General Discussion

Monitoring Payment Fraud: A Key Piece to the Puzzle

Mr. Dubbert: Alexandre, would you like to take a couple of minutes to respond and reflect on Chris' commentary?

Mr. Stervinou: I think there are two different things, two different dimensions. The first is everything about the collection of data and the idea of collecting data. The second dimension is how a public authority intervenes in the field of security. And those are two different things. The fact that we as a central bank wanted to intervene in the field of security also pushed for a central bank-led initiative of collecting the data. We had to have this necessary means to get to the ability to issue recommendations. That said, in the U.K. and Australia, there has been this market-led initiative of collecting data, and we see more or less the same trends and more of the same concerns.

Having an authority get involved in collecting the data may be the neutrality of things, which also has been said this morning. Collecting the data must not be a competitive issue. Having a public authority with confidentiality agreements that are mandated will ensure confidentiality. Collecting those data, having the ability then to drill down into details, that may be something market-led initiatives would not be able to do? I do not know. But having this ability helps us get more insights on how fraud is moving, where it moves, and sometimes the cost of it. That also is something we learned to do; ask beyond the fraud figures, ask about the cost of the security measures you are deploying. Again, having the public authority doing this exercise is of benefit to everyone. We have done that with EMV and with two-factor authentication. With EMV, it helped not only the banks but also the merchants to understand a little bit about their fees and the way we are paying for security. The benefit may be realized in the mid- to long-run, not in the short-run, and that was one point in Chris'

presentation. I agreed: in the long-run it actually helps them fight fraud. Showing through a public authority that the investment on EMV was fruitful for them in the long-run is of benefit. Those would be my comments, which are just complements to Chris' presentation.

Now for actual public intervention, I am convinced that this is useful. As Kelly Dubbert and Governor Powell talked about it, we have to find the right balance between the flexibility of having the economy and the market players doing what they want to do and innovate in several fields, and having too much, too strict regulations. In France, regulations have always been quite heavy and quite present. It is becoming more or less the same in Europe; European-led initiatives in regulations and directives are getting stronger and stricter. Is it the right path? I think only the future will tell, but I think it can help at least on issues like security that are definitely of public interest. It can at least help to state the scene and not let market players do things that are not good for them, for consumers, or for their merchants.

Mr. Hamilton: I think we are not so far apart. I would not deny the role and importance of having a public policy regulator, if for no other reason than because the only organization that can prevent what the thinkers in this field often call regulatory capture is the public policymaker. If your self-regulatory system is in fact captured by special interest groups, the public policymaker has to decide when to intervene. One of my colleagues at the Reserve Bank of Australia used to say that it is very important to have a very large club to hit people with, but ideally he never wanted to take it out of the cabinet. I think there is some logic to that. For a long time, the Reserve Bank has had direct and specific regulatory paths over payments in Australia. And I know that it has a global reputation for being quite interventionist because of the interchange fee regulation that it undertook some years ago. But in fact it has used regulation extremely sparingly. It only had to prove that it was prepared to take the club out of the cabinet once, and that has been very, very helpful in engaging industry in a fruitful discussion because the industry would always rather organize to meet the public policy goal itself than be forced to. That certainly is a valuable way to balance the public and private interests, and I think it is going to be a partnership.

Mr. Dubbert: Very good. We will open it up for questions.

Mr. Horwedel: Two questions. First, you had those two slides in the five-year period. What is your view of the allocation of fraud between

issuers and merchants five years ago, and then what is it today? The second question is what is your view of the fact that we are going through this expensive conversion to EMV in the United States without mandating PINs?

Mr. Hamilton: The honest answer to your first question is I do not know because I do not know what the picture looked like five years ago between merchants and issuers. I suspect there probably has been a shift toward merchants over that period. A little bit of background on that: the Reserve Bank of Australia, although it has a lot of power, has never done anything in a regulatory way in relation to fraud prevention in the card system. It has never found the need to. And when you ask them why, they say some version of—and I can say this, but you probably would not get them to say this publicly—as long as the responsibility for fraud is well aligned with the people who bear the consequences of fraud, then we are going to be happy because they will find the right level of fraud prevention. They keep an eye on the relative ability of different players in the marketplace to manage the fraud problem versus actually bearing the costs of the fraud problem. As long as those two things are roughly aligned, their decision is not to intervene. Or at least, that is my observation of their behavior. So if that balancing shifts, it should be because the ability of different parties to prevent the fraud has shifted and that is what things like scheme liability shifts are about. They are trying to say that if you implemented the right security measures, you would be able to prevent this fraud and therefore we are going to allocate some of it to you. That might be right, and it might be wrong, but that is the theory.

Your second point was about the cost of EMV? It is a done deal; it does not matter anymore. The reality is globally the world is going to EMV and even if there was not any fraud cost benefit, you need to do that as a transitional mechanism to get to this. And we are all definitely going to this eventually. That is the way it is.

Mr. Horwedel: My question, though, is going to EMV without PINs.

Mr. Hamilton: OK. Both are useful on their own, but the better configuration is to use chip and PIN. Whether it is better to do one first then the other, I do not know, but presumably that is the path that you are on.

Mr. Stervinou: Regarding the split of fraud between issuers and merchants, this is something we ran and saw as data for a few years, but we decided to stop in 2011. The data were not reliable enough. The issue

we have, and this is also why there is a delay in creating fraud data, is we may have fewer chargebacks due to commercial litigations between merchants and consumers. It takes maybe two or three months to settle the transactions properly. When it comes to the actual split of the fraud cost between the issuers and the merchants, it can take longer than that. It also requires us to know exactly how things happen between the acquirer and the merchant, but that is difficult because the acquirer and the merchant may have agreements that the acquirer is not passing the cost of fraud to the merchant, or is passing it differently in different contractual terms. The last data showed the split was like a 50/50, but if you look in detail it was actually more like 40 percent for the issuers, 40 percent for the merchants and the rest for the cardholders. I would say, with the liability shifts, the split should have evolved to the issuers taking more of the cost of fraud, but I do not know. We do not have concrete data anymore and it is rather difficult to collect.

On your second point, yes, I would agree. Chip is half the way through: It is a good half, but it is still half the way through.

Mr. Santana: You talked about collecting data, disseminating fraud data. We have a unique problem. In our market, at least in the United States, if you look at the card, the share of the card market, the cards in force, you would see the top issuers control maybe over 70 percent. As a result, if you start sharing fraud data, there is a general fear that it only benefits the smaller issuers, and it exposes their card data to merchants and that may have unintended consequences on interchange rates. How did you overcome that problem in Australia and France? We have this ongoing dialogue with issuers and card acquirers and this is their general fear.

Mr. Stervinou: I will take the case of France. We aggregate a lot of the data that we have. Data aggregation gets a lot of the details out of the picture. Our market is made of maybe nine to 10 major banks, and we have probably 100 behind those. Aggregating the statistics and choosing to give only a certain level of information to the market helps address the issue you are underlining.

The fraud data help with another thing, which is also part of your question regarding the actual cost of fraud and the cost of the measures being deployed. For example, seeing CNP fraud being at 25 basis points gives you ideas about the price of security in contracts between the acquirer and the

merchant, which can help in a way because it is how it works in the overall market; it is not with a specific acquirer, but it is with all different banks. I remember one thing I did not talk about. When we wanted the industry to tackle CNP fraud in 2008, we said let us push for strong customer authentication, two-factor authentication. One or two years after that, we realized some of the acquirers were offering 3D Secure to their e-merchants with an additional fraction of merchant fees, which was higher than the cost of fraud. So, how do you work on this? This was part of the presentations this morning regarding what is the right level first of all, and also how do you choose your incentives. With public interest in mind, I think showing that type of measure or that type of statistics helps to have a responsible action or behavior from the banks and from the merchants.

Mr. Hamilton: I agree with that. I think the way in which the Observatory presents the data is very important in answering that question. I would add that it is important to trust who is collecting the data and presenting it because you do need to mask information that is competitively sensitive. We in Australia had quite complicated negotiations with the card schemes, not with the issuers, around their competitive positions. There is a lot of competitive tension between the domestic debit card environment and the international schemes in Australia. Neither wanted the other to know what either their volumes or their fraud experience was. So we need to manage that issue. We need to be trusted as an organization that is able to hold that data and keep it confidential and only present the information which is acceptable. Although there is a negotiation to go on there, the short answer is it should not impede getting the benefit out of the data.

Mr. J. Williams: Adam Levitin said earlier on that one of the key things is sharing data, and as part of that it is the definitions you are using as to what you count as fraud and what you do not count as fraud. There is great potential for unintended consequences to shift what actually is fraud into something you are not currently counting. I think there are some good examples of that. So how important do you think consistency is in our definitions of what fraud is, either across payment mechanisms or between different countries? Because I think it could be a key chink the fraudsters could take advantage of if they can move their fraud to some other mechanism you are not counting at the moment.

Mr. Stervinou: Maybe two aspects on this. If there is fraud, at some point, it will be counted as fraud. So, I do not think the general value

such as overall fraud rate or amount will be different. But what becomes important is to know where the fraud comes from. So, the distinction between proximity payments, ATM withdrawals and then remote payments from mail order, telephone orders and Internet payments becomes more difficult. Defining the fraud types for cards today is not a concern anymore. The problem is that you still need to count correctly the data from the payment chain. I think what the Observatory presents is pretty reliable—we have been dealing with this for 13 years now—but we still have concerns. There are areas where we are not sure. For remote payments, for example, the split between mail and telephone orders on one side and Internet fraud on the other side is still a concern because the data quality itself is a problem. Also, merchants have to be in the right merchant category code. Merchants have to correctly split those transactions between what they do in proximity, in mail order, on the Internet, and so on, which, however, is not always allowed by the systems. The IT systems behind the merchants aggregate transactions too early in the process. The acquirers are trying to convince their merchants to follow the guidelines, but sometimes it is a little bit difficult. I think we are still victims of that, and everyone is, including the card schemes. The card schemes have a global view on all this, but their view is as good as their member banks. So, we have trajectories in place to try to improve this, but it is rather difficult.

To conclude, you said consistency is important. Yes, for sure. Again, I think consistency is achieved because fraud on cards is known for years now. So I do not think there is a big issue in that. In Europe, we are trying to bring that consistency for the figures we are now starting to release on fraud for cards all across Europe. When we worked with the ECB within the Eurosystem, we did not face any stronger issues in having consistency across the figures released by the ECB and our figures. But the issue is definitely still there in data quality and the way the people, the economic agents, report the information back to the authority, the card payment schemes and all associations.

Mr. Hamilton: Absolutely, it is a pain. It is hard work. We have been collecting information on these phone and Internet-based fraud events for a couple of years now. It is not in publishable quality at the moment. Indeed, the only way you can get it there is by collecting it for several years and going back around, testing, retesting, checking it and making it more consistent. The key thing is do not use this as an excuse not to get going because it actually is a process of gradual refinement. But it is kind of interesting because it

does show things like malware is a much bigger problem than phone porting or at least on the data we have. Is that true? I am not really sure yet, but you have to start, and you have to refine the categories as you go along and prove it over time. And I would try and do the international bit last. I think it is probably more important to produce quality data that gets relied on domestically and then try and adapt.

Mr. Moore: I have a question following on some of what was raised earlier. In addition to the competitive concerns about not wanting to reveal the fraud basis points and the volumes, another objection that typically is raised against collecting data like this in the United States is that it could have these adverse effects on consumers and may drive up their concern about fraud. You have been publishing these data in Australia and France for several years now. Have you seen any evidence that the publishing of these data has in fact created some negative concerns among consumers or has the reception been positive or nonexistent?

Mr. Stervinou: Yes, it does get a little bit of media attention, especially for CNP fraud on the Internet. But this is always an opportunity to underline safety behavior on the Internet for your consumers. I did not talk about that, but the way we publish and do the press conference around it is to also send reminders on how to properly transact online, such as to go to websites you know, to not leave your cards somewhere, those kind of basic things. Reinforcing the message that you have an instrument that is not perfect—it has security but it has fraud—helps. You, as a consumer, can do something about it. And the second thing you have to put in perspective is that the law in Europe now, with the Payment Services Directive since 2007, is very consumer oriented. This means that it is protective of the consumers. If you have an unauthorized transaction on your account, that being credit transfer, direct debit, card, whatever, you have 13 months to complain, to go back to your bank and to say basically, "I was not the one doing this, and you have to reimburse me." And the bank has to reimburse you and then can investigate. This is very important. The directives or the regulations coming from the legislature in Europe have a tendency to defend the consumer heavily. That can be good or bad; I am not here to judge. But this is the way it works. That also gives some counterarguments to the fact that, OK, well it could raise fear, but in any case the consumers are protected by laws. So it is not the same.

Mr. Hamilton: Yes, I think that is reflected in Australia as well. In fact, if anything I would have said that now that we have a well-established process of issuing an annual, reasonably easy-to-read piece of paper and a six-monthly update, that has actually reduced the consumer fear and concern about fraud. Because having real data is a lot better than having fears, particularly when they are stoked by sensationalist television programs. Before we published fraud data, you would have "A Current Affair," doing the latest exposé about some gang that is doing some card counterfeiting or something. Now, when they do that, they know they cannot get away without quoting the actual numbers and whether it is going up or down. So context provides some rationality to the debate and that is a really positive thing.

Mr. Sullivan: I just want to ask a unique question because I think Australia is the only country I have seen that collects and reports statistics on check fraud. I would be interested in Chris' commenting on that. Why is it done, and is it as interesting as the types of discussions that we have had so far which is mostly on electronic payments?

Mr. Hamilton: You are probably the only person who reads that check fraud statistic. It is history. When we started doing it, it was a lot more important than it is now, to be honest. Checks are well and truly on the way out in Australia as they are in many, many countries around the world. So, any self-respecting fraudster is not going to go into check kiting, I am afraid. But that said, one of the reasons for getting going on fraud collection and presentation was a series of sort of nasty incidents partly in the check space. So it was a response to the environment.

Mr. Stervinou: Just one word on this because it actually is interesting. We also collect fraud on checks in France, but we do not publish, so not the same treatment as for cards. Interestingly enough, the absolute fraud amount for checks is very close to that for cards. The checks are still garnering a lot of transaction amounts. So, the person should follow up for checks in relative terms. This question gives me the opportunity to talk about the way to collect the data. With check fraud, we collect data directly from the banks, from the issuers. With card payment fraud, we collect data from the schemes and we also recently started to collect from the banks, not only to cross-check but also because it can help us understand as a public authority which banking network is better than the other, or which banking group is better than the other.

Mr. Dubbert: Gentlemen, thank you very much. An outstanding job. Alexandre, just tremendous progress. Chris, thank you for your views. I appreciate your insight.