# General Discussion
## Session 5

***Mr. Greene:*** So, the theme of the panel is about integrity, which seems to have two threads from these remarks. There is a trust thread. Integrity speaks to the belief of all the participants that good things are happening with known counterparties. But, then, there is also a subtext as far as security threats and technical challenges and penetration in attacks, which of course are amplified in an environment where trust is lacking upfront.

Comments and questions from the audience on any of those?

***Mr. Grover:*** I have a comment and a question for Daniel Eckert. You touched on the difficulty of building critical mass in new payments systems and referenced specifically Discover. Discover is on a path to achieving acceptance parity with Visa and MasterCard, at least in the United States, by in effect emulating their open model and by harnessing existing delivery infrastructure through merchant acquirers. At least on a national level, it is difficult but achievable.

You also touched on Debitman. The original Debitman business model was predicated upon retailers originating new cardholders. Any thoughts on why retailers weren't more successful, didn't more vigorously originate Debitman cardholders?

***Mr. Eckert:*** I would say, as reference to Discover, you're absolutely right. They are in many ways emulating the four-party system by working through merchant processors now to gain broader acceptance. It would be interesting—and I have not done this research; if anyone has I'd love to hear a comment on it—to see what the cumulative paid-in capital is into Discover card since its inception and how much it has cost them to achieve the acceptance marks they've had.

The most recent empirical data point is what they paid for a deteriorating network acceptance model, but still, nonetheless, $160 million for Diners Club to at least get some overseas acceptance. If you look at DFS, which was really a domestic

acceptance model with very limited ability to do anything overseas, Diners Club offers them an opportunity to do so at $160 million price tag. I don't know of many new venture capitalists that are willing to plunk down $160 million on a new network. You do have a challenge in terms of how much investment it requires.

As it relates to the Tempo Payments model, you are absolutely right. It was conceived with the purest of intentions and that was one of the reasons why we were so attracted as HSBC to the model—it seemed to have provided the answer to the merchant model. It's PIN-friendly. It seemed like customers prefer PIN, although there is refuted evidence now that says it's a toss-up. It was a low-priced model, a fixed fee for payment; it seemed to have all the characteristics that made sense for merchants' acceptance.

The challenge was two-fold and a bit nuanced. The first challenge is you are dealing with a two-sided market. In hundreds of meetings I've had with retailers about acceptance, the challenge is, "That's great. You're offering me a low-cost model. But, for four cardholders, that doesn't help."

That's just a fact. That was exactly what was said behind closed doors.

The second challenge is then working on the acceptance model through an emulated structure, such as going through merchant processors. It's nuanced because you can sign a deal—let's say with First Data—to gain a great press release that says you have access now to 400,000 accepting retail locations. But that is actually a misnomer.

What that means is you have "technical" access to those accepting locations. You still need to talk to one merchant at a time for them to turn on that access and put up the acceptance marks so that customers are aware the network is accepted. That is a monumental challenge. It is a $1 billion-plus brand-building exercise. It only happens with sneakers on the street, knocking on doors at the local bodega. Yes, you can get some big chunks down with the IKEAs, the Walmarts, the Targets, the Home Depots, the Best Buys, and the Costcos, which is exactly what Revolution Money has been doing and what Tempo had tried to do and finally threw in the towel. By the time you get to, say, 200,000 locations, which sounds like a large number relative to the 4.5 million locations you really need to have somewhat ubiquity in the United States, the amount of money that was required to do so was not able to be raised within the venture capital community.

***Ms. Garner:*** One thing we hear in Washington is banks—and in particular small banks—rely on interchange fee revenues to help cover fraud costs. One example is the reissuance of cards in the event of a data breach, which I would argue is a very reactive type of response.

So, my first question is basically for Catherine Allen and James Van Dyke. Do interchange fee revenues stifle bank incentives to proactively innovate to best protect their customers' data from fraud?

Second, given numbers from James' presentation that merchants absorb 90 percent of commercial fraud costs, etc., does that further disincentivize banks and networks from innovating and implementing stronger fraud prevention technologies proactively?

***Mr. Van Dyke:*** Both merchants and banks do incur significant mitigation costs for all the technologies upfront and all of the customer handling costs of managing costs, so on that front, they're fairly equal. But I do think from an economic analysis standpoint, there are some incentives issues, significant questions raised, when the interchange system allows the bank to keep the profit but pass on a lot of losses to merchants. That is a concern, particularly with the increased amount of data breaches going on. If that cost is largely landing in merchants' laps, that does bring about a motivational question.

***Ms. Allen:*** One of the issues is fraud is increasing. We have sophisticated criminals going after the system, and we have a mandate in the United States to make our customers whole. Somewhere, somebody is going to have to pay for that—the financial institutions. So interchange is one of the places they look to have some revenue coming in as other revenues are moving down. It's unfortunate. As I was talking about the perfect storm, we're hearing banks are increasing fees at all different levels because the revenue streams have gone down in the mortgage area, they've gone down in the basis points in a number of their interest products.

At the same time, the costs of fraud and cyber-security threats are increasing. Unfortunately, right now, financial institutions are even decreasing the amounts of money they are spending on fraud and cyber-security. It's a disaster waiting to happen.

***Mr. Greene:*** As things are going, we take it as a given the consumer will be made whole. The subtitle of this conference is "The Role of the Central Bank." Is there a role for the Fed or other central banks to play in the allocation of loss between banks and merchants—because it's the 90-10 you pointed out, right?

***Mr. Burns:*** I'm fascinated by this whole discussion. Jim, you talk about the possibility of some imbalance in incentives. And Cathy argued interchange is needed to pay for that side of the balance. If you think about these costs, and I'll take your point and I'd like to hear more about it if you do truly believe there may be some imbalance in terms of the allocation of costs. I think, Mark, that is what you're getting at.

How do you create the balance? And I've been thinking for some time that one of the economic tools is to use an interchange vehicle, which from its inception was designed to create a better balance between costs or whatever you might want to call it in terms of acceptance and the original motivation. But can't that tool be extended or can't that conflict be extended to improve or to provide appropriate incentives for other parties within the payments system to invest in fraud protection?

***Mr. Van Dyke:*** Your question is, Should there be more incentives for any other entities to create more effective fraud mitigation capabilities? To me, those are the two issues I see when I look at research on all the entities and the two crimes that are always there of "steal the data, use the data." The most effective way to profit from PII exploits is to go directly into an institution yourself as a bad guy and ride on somebody else's good reputation. That's the most profitable way to do it.

The two issues that stand out in my mind are 1) that you have the person whose identity is being used, no one is empowering them, and people say things that aren't true, like the person is not motivated, they can't make a difference or they will just bother our security experts. Behind the scenes, things have to be there. I'm not saying those aren't important. There's that and then 2) there is this funding equation. I would agree with what you're suggesting, which is that some kind of funding stream needs to go at fixing this problem—which is to take the identity holder and get more tools in their hands. Cathy's point: There are peer-to-peer tools, social and networking tools, and especially mobile tools. I think mobile banking has the safety advantage and is the greatest monitoring device that's with you all the time. But, if the information is not real time and it is not easily modifiable, it's not going to work.

***Mr. Greene:*** There are maybe two thoughts there. There is the incentive to better equip the consumer, but also the 90-10 ratio suggests there is some pricing incentive to move more of the pain toward the banks and away from retailers.

Do you want to defend yourself, Daniel?

***Mr. Eckert:*** Like I said, there will be a tar-and-feathering afterwards. This is the first I've heard of this 90-10 statistic. It seems pretty dramatic. If I look to the marketplace and understand empirically how things could change, one would imagine if 90 percent of the fraud loss occurring in the retail payments system is actually being borne by retailers, then one would think that there would be much greater collective action by that set to improve security at the point of sale. It is my understanding in the ecosystem, the reason why you see a lot of fraud push back, particularly the account takeover, identity theft, etc., is the notification happens to the issuer, the issuer goes to the retailer through its merchant processor to verify whether the appropriate checks were made when accepting that payment and—failing that verification—the chargeback procedure puts the onus of responsibility back to the retailer.

One of the ways to solve that problem is to increase authentication at the point of purchase, so the person who has the card has a dual or even three-factor authentication procedure to keep the retailer in good status.

What's happening in the UK chip and PIN environment is truly the risk now is borne back to the consumer because of the multiple authentication systems that occur when a chip and PIN card is actually accepted. That's good for banks, that's good for retailers, maybe it's questionable whether or not it's good for cardholders,

but it at least *puts* the onus of responsibility for safety, soundness and security of those card payment instruments back on the people who have them in their purse or wallet.

But we don't see that in the United States. We continue on with the same retail acceptance model we have largely because, I would believe, no one wants to bear those costs. If 90 percent is being borne by merchants, it is amazing that we don't see chip and PIN becoming a much greater argument for investment within the retail POS landscape. There are some strides. I know Wal-Mart does a very good job of terminal driving to PIN acceptance for a couple of reasons, both for cost-efficiency and for authentication reasons too.

***Mr. Greene:*** Stuart, if you and Dick Porter were looking to take some research topics from this session, maybe that's one: What is the role of the Fed in helping to allocate responsibility for assumption of loss, given where the burden currently lies today in the incentive structure? And it's increasing.

***Mr. Taylor:*** I've spent the last year working with small retailers on data security. PCI, as we all know, is one of those amorphous moving targets that is more stick than carrot. What I'm finding is there is a huge degree of noncompliance in what we call the Level 4 merchants. We are talking about 5 million merchant stores out there that are not compliant.

The reasons why there is pushback are multiple. One is—the Verizon study was quoted—while about 40 percent of the breaches occur in retail, 97 percent of the *cardholder* breaches occur in financial institutions. So, in other words, retail only accounts for 7 percent of the card accounts that are compromised. When I talk to my members and they're spending, on average, $20,000 per store to become PCI-compliant, last year their pretax profit was $40,000. With $20,000 a year to become PCI-compliant, they're finding it much more effective to self-insure. If you take my industry to the $n^{th}$ degree, it's $1.5 billion.

We are being mandated by the five card brands to pay $1 per outstanding card for security. At the end of the day, if you still get breached, you're not in compliance and all of the Account Data Compromise Recoveries (ADCRs) and everything else are going to come back down on your head.

I guess my question back to you guys is, first and foremost because we are talking about the Fed's role, Isn't that a role of the Federal Reserve to protect what is becoming the next generation of currency called plastic and the integrity of that currency? Taking a lead role in determining what that data security standard is going to be is part of a national framework that also includes health records, personal records, data security for electrical grids, etc. Shouldn't there be a national conversation that includes, as a subsection, the financial sector on what the national data security standards are going to be? The main reason is there is another factor that's coming in, and the states are individually legislating data security policies in the absence of a federal policy. So, if you are a multistate retailer, you now don't know

how to comply with any of the state legislation that's out there. What we have is a Tower of Babel. There is an absolute role for the Fed to come in, take a realistic role, don't tell retailers to go to triple data encryption standard (DES) when there is not a problem on single DES output. Take a more rational approach. And also you need a third party who is going to be willing to throw out the existing antiquated rails.

***Mr. Greene:*** We don't have a Fed representative up here, but there are lots in the audience. Anybody want to speak to that?

***Mr. Weiner:*** I might say that the next session, of course, is on the Fed as operator and, by that, there are some central banks around the world who, in fact, are maintaining security databases now. That seems to be an extension of that idea, so perhaps we can get into that in the next session.

***Mr. Greene:*** Paola, one of the things you've been talking about is the need for more international collaboration.

***Ms. Masi:*** That's one of the aspects we can add to the debate on fraud. As overseers, and from a system perspective, we are trying to agree on and build a database on fraud at the international level. At the European level, we are trying to agree on a common definition of what fraud is, how we can properly measure it, and who is the authority/institution allowed to store and use confidential data. We, as central bankers, are trying to understand how to build up a reliable and "official" database on fraud, since the available information is too often dodgy and the evaluation of the impact of the fraud on the economy is very different. We are working on this, at least at the European level (as Wiebe Ruttenberg can testify), as a part of the project to have a single database on cards payments.

I must tell you it is a difficult project. We are talking to different categories of stakeholders of any card scheme, starting from issuers and acquirers, and it is really hard to strike the proper balance among conflicting interests; moreover, we have to define how to compare between different nations and between different kinds of card payments. That is why I believe we need to increase our effort at the international level—not only at the European level—to understand, standardize and collect reliable data on fraud. I think also the World Bank should be involved in this effort, and together we can address the question.

***Mr. Greene:*** So international cooperation is needed, but I think your point was, even within the United States, there is plenty of room for improving the standards. The story as I understand it so far is the risks in the retail system are growing, they are growing perhaps by leaps and bounds as a result of some of the new products, the new technologies, the new entrants coming into the space and yet retailers who bear the disproportionate burden and cost of all this are not given the proper regulatory structure to rely upon. They don't know how to operate. They are not sure about the rules of the road. So, is the role of the Fed domestically and similar central banks internationally to help pave that road?

***Mr. Taylor:*** Databases are great. But that is all rear-view mirror. Essentially what the retailers are involved in is a chase-the-crook type of investment strategy,

which is as soon as we find out some new breach, everybody gets lawyered up. Two years later we find out what the breach was and then we can't even react to it because the same exploit has been replicated. It's all because we're trying to incrementally fix a system that really needs a fundamental redo.

For instance, why isn't there a PIN on every transaction? In my market, the solution is to have somebody put in their zip code. If customers can't stand PIN, why do they like a five-digit zip code?

***Mr. Eckert:*** I would like to jump in on that and reiterate that my views aren't the express views of HSBC on this front. However, this is precisely where a regulatory intervention could be very helpful because it is a shared problem for which there is a clear market failure. We're all bearing costs. It's costing the consumers in terms of hidden costs to manage this, and we don't have a lot of joint cooperation among all the parties that are victims to this fraud playing well and nice together.

For example, we have third-party databases where banks have come together in a multilateral fashion to try to share information. But it is voluntary. Early Warning Systems is one on the checking account side. Another one is Certegy Check Services, which is run by Fidelity Information Services, but it has its challenges. First of all, it's based on legacy plumbing information (checks, which we all know how voluminous checks are nowadays), but then secondarily, it is voluntary participation by usually the largest banks, but not necessarily always.

Fraudsters know this. So what do they do? If you looked at some of my subsequent pages that I didn't share in my opening remarks, just as soon as we have a countermeasure to try to help detect and eliminate this at least from the issuer front, then there are five websites that list those institutions that choose not to participate in those Early Warning Systems and ChexSystems to tell the fraudsters where to go! That is clearly a market failure, where you could see a regulatory body, such as the Fed, start to set standards for the betterment of market efficiency as opposed to intervening in a way that could potentially create some unintended consequences.

***Mr. Van Dyke:*** A couple of points: 1) PIN versus signature has been talked about a lot, so I'll just say from our data—and we have seven years' longitudinal survey data—it's pretty clear. The more knowledgeable you are about technology, the more you prefer PIN. The less knowledgeable you are about technology, the more you prefer signature. So the group that prefers signature is going out of the economy. Truly, I think it's pretty straightforward.

This issue of how we would implement these systems, and I appreciate what you said about people entering their zip code, so why wouldn't they enter a PIN? That's a good way of characterizing it. One of the challenges is these crimes we are talking about are inherently complex. Just on the surface, there are two crimes within this one crime of so-called identity theft—steal the data and use the data—and there is often a supply chain of criminals. They are international. They are the

person next door. It's everybody.

Where I think we fall short, because it's hard to take boring research data and convert it into action with these multiple crimes, multiple criminals and evolving things, is that we look at things like malware and Trojan horses and we stop right there at the first crime, which is security. We don't consider how people can use this in transactional fraud. You really have to keep both scenarios alive at once and involve the identity holders and the multiple participants in the supply chain of payments.

***Mr. Peirez:*** I find myself agreeing with many of the comments on this issue, although the Fed's role in terms of what it could study and do is probably broader than what's been discussed because the 90-10 discussion is frankly the exact opposite of what our data show in terms of who is bearing losses. No disrespect meant, Jim, I usually agree with most of your numbers. However, with this one I don't see it. The Fed could do a really great service by trying to identify what costs are being borne by whom. That would be fabulous information for all of us.

Frankly, Peter, to your point. We do provide interchange incentives based on authentication method. It is one of the core rate-based decisions we make. So, if we could get better information on who is bearing what costs in that regard, that would help us independently set our prices in the way free markets should. That would be great information to have. But I don't think we should assume one side is bearing more costs and then start studying how to create incentives around it. We should study who is bearing what costs *first*, then we can try to decide where it should be placed.

And, then, just for the sake of argument on the PIN situation, PIN with chip is a very secure system worth discussing. Dan's points are right on in terms of the cost and the incentives. Personally, I would hate to see us push PIN with magnetic stripe more. It is actually quite insecure and opens up ATM fraud in a way I would hate to see. It's what the Europeans have started to experience, particularly the United Kingdom, based on how they still mag stripe their cards with PIN. I would discourage us from thinking of PIN as a panacea. It's not. Frankly, my zip code is public information that anyone could find and my PIN is not. That is why I enter my zip code happily at the gas station. I wouldn't want to enter my PIN—personal knowledge. It's research-based.

***Mr. Eckert:*** I actually like Josh Peirez's comments, because one of our challenges is you deal with the limited data that are available. What you are suggesting is a system whereby we motivate more participants, financial institutions and merchants to share data.

I agree on the other. The better the quality of data, the better the quality of the decision. I feel pretty good on the numbers we have, but we need more.

***Ms. Allen:*** I want to go back to your question of the role of central banks. I see three important roles that also need to be in the mix. First, I do think the Fed

needs to take a much stronger role in consumer protection. There may not be a need for a consumer protection agency, if the existing regulatory agencies took a much stronger consumer protection position.

Second, the Federal Reserve Board has taken a leadership position in Washington around the cyber-security issues. It's very complex. There has to be global law enforcement, financial institutions, technology providers, and telcos at the table. Again there is a stronger role the Fed could take.

Third is this concept of nontraditional players—nonbanks—acting or looking like banks or doing financial services-types of transactions or activities. Maybe it's the *activities* that should be regulated, not necessarily the entities, and all of that should be done in the name of security and creating the safety and soundness we need to preserve in the United States.