

THE FIGHT AGAINST FRAUD



A study of experiences and opinion within leading banks across Europe, Middle East and Africa

EXECUTIVE SUMMARY

Introduction

While fraud is a significant issue for the banking industry today, its impact is difficult to assess or quantify. Card and payment fraud losses at a European Union level have been estimated at up to €1 billion annually but there are very few fraud statistics available at a country level. The opportunity cost in terms of lost business due to consumer anxiety about fraud, whether online or in the physical world, is much higher and fraud is a sensitive subject for banks concerned about profitability, reputation and competitiveness.

Increasingly recognised as a global phenomenon, fraud will continue to have a major impact on the industry despite our best efforts to counter it. As one of the respondents to our study says:

“Fraud will never be stopped. I disagree with anyone who says that you can completely prevent it. The fraudsters are now about six months ahead of the industry.”

Yet there are steps to be taken and initiatives to be introduced that can seriously limit the scope and success of fraudsters. This study seeks to examine trends in the detection and prevention of four key types of fraud: ATM, POS, card not present (CNP) and online. The research looks at current practices, the attitudes of banks across Europe, Middle East and Africa towards fraud and their views on how fraud can be countered and contained. In commissioning the study, First Data hopes to promote greater understanding of how we can successfully work together to combat the fraud challenges facing the payments industry.

Key findings

The research findings reported here represent the views and experiences of senior fraud experts from 52 banks across Europe, Middle East and Africa. Research was carried out by Olive Insight, an independent research firm, between December 2006 and February 2007.

Commentary is also provided by senior representatives of APACS, the UK Payments Association, and the European Payments Council's Card Fraud Prevention Task Force.

- Fraud attacks the bank where it hurts the most. Over 80% of respondents see damage to the bank's reputation as one of the most important ways in which fraud threatens the organisation.
- ATM device fraud is seen as a significant problem today for 48% of banks. Fifty percent of banks are increasing expenditure on countermeasures to combat ATM fraud.
- Respondents are most concerned about new and emerging frauds. Online fraud - which offers the fraudster scale efficiencies and reduced personal risk - is a real problem across Western Europe and a significant threat elsewhere in the region. Thirty eight percent of respondents report an increase in phishing attacks.
- Fraudsters operate on a global stage. Fraud moves rapidly across types of business and geographies; 96% of respondents believe that fraud is learned and passed from one part of the world to another.
- Two thirds of respondents believe that fraud is to some extent predictable - we have the opportunity to anticipate how fraudsters will strike next, though not necessarily where they will do so.
- Technology is a key weapon in the fight against fraud and a priority for over 50% of respondents. Many organisations are introducing anti-skimming devices and improving security at ATMs.
- Chip and PIN is widely endorsed although its extension across the region is expected to drive fraud into card not present environments.
- Technology is a double-edged sword. Just as it assists banks to counter fraud so it provides fraudsters with new gateways and loopholes through which they can attack.
- The training and education of staff is seen as crucial in the fight against fraud. Skilled staff are essential in tackling this highly flexible and fast moving threat to the banks and their customers.
- Study respondents have mixed views about the impact of regulation on fraud. Fifty five percent believe that regulation helps while others, especially in Western Europe, are concerned that regulation may prove too restrictive in a rapidly changing environment.
- There is general agreement that a concerted industry-wide effort is needed to combat fraud, with banks, merchants, law enforcement and other agencies working together and sharing information. However, issues of competitiveness and data protection legislation are both seen as significant barriers to open communication and industry co-operation.

First Data Insight

This study clearly reveals the extent to which information sharing is the key to the effective detection and prevention of ATM, POS, online and card not present fraud across Europe, Middle East and Africa. It also demonstrates the ways in which uncertainty and ignorance, of both the scale of the threat and its many sources, cloud attempts to combat fraud. Inadequate information about the costs of fraud combines with sensitivities about reputation and competitiveness to limit the willingness of some banks to share data. Data protection legislation restricts - or is believed to restrict - their ability to do so. Regulation is seen by many as essential and by others as a strait-jacket that denies banks the flexibility they need to meet an ever-changing and ever-advancing threat.

Technology is widely recognised as a significant weapon in countering fraud and many banks are evaluating or introducing advanced tools and techniques, both to tackle fraud and to understand the extent of its hold on their organisations. There is also a clear understanding of the importance of staff training and education in the fight against fraud.

Ultimately, though, banks will need to look beyond their own organisations for solutions. Many believe that fraud is predictable. As a result, the appearance of a new fraud type on the global stage should be the focus of careful study for those yet to experience it. As initiatives like Chip and PIN are rolled out, we know that the fraudsters are already looking for new areas of weakness - banks and their partners must be vigilant in examining every new development, every new product or sales channel to ensure that it is as robust and as fraud-resistant as possible.

It is in the sharing of information and intelligence that our best hope lies. Banking and other trade associations are already actively promoting data exchange between banks, as well as more effective co-operation with law enforcement agencies. The European Union and European Payments Council have signalled their belief that multi-national fraud databases will be necessary to counter fraud in the Single Euro Payments Area (SEPA). We must work together to ensure that words translate into action and that the industry, including regulators and law enforcement agencies, takes practical steps to deliver a strong, unified response to the global fraudster.

RESEARCH FINDINGS

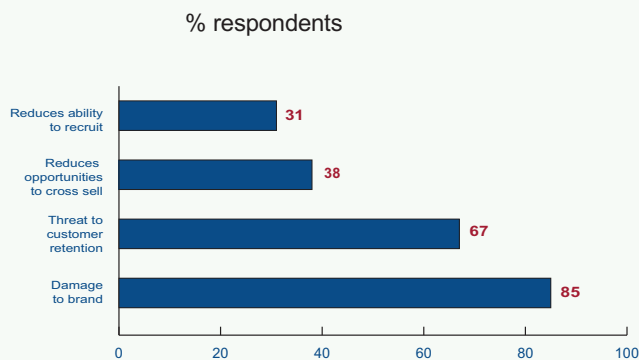
Experiences of fraud

Fraud is a major concern for banks across Europe, Middle East and Africa. According to the EU Fraud Prevention Expert Group (FPEG), some €500 million - €1 billion is lost annually in card fraud across the European Union alone and the FPEG notes that this statistic "is not necessarily decreasing".

Furthermore, banks cannot consider their 'appetite for fraud' in a financial sense alone. Fraud is increasingly seen by governments and law enforcement agencies as an important method of bankrolling serious and organized crime, including drug trafficking, people smuggling and terrorism. There is now an ethical dimension to fraud prevention.

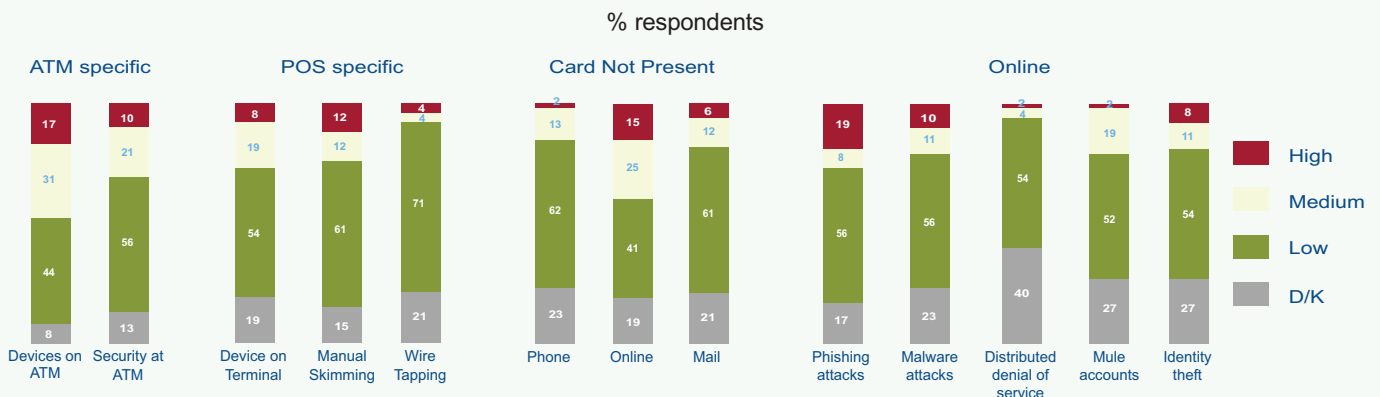
There are also important issues for banking reputations and consumer confidence. Over 80% of respondents to the First Data study see damage to the bank's brand and reputation as one of the most important ways in which fraud impacts the organisation. Customer retention is also clearly an issue, especially for banks in Central and Eastern Europe, but the potential for fraud to damage the bank's brand means that fraud has an impact well beyond the financial losses it generates. Fraud attacks the bank where it hurts the most.

What are the most important ways in which fraud threatens your organisation?



The concerns of our study respondents are focused more on future threats than on current realities. Around half of all respondents believe that fraud - whether ATM, POS, online or card not present - is at relatively low levels today.

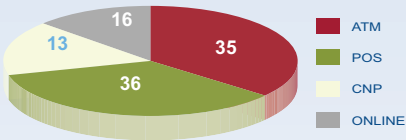
At what level are different frauds operating within your organisation today?



First Data Insight

The research firm conducting this study reported a very high level of interest in the project and a strong appetite for information from across the region. However, concerns about the sharing of sensitive information prevented some from participating and lack of information meant that others provided incomplete data. This clearly has implications for the industry's ability to get a true picture of the impact of fraud - and for our ability to counter it.

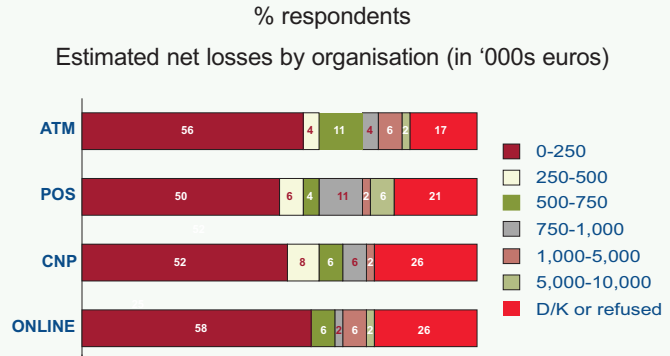
What % of the fraud experienced by the bank does each type of fraud represent today?



In 2005, the European ATM Security Team (EAST) reported 3,143 card skimming attacks resulting in losses of nearly €44 million across Europe.

A minority of banks are losing more than €250,000 annually through any one type of fraud - although study results with regard to financial losses need to be treated with caution since around one fifth of study respondents either don't know the financial impact of different frauds on their organisations or refuse to provide this information.

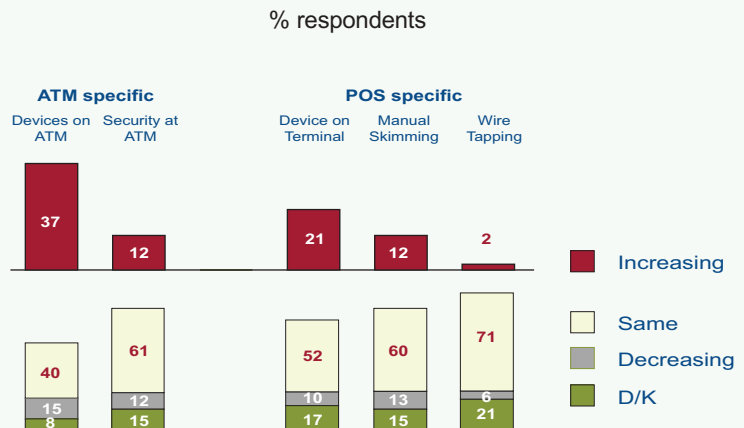
What do you estimate to be the total net losses of each type of fraud to your organisation, in a single year?



POS and ATM fraud account for over 70% of all POS, ATM, online and card not present fraud today. Estimated losses are highest here and almost one fifth of respondents report losses over €750,000 a year from POS fraud.

While the cost of POS fraud may be higher, the banks in our study appear more concerned about ATM fraud - in particular, about ATM device fraud. This is rated more highly in terms of incidence - with 48% of our sample reporting ATM device fraud at high or medium levels today - and in rate of increase. ATM fraud is a particular concern for respondents in Western Europe, who report higher levels of fraud overall, and in Eastern Europe where respondents fear the migration of skimming devices from the West.

Are fraud levels increasing, staying the same or decreasing?

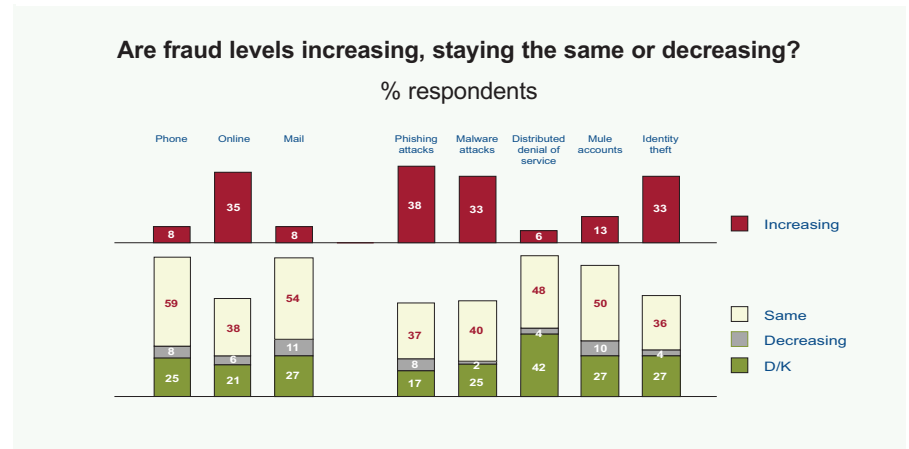


The UK's Financial Services Authority reported that over £23 million was stolen in the first half of 2006 through phishing attacks involving fraudsters representing themselves as bank officials via email to gain access to consumers' bank security details. UK card fraud losses were down 5% over the same period.

First Data Insight

While losses are far higher in traditional fraud areas today, the 'worry factor' is concentrated on upcoming frauds. Respondents perhaps feel better able to predict and manage ATM and POS fraud while some may experience an understandable 'fear of the unknown' with regard to online fraud. We may also be seeing an indication that new types of fraud are expected to result in much higher fraud losses in the future, if the problem is not tackled quickly and correctly.

While online and card not present fraud are less significant problems today, around a third of respondents report increases in online fraud and 38% report increases in phishing attacks. These attacks are gaining in sophistication as well as in number as attacks previously made in (often poor) English now come increasingly in local language.



"Phishing is very popular in this region. First in English and now much more effectively sending in local language. This is the new type."

Gabor Weissmuller, Citibank, Central Europe

Online fraud is a real concern today for banks in Western Europe and is seen as a significant threat for the future in other regions, where internet usage is currently at lower levels but expected to rise. Fraudsters are believed to be migrating towards these forms of fraud for a number of reasons including efficiencies of scale (online offers the capability to defraud more people, more quickly) and reduced personal risk.

"Online fraud is the future because they are becoming increasingly technically proficient and can remain relatively anonymous. It also allows fraudsters a high degree of flexibility."

Konstantin Tsanopoulos, Dresdner Bank, Germany

Looking to the future, malware, database compromise - resulting in massive loss of information - and identity theft are the major concerns for banks in more developed markets. Several respondents in Western Europe believe fraudsters will focus their efforts on cracking PINs, while another more sinister view is that, as the spread of Chip and PIN makes cards more secure, fraudsters will turn to kidnapping and violence to satisfy their demands.

First Data Insight

The theft of personal data is a major issue today and effective transaction monitoring combined with experienced local fraud analysis is the key to early identification of data compromise. Banks have long been subject to scrutiny and penalty in relation to the security of personal data and this has resulted in the tightening of procedures within many banks. The same level of scrutiny and penalty now needs to be aimed at other organisations holding data that could potentially be compromised and expose consumers to financial fraud. These would include merchants offering online shopping and loyalty programmes, insurance companies and others. First Data is currently working with its merchant clients to identify databases that contain sensitive data and ensure that they comply fully with card scheme regulations and PCI data security standards.

“We are seeing a sharp decrease in fraud as a result of Chip and PIN at UK point of sale - but what we didn't anticipate fully was the extent and speed with which this would migrate fraud across borders - cards skimmed in the UK are being used in over 60 countries sporadically, with no real hot spots.”

Katy Worobec, Head of Fraud Control, Cards and Fraud Control Unit, APACS, the UK Payments Association

A global phenomenon

Fraud might be easier to tackle if it would stand still - but respondents to the First Data study are very conscious of the movement of fraud across types of business and across regions.

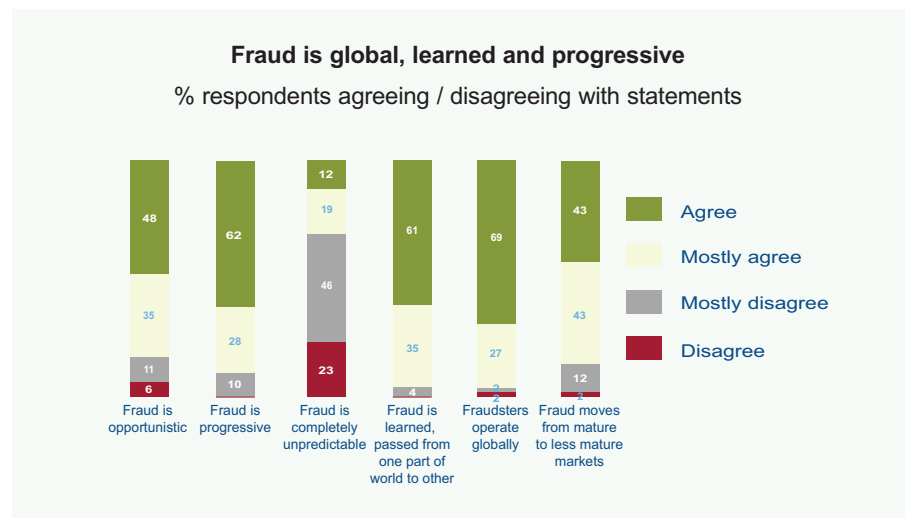
“Fraudsters always target the weakest link. If we improve online security but not the contact channel then they will hit contact really quickly.”

Howard Rawstron, HBOS, UK

“A change in technology to a more advanced level will hinder the fraudsters using that particular payment method. They will either move to a different payment method or go back and find a better way to hurt the organisation.”

Carl-Henrick Freij, SEB, Sweden

Overwhelmingly, fraud is recognised as a global phenomenon - the majority of card frauds involve activity in more than one country and 96% of respondents believe that new frauds are learned and passed from one part of the world to another. A similar percentage recognises that fraudsters operate globally.



“Fraudsters will become more organised. There will be 'Corporations of Fraud' as they get together and pool resources. It is very organised and we need to be very organised to stop it.”

Sreekumar Pockattu, National Bank of Kuwait, Kuwait

First Data Insight

If fraud is predictable, keeping abreast of global fraud developments is crucial. Vulnerabilities in new products, delivery channels, services or technologies are identified by fraudsters, then quickly exploited. The first instances of these new attacks show up in small pockets of activity initially but fraudulent activity then spreads quickly as organised criminals communicate with one another. Understanding the fraud experiences of those suffering the losses is imperative, to enable others to apply software or technical solutions to mitigate the now-known vulnerabilities before the service or product is offered in their market. This requires a highly co-ordinated approach to the sharing of fraud intelligence between all members of the financial services industry across the globe.

Interestingly, there is a widespread view that fraud is initiated by *foreign* crime organisations - organisations that come in from abroad, bringing their fraud skills with them. Western European banks report that, while cards may be skimmed in the West, white plastic is made abroad and then used in Eastern European and Far Eastern markets. Banks in the Middle East, where fraud levels are seen to be low, cite the Far East as the market in which their cards are most commonly skimmed and used fraudulently.

The good news is that two thirds of those studied believe fraud is predictable, at least to some extent. Because most fraud is 'learned' and transferred from one part of the world to another, this means that those yet to experience the fraud have some opportunity to predict how the fraudsters will strike next - and so to guard against their attacks.

Countermeasures

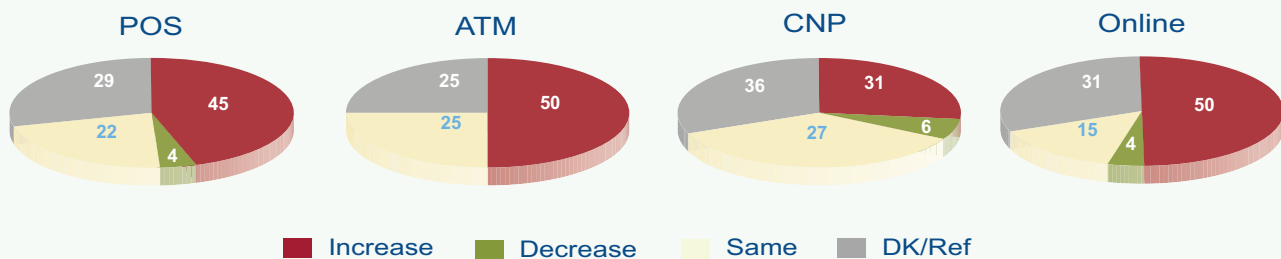
In examining the steps being taken to combat fraud, the First Data study looks both at countermeasures within individual banks and at respondents' views on industry-wide initiatives.

Bank initiatives

In view of both the perceived threat and the reality of fraud, it is unsurprising that many banks are increasing their spending on countermeasures. Fifty percent of study respondents report that they are increasing expenditure on countermeasures to combat ATM and online fraud.

Are you increasing or decreasing expenditure on fraud countermeasures?

% respondents



Cédric Sarazin, Director, Development & Strategy, Cartes Bancaires and Chairman of the European Payments Council's Card Fraud Prevention Task Force - on the major challenges in combating ATM, POS and online fraud:

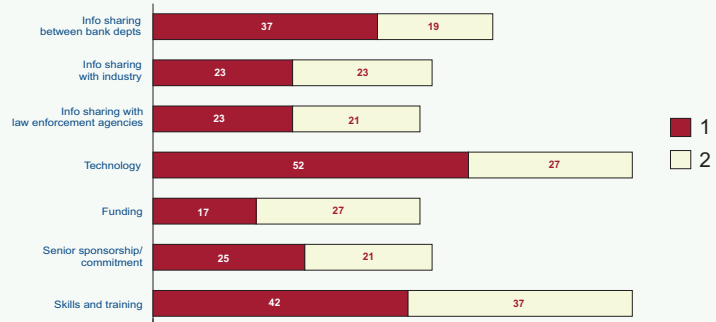
"The first big challenge is for those countries that haven't done so yet to complete the migration to EMV. When this happens they will see good results in terms of fraud reduction at both ATMs and the point of sale. For example, EMV is working well at combating skimming at vending machines.

However, EMV is not a short term solution for online fraud and other mail order/telephone order (MOTO) transactions, so combating online fraud is the second challenge. One common trend across all major markets is that CNP transactions are generating more and more fraud. While total fraud is decreasing we should be very cautious as CNP fraud may well become a much larger problem."

Technology is seen as a key weapon in fighting fraud. Over 50% of respondents see technology as a clear priority in both fraud detection and prevention. Technology supports fraud monitoring and rapid detection and is seen as vital in combating the increasing sophistication of fraudsters.

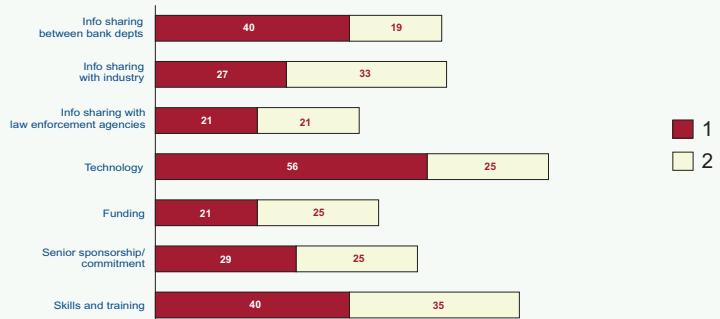
Which are the most important factors in fraud detection to your organisation?

% respondents rate factors 1 or 2, where 1 = very important and 10 = not important



Which are the most important factors in fraud prevention to your organisation?

% respondents rate factors 1 or 2, where 1 = very important and 10 = not important



Many organisations report that they are taking action against skimming, with the introduction of anti-skimming devices, as well as improving security at ATMs. In the fight against online fraud, banks are actively investigating two factor authentication and the use of SMS passwords.

Chip & PIN is widely endorsed and study respondents believe this development has made fraud more difficult in markets where it has been adopted. Its introduction is seen as key to reducing fraud levels elsewhere although there is a general view that fraudsters will then migrate to card not present environments that offer less protection.

First Data Insight

Existing methods of fraud prevention and detection, including transaction monitoring, customer profiling, application validation and public record checks have provided good levels of success over recent years. However, we all know that traditional tools will not enable us to detect and resolve fraud vulnerabilities as quickly as we need to do in future.

Innovative ways of analysing data need further exploration and application. Link analysis, for example, can help banks to gain a joined up view of fraud - and its cost - across the entire organisation. Some institutions have already had considerable success in identifying potential First Party fraud rings and networks of accounts that indicate potential bust-out fraud patterns. Two factor authentication also promises to reduce our reliance on static data. Implementation costs and concerns about the customer experience are challenges here but this technique offers real advantages in lowering concerns around fraudulent access to bank accounts and the loss of consumers' personal data.

There is widespread appreciation that, while technology is an essential tool in combating fraud, it also benefits the fraudsters. It enables more efficient targeting of potential victims and reduces the risks associated with personal contact. Each new technology application introduced by the banks to enhance customer service opens up new opportunities for fraud, new gateways and loopholes through which they can attack.

“The problem now is that there are criminal organisations ready to make big investments in technology to get high profits out of them. Good technicians are becoming criminals. We have, in Spain, IT specialists from Eastern Europe working full time on fraud.”

Andres Martin Ludena, Caixa Galicia, Spain

“Technology will of course both increase and decrease fraud. It has improved our monitoring and means that we can spot fraudulent activity much more quickly. But it also presents the fraudsters with more opportunities and points of vulnerability.”

Sreekumar Pockattu, National Bank of Kuwait, Kuwait

Technology is not the only weapon in the banks' fraud detection and prevention armoury - skills development and training are also important factors. It is widely recognised that new technologies are only as good as the staff who implement them and that many factors are involved in the battle against fraud.

“We will need to keep upgrading technology, procedures and systems and ensure that the knowledge pool remains high. It is having good people to fight fraud that is the most important thing.”

Sreekumar Pockattu, National Bank of Kuwait, Kuwait

Particularly among Western European banks, expenditure is also increasing on the development of organisation-wide initiatives to counter fraud. These initiatives operate across product groups to give the bank an holistic understanding of fraud and the ability to develop a similarly holistic approach to its control.

Technology solutions, training and other initiatives demand investment and it is encouraging to report that banks in the First Data study generally believe that senior executives recognise the importance of tackling fraud. Perhaps because they understand the impact of fraud on the brand, these executives seem prepared to provide the funding deemed necessary by their colleagues and there are very few complaints of insufficient funding.

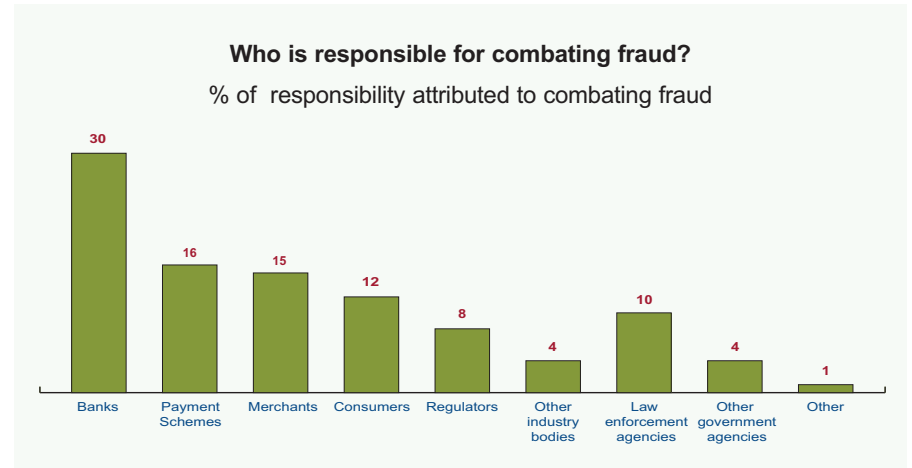
Finally, the banking executives in our study recognise that there are limits to the countermeasures they can implement. These limits are provided by the cost that countermeasures represent to the bank - which should not exceed the perceived value to the customer - and by the need to balance customer protection and customer convenience. There is little advantage in protecting your customer if, in doing so, you make it too difficult for him or her to enjoy the benefits of convenience and accessibility that card use can offer.

“We are a business - it is about the right balance between managing risk and inconvenience to the customer.”

Howard Rawstron, HBOS, UK

Industry initiatives

Banks across the region recognise that they have a significant share of the responsibility for combating fraud.



“We (the banks) recruit customers. We manage payment and transaction flows, we have the ability to review all customer data and understand demographics, and therefore we have an holistic view of that individual, so we should have the major responsibility.”

Howard Rawstron, HBOS, UK

“It is up to the banks to educate the merchants and the customer so that we work together to prevent fraud.”

Nagabhushan Balaji, ABN AMRO, Dubai

It is a responsibility that they are taking seriously and half of our respondents believe that they are doing enough today to counteract fraud. At the same time, they recognise that the job is never done - that fighting fraud demands constant attention and vigilance.

“Fraud is always developing and moving - we have to invest and develop to fight fraud. Fraud never sleeps.”

Iveta Behunova, OTP Bank, Slovakia

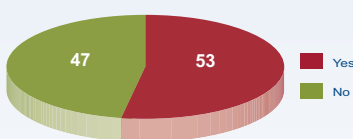
In this context, eliciting the support of others in the fight against fraud is crucial.

“Payment schemes are key in the battle against fraud as they are establishing the general system parameters applicable to the transactions made by the cards and roles and requirements for banks that issue cards.”

Ann Waszczuk, Mazowiecki Bank, Poland

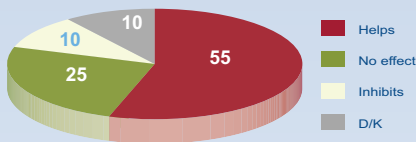
Is the industry doing enough to counteract fraud?

% respondents



What is your view of the impact of regulation on countering fraud?

% respondents



“Regulation could potentially have the effect of focusing the mind a little too much on compliance, rather than on the spirit of what you are trying to achieve. Additionally, regulation may not allow for the changing face of fraud and may not incorporate the flexibility necessary to meet new developments. Fraud changes and migrates too quickly to have strict legislation around it.”

Katy Worobec, APACS, UK

First Data Insight

Fraud migrates, mutates and develops extremely quickly, at times coming from angles that were completely unpredicted. Any regulation must remain flexible enough to allow financial institutions to move with the same dexterity and speed shown by the fraudster. Perhaps regulation should initially be targeted at how institutions apply fraud management strategies, rather than concentrating on the detail of the solution.

Merchants are seen to have an important part to play - although several respondents question whether merchants are as active as they could be in this regard.

“Merchants could be more interested in fighting against fraud. They don’t seem to be very interested actually. And that is because they are not affected by fraud.”

Fabio di Benedetto, Fineco Bank, Italy

In this context, views on the role of regulators are mixed. A little over half of all respondents believe regulation is important in countering fraud. Regulation is seen to facilitate process development and to encourage senior buy-in and essential investment. Appropriate laws and punishments are seen to provide deterrents.

Some regional variation is evident here, with banks in Central and Eastern Europe and the Middle East believing more strongly than their Western European counterparts in the part regulation should play in combating fraud. Regulators and law enforcement agencies don’t always meet the highest expectations of the banks, especially in the UK and Spain where legislation is seen to be weak, but their role is clear to many.

“If we take regulation for example, my personal opinion is that it is pretty weak.

The law does not regulate what different financial institutions should do with regards to increasing the security of their customers. If you are a criminal and you get caught, you just get a slap on the wrist. It is most likely for a first offence that you do not end up in prison. I would say the regulation is pretty weak at the moment.”

Audrius Sapola, AB SEB Vilnius Bank, Lithuania

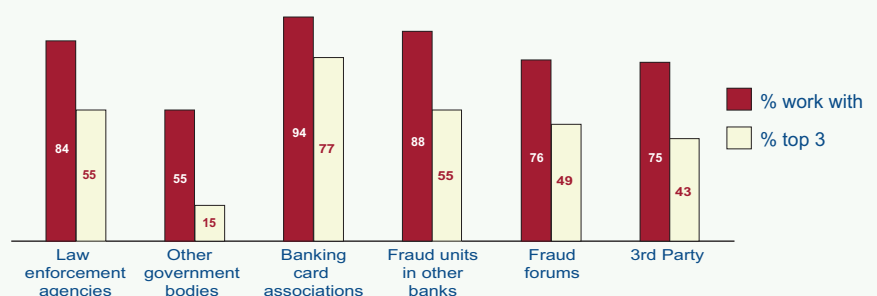
“Making it a criminal offence and dealing with it appropriately serves to combat fraud. If it is clearly written down in law, it helps.”

Nagabhushan Balaji, ABN AMRO, Dubai

Whatever the roles of different parties, respondents to the First Data study overwhelmingly agree that a concerted industry-wide effort is needed to beat the fraudsters. Encouragingly, most organisations are already actively engaged with others to combat fraud - 88% are working with other banks and 94% are engaged through their banking or card associations.

Which organisations do you work with to combat fraud? Which are the three most important?

% of respondents



“The ability for law enforcement and the industry to co-operate and react quickly relies on such a wide variety of issues coming together - variations in knowledge levels, internal processes and local legislation for both public and private industry are huge and can become a barrier to progress.”
Katy Worobec, APACS, UK

During a social engineering experiment in the United States, auditors posing as network technicians managed to trick one third of users into giving out their passwords over the phone. In an experiment at the Infosecurity Europe Conference, more than 90% of users revealed commonly used identity data in exchange for the chance to win theatre tickets.

“Consumer education is crucial in the fight against fraud. APACS has been instrumental in developing educational programmes such as the Card Watch website and the ID Theft website launched by the Home Office.”
Katy Worobec, APACS, UK

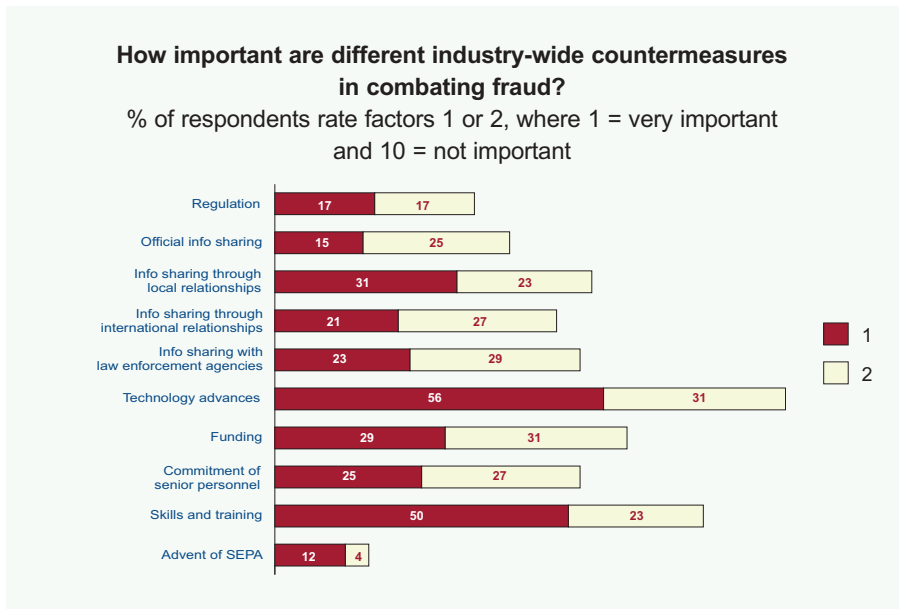
Consumer education is seen as an important area for co-operation, especially as it is viewed by many as being fundamental to the success of efforts to beat fraud.

“We need to educate customers about being wary on the internet about giving over personal details...however it is all about balance - you want them to use the internet...it’s about mild instruction rather than heavy handed warnings.”
Sreekumar Pockattu, National Bank of Kuwait, Kuwait

“We will need to increase consumer and customer awareness and develop a stronger certification infrastructure with regards to online card usage.”
Konstantin Tsanopoulos, Dresdner Bank, Germany

Perhaps the single, strongest call from study respondents, however, is for increased information sharing - within and between banks, locally and internationally, between banks and law enforcement agencies. This message is clear from across all parts of the region, reflecting the damage inflicted by fraud, its increasingly global nature and the belief that we can learn from one another in fighting those who practice it.

“I think there is not enough sharing of knowledge internationally. We can learn from each other.”
Ivan Kubas, Ludova Bank, Slovakia



“We need to make it easier to investigate and share data between institutions. Fraud is international - we need to have a quick, useful and simple process to protect ourselves. Right now, the industry has different processes in different countries and even in different banks within countries. It is very complicated.”
Gabor Weissmuller, Citibank, Central Europe

First Data Insight

Banks need first to understand their own legal position, so that they are clear about what they can, and cannot, share. This is relevant for countering both national and cross-border fraud. Without this knowledge, it is too easy to say 'no' to requests for information, whether from within or outside the bank

"From a UK perspective, APACS members are extremely open and we are setting up a fraud database that will allow them to share fraud intelligence. However, the industry as a whole is nowhere near the starting point that will facilitate the sharing of data. APACS is active within the European Payments Council Task Force where the question is continuously discussed, but a resolution is a long way off. In many countries within the European Union, the data protection legislation - or, at least, the interpretation of it - is far more draconian than it is in the UK - and sometimes legislation is also used as an excuse not to do things. There is a lot that needs to be done in this arena. The key is to foster a 'spirit of openness' that generates opportunities for the sharing of fraud data, fraud intelligence and also best practice."

Katy Worobec, APACS, UK

"The industry could do more because we lack a system for sharing data. This data should be shared and managed in a centralised way by a central body."

Fabio di Benedetto, Fineco Bank, Italy

"We need global standards. A minimum platform that everyone has to adhere to across the world."

Carl-Henrick Freij, SEB Bank, Sweden

This sounds good but study respondents recognise the difficulties and the barriers to greater information sharing. Fraud is a sensitive issue, impacting reputation, profitability and, ultimately, competitiveness.

"There is not enough join-up between organisations, both financial and non-financial. Organisations are secretive of fraud losses and that inhibits our ability to work together."

Howard Rawstron, HBOS, UK

Several respondents cite data protection legislation as a barrier to effective information sharing across countries. This issue is recognised and under active consideration by the European Union and European Payments Council, particularly in relation to the advent of a Single Euro Payments Area which will bring with it a significant increase in cross-border payments.

CONCLUSION

Respondents to the First Data study are looking to the future - and they don't like what they see. Fraud is increasingly a global phenomenon, demanding a global response. Banks clearly understand the need for all parties to co-operate in the fight against fraud but they are also well aware of the barriers that stand in the way of co-operation.

As we approach the introduction of SEPA in Europe, the need for a united approach to fraud detection and prevention becomes still more urgent. Fraudsters work collaboratively and we must find the will and the means to do the same.

First Data Insight

The impact of SEPA on fraud

Europe's fight against card fraud takes on an added dimension with the introduction of SEPA on 1 January 2008. Fraud experts are concerned that, while great efforts are being made to deliver the single payments market at commercial, regulatory and technological levels, tackling fraud in the brave new world of SEPA may become even more challenging than it is now.

First, the scheme standardisation requirements of SEPA will lead to the opening up of national debit card schemes. Many of these schemes have highly sophisticated anti-fraud solutions, often based on national technical specifications which are not compliant with the SEPA Cards Framework. As they move towards compliance, these schemes will become more vulnerable to the attentions of fraudsters.

Secondly, the introduction of a 'borderless' payment space will bring increased volumes of cross-border payments and, with it, an increase in fraudulent cross-border transactions. Our ability to counter this growing threat is severely limited by our inability to share fraud prevention and detection data effectively across borders.

A unified approach?

While fraudsters operate across borders without restrictions, the same is not true of banks and law enforcement agencies. The dangers here are clearly recognised by the European Union and the European Commission. In October 2004, the Commission said that it wanted data protection rules in the EU to be clarified and harmonised while the EU Fraud Prevention Expert Group (FPEG) warned in December 2006 that fraudsters could take advantage of the European Union Member States' fragmentation to increase their cross-border activity. The FPEG advised that the payment industry had to respond to this threat by developing tools to detect and prevent fraud at a wider EU level.

In a highly significant statement, the FPEG subgroup on data management noted that: "In the view of the payment industry, the emergence of SEPA-wide schemes should naturally lead to the need for SEPA-wide databases (either within a scheme or through consolidated databases across schemes)." However, the group noted that "the existing legal framework in relation to data protection is not adapted to the future SEPA world, which will need pan-European databases".

Cédric Sarazin, Director, Development & Strategy, Cartes Bancaires and Chairman of the EPC's Card Fraud Prevention Task Force comments:

"Fragmentation has both positive and negative effects. Sometimes fragmentation protects us because fragmented systems are more difficult to attack for fraudsters. But when it comes to fighting fraud, fragmentation doesn't help. Banks must all work together in a co-ordinated way.

In terms of the fragmentation of databases, collecting fraud statistics and creating anti-fraud databases at a European level are two of many ways to fight fraud. However, in many countries it is not easy to exchange data about fraudulent transactions, and neither is it possible to share fraud statistics between countries. We're working on that with the Eurosystem - the central banks of the 13 Eurozone countries - and European Central Bank (ECB). The reason for this is that it is easier for the public sector than for the private sector to exchange data. We're currently examining if this exchange could take place via the Eurosystem. The first phase would be an exchange of statistics followed by the creation of anti-fraud databases."

Significant barriers exist today to sharing fraud prevention and detection data across borders. These include practical obstacles to data flows and strict conditions for personal data processing at national level which, in many countries, hinder the creation of anti-fraud databases. While creating a uniform level of data protection within the European Union would be one answer to the current problem, this is some way off.

Article 71 of the December 2005 draft of the Payment Services Directive included a clause obliging Member States to "permit the processing of personal data by payment systems and payment service providers when this is necessary to safeguard the prevention, investigation, detection and prosecution of payment fraud". However, mandating the sharing of data across borders is not envisaged and implementation of Article 71 would still leave data protection authorities in each country with significant control based on existing legislation in the European Data Protection Directive.

Cédric Sarazin:

"I fully understand the problem that the data protection authorities have. They are concerned about what will happen to personal data once it's exported to another country. Therefore, they tend to say no to any request to share data cross-border. This is the case even within Europe - we're not even talking about exporting data outside of Europe. We need to reassure the authorities because organisations may want to consolidate data processing in a single location in Europe which may not be a place where they do business in Europe. This is an issue not only for fraud data management but for all data processing."

The risk of increased fraud within SEPA remains high - and the stakes are high too. As the FPEG notes: "the adoption of sound preventive measures in relation to fraud in non-cash means of payment is of paramount importance for the creation of a EU Single Payment Area." Without these measures in place, there is a very real danger that rising fraud will lead to a fall in consumer confidence in electronic payment methods and so undermine the principles that underlie the creation of SEPA.

STUDY SAMPLE AND METHODOLOGY

Over fifty leading banks from Europe, Middle East and South Africa participated in the First Data study, from 23 countries

Country	Banks
Austria	1
Croatia	3
France	1
Germany	3
Greece	2
Hungary	1
Ireland	1
Italy	2
Kuwait	4
Latvia	4
Lithuania	4
Netherlands	1
Poland	3
Portugal	1
Republic of South Africa	1
Romania	1
Serbia	2
Slovakia	6
Spain	4
Sweden	1
Switzerland	1
United Arab Emirates	1
United Kingdom	4
TOTAL	52

The study sample includes a significant cross-section of banks. Many respondents are from banks operating in one market, but the study also includes nine banks that are active across multiple markets in the region.

Respondents are senior business executives with responsibility for fraud prevention, detection and/or management within their organisation. Approximately 35% of respondents are responsible for all areas of fraud across the entire organisation.

One third of the interviews were carried out face-to-face, the remainder being conducted by telephone.

All interviews used a structured questionnaire that was sent out to respondents in advance. Several of those interviewed either circulated the questionnaire internally or invited colleagues to participate in a group interview - so providing a consensus view from across departments with responsibility for fraud.

GEOGRAPHICAL REACH



First Data's presence in support of clients across Europe, Middle East and Africa

ABOUT FIRST DATA

First Data International is a leading independent payments processor in Europe, Middle East and Africa. We are committed to working with clients and colleagues across the payments industry to develop fraud detection and prevention tools and systems which match the speed of change, flexibility and ingenuity displayed by today's global fraud industry.

First Data has over 20 years' experience of European payments and processing and a presence supporting clients in 35 countries across EMEA. We deliver a comprehensive range of services with speed and security through an unrivalled network of regional hubs and local operations, in local language. Our services include:

- Debit issuer processing
- Consumer finance processing - cards and loans
- Acquiring processing and switching
- Merchant acquiring
- ATM and POS management
- Value-added services such as risk and fraud management
- Contact centre, back office and output services

To find out more about First Data International's fraud management capabilities, please contact Jackie Barwell

Director of Fraud Management, EMEA

tel +44 (0) 1268 296421
email jackie.barwell@firstdatacorp.co.uk

For general information about our company, or if you are a journalist, please contact Suzi West

tel +44 (0) 1268 297179
email suzi.west@firstdatacorp.co.uk