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.

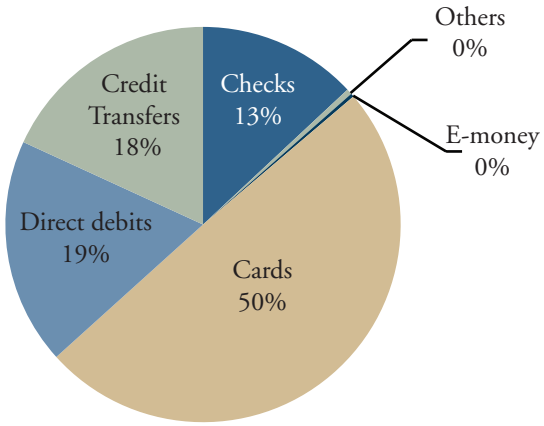
The composition of the technology watch working group is similar to the working group on statistics. Its mission is to maintain a technology watch with the aim of proposing measures to the plenary and its members to increase or maintain the security of card payments. Everything around innovation, mobile 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



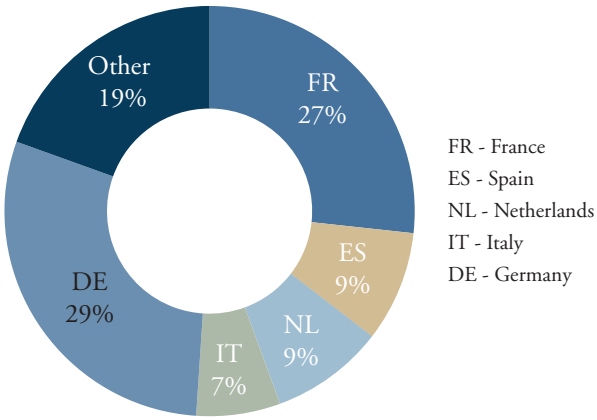
Source: Banque de France.

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.

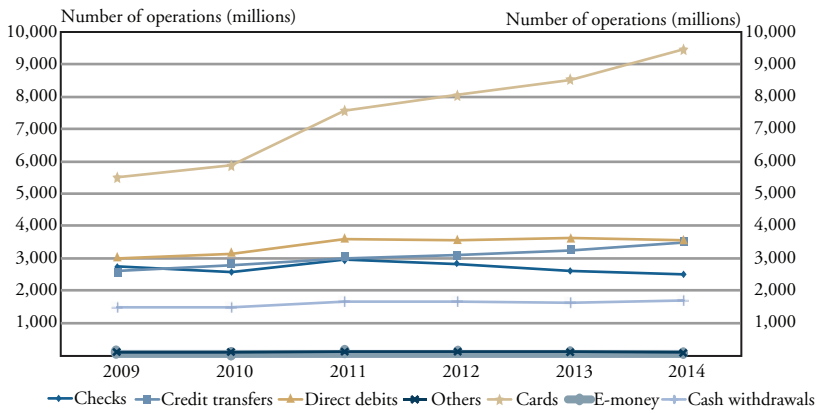
All of this leads us to the concrete figures on fraud. We have to follow up on what is happening there. If you look at the value of transactions for cards, we have reached around €600 billion (Chart 4). There is constant growth in the actual value of card-based transactions. So, the amount of fraud is 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.

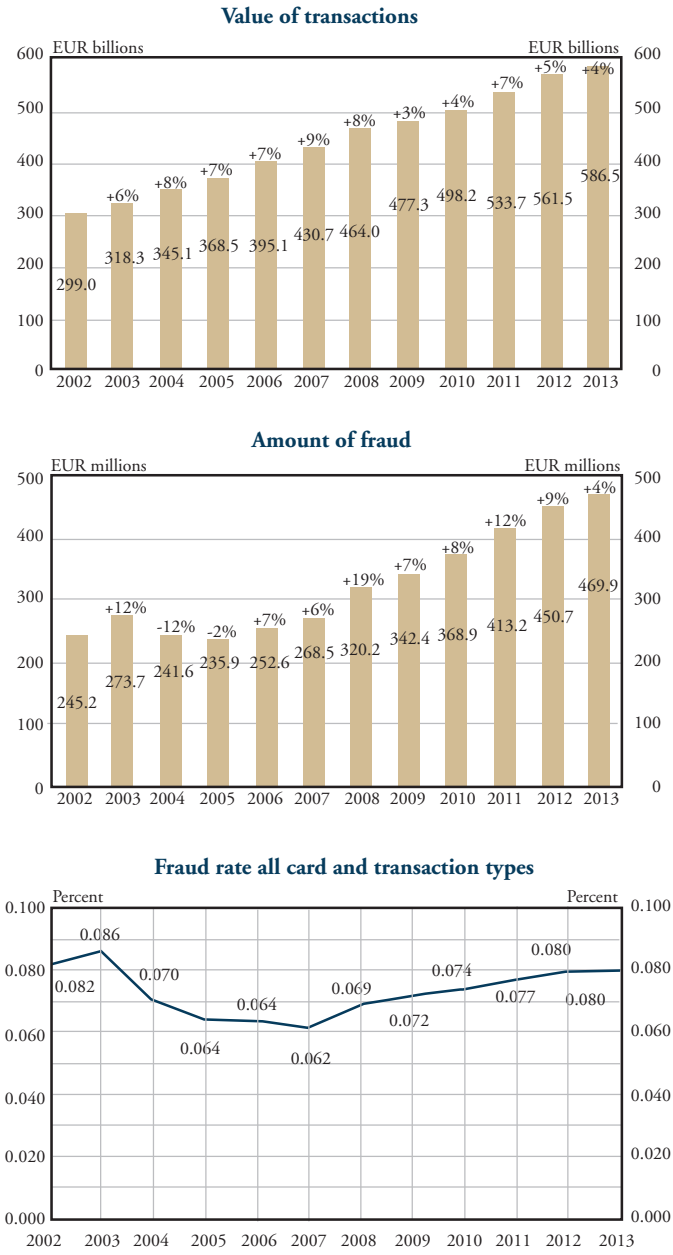
Chart 3
Payments in France by Type, 2009-14



Source: Banque de France.

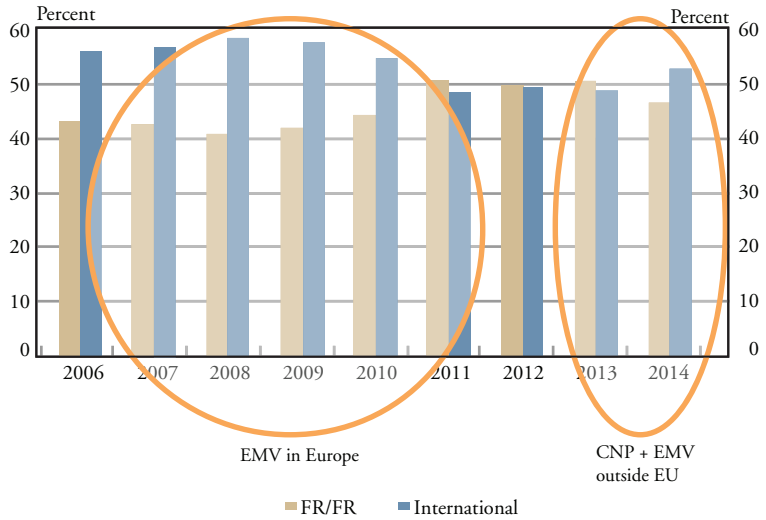
Now we will look at it in more detail and what all this means because there are huge variations between the territories and the type of transactions. If we first focus on the share of domestic fraud versus international fraud, we already see some differences (Chart 5). The data in brown concerns only 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

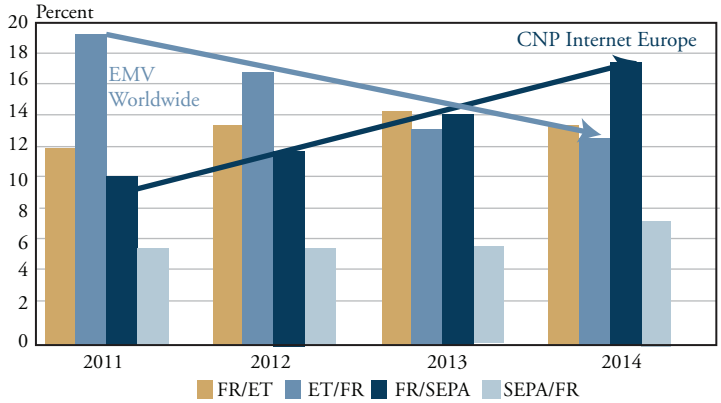


Source: Banque de France.

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



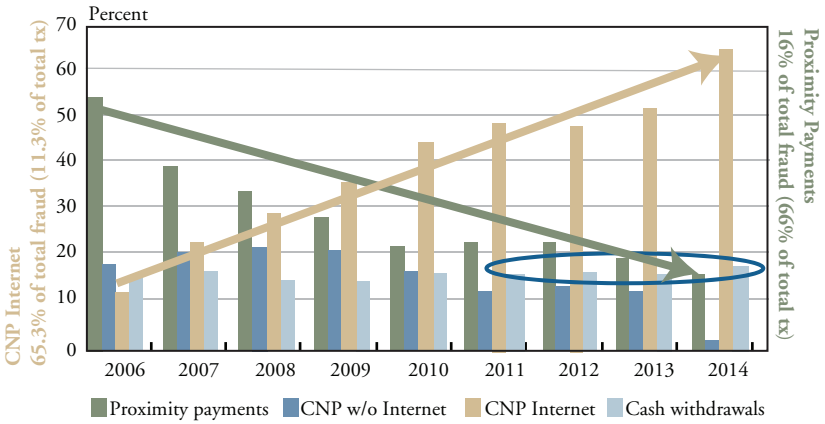
Note: Figures are for cards issued in France and frauded in the Single Euro Payments Area (SEPA) and beyond (ET) and for cards from SEPA or beyond and frauded in France.
Source: Banque de France.

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

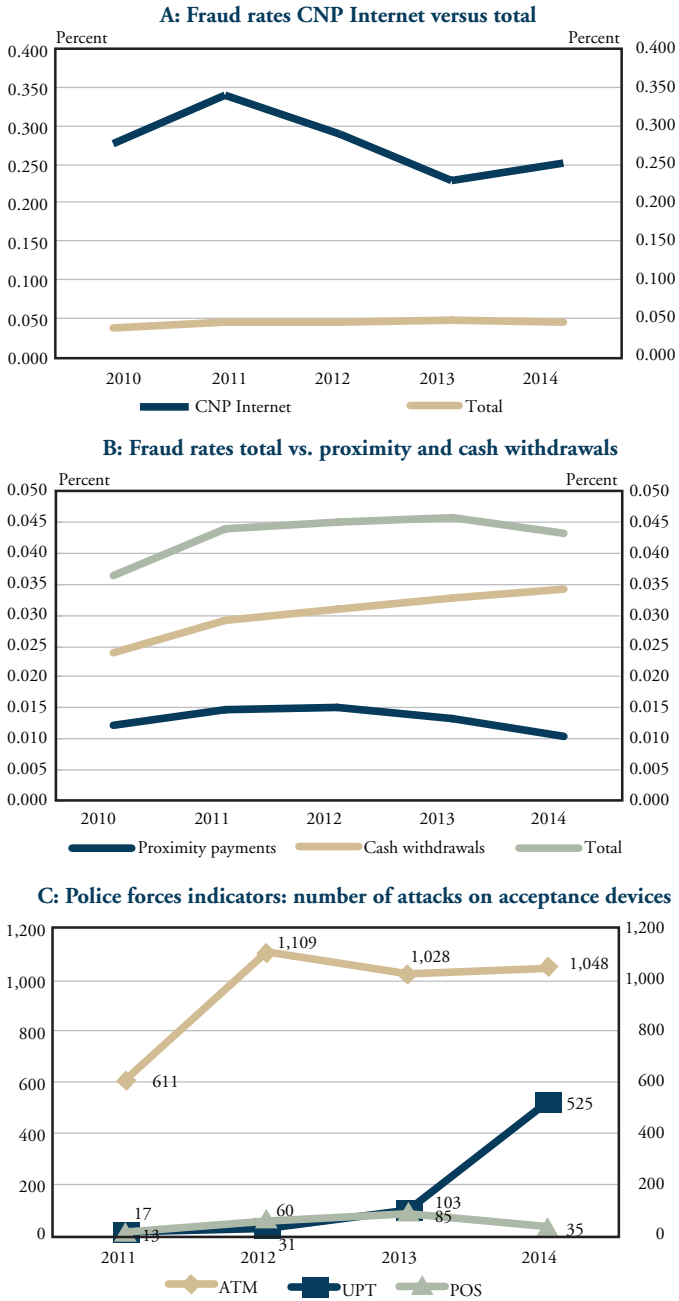


Source: Banque de France.

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.

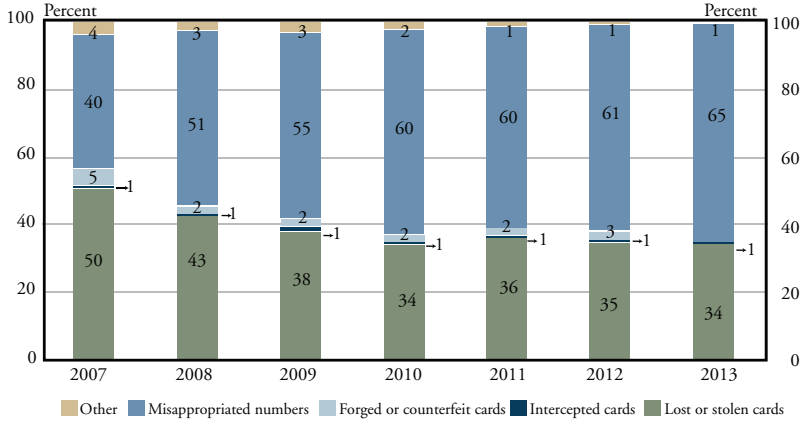
Another interesting thing is to try to determine where the fraud comes from, and the fraud type itself. For domestic transactions, looking at the data since 2007, we see the main two areas where fraud is coming from (Chart 9). The first area is misappropriated numbers, which is basically the numbers 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)



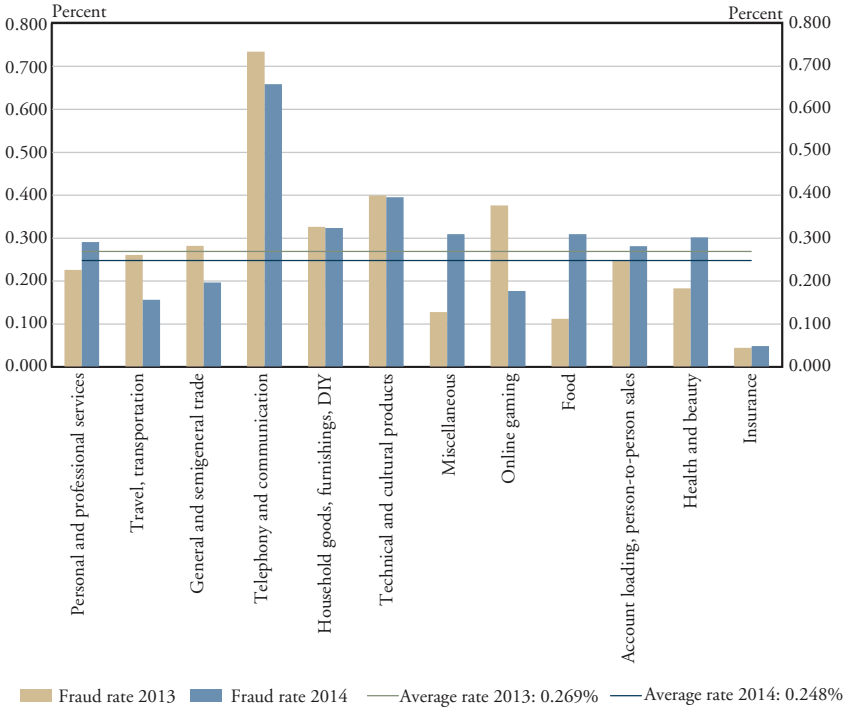
Source: Banque de France.

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

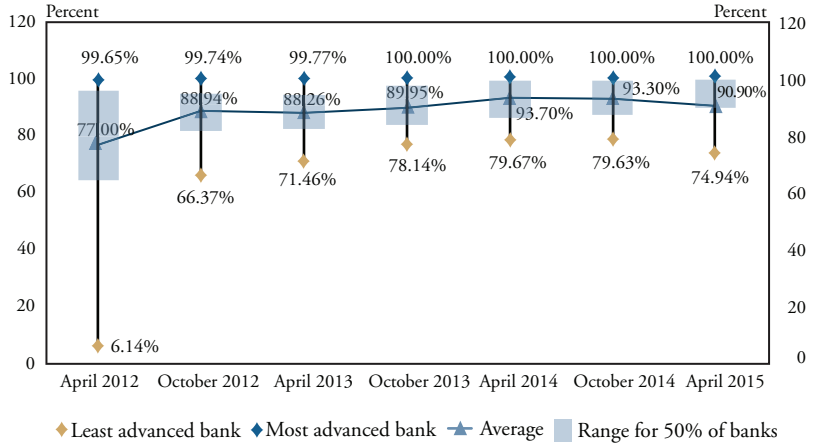
Chart 10
French Fraud Rates for CNP Payments by Sector



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

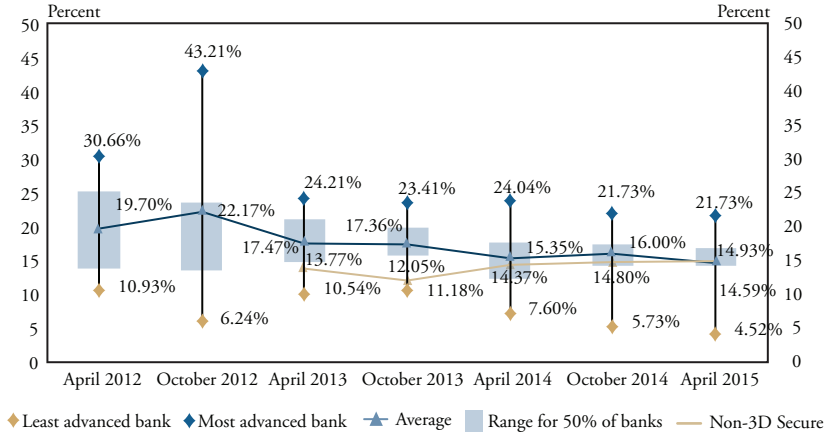


Source: Banque de France.

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.

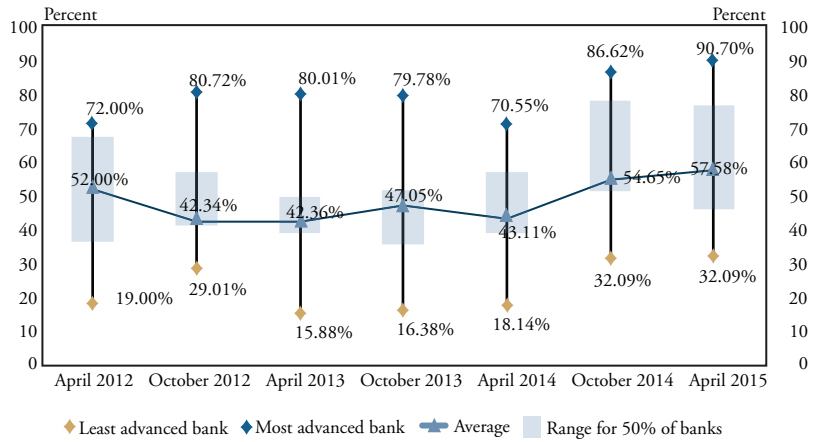
As depicted in Chart 11, cardholders are now fully equipped with strong two-factor authentication. The majority of the banks have a very high adoption rate. Now let us look at the failure rate for 3D Secure, given 3D Secure is the most widely adopted protocol for ensuring the security of online card 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.