General Discussion

The Economics of Retail Payments Security

Mr. Moore: Thank you for your comments, Adam, and I do think they nicely built on a lot of what I started. I just have a couple of really quick responses. One is the discussion about spillover effects and externalities. I completely agree that externalities are hugely important in this space, and it is true that game theory does not directly account for third-party externalities and that our models sort of ignore them. But what I will say is that game theory is so helpful in describing the private actors taking the decision: it is true that they do not care if they are causing negative externalities on other parties, and so they are still going to take the decision that privately suits them best. I think where it comes into it is when you are thinking from the public/social optimum, we need to actually have a real conversation about externalities. And if nothing else, the fact that we have such pervasive externalities at play motivates the need for greater public oversight and involvement.

The challenges of moving to this sort of public ordering and having a greater public direction, which you also rightly pointed out, are that it is really difficult to envision public authorities developing a better solution than the private sector. What that really points to is the need to have private sector engagement in this, but there is still a role for the public sector to help shape and coordinate the response.

On the point about data, I completely agree, and I think data on fraud can be very helpful in mitigating these key information asymmetries. Many other countries are already collecting data on payment fraud and also security in general. I think it is a key to actually improving the long-run security of our system. It is also potentially less controversial because you are counting things and not prescribing action.

As for an aside point—your question about insurance—cyberinsurance is something that might arise as a result of collecting better data. We have seen this come true in the case of data breaches in that data breach legislation is a very decentralized/indirect way of forcing data collection because you are waiting for the bad event to happen, and now information is being published. But the fact that has happened has engendered a very growing and important cyberinsurance market for insuring against data breaches. I think we could expect to see them. If we start collecting better data and publishing the data, which are also related to other security threats including payments security, it would probably work better. One anecdote: I have talked to many cyberinsurance underwriters, and you are wondering how do they price this stuff? The best I have heard is that the underwriters get on the phone with the security teams at organizations and get a sense of how good a job they are doing and they pull a price out of the air. It certainly is something that could be improved if we had better data on the problem.

Regarding the discussion about consumer liability, I agree the lack of consumer liability can have some of the consequences you have described, but from other research into cybersecurity in general, the direct losses that have been attributed to cybercriminals tend to be dwarfed by the indirect costs related to negative changes in consumer behavior. What I really worry about is that if we increase consumer liability it will shift behavior in a way that is net harmful to the economy by having less engagement in new technologies.

Mr. Levitin: I find cyberinsurance really interesting because one thing we have seen in other markets is that insurers will start to drive practices, levels of care, everything from building codes. Casualty insurers are concerned about having buildings that are less likely to burn down. Life insurers are concerned about people using seat belts. Do you know of anything like that in the cyberinsurance market where insurers are pushing for better practices?

Mr. Moore: This is the great big hope for cyberinsurance. The Department of Homeland Security has been pushing for greater availability of cyberinsurance, hoping this will happen. I have yet to see many examples. There have been informal conversations between underwriters, but the sophistication is not there yet in identifying key controls. But I will say that sometimes they run checklists. If you are not adopting very standard security controls like the SANS 20 Critical Controls, if you cannot show you have taken some baseline measures, then they set a higher price. It is starting to happen, but it is still at very early stages.

Mr. Dubbert: Let us open the discussion to questions from the audience for Tyler, or Adam, or both.

Mr. Grover: Tyler, you commented that Bitcoin was more secure than existing payments systems. By some estimates, roughly 10 percent of all the bitcoins ever issued have been stolen or lost. There is no 24/7, there is no centralized support, and as a network it lacks critical mass. Given that, beyond illicit use cases, do you have a view whether Bitcoin can or will be a long term, viable retail payment system?

Mr. Moore: Yes, the ecosystem is not secure, which you rightly pointed out. We did a study. And around the time of our study, 45 percent of the currency exchanges in Bitcoin subsequently closed. The currency exchanges in bitcoin are effectively de facto banks and so that is a pretty bad bank failure rate. Many of those failures led to a loss of consumer, customer deposits. So, it is not secure in that respect. When I say it is secure, I mean that the payment itself within the network is quite secure and that if you have your Bitcoin account or Bitcoin address, and if you can maintain the secrecy of the corresponding private key, then it is completely secure. But as we know, if you are running this on your computer and the computer gets malware, then someone can obtain the key. There are a whole host of operational security challenges that would need to be dealt with through greater governance and perhaps changes to how they deal with things like revocability of payments. Whether or not it is going to make a long-run impact, I do not know. There are some encouraging signs in a few areas, including one in the remittance market. If you look at international payments, this is an area that is very expensive for people sending money to their home country, and there is a real opportunity for someone to come in and charge less money. The problem is that people may not be able to overcome the technological challenges of having bitcoins, not to mention the risk of holding them. But there is a company called BitPesa, which hooks up with the existing M-PESA system in Kenya so that people in the West can go to their website, send money, and the payment goes through the Bitcoin network and then is received in Kenya through the M-PESA network. The charge is a transaction fee of 3 percent. That is a concrete use case where I could envision this receiving wider adoption. But whether it could also be used to challenge existing payments, I think for it to be successful, first, consumers should not even know there are bitcoins involved. They should not be holding the bitcoin and they should be able to pay in the currency they actually use. There are some efforts to move toward that,

but nothing on the market is really good yet. But there are people working toward that goal. The broader question is what happens with fraud? How does fraud get resolved? I think that has to be dealt with to get wider adoption.

Mr. Levitin: Eric, let me just add, I think where we may see the real value in Bitcoin is as an alternative clearing method. As an alternative currency it is hard to see Bitcoin being very attractive in developed economies with stable inflation. If you are in Venezuela or Zimbabwe, however, Bitcoin may be a more stable currency. But it is exactly what Tyler was saying; that is basically the clearing mechanism, which could be potentially dealing from the currency function and you could have essentially this open source clearing.

Mr. Moore: And there is some technological innovation with blockchains. So, we have this distributed, pretty secure system for processing payments that potentially could be quite valuable. And that is where a lot of the interest seems to be focusing among venture capitalists.

Mr. Hamilton: Very, very interesting. Two quite different lenses on the economics of payments security. If I can, I want to take you back to the fundamentals. I am trying to get away from the "Bitcoinitis" that many conferences fall prey to now. Back on the fundamentals of payments security, it seems we really need to work on defining our underlying policy goal. We have talked a lot about the motivations of the different parties, but what is it we as a community really ought to be trying to achieve? There is an unstated assumption that it should be zero fraud, but I am not sure that is right. So, what is the right policy goal, and where do you think we should be starting in this journey?

Mr. Levitin: There is an efficient level of fraud, but it is not zero. We want to get to where the marginal cost of fraud, or marginal fraud losses, is equal to the marginal cost of fraud prevention. Again, that is not going to be zero. I do not know exactly where that is, and I think we cannot really figure that out until we have better data. But zero fraud should not be our goal. Instead, it should be whatever the efficient level of fraud would be within the system.

Mr. Moore: And zero fraud means that you could always spend an infinite amount on security and you still would not achieve it. One of the things we could do is facilitate adoption of technologies that make payments secure. It is kind of a dance because you do not want to be prescriptive in saying we need to adopt this technology because that tends to favor

the wrong winner. But you can see most of the credit cards in my wallet are running on this 30-year-old-plus technology that is completely insecure. And I think there is a correct perception that what we need is to try to take advantage of some of the technological improvements to security and get them adopted with the idea being that they could reduce fraud rates, potentially also reduce the incidents of data breach and ultimately the amount of money we spend trying to protect this. Because we have this very valuable data that is now widely distributed across tons of companies, we have to turn around and spend all this money to protect the data, but we are protecting it poorly. I think we need to take a step back and say, well, what we need to do is to find technologies that allow us to eventually reduce the overall amount that we have to spend. But to do that, you have to actually spend some money, change the technology and coordinate on the more secure technologies.

Mr. Butler: First, let me preface my question by saying this is not my exact field of expertise. I want to jump back to ask a question similar to the policy question. I recently saw the update to the National Institute of Standards and Technology (NIST) standards, the Federal Information Processing Standards (FIPS) 201 Compliance update for Personal Identity Verification (PIV) cards and federal IDs, et cetera. I would like to understand why we do not use more of what that standard is for federal practices, more in terms of a broad-based consumer application. So, maybe a layer above; use that standard as a means to facilitate and lock down security in a device like a mobile device or card or whatever it is and being able to expand that to just more than maybe access to something, but also using it as a payment device. Does that make sense?

Mr. Moore: So, the NIST standard you are referring to has to do with identity? Like the chip cards federal agents use?

Mr. Butler: Yes, chip and PIN.

Mr. Moore: Well, there is an effort that NIST led, the NSTIC, the National Strategies for Trusted Identities in Cyberspace. That was an attempt to get broader adoption of greater identity management technologies. But it is interesting in that they have some problems in common with payments: a two-sided market. You need to get identity management providers who can authenticate the users, and you also need to get more subscribers who are going to actually have that. It works in the federal government's case because the identity management provider is the government, and it can say employees have to do it. But as soon as you get it to a much greater

distribution scale, it is much harder to actually require or build up that adoption. Then you are stuck with all the challenges of building up a two-sided market, which can inhibit the adoption.

Ms. Garner: I wanted to come back to Adam's chart of public ordering versus private ordering. If you had to rank these from a public policy perspective, and these are all good items to think about, which one or two are the most important to get the best policy outcomes if we do a side-by-side comparison?

Mr. Levitin: I do not have an answer. The chart just represents my own "druthers" and reflects my own priors. I am particularly concerned about externalities. I do not like them in general. I do not want to smell the smoke from the person in the next apartment. I do not like externalities. That would be my first and foremost concern. One general reason for regulation is to try and address the market failure that you have when you have externalities. But certainly, I think we also need to be concerned about market power. We know we have a system within payments where there are network effects that both amplify market power and create an incentive for parties to try and grow their market share; the system has outsized benefits from larger market share. I think that needs to make us very wary of the outcomes in private ordering. Again, I am not sure we know what to do in terms of a regulatory response, but I think we need to be very skeptical about the optimality of the private market in this space.

Mr. Moore: For public authorities, how to deal with these platforms that have such market power is still being figured out, dating back to Microsoft and interventions taken against them. The economics of IT suggest that across many systems you are going to have these dominant platforms that emerge, and they emerge through competition. And so there is a conflict between that and what we espouse in antitrust law and policy. Antitrust was developed in an age where you did not have information markets, and even though there was market power, it did not emerge in as many places. I do not think regulators have really figured out how to deal with it at this point. But that does not detract from the significance of the challenge.

Mr. Taylor: I have a question for both of you. I am with the National Association of Convenience Stores and Conexxus. I run a standards organization. When we talk about PCI and EMVCo, I think the biggest mistake people make is that they are perceived as standard-setting bodies, which they are not. They are specification bodies. A cursory look at the bylaws would tell you they do not have the same accreditation as an American National Standards

Institute (ANSI) organization, or even a NIST would have where you have voting on candidate standards. That being a fact, my question is what value do you see in a true standards body mitigating that market power, which is in the box in the private ordering, that might make private ordering, if it was done through a public standards body, a better alternative?

Mr. Moore: What EMVCo creates are de facto standards. But they currently do not go through the same open process you have in bodies like ANSI and even the Internet Engineering Task Force (IETF), which is a private organization. IETF deals with standardization of Internet communication protocols. And what is interesting there is that it is not facilitated by the government. It is a private organization that still does standard setting. I think what that tells us, first, is that standard setting can be seen as valuable to the private sector, even irrespective of government involvement. But the challenge I think that comes from things like EMVCo and the different de facto standards that come up in the payments security space is that with truly open standards, you get much more outside evaluation prior to deployment. I think this is quite critical for the success of the overall security of the resulting mechanisms that are used. Time and again we see secure protocols and mechanisms deployed outside the standards process that are found after the fact to be insecure. I think moving to a platform that has greater openness could really benefit that by making sure the technologies we deploy are in fact more secure. Now, it could still be done, and I am not saying you have to switch to ANSI to do this. You could just have greater openness and move these platforms to have a lot of the same characteristics you have in standards bodies. I think that would be a good step forward.

Mr. Voormeulen: I would like to share one experience from the Netherlands about this topic. I liked what Adam said to broaden Tyler's presentation on what choices people have. What we see in the Netherlands, for instance, if you look at the retailers, even if they have no direct liabilities, they still have a great interest in security. They like to be paid by debit cards because that is cheaper and has less handling costs than cash. But if people experience fraud, they will turn back to cash payments, and cash is more expensive for retailers and leads to more crime, robberies in shops. That is the interest for the retailers. If you look at the Web shops, they have been really pushing for security because they feel that if consumers have some doubts about the security they will not buy things. Their market will expand if security is at a higher level. And if you look at the banks, I do not know how it is in the Unted States, but in Europe banks today have a little reputation issue. There are many consumer programs on television about bad experiences with banks,

and the banks are really caring about their reputation. If they can find ways to make payments more secure, whether that is through the Internet or at the point of sale, that increases their reputation. If you bring all those parties together, then you come at what Adam called soft policies, and maybe that is also a solution of what to choose there, private or public ordering. In the Netherlands, the central bank tries to bring together the parties—retailers, banks and consumers. I admit that is easier in a country of less than 20 million people than in the United States. But that really works in the sense that, I think, the externalities are taken more into account, and the problems Tyler sketched in game theory can be overcome so that you can go to the bottom block immediately without problems because you take the common interest, which is that everything becomes more secure. Every party in the game profits from that.

Mr. Moore: I will briefly say one thing to that. It is no coincidence that you have had chip cards adopted in Europe sooner than in the United States, in part because you have a much more consolidated sector, which makes it easier for the central bank to bring together the stakeholders and get everyone in the room to agree that they need to move. It is nice if you can do it.

Mr. Levitin: Beyond that though, at least in some countries, the central bank has the authority over most of the players within the payment space. We lack that in the United States.

Ms. Alter: I have an unlucky colleague who had an experience where he was mugged at gunpoint in his neighborhood in Chicago. Within maybe a month, he also had his debit card compromised and his account basically drained of cash. And the way those two crimes were treated was very different. Of course, one was a police report, and the other really was not. And I am just wondering in the case of having a victim, and I do not know if this was viewed as him being the victim of the payment card being compromised, but if those two were treated similarly, would that have facilitated a little better data collection? To your point about gaining a little bit more information about fraud rates and those types of crimes?

Mr. Moore: I would say that if it is physical crimes, they tend to get reported to the police more often, but there are ways to report online crimes. There is an Internet Crime Complaint Center (IC3), which is a partnership between the FBI, the National White Collar Crime Center and the Bureau of Justice Assistance, but there just is not as much incentive to report these cases.

Mr. Levitin: I grew up in Chicago. I would hope the Chicago police would try, if you can identify the mugger in a lineup or something, that they would try and catch the mugger. But I cannot imagine them trying to track down the cybercriminal. Part of it is just the expertise involved in trying to deal with a cybercrime. To the extent we have any expertise there it is not on the local police level. There is a mismatch there. But your general point that it is all crime, that we need to be thinking this—it is all property crime whether it is at gunpoint or electronic, and that we should be collecting data on it the same way—I think is exactly right.

Mr. Marshall: I have a question. This may be describing the problem we are going to have in the next two or three years, but we are already seeing this. Increasingly in the financial industry, we are using one-time passwords sent via email or phone, and we are finding that email companies and phone companies have significantly less controls than we do in financial services, and the losses we are seeing from those one-time password compromises, there is no financial incentive for the email providers or the phone companies to improve their controls. Do you have any advice on what we should do?

Mr. Moore: Because we are talking about platforms, the largest webmail providers account for a very large share of all email. And working directly with Yahoo, Microsoft and Google can certainly help to improve that security. That is kind of a narrow but unsatisfactory answer.

Mr. Levitin: You may want to think about ways of sending that one-time password that do not involve going through the telecom. One example would be having some sort of RSA token built into the device itself. I remember several years ago seeing a Turkish bank issue a card that had that feature.

Mr. Moore: For example, Google has a one-time password authentication token generator built into an app on smartphones. And that avoids network communications, but obviously then you have to worry about the security of the end-user device. But generally speaking, and certainly in the West, smartphone security is much greater than desktop security.

Mr. Dubbert: Tyler, thank you so much for the co-authoring the work to look at the economics of payments security, and Adam for taking the time to respond to that and give very insightful comments.