The Economics of Retail Payments Security

Commentary

Adam Levitin

Thank you very much for inviting me to respond to a really interesting and much needed paper by Fumiko Hayashi, Tyler Moore and Rick Sullivan. I should say as an initial note, there is an irony that this is a session on the economics of payments security, but we have a computer scientist as a co-author and the presenter, and a law professor as the discussant. While I am a law professor, I do practice economics, but without a license. Despite the scale of the transactions involved in payments, payments remain really an understudied area across academia. Payments security, in particular, is pretty much virgin soil. I think that makes this paper Tyler, Fumiko and Rick wrote really important. It is a great foundational paper, and I think it is going to lay the ground for, hopefully, a lot of future work.

Now, I have no bone to pick whatsoever with the paper's basic argument that economics is a useful tool for understanding payments and payments security, and in particular game theory as a method of thinking about the coordination and cooperation problems involved with adopting payments technology. But, like all modeling, game theory is a type of modeling that is built on a number of assumptions. I want to underscore a few assumptions that I think can be a little problematic when applied to payments security. My point here is not to criticize the paper on these assumptions, because all modeling is built on assumptions and necessarily simplifies. But instead, seeing where the game theoretic assumptions do not hold up is very valuable because it points to where some of the challenges are in payments security.

Let me start by going through what some of the assumptions are that I think are a bit problematic. The first assumption is what I term the "knowledge assumption." This is an assumption that the parties in a game know

how the game works and what the outcomes are, implying that the parties are able to choose rationally between choices such as whether to adopt EMV or not adopt EMV. The second assumption is what I call "causative assumption." This is often termed as a rationality assumption, but I do not think it is quite that, as I will explain later. The third assumption is "bilateral game," which is not formally an assumption in game theory because you can have multilateral games. But very often game theory likes to do simple, very clean models with bilateral games. A problem is in payments it is not just two parties in the room. Another problem is that game theory never accounts for externalities or spillover effects on parties that are not involved in the game. If you are thinking about, for example, the EMV adoption game, what about the effect on consumers? Although consumers generally bear very little direct pecuniary liability for fraud, there are all kinds of other costs that consumers do bear when there is fraud; the hassle of having to change your automatic bill payments, the hassle of having to get a new card, and so on. The fourth assumption is "binary choice." You can have games that have more than two choices but that gets much harder to model. Let me go through these assumptions in a little more detail.

Our knowledge assumption is that the players know what the outcome values are, making a game a static model. In the EMV adoption model, for example, if I adopt EMV, my payoff is 1; if I do not adopt it, my payoff is 2. The problem with this assumption is that we are in a dynamic world where the values of adopting a technology are going to change. We are in a world where hackers never rest, and security within a system can be upgraded. EMV is not a static technology, making it much more difficult for parties to know what are going to be the costs and the benefits of adopting the technology. This dynamic nature, I think, tends to push toward stasis because there are always immediate costs, but the benefits are often less clear.

On the causative assumption, game theory assumes players act based on expected game outcomes. This assumption is often expressed as being a rationality issue, but I think the problem here is not rationality but the fact that security is not a standalone product. Financial institutions, merchants and consumers do not buy security; instead, they get a bundled payment product with various features. Their choices are based on that total bundle, not necessarily on security. Google Wallet, Apple Pay and CurrentC were shown in Tyler Moore's presentation, and for each one of those businesses, security was a feature, but not what was driving those businesses. For instance, Apple was

concerned about selling phones, and if security helps it sell phones, it is going to double down on security. But at a certain point if additional security does not help sell more phones, the added security may not be an interest of its customers, and thus Apple may stop adding security. There is a limit to how much effort businesses want to put into security, I should say.

How about the bilateral game assumption? Game theory usually models games of two players; multiplayer games are harder to model. But you look around the room and you see all kinds of multiplayer coalitions being represented here. Google Wallet, I think, is a nice example where you had MasterCard, Google and Citibank initially as partners. While two-player games always have a stable equilibrium, with possible coalitions in multiplayer games, we do not know if we necessarily have a stable equilibrium within the games. Of more concern, at least to me, is that game theory never accounts for third-party externalities. Let me give you an example of why this is a problem. If we have a data breach at Merchant 1, that can result in fraud losses not just at that merchant, but at other merchants, and also for banks that do not do any business with Merchant 1. The spillover costs to banks are never accounted for within a game theory model (in which players are merchants only, not including banks), yet that is often how we have fraud losses allocated. I think we need to be a little careful about the bilateral game assumption.

Finally, the last assumption is binary choice; cooperate or not. That is how game theory often sees things. Real life is not a binary choice. An alternative to cooperating in one game is often playing a different game, and it is much harder to model a universe where you have multiple simultaneous games going on. In theory, you could try and add things up, but additivity can be a problem.

What is the implication of these limitations on game theory? Game theory works really well to analyze an idealized version of the world. But when we see where the assumptions do not hold up, I think it starts to point us to a payments security agenda of sorts. Obviously, there is not one single correct setting for security for all payments, but I think there are some broader policy principles that we should be pursuing. I am going to emphasize three of them; data about fraud losses, the need for competitive markets and the need for fairness.

The knowledge assumption points to the need for data. If parties do not know what the outcomes are in the game, they cannot make a rational

choice within the game. That says we really need good data on fraud, which are not just fraud rates. We also need to consider things like definitional questions. How do we define fraud losses? You have the direct fraud losses: someone steals my credit card information and buys a TV from Best Buy. There is the cost of the TV. But then there are all kinds of collateral costs. What about the restocking that Best Buy has to do? What if someone has to run a call center, or add employees to a call center? What if there is data breach notification? Figuring out what costs go in is, I think, a part of getting data and hopefully we can standardize it. The causative assumption and the binary choice assumption point to the need for competitive markets, trying to get an efficient outcome in terms of security decisions. The bilateral game assumption points to the need to be concerned about third-party externalities and try and have fairer markets in that sense.

To achieve the goals of data, competitive markets and fairness, we may need different tools. So let us drill down a little deeper about these three goals. Data is important because it helps facilitate efficient outcomes. This is not just about the choices in the primary market, but we can also think about secondary markets. Normally, when we have risk, we like to see secondary markets develop. The secondary markets not only help parties spread risk but also instill market discipline. There is insurance in payments but we do not have very good secondary markets in fraud risk for payments. One could imagine fraud derivatives existing. I would think that the market would want to create it, but you need data for it. The concern about competitive markets is who is making the rules. We have the problem that rules, or the security standards, may not be set based on what is going to be the most efficient or the most secure, but instead based on other considerations like growth. This is a concern particularly in network industries because if you can grow your market share, you get the benefit of network effects and you may be able to shift the costs of doing so on to other parties. Lastly, fairness is, again, the spillover effect.

How are we going to achieve these goals? There are currently three major approaches we see used. There is private ordering, which is just contract. There is what I am going to call hard regulation, which is command and control; "Thou shalt do, thou shalt not do." And there is soft regulation, which is a pretty big catch-all bucket for various types of niches, guidance, and I would even say litigation enforcement might go in that bucket.

I want to drill down on soft regulation a little more. That includes a convening and coordination role from the government, and we see the Fed starting to do that now with the Faster Payments Task Force, the Secure Payments Task Force and the Atlanta and Boston Fed's Mobile Payments Industry Working Group. There is potentially data collection which can be voluntary or mandatory, but the Fed is not saying to businesses that they have to adopt a standard or not do something. The data collection is so critical because it allows empirical research and the potential creation of (secondary) markets. It also starts to actually form a common language—it has its own standard-setting role because if you are reporting data in standardized categories, that is a form of standards setting. There are all kinds of regulatory guidance. Governor Powell mentioned the FFIEC guidance. Regulatory guidance is formally not binding, but it is hard to find a financial institution that is likely to openly say no to guidance. We have antitrust enforcement; it is case specific and it is not a great way of doing industry-wide policy. We even have a provision of public options, although I am not quite sure whether to put it in the soft bucket or something else. The Fed as an operator in the payments system is providing public options in terms of ACH clearing and check clearing. And that competition itself helps to frame the market and shape market standards.

Going back, we see these different approaches appearing in different contexts. We see them appearing in security rules, fraud prevention or mitigation rules and loss allocation rules. Security rules are pretty much all set by private contracts, such as direct bilateral contracts, network rules, collaborative standards like PCI, though PCI is implemented through bilateral contracts. There are different ways that these rules get set within private contracts. We also have lurking in the background things like anti-money laundering, national security, and just kind of general reputational concerns that put some soft pressures on security.

For the fraud loss prevention and mitigation, an approach really has been on the state level and it has been state data breach notification laws. These laws are somewhat of a puzzle. They function in some ways as a type of loss allocation rule in that they impose costly duties on certain parties. It is unclear whether these laws in the end are actually a good thing or not. They may help avert some losses, but they are also very expensive. To the extent that the costs of data breach notification outweigh the losses that are averted because of notifications, these laws are actually

Table 1
Consumer Liability Rules

System	Law	Consumer liability for unauthorized transaction
Credit	TILA/Reg Z	Strict liability, but capped at $50.
Debit	EFTA/Reg E	Strict liability, but capped at $50, unless consumer was negligent, then $500 or unlimited.
ACH	EFTA/Reg E + NACHA Rules	No consumer liability.
Checks	UCC Art. 4	No liability unless negligent.
Cash	Common law	Unlimited liability.

functioning as a penalty and we might want to think about whether that is a sensible approach.

Finally, we get the loss allocation rules. They are really important because, as explained in Tyler's presentation, they start to shape the incentives for adopting security rules. The fraud loss allocation rules are a weird mix of private contracts and public laws. As private ordering, we have the network rules for credit and debit cards and for automated clearinghouse (ACH), and even bilateral checking arrangements which in theory can be private arrangements. But then, UCC Article 4 for the checking system creates some hard rules and the consumer liability rules across the board—the Truth and Lending Act (Reg Z), the Electronic Funds Transfer Act (Reg E)—create hard rules on the consumer side (Table 1). Why does this matter? Tyler reasonably expressed some skepticism about whether we should ever be increasing consumer liability; however, there can be some unintended consequences of exculpating consumers from liability. When we look at the consumer rules, first thing you need to see is they are not consistent across products, and it is hard to give a good explanation for that other than historical development. But at this point, if consumers are using Apple Pay, that means they have their mobile device, their new card, their wallet and their hub. With that hub, consumers may not really be distinguishing very carefully between different payment methods. It seems strange to have different consumer rules that depend on the method. Consumer liability is all over the place: in some systems there is basically no consumer liability, while in other systems there is unlimited liability for the consumer. Generally though, other than for cash, consumers have little or no liability for

unauthorized transactions. That oversimplifies, but I think it is generally correct. That is a rule that protects the player with the least market power. But there are some unintended consequences.

Let us think about faster payments, which can often be less secure payments. There can be a trade-off between speed and security. On a very high level, single factor authentication versus multifactor authentication, unencrypted versus encrypted data. Some merchants want faster payments in order to increase sales. I think what comes to mind is McDonald's adopting contactless payments thinking it was going to speed up the lines at lunch time. Consumers do not care much about marginal differences in payments security because they do not bear the costs, which means the costs of having faster, less secure, payments are not fully internalized by the merchants because some of them go on to consumers. But more importantly, some of them are going to go on to other merchants and banks. So here we have this unintended consequence where we have these essentially consumer protection rules, but they may actually be facilitating the use of less secure payment methods. This is a trade-off we have to address. It is not clear that there is a real great answer for how to do this.

Let me throw out two solutions and you are going to see why neither is very appealing. One solution is to change consumer liability; increase consumer liability for unauthorized transactions with less safe systems. That would start to incentivize consumers to demand safer systems if consumers actually end up being liable. But we have card network zero liability policies and it may not be worthwhile for issuers to pursue putting costs on consumers for small transactions, and thus this solution does not really capture the full spillover problem. Additionally, and most importantly, this solution is really politically difficult. To try and change consumer liability rules I just think is a political nonstarter.

A second possible solution is to mandate minimum security standards across systems, which may include mandatory two-factor authentication, mandatory encryption, and so on. That would start to prevent the uncompensated externalities and allow us to have product safety minimums, just like environmental regulations do. But then there is the huge question of who will set the standards and what should they be? That is going to be a real mess.

That brings me close, but not quite, to the end. When we are thinking about private ordering versus public ordering, we have a set of trade-offs

Table 2
Private Versus Public Trade-offs

	Private ordering	Public ordering
Responsive?	More	Less
Expertise?	More	Less
Accounts for externalities?	No	Potentially
Transparent and open process?	Less	More
Other influences?	Market power	Politics

and I think we need to recognize that neither route is really perfect (Table 2). Private ordering is, not necessarily, but probably more responsive and more expert than public ordering. But private ordering may never account for spillovers on to third parties: the parties that are not at the table may not be protected. Public ordering has the benefit of being able to try and address externalities. It does not always get that right, but at least it is possible. Public ordering tends to be more transparent. But what I think really matters is what other influences are at play in private ordering or public ordering. In private ordering a problem is that market power often affects private ordering. In public ordering, it is politics.

When we think about security standards, mitigation rules and loss allocation rules, we see these trade-offs in effect. The security standards, the security rules are technical issues. It makes a lot of sense to have them done by the more expert and responsive body. But exercise in market power may very well mean that we do not get optimal rules as a result. Similarly, for mitigation rules it makes sense to do through public ordering because we are worried about externalities, and the private ordering is never going to account for that. But we may get inefficient outcomes because the rules are driven by politics. So the data breach notifications may very well be inefficient. But the public sees headlines about data breaches and wants something done, and that is as good of a solution as we have come up with so far in terms of loss mitigation.

The real nub though is the loss allocation rules because they are not just about loss allocation. They are about creating incentives for adopting security standards. I think this is where the rubber hits the road. We know

that there are problems with private ordering in this area. Tyler's paper did a wonderful job of showing this. We know that market power affects the incentives of adopting the best security technologies we can have. That said, it is less clear how well we are able to and how good of a result we get, if we were to move in some way toward some form of public ordering. I think though, simply that we are discussing this at this conference is a sign that we are on the way and moving in that direction.

Two things, I think, are really going to drive payments security. One, the headlines about data breaches are creating legislative and regulatory interest in responding to the problem of getting involved. Two, national security concerns are really going to start driving payments security. This is not just a matter of individual consumers and private business concerns, but there is a systemic concern about national security in this case.

Let me suggest that there is a broad agenda we may want to think about. This is a recap and three points again. Data collection—this would be the easiest and simplest starting point for regulatory intervention in the market. Let us just get some data so we can all know what we are talking about and make some sensible decisions. Having that data will also help the private market. We need better antitrust enforcement, but we need to recognize that antitrust is not a good policy tool. We want our markets to work better, but that alone is not going to get us to the right security solutions. And then, we need to be thinking about the problems of how to reduce externalities without creating unintended consequences and often there are not clear answers to how to do so.

I am really glad to have the opportunity to respond to this really interesting and I think very foundational paper on payments security. I hope that this paper will be the start for a lot of future work in this area.