number to merchants with every transaction, and will merchants transfer -- transfer special offers or coupons to the consumer every time that they make a purchase? And what about adware for your purchase data? That is, what you purchase, when, and where. The issue, really, is whether consumers have a choice as to whether or not their data will

be used for delivering advertising to their mobile services. And the law does give them some limited choices.

When it comes to targeted mobile advertising, the CAN-SPAM Act requires advertisers to obtain opt-in consumer consent in order to deliver targeted advertisements to mobile devices using the Internet. So what counts as opt-in consent? It has to be an affirmative act. It can be done orally, and it must include the address, or in this case the phone number, to which the messages will be sent. But does it count if a consumer makes a purchase that automatically divulges their phone number? Perhaps more likely, merchants will use a box-checking system, so you can uncheck the box if you wish to decline mobile ads, or check the box if you wish to receive them. We are familiar with these. CDT thinks that the box should remain unchecked. This is more in keeping with the opt-in regime.

So I'm going to talk more about consent here in a moment, but I also wanted to raise the issue of adware. So what about adware on mobile phones? Adware, I'm sure you're familiar, is basically software that displays ads on your computer or on your mobile phone. And it may or may not operate by targeting your browsing history and delivering ads based on your activities. It can be installed, for example, as part of a software package, like a media player or an app that you've put onto your system. And to my knowledge, there is no federal law that directly regulates adware placed onto mobile phones. Adware loaded onto a phone could not use auto-dialing, nor use the Internet to deliver targeted ads, theoretically exempting it from CAN-SPAM or the Telephone Consumer Protection Acts. It's here the Mobile Marketing Association does have a set of self-regulatory guidelines that are reasonably protective of privacy, and they require opt-in consent from consumers before they can be entered into a messaging program.

But still, the codes requirements don't address adware directly, nor does adware fit quite as neatly into the codes requirements as SMS. States have -- several states have anti-spyware laws, but they define adware and spyware very, very narrowly, and they require only notice and consent, and some don't even require that. They only require that the adware is not intentionally deceptive. But many times, the consumers have already consented to the presence of adware on their phones through license agreements or terms of service. So I think that obtaining consents may be a practical problem for the industry that seeks to monetize consumer information for advertising purposes. CDT strongly disfavors blanket consents, the sort of consents that you see in terms of service. Terms of service, most people don't read them. They're notoriously long and complex. One suspects this is almost done on purpose. And people won't read terms of service on a mobile phone screen, they'll do it at a lesser rate because of the small screen size. It'll put a significant challenge to reading it. But if we don't offer consents in terms of service, then consumers will be faced with a screen every time they make a payment asking them for their consent. That might be as annoying as advertising itself, and would it in any case diminish the convenience of mobile payments.

So I have several privacy recommendations. As I mentioned earlier, CDT encourages end-to-end encryption, as well as authentication controls in mobile payment transactions.

Merchants and service providers should specify what information from consumers they're going to collect, and what they're going to use it for no later than the point of collection. And they should give them choices with respect to their data. To the extent that this is a software and hardware manufacturing issue, we urge manufacturers to preserve the ability to withhold excess data from transactions, such as your phone number or your purchase history, and as I mentioned, a kill switch for your NFC communication device. I urge regulators to be vigilant in observing what happens to consumer data, the buying, selling, and data mining consumer data in the new mobile environment. The current mix of legislation and self-regulation is pretty good, but whether or not consumers will need more stringent protection remains to be seen. And I urge regulators to pay particular attention to the proliferation of adware, and whether or not self-regulation and state laws are protecting consumers adequately, or if more stringent federal regulation is needed.

And then lastly, I urge companies to do everything that they can to mitigate data spills and the abuse of consumer data. Data abuse can seriously damage the industry, eroding consumer confidence and encouraging reactive regulations, so companies should continue to take these issues very seriously if mobile payments should take off, and we hope that it does. Thank you very much for having me.