Monitoring Payment Fraud: A Key Piece to the Puzzle

Alexandre Stervinou

Today I am going to talk about the responsibilities the central bank of France took on a few years ago to tackle the issues we faced, and still face, with payment card security and fraud. I will give you some history and background, but I also will focus on fraud statistics and the trends we see. Some of the data is confidential. I will try to be careful because the 2014 annual report is not out yet, but will be in a few days. And then last, I will talk about some interventions and recommendations we issued to the various market players, and especially the regulated entities.

First, there definitely was a need for public intervention as we saw it, at least in France. In the 1980s, we had two leading domestic card schemes, competing. They decided to merge and offer a universal card payment to cardholders, to everyone. The effort also was accompanied by a push for card acceptance and some kind of connection with the international schemes like Visa and MasterCard to have more widespread adoption and development of cards as a payment instrument in France. Security has always been perceived as a key development for those card payments, and in the early 1990s we had already adopted chip and PIN. It was not EMV because EMV did not exist as a standard at least. But the underlying technology was quite close. Then we had chip, and we also had PIN for protecting proximity payments. But the problem with any type of standards and security, which was part of the discussions earlier today, is that sometimes security is broken. And those issues were arising in the late 1990s. This attracted media attention. The security of the chips was compromised and a lot of the media and consumer associations turned to the public authorities—especially the central bank—to ask what was happening. But it was not only the central bank, but also police forces and the government. We saw that, and perceived the potential to endanger public confidence in cards. Cards and card payments had been taking off for a long, long time in France, so we

had to do something about it. And it came through the French legislature, which took concrete measures with the Everyday Security Act of 2001. That Act, given the tragic events in the United States, led to many different measures regarding security in France, and also, interestingly enough, that included security measures for payment cards. The central bank's mandate basically was extended to payment instruments. The legislature also asked for the creation of a so-called Observatory for Payment Card Security, ensuring the security of card payments, and involving all stakeholders so that what we saw in the few years before could not happen again.

As a result, and I will talk about those two different things, the central bank got that extensive oversight mission and mandate of payment instruments, covering all types of payment issuers and the whole payment chain—the issuing, administering and outsourcing of means of payments. It not only covers cards, but also credit transfers, direct debits, checks and so on. We have extensive power of off-site and on-site inspections regarding all relevant entities in the payment chain. For example, we have the right and ability to go to technical providers or vendors and ask them for quite interesting information about their systems and what they offer to licensed institutions. The central bank also cooperates with the banking supervisors. We have taken review of annual reports from licensed entities on operational risk and the reports have a dedicated annex for payment instruments, including payment cards. There also are some new actors we have to deal with. The EU Payment Services Directive and the E-Money Directive in Europe introduced new categories of payment service providers. We now have some kind of overarching categorical payment service providers. And those payment institutions and E-Money institutions have to be licensed or sometimes may be exempted by the licensing authorities, which very often are the supervisors. At least this is the case in France. But what the legislature wanted was for us to also be part of the actual licensing process, and we have to develop an official statement on the security of payment services and instruments. This also reflects the earlier discussions; we have some kind of clear intervention with the different regulated entities regarding the payment instruments and their regulations.

Now, for the Observatory for Payment Card Security. It is chaired by the governor of the Banque de France. We have many different members around the table. We have a member of Parliament, a senator, and representatives from all stakeholders, including issuers, acquirers, schemes, merchants, consumer associations and government bodies—the Justice Department, the police forces, the Ministry of Treasury. There is a broad

representation of all stakeholders. There are some confidentiality agreements in place because we have issues with some of the data we collect. And the secretariat is insured by the Banque de France. We have three main missions through the Observatory: Deliberating full statistics is a key element, "knowing the data" as it was said earlier; we also have to ensure technology watch and issue security recommendations to issuers, merchants, and all the different actors in the chain; and we have to closely follow up on those security measures, which are deployed by the various entities, various actors. The Observatory publishes the annual report online, which is also available in English, but first in French.

The Observatory has two main working groups—one on statistics and another on technology watch—linked to our mandate. The composition is made of experts nominated by Observatory members, but we also can ask for extended expertise on specific topics—obviously, we have to be careful about the confidentiality of the exchanges. Regarding the working group on statistics, the main mission was first to define what we call fraud and then to define the different fraud types. This work was carried out in 2002-03. We tried to define the different actors, schemes and issuers, how to categorize fraud, how to rely on technical aspects in the networks in the actual clearing mechanisms, and how to take into account, for example, merchant category codes, or error codes from the payment schemes. There was a lot of background work on defining the fraud types and connecting those fraud categories to the reality of the market's different entities. The main goal of this group is to follow up annually on the statistics gathered from the card payment schemes themselves.

We now have a focus on two main things. One is 3D Secure, which has been put forward as one of the main mechanisms to secure online card payments, along with strong two-factor authentication. I will talk about that later. Another focus is on contactless payments. We began to see widespread adoption in France and there was some fear about what contactless payments can mean from a fraud and security perspective.

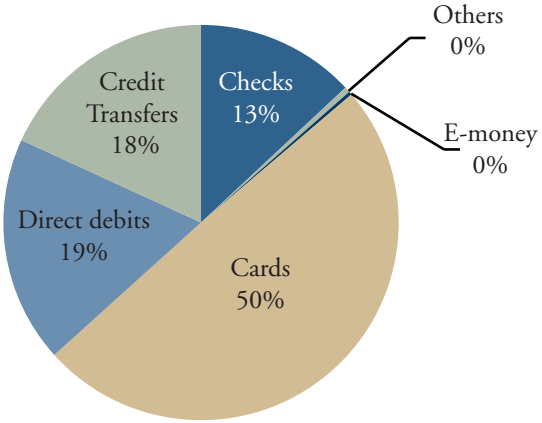
The composition of the technology watch working group is similar to the working group on statistics. Its mission is to maintain a technology watch with the aim of proposing measures to the plenary and its members to increase or maintain the security of card payments. Everything around innovation, mobile payments, contactless, whatever, has to be considered and taken into account within this group. We also have some private or confidential exchanges with a few different actors outside the Observatory membership.

When we talk about technology watch, the Observatory in recent years has looked at different things. For example, we looked at terminals and terminal security. There has been a lot of hype about breaking point-of-sale terminals in the last few years. Regular bus terminals, unattended payment terminals in petrol stations, our networks of connected payment terminals; all of these are security concerns and issues. We looked at that and made extra recommendations. And, in the general topics area, we looked at standardization and certification. This also is a rigorous topic and we need to update our views on this and how things are progressing. With EMV migration, the security of mail and telephone orders and remote payments are things we have to consider; and not only Internet payments. If we secure Internet payments, that means the fraudsters will go to mail order and telephone order. So, we have to look at that and other things. Recently, there has been quite a trend to also look at biometrics as maybe the next step in strong authentication. But today, I will talk mainly about the security of online and card-not-present (CNP) transactions, for which we have gathered statistics in 2008 and 2013, and also about contactless cards, for which statistics have been gathered in 2004, 2007, 2009, 2012 and 2014.

In looking at this annual report and what we do with it, the structure is pretty standardized. We usually have a specific case study that we do as the first chapter. In the last two or three years, we looked at the deployment of strong authentication, and I have a few charts on that. But years before, we also looked at the cost of security and how to compare the cost of security with the cost of fraud. The different market players asked for more data on that, and we tried to run surveys and to have concrete data from banks and merchants regarding the migrations to EMV and the migrations to strong authentication for securing online payments. There also are chapters on statistics and technology watch with the recommendations, and usually a dedicated chapter that has more emphasis on other topics and a little bit more satellite topics or Europeanwide topics. For example, a few years ago there was discussion about the emergence of a European card payment scheme. More recently, it has been the protection of personal data in fraud prevention systems, which raises questions about how you draw the line with problems or issues with data privacy.

I will not say too much about the adoption and publication processes, but basically, the Banque de France is responsible for following up on the recommendations 100 percent of the time. The central bank is doing the work here and using the mandates I explained earlier to follow up on the different recommendations from the Observatory and giving back aggregated information in the annual reports.

Chart 1
Payments in France by Volume, 2014



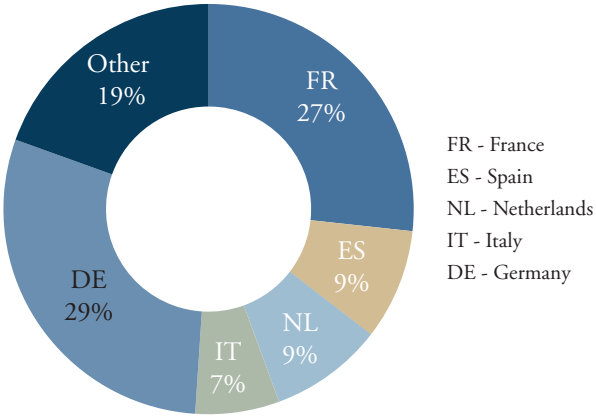
Source: Banque de France.

Now to the full statistics and trends. Before going to fraud, I will give you a view on the importance of cards in France. If we look at the volume of transactions in France and the way they split for cashless payments in 2014, cards now account for 50 percent of the number of transactions (Chart 1). So, card payments are already used, convenient, and the main cashless payment instrument in France. If we look also at the weight of the French market in Europe for cashless payments (data are for 2013; 2014 data will be available in September), France accounts for almost 30 percent (Chart 2). So, if you make the calculation, that means we definitely have an important weight just for cards, not only in France, but also in Europe.

Now for the trend we have seen more in the domestic market. Card use is actually increasing, which is the upper line in the chart (Chart 3). Check use is declining; so, less used and less important. For years we more or less have seen the transfer from checks on one side to cards on the other.

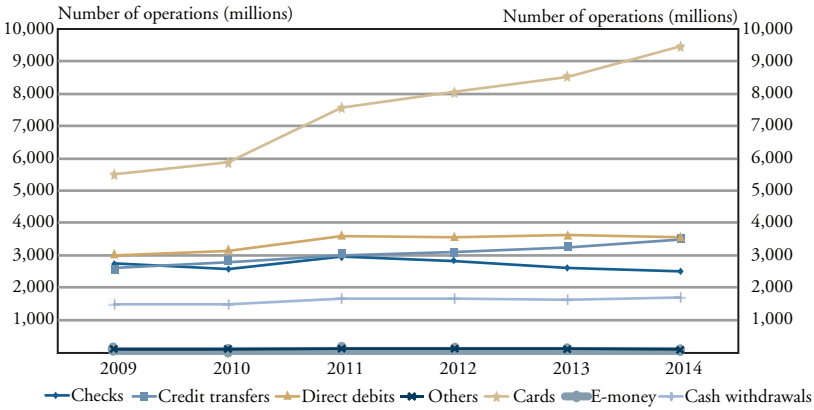
All of this leads us to the concrete figures on fraud. We have to follow up on what is happening there. If you look at the value of transactions for cards, we have reached around €600 billion (Chart 4). There is constant growth in the actual value of card-based transactions. So, the amount of fraud is also going up. Even if all cards and transaction types, all are being considered, the fraud rate is pretty stable now, around 0.08 percent. Again, that is considering all cards and transaction types.

Chart 2
Payments in the Euro Area, 2013



Source: Banque de France.

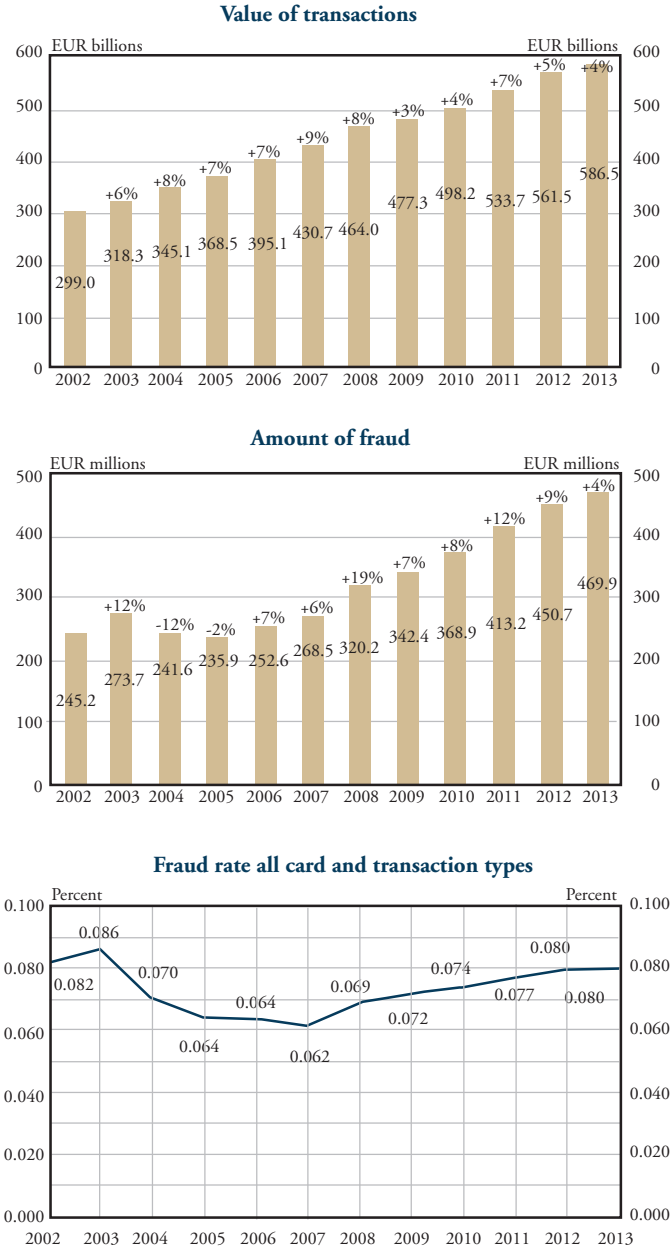
Chart 3
Payments in France by Type, 2009-14



Source: Banque de France.

Now we will look at it in more detail and what all this means because there are huge variations between the territories and the type of transactions. If we first focus on the share of domestic fraud versus international fraud, we already see some differences (Chart 5). The data in brown concerns only domestic fraud and the data in blue is basically everything outside; we have French cards being frauded outside of France and international cards that

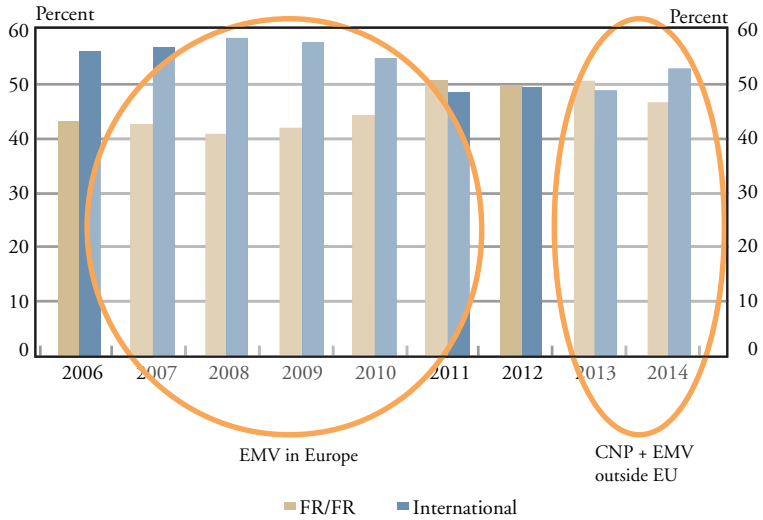
Chart 4
Card Payment Landscape in France, 2002-13



Source: Banque de France.

Chart 5

Share of Fraud in France versus International Fraud, 2006-14

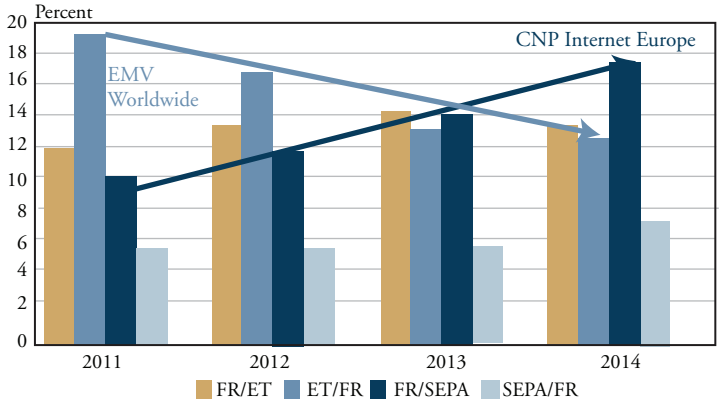


Source: Banque de France.

can be from the eurozone, the United States or anywhere in the world coming to France to be frauded. So, that is the relative share difference. The domestic fraud share in 2006-08 was quite low compared to the international share. And then we observed that the international share has diminished in recent years, mainly because of the adoption of EMV, after which we saw less proximity-payment driven fraud on the international side of our data. The more recent evolution in 2013 and 2014 is on the right part of the chart, where we see domestic and international diverging again with international fraud increasing. And there are potentially two reasons for that. CNP fraud obviously is still there and very important; and otherwise the adoption or not of EMV outside the European Union.

If we go a little bit further and focus on international fraud only (the blue bars in Chart 5), we have the ability to split this data more, which is quite useful (Chart 6). When we split the data—on one side cards issued in France and frauded in the SEPA or the European zone and beyond, and on the other side cards coming from SEPA or other foreign countries and frauded in France—we see two different trends. First, we see that much of the fraud in the recent years from France has been reported to the SEPA zone, and this is CNP. This would be linked to what I said earlier about the intervention that we have. We took actions to tackle CNP fraud. That fraud then started to deport itself to nearby countries. That is a lesson we

Chart 6
International Fraud in France, 2011-14



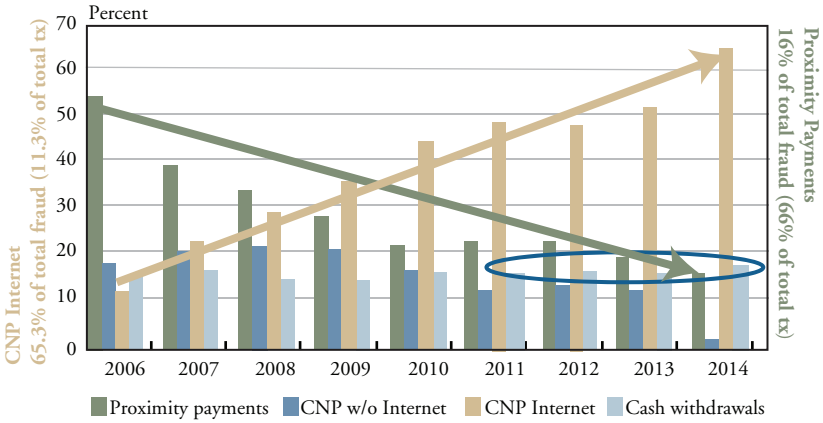
Note: Figures are for cards issued in France and frauded in the Single Euro Payments Area (SEPA) and beyond (ET) and for cards from SEPA or beyond and frauded in France.
Source: Banque de France.

learned from those figures. Internet-based CNP fraud moved to our close countries. The second thing we can see is related to fraud outside Europe coming to France. We see a downward trend here, and this is the down trend I summarized earlier that we saw in 2006-08. We saw the impact of EMV becoming more positive. When I said international fraud is going up again, this is because when you add up those two different things, you see that CNP fraud is taking over and basically the weight of CNP fraud is much, much higher now than the weight of proximity payment fraud. And this is confirmed by those figures. If the EMV adoption rates could be faster, this down trend would be even better for us and we would see less of that foreign fraud coming to France.

If we focus on domestic fraud, we see two interesting trends (Chart 7). CNP on the Internet has been going up steadily and now is 65 percent of the total fraud but only a little more than 11 percent of the transactions. And the fraud in proximity payments has been going down steadily since 2006, and it is only 16 percent of the total fraud for two-thirds of the total transactions. There definitely is an inverted effect between CNP fraud and proximity payment fraud. We also have a slight concern about the increase we witnessed in the last two to three years for fraud on cash withdrawals. I will come back to this.

If we look at the actual fraud rates for domestic transactions, CNP on the Internet is obviously far higher than anything else (Chart 8, Panel A). And

Chart 7
Domestic Fraud in France by Type, 2006-14

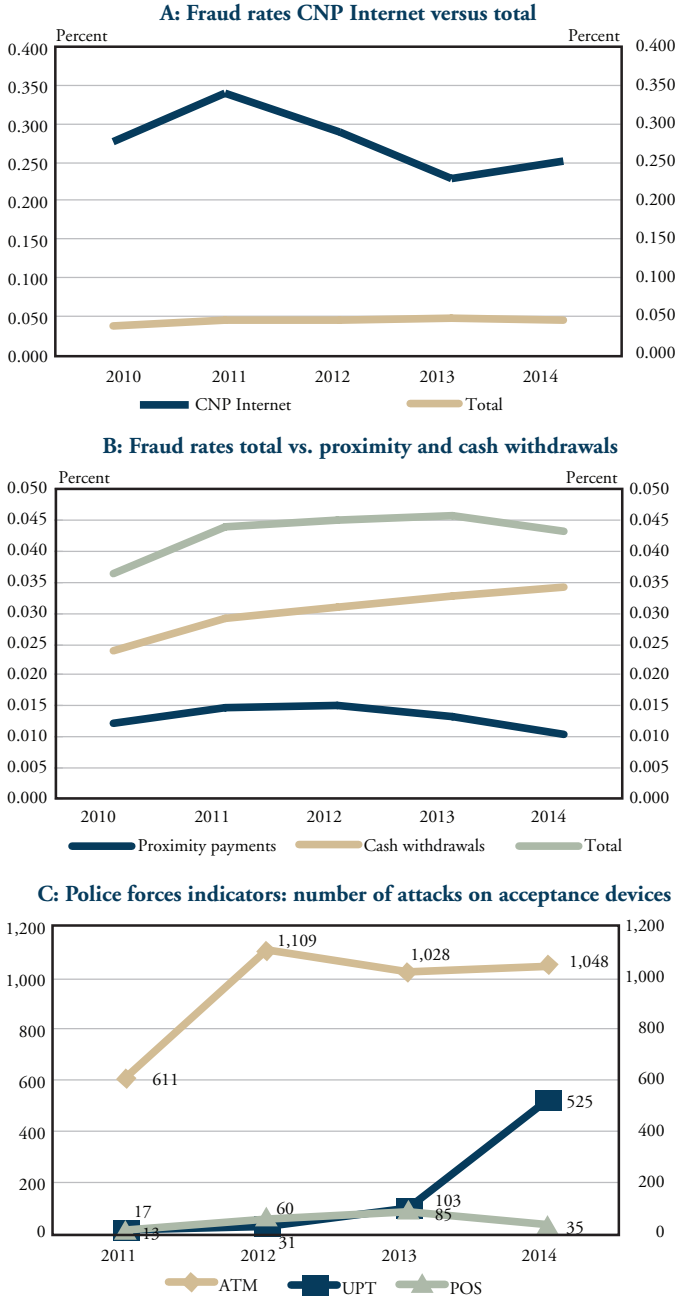


Source: Banque de France.

if you compare with the actual total fraud, the total figure for 2014 is 0.043 percent, and CNP Internet is 0.251 percent. That means you have 20 times more CNP fraud than what you have on average. And it is the other way around for proximity payments and cash withdrawals. Proximity payments are very low; cash withdrawals are increased a bit (Chart 8, Panel B). To give us some insights, we obtained indicators from the police forces, the number of attacks on acceptance devices such as ATMs, unattended payment terminals and point-of-sale terminals (Chart 8, Panel C). What you see is that attacks on point-of-sale terminals are quite low. We saw a surge in 2013 due to one terminal being frauded, but not many cases. ATM fraud is still quite significant, and obviously there is a concern. There also is a surge at unattended payment terminals, like at petrol stations. We have to be careful because what you see in proximity payments, even if the trend is going down, someday we may have some concerns about the actual unattended payment terminals and the security associated with those. That is giving us ideas for concrete actions in the next few months or years.

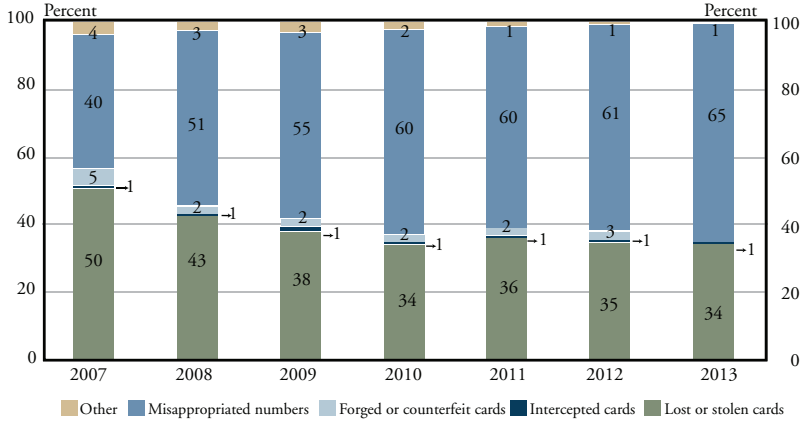
Another interesting thing is to try to determine where the fraud comes from, and the fraud type itself. For domestic transactions, looking at the data since 2007, we see the main two areas where fraud is coming from (Chart 9). The first area is misappropriated numbers, which is basically the numbers fraudsters gather from, for example, card skimming or on e-merchant websites and reuse in online transactions. This is linked to CNP fraud and now accounts for 65 percent of the fraud type origins. The second area is lost and stolen cards. With a lost or stolen card, fraudsters can

Chart 8
Card Payment Fraud



Source: Banque de France.

Chart 9
Breakdown of French Fraud by Type (domestic transactions, fraud amount)



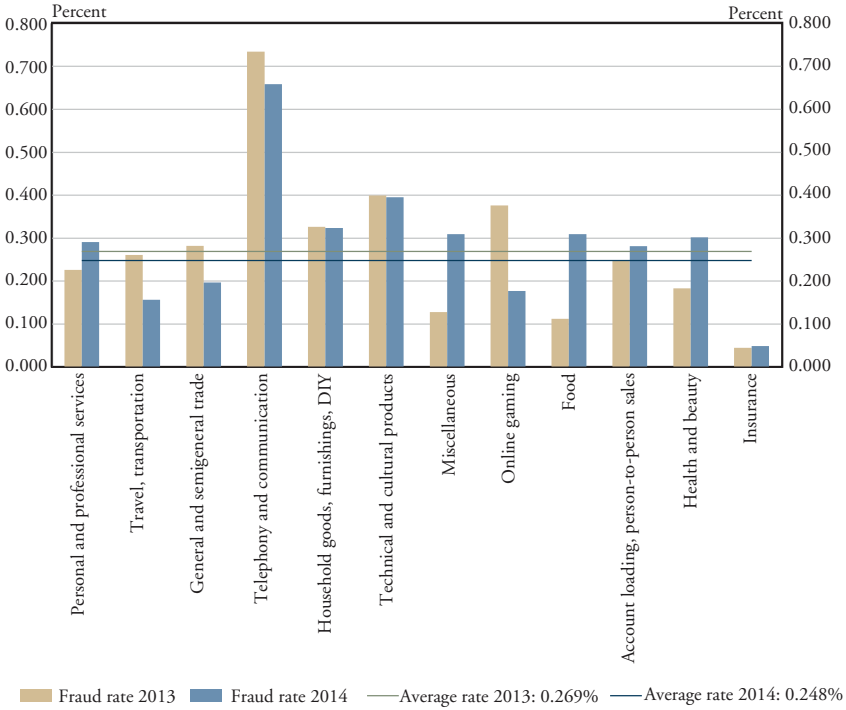
Source: Banque de France.

reuse the numbers and also do some contactless payments. These are the two main trends we see. Anything linked to counterfeit cards has disappeared from the radar screen. In 2007, we had 5 percent of fraud coming from counterfeited cards, but this is not the case in the last few years.

Another thing we do is identify the categories, the sectors where the fraud is being concentrated. We do that on domestic fraud rates and domestic numbers. As depicted in Chart 10, we can see they are always the same type of merchants, which are concerns especially for online card payments and online fraud. Telephony and communication is a main sector of fraud. Prepaid calling cards, for example, are where the fraudsters are going. So, there is an eye of concern there. Electronics, high technology goods—with online payments—are also where the fraudsters want to go. And online gaming; that was something that developed as soon as there were licenses given to the operators of online games. It was forbidden in France before 2010, and then authorized with a specific license. We saw straightaway a surge in the fraud rates for those online gaming sites, so we took some concrete actions to diminish that fraud and to impose stricter security rules. Now we see that fraud rates are coming back to normal—quite close to the average rate.

To finish, let us focus on the main security threats we see and recommendations we issued. I will look at what we say about counterfeiting, theft and other areas, focusing on two hot topics in the last two to three years—online identity theft or basically CNP fraud, and contactless

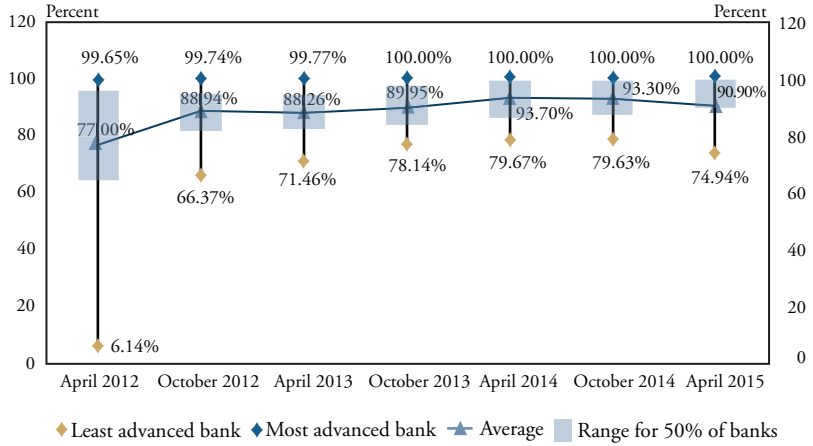
Chart 10
French Fraud Rates for CNP Payments by Sector



Source: Banque de France.

payments. We had to enhance the security of online card payments, based on the fraud figures we saw. The CNP security issue has been the main one since 2008. We pushed for strong customer authentication. We did not push for a specific technology to achieve this goal; we pushed for a level of security. They used 3D Secure, fair enough, but we do not want people to use 3D Secure with static passwords. We want people to use 3D Secure with strong customer authentication—tokens, SMS codes, those types of things. It has been an interesting game. We started first to make sure that the issuers had fully equipped cardholders. So the cardholder indeed has the ability to strongly authenticate when he is making an online card payment. And then we tried to convince merchants that there was a good incentive, like the liability shift, for example, in 3D Secure, to go to strong customer authentication and 3D Secure altogether. To ease the process, we decided to allure them to have a risk-based approach to progressively deploy those technologies at e-merchants at their websites. It is not only a French initia-

Chart 11
Cardholder Two-factor Authentication Equipment Rate

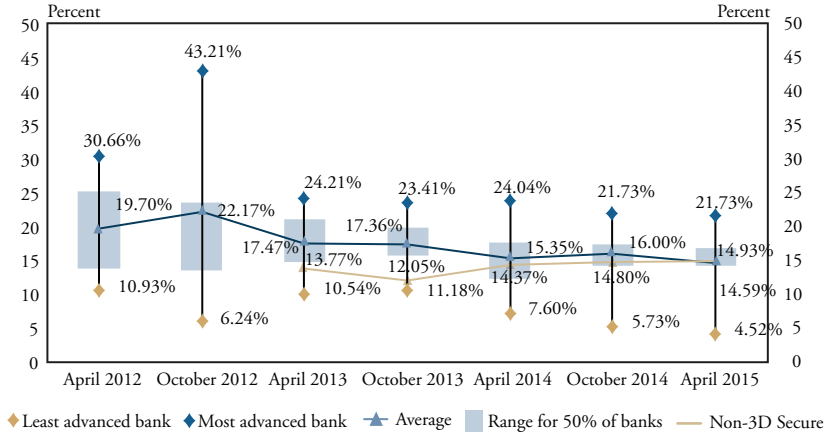


Source: Banque de France.

tive, or it cannot be a French-only initiative at this point. If we try to solve the situation in France, that situation will be brought to countries just next to us. So we also strongly supported the emergence of a European initiative on the security of payments and payment instruments, and especially the security of online payments. That is why there is this SecuRe Pay Forum, which was created in 2011. We also tried to push the legislature, at least with the connections we have there, to have more integration of those security concerns within the law. The European Payment Services Directive from 2007 is being revised right now, and will implement strong two-factor authentication in the law, with some kind of a risk-based approach in it. And obviously, we are running data, again, just to understand where we are with all this.

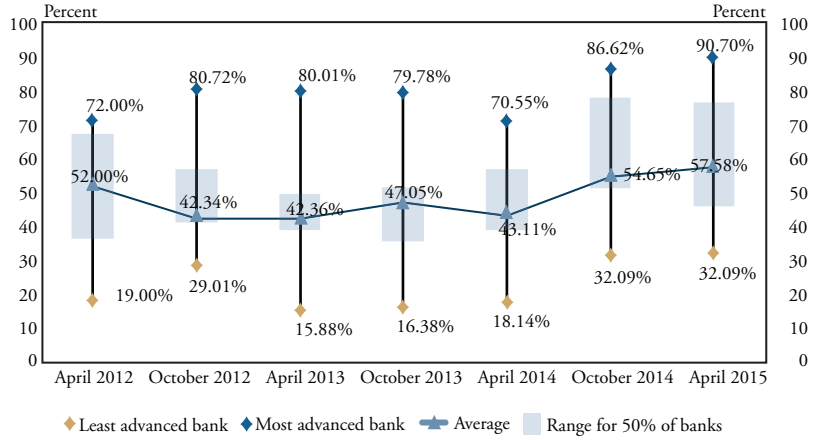
As depicted in Chart 11, cardholders are now fully equipped with strong two-factor authentication. The majority of the banks have a very high adoption rate. Now let us look at the failure rate for 3D Secure, given 3D Secure is the most widely adopted protocol for ensuring the security of online card payments (Chart 12). The merchants have told us they will lose business if they go to 3D Secure. We decided to compare the failure rates of 3D Secure transactions and non-3D Secure transactions. It is very interesting to see that first, there is a large disparity between the different banks on the "crying side." Some of them have high figures, high failure rates; some of them have low failure rates. But on average, we can see failure rates for 3D Secure and non-3D Secure—these are the two horizontal lines—are getting very,

Chart 12
3D Secure Failure Rates



Source: Banque de France.

Chart 13
E-Merchants 3D Secure Equipment Rate



Source: Banque de France.

very close in the last year and a half. I mean, the failure rate for 3D Secure was down from 17 percent to 16 percent and to 14.5 percent now, which is now about the same as the failure rate for non-3D Secure. So we are convinced, and especially with this risk-based approach in mind, that there is not a compelling counterargument to moving toward those types of secure transactions. That said, we still are developing the adoption of 3D Secure at merchant websites. Right now we see that a little less than 60 percent of the

merchants are fully equipped (Chart 13). That means there is still a long way to go and there are a lot of people still to convince.

Now, I will finish with contactless card payments. It has been a concern since 2007. We have regularly analyzed the lines of contactless technology, looking at threats like remote activation of cards, and eavesdropping on the transactions, so getting the numbers from the cards without the cardholder wanting that. We still conclude that there is more of a reputational risk than a financial one thanks to the transactions thresholds such as the numbers and the amounts of transactions, including cumulative, being there in the cards. And the reuse of the data is actually very, very limited even if fraudsters can still use some of the data on some websites, for example, which is a concern. But we made some new recommendations that issuers have deactivation mechanisms for the contactless interface just in case the technology gets broken at some point. For example, through remote EMV scripts, when you enter your card into an ATM or when you do a proximity payment with an EMV chip, there is the ability to just shut off the NFC communication, so the contactless payment application itself is deactivated. Also, we want the customers to be in control. So if there are fears about that, we ask the banks and the issuers to issue contact-only cards based on customer demands.

For the first time we have fraud figures for contactless payments for 2014, actually for the last nine months of 2014. First, the fraud rate is very close to proximity payments. It is 0.015 percent, which is very low, which is a good sign. Then, a concern was obviously, what is the origin of this fraud? Is it the technology itself being broken by some people? Actually, the origin of fraud is lost and stolen cards, so as I said earlier, if you lose your card or your card is stolen, the fraudsters will get the numbers, go on the Internet, and try to pay with it. But some of the fraudsters also know it is a contactless card, so they usually just go to a merchant somewhere and pass the few transactions they can before the thresholds are met. The data confirms, at least for now, our analysis and conclusions. But we will definitely focus more or continue focusing on contactless payments in the next few years.

Monitoring Payment Fraud: A Key Piece to the Puzzle

Commentary

Chris Hamilton

We are going to change accents now for a little while. First, I am filled with envy for the quality of the material the Observatory collects and publishes. We are still a far cry from that in Australia. It is wonderful to see that kind of quality of data available. I do not want to spend a lot of time on how we do what we do in Australia. In fact, I am going to draw into a statistics presentation without talking about too many statistics. The sheer depth of what Alexandre Stervinou presented to you is a testament to how interesting and potentially useful these data are. But I would really rather talk about the whys and the politics and policy behind this kind of data collection because I think it is more relevant to coming to grips with the public policy implications and what should be done by the industry. Let me start with an anecdote about my past life.

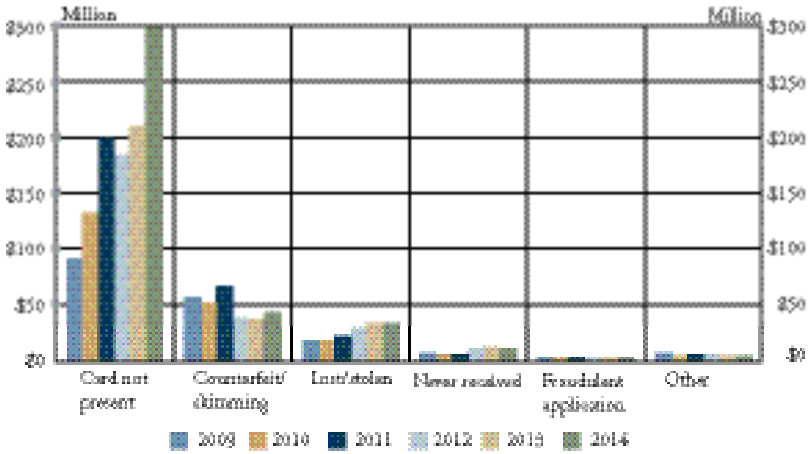
A long time ago, when I was a much younger man, I used to work for the Australian Stock Exchange. You probably know that more than 20 years ago stock exchanges around the world went from being what is called "open outcry," where everyone yells at each other in a big room, to being electronic, where they all sit at computers and do not talk anymore and just tap the keyboard all day. Some stock exchanges still have a bit of theater around them; the New York Stock Exchange is an example. One of the side effects from going from open outcry to computerized trading is that you go from a situation where the information that is known about the stock market, who is doing what where, the speed of transactions, what stocks are moving, all that is being picked up at the event. If you really want to know it, you have to stand in the room. That is open outcry. We have gone to a world where the entire performance of the stock market is available, down to keystrokes at the hundredth of a second level to anyone who wants it as long as the stock exchange is prepared to give it to them. You go from a situation of quite limited data about what is going on in a very complicated

human environment to where you have almost unlimited data. And that has some very interesting effects on how things are done. This is the analogy I am trying to draw. When the Australian Stock Exchange computerized, which it did relatively early by global standards, insider trading became extremely hard. Although you cannot always tell when it is happening in the market, surveillance experts say an electronic record of trading can always tell you if someone is insider trading because you can see them moving before the announcement. If you have keystrokes down to the hundredth of a second, it does not matter how clever they think they are. You can work it out from the data. What you need is a good surveillance unit that puts two things together—detailed information about trading on the marketplace and key events in a company's history. The trouble with insider trading is that sooner or later the event has to come out, you have to know, and so you catch the crooks that way. One consequence of really good data is a completely different approach to enforcement and quality of law enforcement. But another very important consequence of that change was that a whole academic discipline and tradition grew up around analyzing this volume of data about the trading market to understand how markets work. As we heard this morning, the application of game theory to how stock exchanges work has become an enormous academic growth industry and people understand much more deeply now how markets work because they have this detailed information. There are, however, all sorts of unintended consequences from being able to capture this data, some positive, which are worth bearing in mind.

When I moved to work in payments, about 10 years ago, I felt like I had been blindfolded. We are lousy at data, and we should be ashamed. The quality of detailed data about performance of the payments systems around the world is really lacking and someone should do something about it. The information that we have is after the event. We have publications; I did my publication a couple of weeks ago and Alexandre is doing his in a week. We have data coming out six months after the relevant period. We have relatively high level data about how things work, and we are only able to draw very broad inferences, which we then need to explore further. So, the first thing to say is we should do this a whole lot better than we do, and there is no technological reason why we cannot. As always, it is the human, the economic and social organization part of it that is the challenge.

I want to talk about that. What is it we are trying to capture, and why? Why is that a good idea? Who should capture it, and who benefits from

Chart 1
Australian Card Fraud by Type, 2009-14



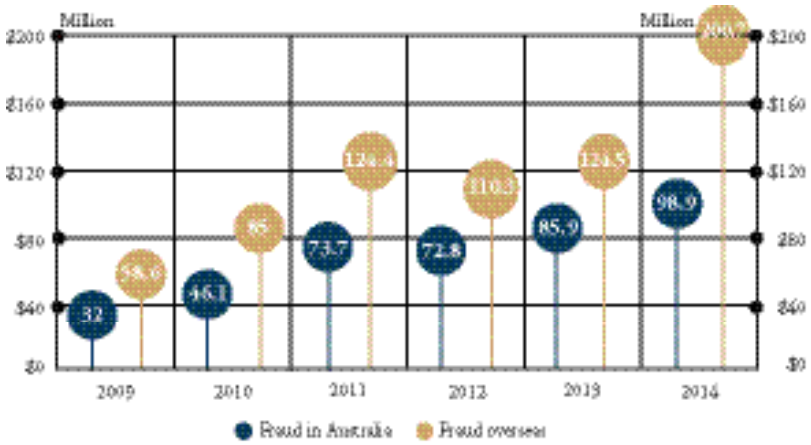
Source: Australian Payments Clearing Association.

that capture? Those are the things I want to address, and I will try and draw some reference points from the French experience.

What we want to capture is reasonably clear, and there is an endless further level of detail you can go down to, but the Observatory gives us a very good starting point in terms of what are great things to capture. You want to know about the sheer rate of fraud, the prevalence, and have it broken down in as many different categories as you can. In Australia, we do something similar. We recently published our 2014 numbers (Chart 1). We have been tracking fraud data for about 12 years. This is just a five-year horizon to give you a sense of what is happening, and you can see very starkly the kind of experiences you see in the French data. Card-not-present (CNP) fraud is the big problem of the day. Everything else is nearly solved. It is either flat-lining or dropping. But CNP is the big problem of the age on card data. There is another story elsewhere. Not only is CNP the problem, but offshore CNP is the big problem in Australia (Chart 2). That differs from the French experience just because we probably are on a cycle that lags Europe by a couple of years. I have observed that before, the cycle happening in Europe and then coming to us. That is another good thing to bear in mind as you look at these numbers. And of course, the consequence is, and this is again very similar to the Observatory's experience, over a five-year cycle we have gone from CNP fraud being half the fraud problem to being more than three-quarters (Chart 3).

Chart 2

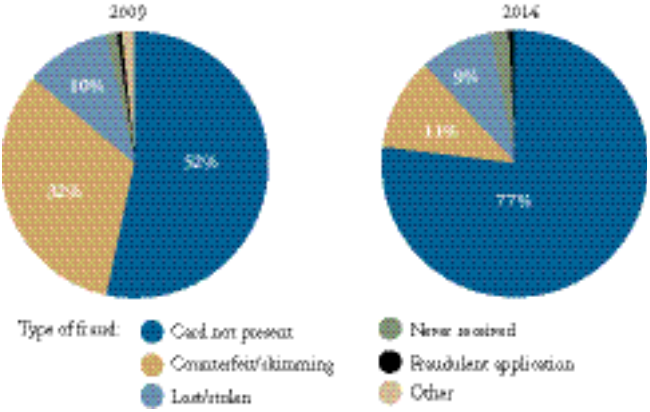
Card-not-present Fraud in Australia, 2009-14



Source: Australian Payments Clearing Association.

Chart 3

Growth of Card-not-present Fraud in Australia, 2009-14



Source: Australian Payments Clearing Association.

Capturing the prevalence, the trend line, is really important, but it is only the beginning of the challenge. The other thing the Observatory does well, and which we do but in a different way in Australia, is capture the threat matrix to determine the upcoming problem—what Alexandre called the technology watch. In Australia, we do that in a much more informal way, sort of a clearinghouse approach where you get the large organizations involved in comparing notes on fraud events. They take away the raw data of observations and do their own analysis. It is a much more decentralized process. You can argue it is both more and less effective for different purposes. It probably is better if they are looking specifically at protecting their own shops because they will have much more detail on the standing of their own customer environment and their own particular risks and vulnerabilities. On the other hand, it is not very helpful for looking at the global picture and seeing what is happening in a broader sense. One thing that has started in Australia is the formalizing of a longstanding informal structure called the National Fraud Exchange, which is sort of a clearinghouse of ideas. The major participants will all fund and provide threat information and use that as a shared resource across the industry. So, formalizing and automating that process is one of our current priorities.

The third thing, which none of us does very well, but which is actually really important, is impact analysis. What happens when fraud happens? Who actually loses, and what are the costs both of prevention and of the actual event itself? And this is really hazy. We saw some of that in the first series of presentations. Is it really right that the consumer does not bear the fraud? Is it really right that the issuer does? In Australia, officially the issuer bears the fraud, but in practice the great bulk of the fraud is probably borne by merchants because of the various liability shifts. That has very big impacts on their incentives to change and the way they are going to work or not work with the industry. For me, that is the least well-developed of data areas that we should be working on. What are the real costs of this stuff? I am sure the global cost of EMV implementation dwarfs the actual savings in fraud. There is no question that we have all spent a great deal more putting the EMV chips in cards than the fraud that we have saved from doing so. That does not necessarily mean it is a bad idea, but it probably is a useful thing to know. There needs to be much more on that work. If that is what we are trying to collect, then it is worth thinking about the whys. What are we going to do with this when we get it, and who might benefit?

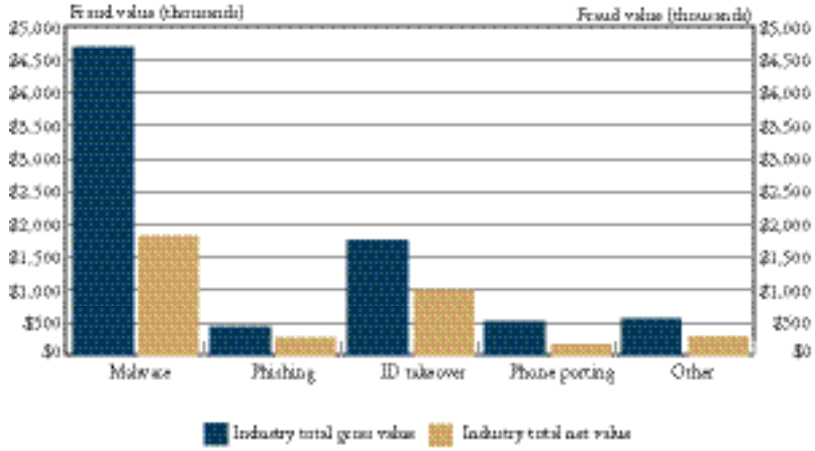
There are several very good reasons. I come at this from an industry perspective. The Observatory thinks about things from a public policy

perspective—what is in the best interest of the community? I am coming at it from a slightly different perspective and I should explain what the Australian Payments Clearing Association (APCA) is. It is not a government body; it is completely privately funded. The nearest equivalent in the United States is the National Automated Clearing House Association (NACHA), but we are not that much like NACHA; APCA is an organization that administers the rule books on behalf of the financial institutions in payments. So, we are only as good as the collaboration we can persuade our members to perform in improving the overall payments system. Our goal is to improve the payments system, but from the industry perspective of how do we work together as a community on what is important to all of us to make the payments system better, rather than what is the public good. Public good clearly comes into it; it is clearly a big factor. But we need to marry that with the collective industry of the community. Coming with that lens to this fraud data, why would you voluntarily publish fraud statistics? In many countries, that does not happen and there appear to be good reasons why. People do not want their brands associated with large reported frauds. People do not want to scare off customers with stories of fraud. But that is a shortsighted view; the much better path is to think about the long-term gain for the industry. So, forget the public good for a second.

The people mostly affected are our collective customers, the consumers and businesses of the community. There is a sort of moral dimension here where they have a right to know so they can do their own risk assessment. That is one reason why it probably is a good idea, but there also is a practical one, which is they need to be participants in the fraud-prevention process. Consumers and businesses all can do fairly basic sensible things to minimize their own risk and prevent fraud. They cannot, however, solve the problem by themselves. There are many other things other people have to do, but it would be nice if they were active participants in that process. You start doing that by educating them about fraud, by giving them a clear picture of what it is (Charts 4, 5). So, that is a good, practical reason for industries to do this work voluntarily. The other obvious benefit relates to a point made before—what gets measured gets managed. Unless we know what the fraud is, we do not know where to focus our limited dollars on trying to prevent it and improve it. It is very important to have that kind of data when you are arguing the case for whether we should do EMV, or go to two-factor authentication or 3D Secure. And not having good quality data is one of the things that makes that process quite hard. In Australia, we had an initial go at EMV, at chip cards, more than 10 years ago; not as far back as the French. That effort

Chart 4

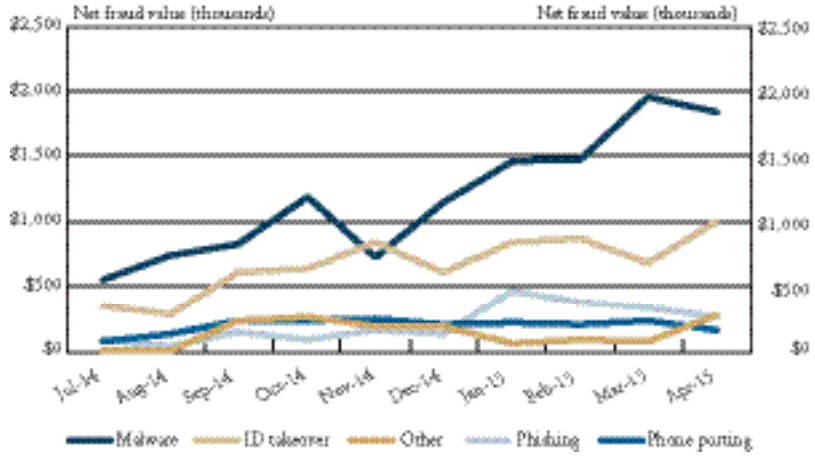
Gross/Net Fraud Values by Fraud Method, April 2015



Source: Australian Payments Clearing Association.

Chart 5

Net Fraud Value by Fraud Method, July 2014-April 2015



Source: Australian Payments Clearing Association.

failed through lack of articulation or a strong enough case for change. I think if we had had the quality of data and the trend lines we have now about fraud, you might have gotten a different result. Indeed, the second time around, having the benefit of that information was at least as important a factor in what has been a very successful chip conversion.

Having a grip on that helps the industry work out what it should and should not do collectively to improve the system. The data also give organizations a much better risk management capability within their own shops. All large banks around the world now are scoring approaches, doing risk approaches to fraud—some are really good at it and some not so good—but they all would get much better if they all had all the data. Seeing their own data is not enough, and having the benefit of detailed information about data is potentially extremely valuable.

If that is what we are trying to achieve, then the last point I want to cover is who needs to do this, and how they should go about it. And I am going to give a slightly different point of view. I do think that this generally is actually better done by industry. I *would* say that, would I not? I work for industry. Natural bias. And yet, my experience is that work to improve the overall payments system, which is done collaboratively by the institutions that work in it, when they are convinced there is long-term benefit both for their customers and for them, is much better done than forced compliance as a consequence of regulation. It is hard to pull off. It is much harder to do. So, compliance in a way is easier. What happens is the banks have outsourced to the regulator the problem of deciding what should be done because the compliance rules tell them what should be done. They can comply and they get to bellyache about it at the same time—sort of a win/win. But in the long run, these things work a lot better if, having been convinced of the need to actually make the change, they then implement it because they will do it in a cost-effective way. They will do it in a way which fits with their business, but still meets the public policy goals.

The last thing I want to talk about is this Australian way of having a go at the public/private partnership. Let me observe that in relation to Adam Levitin's distinction between public ordering and private ordering, I am suggesting that is a bit of a false dichotomy, or at least it should be. What we really should be doing is finding a way of marrying the public and private methods of doing things, and the public and private interests to get the best possible outcome. And I think that is possible, if you can get the industry convinced of the value to them, which is also in the public interest, you can then get a willing, collaborative approach to solving the problems we are talking about. And in fraud, that actually works better than many other areas of changing the payments system because it is easier to convince people that fraud is everybody's problem. It does not tend to have a major comparative element to it. It sometimes does have little bits of competitive tension among the banks, but in general, people agree that if I am lax on

security it is going to affect you and vice versa, and so it is easier to get that collaborative agreement. My suggestion is that in the long run, we need to gather this data because it is in the interest of the industry. But then we need to work on it together to find the best way of improving the payments system using the data itself.

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.