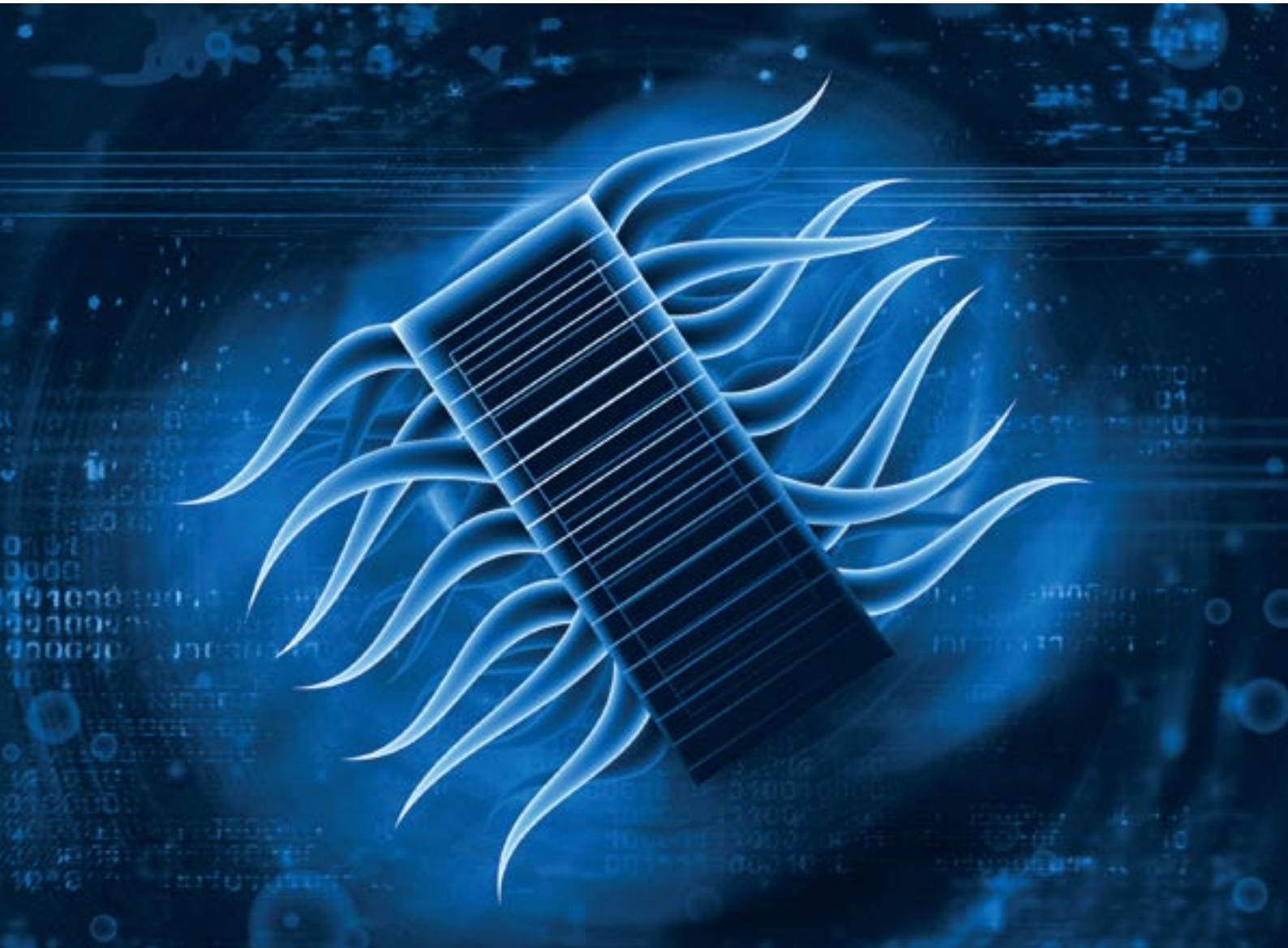


inside

FRAUD

Sponsored by



Payments
CARDS&MOBILE

Need help Fighting Card Fraud or Merchant Risk Management?



The ai Corporation provides real time fraud detection systems to Issuers, Acquirers, Payment Processors and Merchants around the world.

Our flagship solution, RiskNet, is used by major organisations such as Global Payments Inc, one of the world's largest acquirers, and China Construction Bank, the second largest issuer in China. Each year our solutions monitor over 8 billion transactions and authorisations, and many millions of cards.

Our solution range is:-

- RiskNet Issuer – detecting fraud on cards issued by your institution.
- RiskNet Acquirer – Monitor for merchant settlement risk, and detecting merchant fraud committed by merchants that you acquire.
- SmartAuth – detecting CNP fraud, and protecting your merchants from exposure to, and use of, compromised cards.

Our innovative solutions empower the operator with the tools to detect fraud as it happens and stop it in its tracks, by producing fraud alerts instantly and distributing them effectively. Our solutions can be deployed in a multi-product, multi-scheme, multi-institution and multi-currency environment.

Over 100 major financial organisations will vouch for our solutions, and will readily tell you how they reduced fraud exposure and settlement risk exposure, improved analysts efficiency and reduced chargebacks and scheme penalties as a result of deploying RiskNet at their organisation.

If you are interested in reducing fraud or improving your companies profitability, then please make an enquiry to info@aicorporation.com

September | October 2009
Fraud Supplement**Editor**Annie Turner
Tel +44 1328 701 025
Tel +44 1263 711 800
anniet@paymentscm.com**Contributors**Peter Welch
peter@paymentscm.com**Publisher and MD**Alexander Rolfe
Tel +44 1263 711 937
alex@paymentscm.com**Business Development Manager**Wendy Sanders
Tel +44 1263 711 801
wendy@paymentscm.com**General Manager**Gemma Haywood
Tel +44 1263 711 800
Fax +44 1263 456 100
gemma@paymentscm.com**Subscriptions and General**Kaye Skinner
Tel +44 1263 711 800
Fax +44 1263 456 100
kaye@paymentscm.com**Address**Payments Cards and Mobile
The Stable
Hall Yard
Kelling
Holt
NR25 7EW
United Kingdom**Cover, Design and Origination**

www.klg-design.co.uk

Printing

Micropress Printers

All rights reserved. No part of the publication may be reproduced or transmitted in any form without the publisher's prior consent. While every care is taken to provide accurate information, the publisher cannot accept liability for errors or omissions, no matter how caused.

**Payment Cards and Mobile™
is owned and published by
PaymentsCM LLP**

ISSN 1759-829X

© PaymentsCM LLP 2009

Inside

FRAUD

welcome

They say the devil has the best tunes. Certainly fraud is one of the most fascinating aspects of our industry, not least because it is relentless and mutating. While overall, this comparison between card fraud losses and types in the Spanish, French, British and Dutch markets suggests that fraud losses are being contained as a proportion of card turnover, there is no room for complacency.

EMV implementation has done much to reduce domestic losses from lost and stolen cards, but they still amount to €85.3 million and £54.1 million in France and the UK respectively, for instance, indicating that much remains to be done. Likewise international fraud is smaller in scale than domestic card abuse, but is proportionately far more common – by up to 30 times higher than in Spain at the top end of the range. And of course international transactions are growing all the time.

Thirdly we tend to overlook the true cost to the industry – see page 17 for something to hum about.

Annie Turner, Editor



contents

- | | |
|--|--|
| <ul style="list-style-type: none"> 4. Introduction 5. Highlights 6. 1. Total fraud losses 8. 2. Method of compromise 10. 3. Geographic place of misuse 11. 4. Type of misuse | <ul style="list-style-type: none"> 15. 5. Linking method of compromise to place of misuse 16. 6. Concluding comments 17. Total cost of fraud from Visa Europe 18. Appendix:
Note on sources and statistics |
|--|--|

Acknowledgements

The author thanks Visa Europe, Financial Fraud Action UK, ServiRed, Sistema 4B and Currence for their helpful responses to various questions on their card fraud statistics.

Author

Peter Welch is a Director of Research at Payments Cards and Mobile. Peter is also an independent consultant specialising in banking and payments. Formerly Head of Research at the Credit Card Research Group in London, Peter has many years of experience analysing developments in the payment card sector.

Peter has published various research reports and bulletins through PCM, including *Banking at the Checkout* with Professor Steve Worthington, which analyses the move into financial services by leading retailers such as Tesco.

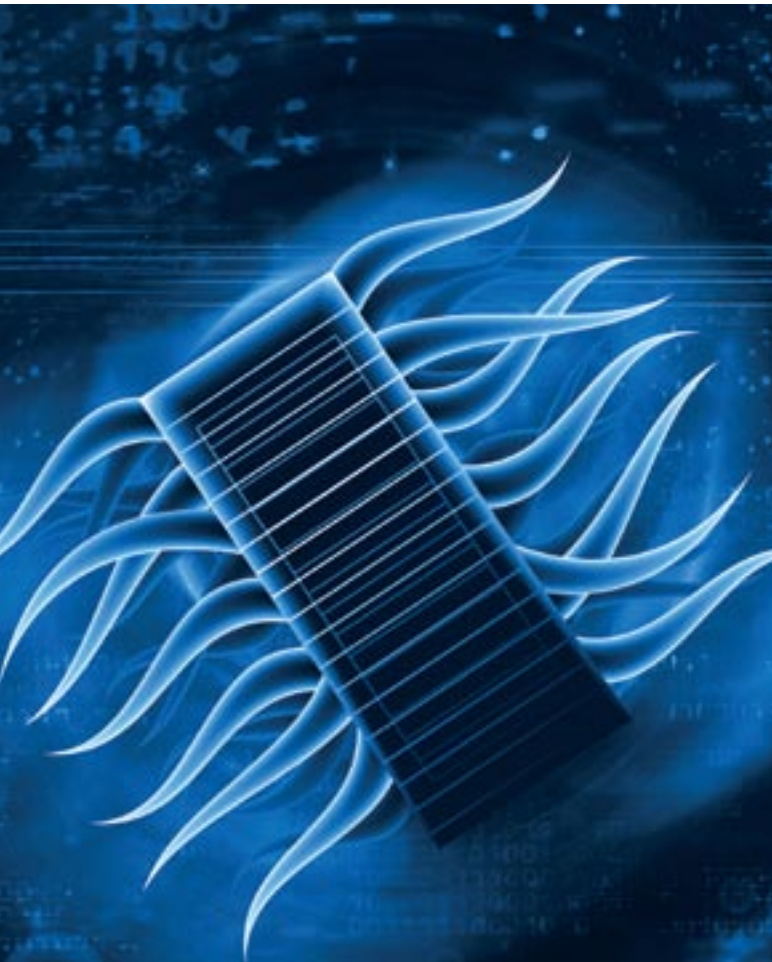
Introduction

It is the driver of major industry initiatives such as EMV implementation to combat the use of lost, stolen and counterfeit cards, while Verified by Visa and MasterCard SecureCode protect against the use of stolen card details online.

But what is the scale of fraud losses in Europe, and how does it vary between markets?

In 2008, we prepared a short report comparing losses in France, Spain and the UK. It drew on data covering the whole market for France and the UK and data published by ServiRed, the largest of the three Spanish payment card networks. This new report updates

and extends the initial analysis. Data from Visa Europe provides a pan-European barometer. The national coverage has been extended to include the Netherlands while the Spanish coverage is enhanced by data from Sistema 4B.



The report is divided into the following main sections:

1. Examines the overall level of losses, including the variations between the countries profiled.
2. Draws on French and UK data to analyse losses by method of compromise, that is the sources of fraudulently used cards.
3. Analyses losses by geographic place of misuse (domestic vs international).
4. Analyses losses by type of fraudulent transaction (purchases vs cash withdrawals, face-to-face vs CNP purchases).
5. Draws on the French data to bring together the analysis of losses by method of compromise with the analysis by place and type of misuse.

Highlights

Overview

- Card fraud losses in 2008 as a proportion of card turnover changed little in Europe. Taking Visa Europe's figures as a barometer for the region as a whole, losses fell from 0.07% (7 basis points) of card turnover in 2007 to 0.06% in 2008.
- However, looking at the major markets for which figures are available, losses continue to vary greatly. They ranged from fewer than 3 basis points in Spain to 10 basis points in the UK.

France

- Losses rose by almost 25% to €249.2 million, with international losses growing from 43% to 47% of the total. The loss rate rose from 0.049% to 0.057% of French card turnover.
- By method of compromise, the rise in domestic losses was largely due to higher losses from the theft of card details. By type of misuse, the rise in domestic losses was mainly due to higher card not present (CNP) losses, particularly internet purchases.
- By method of compromise, the rise in international losses was largely due to much higher losses from the theft of card details and an increase in losses from lost and stolen cards, and counterfeit cards. By type of misuse, the rise in international losses was also mainly due to higher CNP losses, particularly internet purchases.

Netherlands

- Historically a country with one of the lowest levels of card fraud in Europe, losses rose from €44.6 million in 2007 to €68.4 million in 2008, with the loss rate increasing from 0.031% to 0.045%.
- With Dutch debit card transactions still 100% based on magnetic-stripe cards, losses continue to rise due to skimming. Migration to EMV is expected to be completed by 2011/12.



Spain

- Card fraud losses remain low, with both ServiRed and Sistema 4B reporting only small increases during 2008.
- Both networks reported significant falls in domestic ATM fraud, but increases in international purchase fraud.

UK

- Card fraud losses were £610 million (€766 million) in 2008, equivalent to 10 basis points of card turnover.
- By method of compromise, losses from lost and stolen cards fell below 10% of total losses. Stolen card numbers and counterfeit cards continued to account for more than a half and a quarter of losses respectively. ID fraud rose by almost 40% to £47.4 million, accounting for 8% of total fraud.
- By place of misuse (for which only a domestic breakdown is available), CNP fraud fell for the first time in recent years as a proportion of total losses. However, losses from retail face-to-face transactions rose by 35% in 2008, increasing as a share of total losses from 22% to 26%.
- However, recently published UK figures for first half of 2009 show total card fraud losses down 23% to £232.8m compared with the first half of 2008, with international fraud losses down a remarkable 45%.

Comparative Overview (2008)

	France	Spain	Netherlands	UK
Population	64.0m (p)	45.3m	16.4m	61.2m (p)
Number of cards	84.7m	76.4m	30.9m	168.7m
Value of purchases	€329.4bn	€94.4bn	€88.8bn	£400.1bn
Value of withdrawals	€110.3bn	€116.6bn	€62.1bn	£203.0bn
Fraud losses	€249.2m	–	€68.4m	£609.9m
EMV implementation	Largely complete	As at end 2008: Cards: 8.4% POS: 79.5% ATMs: 97.0%	Implementation due to be completed by 2011/12	Largely complete

Notes: 1. Number of cards covers both debit and credit. Fraud losses cover both domestic and international transactions.
 2. **France:** Statistics cover both "CB" bank cards and Moneo e-purses (58.2 million) and "private" cards issued by American Express, Banque Accord, BNP Paribas Personal Finance, Cofidis, Cofinoga, Diners Club, Finaref, Franfinance, S2P and Sofinco (27.2 million). Statistics cover purchases and withdrawals made on French cards both in France and internationally.
 3. **Spain:** While fraud data is for ServiRed only, the data on cards, purchases and withdrawals in this table is for the Spanish market as a whole. Spanish purchases: devices located in Spain and Spanish-issued cards. Spanish withdrawals cover ATM transactions at devices located in Spain and cards issued by any scheme.
 4. **Netherlands:** Number of cards comprises 25.2 million debit cards and 5.7 million credit/delayed debit cards.
 5. **UK:** Number of cards includes 19.4 million ATM only and 0.4 million cheque guarantee only cards. There were 148.8 million cards with a payment function as of 2008. Statistics cover purchases and withdrawals made on UK cards both in UK and internationally.
 6. p = provisional.
 Sources: Eurostat (populations), Observatoire de la sécurité des cartes de paiement (France), Currence (Netherlands), ECB Blue Book (payment cards in the Netherlands), ServiRed, Banco de España (Spain), UK Cards Association, Financial Fraud Action UK.



Download a PDF version from:
paymentscardsandmobile.com/research

1. Total fraud losses

The most comprehensive overall measure of fraud losses is the fraud loss ratio, which expresses fraud losses as a proportion of total payment card turnover.

Table 1.1 compares the fraud loss ratio for 2008 based on losses on both purchases and cash withdrawals, and on both domestic and international transactions.

For Visa Europe as a whole, fraud losses were 0.06% (6 basis points) of card turnover in 2008. However, the national figures show significant variation by country in Europe. Fraud losses of 0.101% in the UK in 2008 were

almost 70% higher than in France, more than double that in the Netherlands and four times as high as in Spain.

Table 1.2 looks at the trends in loss ratios during recent years. Despite the changes in both card use and fraud prevention, it is striking that the loss ratios for France, Spain and the UK (and therefore their positions relative to each other) have changed little

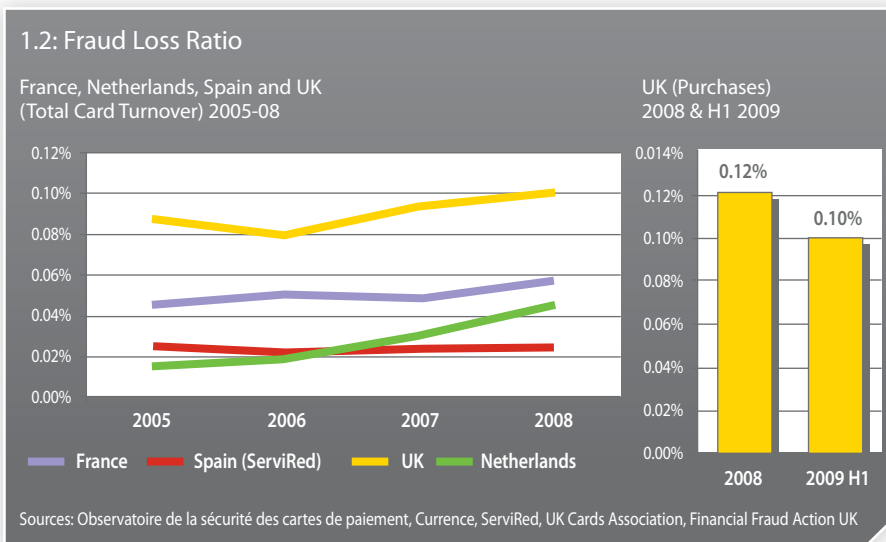
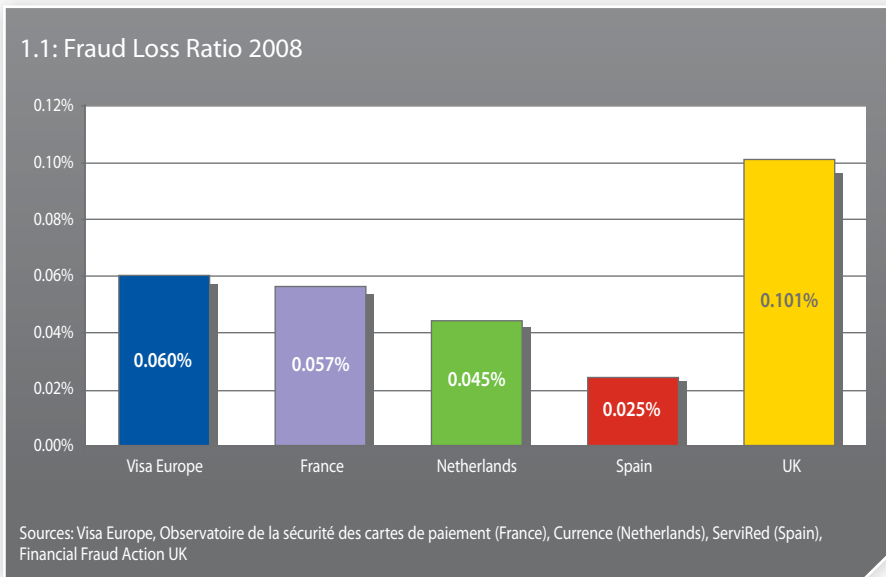
during the last four years. In the UK, the fraud loss rate has varied between approximately 8 and 10 basis points, showing a slight upward trend since 2006. In France, the rate has varied between 4 and 6 basis points, though it rose from 0.049% in 2007 to 0.057% in 2008. In Spain, despite the lack of chip card issuance, the loss rate has not risen above 3 basis points.

However, it is important to note that recently published UK figures for first half of 2009 show a sharp fall, with card fraud losses down 23% to £232.8m compared with the first half of 2008. Financial Fraud Action UK does not publish a loss rate covering all card turnover, and it is not possible to calculate this from the half-year data. However, it discloses a loss rate on card purchases (that is excluding cash withdrawals). This fell to 0.1002% in the first half of 2009 compared with 0.124% in full-year 2008.

The fact that overall fraud losses remain significantly lower in Spain suggest its strategy of online card-issuer authorisation combined with use of neural networks and expert systems has been effective in combating fraud.

However, the level of losses and trends in loss rates also needs to be seen in the context of the importance of cards as a means of payment in each country.

In Spain, the market share of total domestic consumer spending accounted for by cards was only 16% according to ServiRed in its 2007 annual report. This compares with 30% in France and 40% in the UK. Card use is also high in the Netherlands. The value of domestic purchases on Dutch cards was €80.6 billion in 2008, over 80% of the value of domestic purchases on Spanish cards despite a population less than 40% the size.



A second important factor is the high use of credit cards in the UK compared with France and Spain. The fraud loss ratio on UK credit cards in 2008 was 21 basis points compared with 7 basis points on debit cards. Credit cards can be particularly attractive to fraudsters given the line of credit available. Further, lower international and online acceptance of Maestro may have been a constraint on UK debit fraud (Table 1.3).

Dutch Card Fraud Losses

Dutch card fraud losses (Table 1.4) also show a much higher loss rate on credit than debit cards. In 2008, the loss rate on Dutch PIN debit cards was only 0.032% (3 basis points) compared with 0.25% (25 basis points) on Dutch credit cards. However, the contrast is accentuated by the fact that the debit card loss rate only covers domestic transactions (with international debit transactions treated as Maestro transactions) and PIN debit cards cannot be used online (the Dutch direct debit product iDeal is used for domestic internet purchases).

With PIN-entry and the online authorisation of all transactions (and low use of credit cards), card fraud has historically also been low in the Netherlands. However, Dutch card fraud losses have risen almost threefold during the last four years, from 0.016% (less than 2 basis points) in 2005 to 0.045% (4-5 basis points) in 2008. Most of this is due to growing losses on domestic PIN debit card purchases and withdrawals. The loss rate on domestic PIN debit has risen tenfold from 0.003% in 2005 to 0.032% in 2008.

EMV implementation elsewhere in Europe has increased the vulnerability of the Netherlands. In particular, Dutch payments organisation Currence reports a growing problem with skimming.

During 2008, it reported more than 900

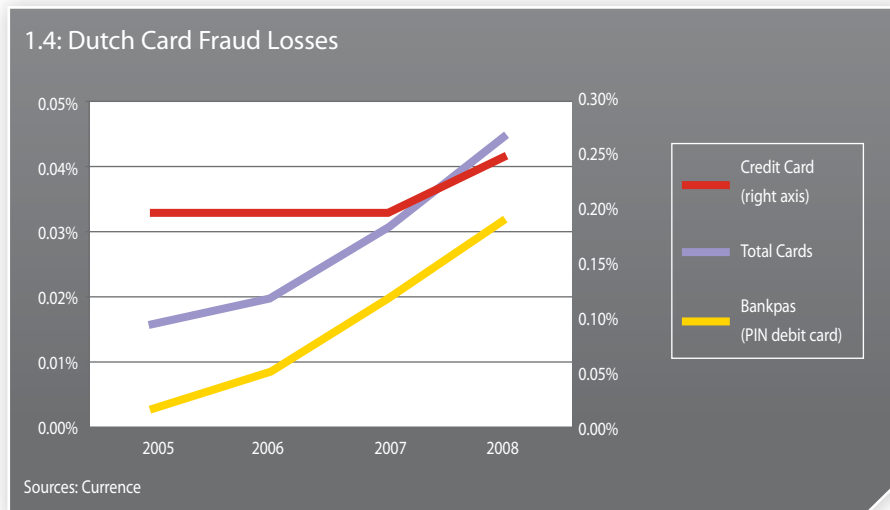
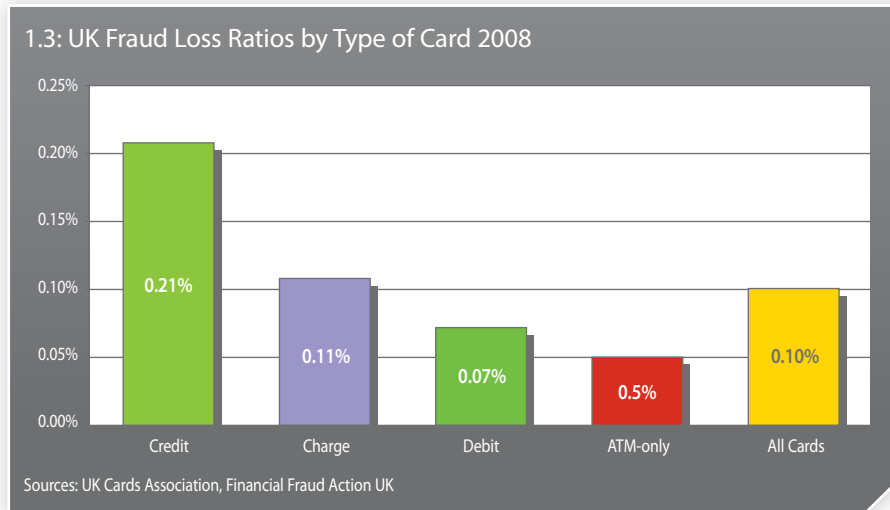


successful skimming attacks on ATMs and POS terminals affecting tens of thousands of account holders and with a value of more than €31 million.

POS terminals were targeted most by criminals, with skimming on unmanned

POS terminals a particular problem.

Currently, PIN transactions remain 100% based on magnetic cards. However, by end 2011, all terminals will be EMV compatible, and shortly afterwards all transactions will be EMV-based. ■



Notes

Table 1.1 Notes:

1. Fraud rate based on fraud losses as a proportion of total card turnover.
2. Turnover covers both purchases and cash withdrawals, and both domestic and international transactions. It excludes losses on foreign cards in each of the markets.
3. Spanish figures for ServiRed cards only.

Table 1.2 Notes:

1. Fraud rate based on fraud losses as a proportion of total card turnover.
2. Turnover covers both purchases and cash withdrawals, and both domestic and international transactions. It excludes losses on foreign cards in each of the markets.
3. Spanish figures for ServiRed cards only.
4. UK figures in the chart on the right only cover purchases. They do not include cash withdrawals.

Table 1.3 Notes:

1. Fraud rate based on fraud losses as a proportion of total card turnover.
2. Turnover covers both purchases and cash withdrawals, and both domestic and international transactions. It excludes losses on foreign cards.

Table 1.4 Notes:

1. Credit card loss rate mapped against right axis, total loss rate and Bankpas loss rate against left axis.
2. The figures for Bankpas only cover domestic domestic fraud losses on Dutch debit cards (that is domestic PIN debit card transactions).
3. "Total cards" series covers PIN debit card transactions plus use of Dutch debit cards internationally (which are treated as Maestro transactions) plus domestic and international transactions on Dutch credit cards.

2. Method of compromise

The method of compromise covers the means by which fraudsters obtain payment cards or card details.

France and UK compared

While detailed breakdowns are only available for France and the UK, they are based on similar categories. This allows a valuable comparison of the two markets.

In France, the main methods of compromise responsible for losses are lost and stolen cards, the fraudulent use of card numbers and losses from altered and counterfeit cards. Together, these three categories accounted for almost 95% of losses in 2008. The theft of card numbers replaced lost and

stolen cards as the largest source of losses in 2008, accounting for 36.5% of total losses.

While theft of card details accounts for a growing proportion of fraud on French cards, it remains significantly smaller than on UK cards. And while lost and stolen cards continued to account for over a third of French losses in 2008, they accounted for less than 10% of UK losses. In monetary terms, losses in the UK from lost and stolen cards have halved since 2004 following the introduction of Chip & PIN (see Table 2.1).

The main method of compromise responsible for losses on UK cards is now the theft of card details

The main method of compromise responsible for losses on UK cards is now the theft of card details (also described as card-not-present or CNP fraud – see the appendix for a discussion of CNP as



targeted media

specialist cards and mobile payments industry publication titles and media, to evolve your presence visit paymentscardsandmobile.com/marketing

applied to the method of compromise versus place/type of card misuse), which accounted for over 50% of losses in 2008.

Counterfeit was the second largest category, accounting for over 25% of UK losses. The higher proportion of losses in the UK accounted for by CNP may largely reflect the greater use of e-commerce by UK cardholders.

For example, according to a survey carried out by Eurostat, the Statistical Office of the European Communities, 49% of UK individuals had ordered goods or services on the internet in 2008 (the highest in the EU) compared with 28% in France and only 13% in Spain (Eurostat: Data in Focus 46/2008, Internet usage in 2008 Households and individuals).

France: domestic vs international

Simply looking at total fraud losses by method of compromise hides the important differences in the profile of domestic and international losses. This is underlined by a breakdown available for France.

The two main methods of compromise responsible for domestic French losses are the fraudulent use of card numbers and lost and stolen cards.

Losses from forged or counterfeit cards fell from 16% of total domestic losses in 2006 to only 5% in 2007 and 2.4% in 2008. However, over the same period, losses from the fraudulent use of card numbers rose from 31% to 40% of total domestic losses in 2007 and more than 50% in 2008.

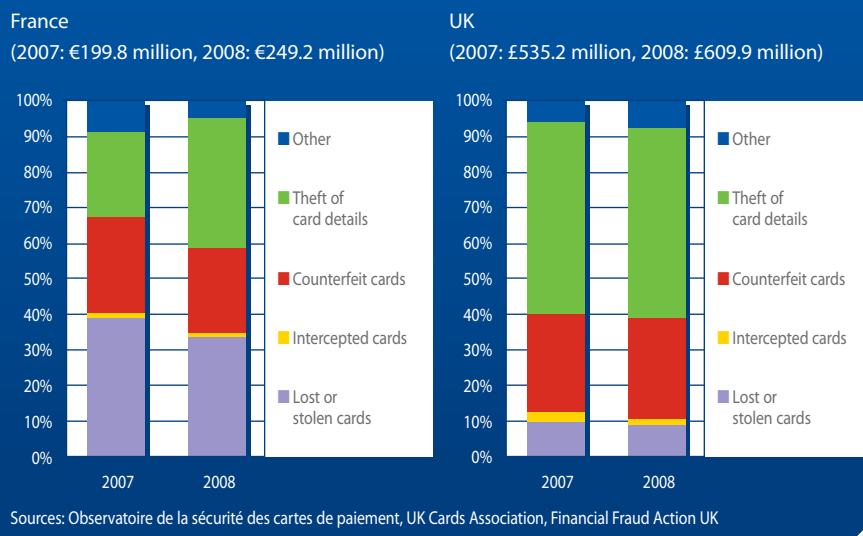
Losses from forged or counterfeit cards accounted for 48% of international losses on French cards in 2008, with losses on lost and stolen cards accounting for a further 25%. However, the most striking feature of the French 2008 data is the spread of CNP fraud to international transactions.

The theft of card numbers accounted for 20% of international losses on French cards in 2008, and 24% of losses from fraudulent international payments (see Table 2.2).

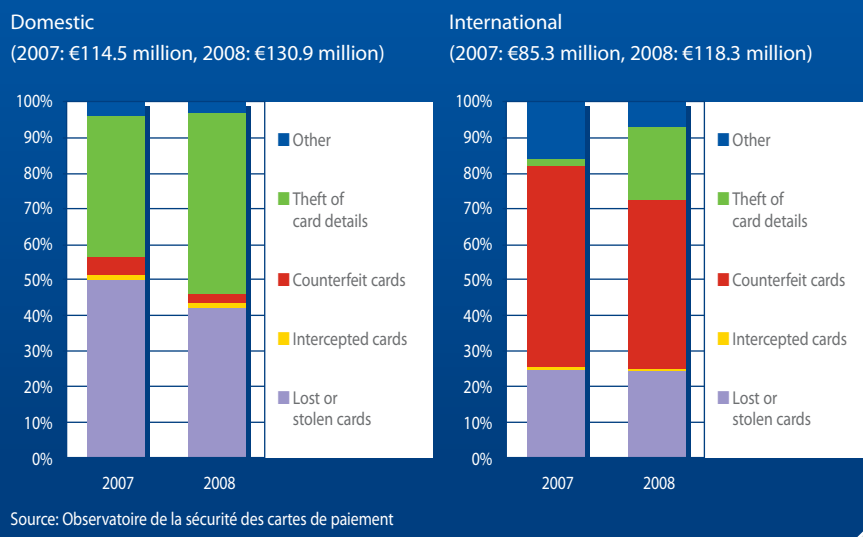
Though data of comparable detail is

not available for other markets, Spanish network ServiRed disclosed that stolen cards accounted for 41% of domestic purchase fraud. Counterfeit cards accounted for 47% of total purchase fraud abroad on ServiRed cards. ■

2.1: Fraud Losses by Method of Compromise – France vs UK



2.2: Losses by Method of Compromise – France



Notes

Table 2.1 Notes:

- Charts cover both domestic and international transactions on French and UK-issued cards respectively.
- France: Data covers both interbank ("CB") cards and private cards. "Other" covers, particularly for three-party cards, fraud resulting from the fraudulent opening of accounts with a false identity.
- UK: "Others" covers third party application fraud and account takeover.

Table 2.2 Notes:

- Charts cover both domestic and international transactions on French and UK-issued cards respectively.
- Data covers both interbank ("CB") cards and private cards. "Other" covers, particularly for three-party cards, fraud resulting from the fraudulent opening of accounts with a false identity.

Concentrating on the new "concentrations"

For European payment card businesses, the fraud picture has changed dramatically in recent years. In fact, the implementation of EMV chip and PIN has changed the whole game – for the banks and also for the criminals.

Fraud managers used to concentrate on domestic losses in the face-to-face environment. Today, the job description is entirely different. The focus has shifted to all those times and places where a transaction is not protected by chip and PIN – that is, magnetic stripe transactions (at either POS or ATM) and transactions in which the card itself is not present (primarily e-commerce).

For European banks, this is where the fraud losses are now heavily concentrated. And, to complicate matters further, today's fraudsters are well organised, they are highly sophisticated, and they operate with ease across international borders.

So, what can be done to address the vulnerabilities?



Where the card is present

Imagine the scenario. You know that it's a chip card, but the transaction originates from a magnetic stripe acceptance device. Is there anything within the authorisation message itself to alert you to the fact that the transaction may be suspect?

If iCVV (integrated Chip Card Verification Value) has been deployed you

may have a clue – in that it acts as an electronic watermark, enabling you to check whether account information derived from chip card data has been encoded onto a counterfeit magnetic stripe

If iCVV isn't present you won't have any clues at all. Indeed, the way that today's criminals exploit compromised data is specifically designed to trick you into believing that all is well.

So, your only indication will be the wider characteristics of the transaction – in terms of any curious or unusual spending patterns, transaction amounts or merchant sectors.

The importance of fraud detection systems

This is why effective detection systems have become so important in the fight against fraud – helping issuers to quickly identify and address suspicious transactions and compromised accounts.

Visa Europe offers a system called Visa Intelligent Scoring of Risk (VISOR), which many banks use to minimise their fraud losses. This is now about to be significantly upgraded with the introduction of a new Real Time Scoring system.

This means that:

- The risk score of each transaction will be incorporated within the actual authorisation message, enabling issuers to factor it into their authorisation decisions.
- Case management will also be handled in real time, with fraud managers able to monitor the status of every account through a web-based workstation
- In response to new risks and emerging trends, fraud managers can also use the system's online capabilities to modify their own fraud detection and case management rules

As with the existing VISOR system, issuers benefit from the sheer scope and volume of Visa Europe's global data. And, unlike most other detection systems, the neural networks routinely consider the profiles of both the cardholder and the merchant in addition to the unique member-reported fraud data available only to Visa Europe.

So, when determining the risk score, the system will consider the cardholder's previous spending patterns and transaction history. It will also take full account of the fraud experience of a particular merchant – including the purchase types and ticket sizes which have been fraudulent in the past. Because Visa sees more merchant and cardholder transactions than anybody else, the system is able to more accurately determine the risk for a transaction.

For issuers who use Visa Europe for their domestic inter-bank processing requirements, the system can automatically scrutinise every single Visa transaction. For all other issuers, it can still analyse the most risky transactions (namely cross border transactions originating from parts of the world that are yet to migrate to EMV).

Real Time Scoring is now being piloted with two major issuers and a production-ready service will be launched during 2010. It will therefore provide a logical upgrade for existing VISOR users, and it should also be a compelling proposition for other issuers – to either replace or complement their existing solutions.

Visa Europe members should therefore factor the availability of the new system into their development plans.

Visa Europe is also developing its own ATM transaction profiling system to help identify out of pattern, cross-border ATM transactions. The ATM Profiling service prototype has been developed and piloted with a commercial launch planned for 2010.



Where the card is not present

For card not present transactions, such as e-commerce, a completely different set of considerations arise. And, in this case, effective fraud management rests on the ability of a legitimate cardholder to confirm their identity.

In this respect, Verified by Visa (based on 3D Secure technology) has made a definite impact. Across Europe, some 270,000 merchants, accounting for 40 per cent of Visa e-commerce transactions, now support the service and Visa card issuers have enrolled more than 50 million cardholders.

As well as encouraging more issuers to participate, Visa Europe is also alerting its members to increased levels of criminal scrutiny. The integrity of cardholder enrolment processes and the “strength” of

their password or passcodes are matters for real consideration. In particular, issuers are being encouraged to migrate from static to dynamic passwords or passcodes.

A particular consideration is, of course, the attitude of cardholders, who routinely expect their Visa payments to be fast, always accepted, hassle free and 100 per cent secure. Visa Europe has therefore been working to enhance the service, with the introduction of a new, enhanced user interface (which should be commercially available during 2010).

A related development is Visa CodeSure, a new type of card incorporating a keypad and LCD-screen, which is able to generate its own dynamic passcodes. Now ready for commercial launch, this has met with a very favourable reaction from the media, and has been successfully piloted by six banks across Europe.

Evolution of card fraud in Europe				
	1980	1990	2000	Today
Fraudster	<ul style="list-style-type: none"> Individuals 	<ul style="list-style-type: none"> Teams 	<ul style="list-style-type: none"> Local crime rings 	<ul style="list-style-type: none"> International crime rings
Target	<ul style="list-style-type: none"> Consumers 	<ul style="list-style-type: none"> Small retailers 	<ul style="list-style-type: none"> Larger retailers 	<ul style="list-style-type: none"> Banks Processors
Leading fraud types	<ul style="list-style-type: none"> Lost/stolen Intercepted 	<ul style="list-style-type: none"> Domestic counterfeiting /skimming 	<ul style="list-style-type: none"> Identity theft Phishing Rudimentary data compromise 	<ul style="list-style-type: none"> Cross-border data compromise Card -not-present fraud ATM fraud
Type of cards targeted	<ul style="list-style-type: none"> Travel & Entertainment cards 	<ul style="list-style-type: none"> Premium credit cards 	<ul style="list-style-type: none"> Mass market credit cards 	<ul style="list-style-type: none"> All types of credit card Debit cards Prepaid cards
Necessary resources	<ul style="list-style-type: none"> Opportunism 	<ul style="list-style-type: none"> Rudimentary knowledge 	<ul style="list-style-type: none"> Technical knowhow 	<ul style="list-style-type: none"> Audacity Technical expertise Insider information Global connections

Source: Visa Europe

Working together in the fight against fraud

As a European membership association, Visa Europe also has an important role to play in working cooperatively across the industry, bringing different players together to agree on collective priorities.

By continually anticipating, analysing and addressing the threat from fraud, strengthening the industry infrastructure, and adopting new risk management disciplines, Visa Europe seeks to protect the integrity and profitability of all those who participate in the Visa payment card system. Also, through its consultancy services and a growing range of fraud management products and services, Visa Europe can help individual members to assess their exposure to fraud and to manage down the associated losses.

For more information on Real time scoring please contact Mark Lee - Visa Europe Fraud Management.

Tel: + 44(0) 20 7795 5645

Email: leemark@visa.com.

3. Geographic place of misuse

The breakdown of fraud losses by method of compromise underlines the importance of distinguishing between domestic and international losses.

A clear effect of more stringent domestic anti-fraud measures is that they push the fraudulent use of cards into countries where protection is weaker. The much higher losses on the international use of fraudulent cards are evident in the figures for France, Spain and the UK.

In monetary terms, international losses accounted for almost 40% of total fraud losses in the UK in 2008, approximately 47%

in France and approaching 60% in Spain.

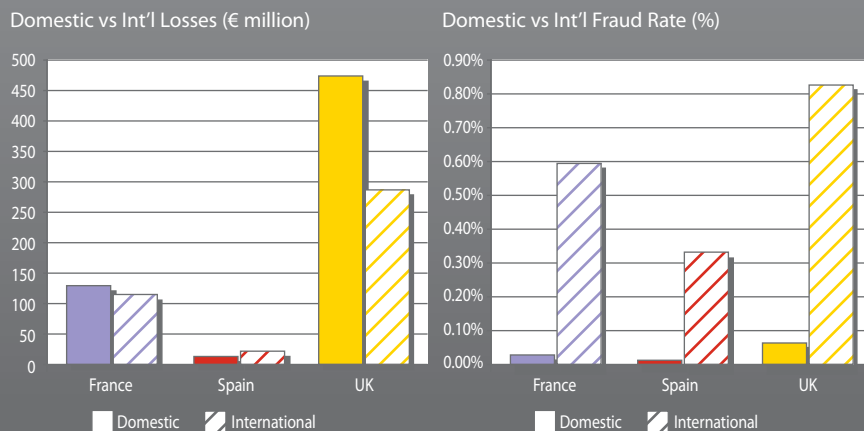
However, this understates the scale of international losses. International turnover on cards is much lower than domestic turnover. The international fraud loss ratios are therefore many times higher than domestic fraud losses ratios. International loss ratios ranged from over 12 times higher (UK) to 30 times higher (Spain) than domestic ratios in 2008 (see Table 3.1).

The differences in domestic and international losses between the three markets have some impact on how the countries' domestic and international loss ratios compare. For example, Spain's domestic loss ratio in 2008 was only a sixth of the UK's while its international ratio was less than a third the level in the UK. However, the ranking of the three countries on domestic and international losses is no different to that overall, with Spain ranking below France, which in turn ranks below the UK (see Table 3.2).

In both France and Spain, international losses increased as a proportion of total losses compared with 2007. For example, of total purchase fraud on ServiRed cards in 2008, 39% took place within Spain and 61% abroad. While domestic purchase fraud grew by 2.4%, international purchase fraud increased by 29%. While ServiRed's domestic purchase fraud loss ratio was unchanged at 0.018% (approximately 2 basis points), its international purchase loss ratio rose from 0.287% to 0.352% (35 basis points).

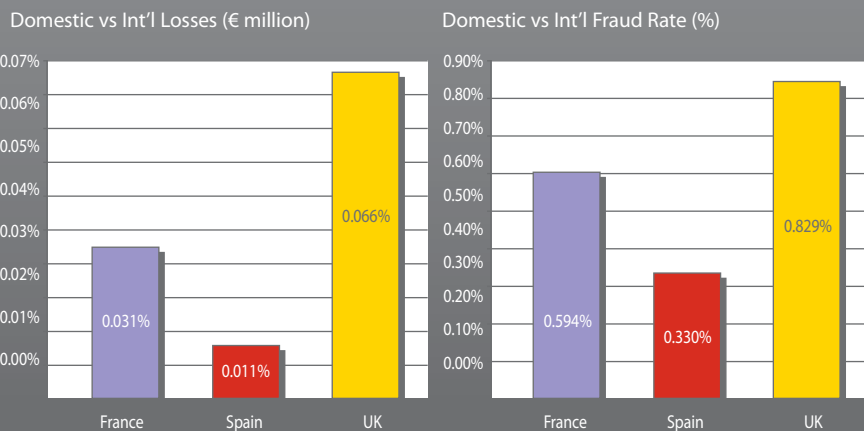
In contrast, though international fraud on UK-issued cards rose from £207.6 million in 2007 to £230.1 million in 2008, the international loss ratio and international losses as a proportion of total losses were little changed. And in the first half of 2009, international fraud losses on UK cards showed a remarkable fall. Losses of £67.1 million were 45% lower than in the first half of 2008. Indeed, losses fell to their lowest level for the first half of the year since the period January to June 2006. This is likely to reflect more pre-notification by cardholders travelling abroad, greater monitoring of international transactions and more transaction declines in locations identified as high-risk. ■

3.1: Domestic and International Fraud Losses 2008



Sources: Observatoire de la sécurité des cartes de paiement, ServiRed, UK Cards Association, Financial Fraud Action UK

3.1: Domestic and International Fraud Losses 2008



Sources: Observatoire de la sécurité des cartes de paiement, ServiRed, UK Cards Association, Financial Fraud Action UK

Notes

Table 3.1:

1. Fraud rate based on fraud losses as a proportion of total card turnover.
2. Turnover covers both purchases and cash withdrawals.
3. International fraud rate covers use of domestic cards abroad.
4. UK losses converted from pounds to euros at 2008 average £/€ rate of 0.79628 (Source: ECB).
5. Spanish figures for ServiRed cards only.

Table 3.2:

1. Fraud rate based on fraud losses as a proportion of total card turnover.
2. Turnover covers both purchases and cash withdrawals.
3. International fraud rate covers use of domestic cards abroad.
4. Spanish figures for ServiRed cards only.

4. Type of misuse

Looking at the type of misuse, the broadest breakdown is between purchases and cash acquisition.

Purchases vs cash acquisition

The available data only allows a comparison of domestic transactions. The breakdown is broadly similar, with purchases accounting for approximately 80-90% of losses across the three markets. Further domestic fraud loss rates on cash withdrawals are lower than those on purchases in all three markets, reflecting in particular the greater security surrounding ATMs and the high loss rates on CNP purchases (see Table 4.1).

Losses by type of purchase

The data available for France and the UK also allows an analysis of losses on domestic purchases.

The main distinction available in the statistics for both markets is between payments at a distance (mail order, telephone order and internet) and losses on other (mainly

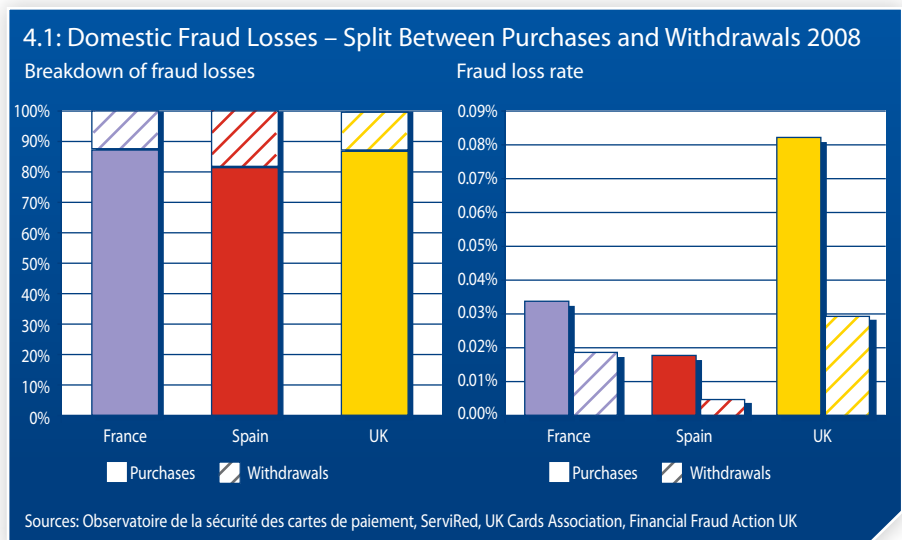
face-to-face) purchase transactions.

Losses from payments at a distance have grown significantly during recent years, matching the growth in the theft of card details. Such transactions accounted for

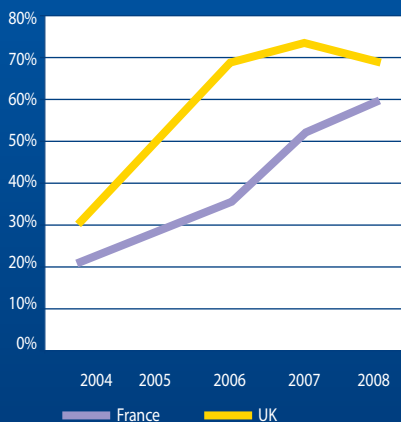
just over half of domestic payment losses by value in France in 2007 and almost 75% of domestic losses on purchases in the UK. As recently as 2004, payments at a distance accounted for only 21.8% of total domestic losses on purchases by value in France and only 31.3% in the UK.

However, while the proportion of purchase losses from CNP transactions continued to grow in France during 2008, it fell slightly in the UK to just under 70%. This is

Continues on p14



4.2: Domestic Purchase Fraud Losses – CNP Share



Sources: Observatoire de la sécurité des cartes de paiement, UK Cards Association, Financial Fraud Action UK

likely to reflect the growth in the number of online merchants implementing Verified by Visa and MasterCard SecureCode. Though CNP losses continued to rise in absolute terms, from £207.2 million to £224.3 million, losses on other retailer transactions (mainly face-to-face) rose more sharply from £73.0 million to £98.5 million (see Table 4.2).

The French data also highlights the internet as a growing source of CNP losses.

Domestic losses from internet payments on French cards almost doubled between 2006 and 2007 to €26.4 million, and rose by a further 47% in 2008 to €38.8 million. They accounted for over 50% of losses from domestic payments at a distance in 2008, and over a third of total domestic losses on payments.

International internet losses on French

cards doubled from €27.4 million in 2007 to €56.0 million in 2008. Losses from international internet purchases were over 40% higher than those on domestic internet purchases, and accounted for almost half of international losses in total (see Table 4.3).

Loss rates

The detailed data available for France confirms that loss rates on transactions at a distance are many times higher than those on other payments. The domestic loss rate on face-to-face and unattended payment terminal (UPT) automatic payments in 2008 was only 0.015% (less than 2 basis points).

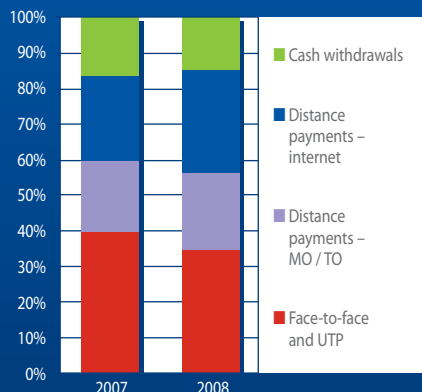
In contrast, the loss rate on payments at a distance was almost 17 times higher at 0.252% (25 basis points). The loss rate on internet payments alone rose from 0.208% (21 basis points) in 2006 to 0.281% (28 basis points) in 2007, though fell to 0.235% (23-24 basis points) in 2008.

International loss rates are much higher across all types of card transaction.

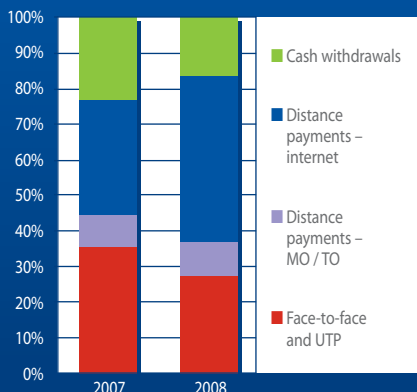
In 2008, loss rates on international face-to-face/UPT purchases and on international withdrawals were higher than on domestic online purchases. The loss rate on international online purchases using French cards was an astonishing 1.8% (see Table 4.4). ■

4.3: Losses by Type of Misuse – France

Domestic (2007: €114.5 million, 2008: €130.9 million)

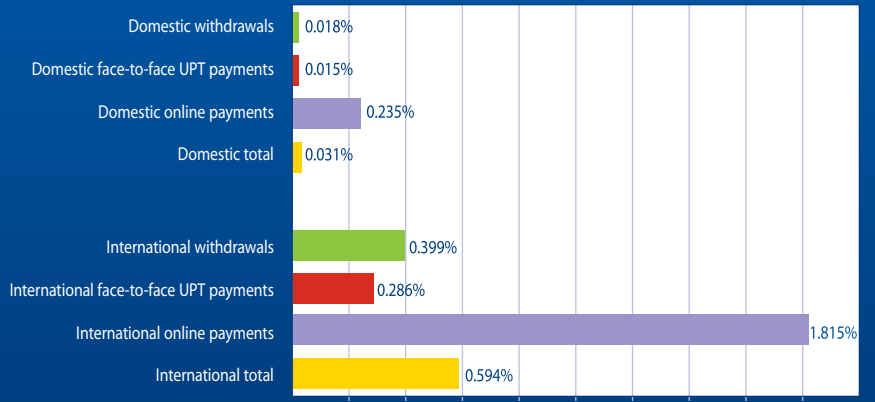


International (2007: €85.3 million, 2008: €118.3 million)



Sources: Observatoire de la sécurité des cartes de paiement, ServiRed, UK Cards Association, Financial Fraud Action UK

4.4: France: Fraud Loss Ratios 2008



Source: Observatoire de la sécurité des cartes de paiement

Notes

Table 4.1:

1. Breakdown covers domestic transactions only. Data on international transactions not available for all markets.
2. Spanish figures for ServiRed cards only.

Table 4.2:

1. Charts cover domestic transactions on French and UK-issued cards respectively. Domestic cash withdrawals and all international transactions excluded.
2. Shows losses on CNP (mail order / telephone order / internet) purchases as a proportion of total losses on domestic card purchases.

Table 4.3:

1. Charts cover both domestic and international transactions on French.
2. Data covers both interbank ("CB") cards and private cards.
3. UPT = unattended payment terminal.
MO/TO = Mail Order / Telephone Order.

Table 4.4:

1. Totals also include losses from payments at a distance made by post/phone.

5. Linking method of compromise to place of misuse

The French data allows the data on fraud losses by method of compromise to be brought together with the data by place and type of misuse, giving a comprehensive overview of the relationships between the two.



Though a little simplified (see table 5.2 for the full data), the main patterns evident in the French data for 2008 are highlighted in table 5.1:

Looking first at domestic fraud on French cards in 2008:

- Lost and stolen cards accounted for 83% of face-to-face and UPT losses, and 97% of fraudulent cash withdrawals.
- Stolen card numbers accounted for almost all CNP losses.

The picture is more complex for international losses:

- Counterfeit cards accounted for over 60% of international face-to-face and UPT losses, and lost and stolen cards for almost 30%.
- Lost and stolen cards, counterfeit cards and stolen card numbers all contributed to international CNP losses.
- Counterfeit cards accounted for almost 90% of international fraudulent cash withdrawals.

The main change in 2008 compared with 2007 is the substantial increase in interna-

tional CNP internet losses, which rose from €27.4 million to €56.0 million.

Analysing the international internet losses by method of compromise, lost and stolen cards and stolen card numbers were

significant contributors. In particular, international losses from internet purchases using stolen French card numbers, which were negligible in 2007, totalled €17.9 million in 2008. ■

5.1: Linking Method of Compromise with Place of Misuse

	Lost or stolen cards	Counterfeit cards	Appropriated card numbers
DOMESTIC			
- Face-to-face purchases	●		
- CNP purchases			●
- ATM withdrawals	●		
INTERNATIONAL			
- Face-to-face purchases	●	●	
- CNP purchases	●	●	●
- ATM withdrawals		●	

Source: Author's analysis based on French data for 2008

5.2: French Fraud Losses (2008) € millions

	Lost or stolen cards	Intercepted cards	Forged / counterfeit cards	Appropriated numbers	Other	TOTAL
Face-to-face and UPT	46.4	0.9	22.8	2.1	4.4	76.5
Distance payments - MO/TO	2.9	0.0	2.9	32.3	1.5	39.7
Distance payments - internet	15.5	0.0	16.4	56.5	6.3	94.8
Withdrawals	20.5	0.2	17.4	0.0	0.1	38.2
TOTAL	85.3	1.2	59.4	91.0	12.2	249.2
- OF WHICH DOMESTIC LOSSES						
Face-to-face and UPT	37.1	0.7	2.8	0.2	3.7	44.5
Distance payments - MO/TO	0.0	0.0	0.0	28.4	0.0	28.5
Distance payments - internet	0.1	0.0	0.0	38.6	0.0	38.8
Withdrawals	18.5	0.2	0.3	0.0	0.0	19.1
TOTAL	55.8	0.9	3.1	67.2	3.9	130.9
- OF WHICH INTERNATIONAL LOSSES						
Face-to-face and UPT	9.2	0.2	20.0	1.9	0.6	32.0
Distance payments - MO/TO	2.9	0.0	2.9	4.0	1.4	11.2
Distance payments - internet	15.5	0.0	16.4	17.9	6.3	56.0
Withdrawals	2.0	0.0	17.0	0.0	0.0	19.1
TOTAL	29.6	0.3	56.3	23.8	8.4	118.3

Source: Author's analysis based on French data for 2008

Notes

Table 5.1:

1. Cells highlighted are those where losses account for more than 5% of total domestic or international losses respectively in 2008.

Table 5.2:

1. Statistics cover both "CB" bank cards and "private" cards issued by American Express, Banque Accord, BNP Paribas Personal Finance, Cofidis, Cofinoga, Diners Club, Finaref, Franfinance, S2P and Sofinco.

2. Statistics cover French cards used in France and internationally.

3. UPT = unattended payment terminals.

6. Concluding comments

Clearly, a short research report such as this cannot cover in detail all aspects of a topic as complex and fast moving as payment card fraud.

It analyses data for direct fraud losses, which provide only part of the picture. As the Visa Europe material in the supplement on the total cost of fraud emphasises, a full analysis of fraud-related costs also needs to incorporate fraud management expenses and opportunity costs.

However, a comparison of the data available on direct fraud losses for various major markets across Europe helps to highlight important aspects.

Though the figures indicate that fraud losses are being contained (as a proportion of card turnover), they also underline that

the challenge is relentless, and mutating.

Looking at methods of compromise, EMV implementation has significantly constrained losses from lost and stolen cards in those markets where it has been implemented. In the UK, losses from lost and stolen cards fell slightly in 2008 while they increased only modestly in France. However, at £54.1 million and €85.3 million respectively, losses remain significant.

The figures confirm continuing high losses from counterfeit cards and the use of stolen card details.

Both are susceptible to fraud on a professional scale that is more difficult to achieve with lost and stolen cards. They remain the largest sources of losses in the UK, with stolen card details becoming the largest single source of losses in France in 2008. And, in terms of emerging threats, the UK figures show a rapid growth in ID fraud.

Looking at place of misuse, the French data in particular highlights the much higher loss rates on online and other CNP payments compared with other forms of card transaction. And loss rates on all types of international card transaction are many times higher than comparable domestic rates.

The scale and changing profile of losses underlines the urgency of implementing existing preventative measures (such as EMV and Verified by Visa / MasterCard Secure Code) and of enhancing those measures through more secure cards and infrastructure, and more rigorous cardholder authentication. ■

6.1: Fraud Prevention Overview

Type of Misuse	Prevention Measures	Developments
Domestic POS & ATM transactions	<ul style="list-style-type: none"> • EMV • Cardholder awareness (protection of PIN, transaction alerts) 	SDA to DDA/CDA
International transactions in non-EMV POS & ATMs	<ul style="list-style-type: none"> • Prevention of initial data capture: <ul style="list-style-type: none"> – Merchant (skimming protection, PCI DSS) – ATM security (skimming protection) • Issuer and acquirer monitoring: <ul style="list-style-type: none"> – Card use – Major locations of POS & ATM fraud • Cardholder awareness (pre-notification of international travel, transaction alerts) 	<ul style="list-style-type: none"> • Geographic extension of EMV • Chip only cards (V Pay)
Card-not-present, especially online transactions	<ul style="list-style-type: none"> • Prevention of initial data capture: <ul style="list-style-type: none"> – Merchant (PCI DSS) – ATM security (skimming protection) • CVV • Verified by Visa / MasterCard Secure Code • Cardholder awareness (use of anti-virus software, secure websites, transaction alerts, etc) 	<ul style="list-style-type: none"> • Dynamic authentication (one-time passwords)

Source: Author's analysis



business intelligence

specialist cards and mobile payments industry consulting,
to evolve your presence visit paymentscardsandmobile.com/marketing

Total cost of fraud from Visa Europe

Evaluating the true costs of card fraud can be a complex business. Different banks calculate the figures in different ways, with many focusing on net losses, and overlooking a number of secondary costs and potentially more significant costs.

On this basis, Visa Europe is concerned that many of our members may underestimate the true costs of fraud. They may not take into account related operational and process costs, and could be unaware of potentially substantial opportunity costs.

Because our members assess their fraud performance in different ways, it can also be difficult to make meaningful peer-to-peer comparisons.

As a response, Visa Europe has pioneered use of a new analytical tool: the Total Cost of Fraud (TCoF) financial model. In assessing the viability of this model, we worked with seven members across six European countries. These pilot issuing and acquiring members helped us to test and refine the model, which was then adopted over six months from June 2008.

Total cost of fraud is a financial model that enables Visa Europe members to better understand the wider business implications of their existing fraud management operations - and make better informed decisions with regard to future strategies, cost allocation and potential investment decisions.

To use the model, members input a variety of cost elements into a spreadsheet.

For issuers, these costs include card issuing, card replacement, PIN delivery, customer service, fraud operations, first party fraud losses, human resources, facilities/overheads, systems and operating expenses. For acquirers, they include customer service costs, fraud operations, human resources, facilities/overheads, systems and operating expenses. In each case, members are asked to split costs

between fraud prevention, detection and investigation and recovery activities.

The model is supported by an assessment framework which defines each cost element in a concise and easy to understand manner, so that consistent, comparable data can be analysed.

The model then produces an analysis of fraud-related costs, grouped within three main categories:

- **Direct fraud losses**
- **Fraud management expenses**
- **Opportunity costs**

The model then generates various performance metrics and management reports. It also has the flexibility to assess the respective costs across an entire portfolio or alternatively segments within a given portfolio (for example, across different card products or specific merchant categories).

The TCoF pilot has demonstrated that the model is robust, easy to use, and provides significant added value to both issuers and acquirers.

The findings from the seven pilot members suggest that fraud management expenses are at least equal to direct fraud losses, and can often be much higher. It is in this area where the most scope for cost savings lies (for example, through the optimisation of PIN delivery and employee costs).

Opportunity costs, which include the behaviour of cardholders subsequent to experiencing fraud, vary considerably - but can easily account for more than 15 per cent of total fraud costs.

Reductions in these opportunity costs may be obtained through better customer care following a fraud or compromised card incident, through earlier card replacement, and by min-

imising the number of incorrect fraud-related declines and referrals. Cardholder or merchant concerns about perceived fraud in certain channels e.g. the internet, can influence card usage and acceptance preferences.

How can members benefit from TCoF?

The analysis generated by TCoF can demonstrably help issuing and acquiring members to assess the wider business consequences of fraud. And, as more members participate, the model can be used to make meaningful benchmark comparisons across the Visa Europe membership.

Additional applications of TCoF include:

- Delivering time series analysis in order to identify and report on key performance indicators and their progress over time
- Justifying new investments, by indicating the cost benefit ratio of investments in human resources, technology, customer service, facilities and other operational areas
- Providing an internal benchmarking tool which, for example, could compare performance across multiple sites
- Demonstrating to executive management teams the wider business consequences of fraud management strategies and processes - and the performance of one's own operations.

"I think implementation of total cost of fraud (TCOF) is very timely, as costs are now being scrutinised much more closely within the industry. TCoF enables this process to be conducted in an intelligent way."

Kevin Smith

SVP Fraud Management, Visa Europe

For more information on Total cost of fraud please contact John Griffiths, Visa Europe fraud management email: griffitj@visa.com or by calling + 44 (0) 207 795 5281.

Appendix: Note on sources and statistics

The report draws on statistics published by:

- Visa Europe
- The Observatoire de la sécurité des cartes de paiement for France
- Currence for the Netherlands
- ServiRed and Sistema 4B for Spain, and
- UK Cards Association and Financial Fraud Action UK

France

The Observatoire compiles its statistics based on those received from:

- The 146 members of the "CB" Bank Card Consortium, with international data provided by MasterCard and the Carte Bleue Group
- Private "three party" card issuers: American Express, Banque Accord, BNP Paribas Personal Finance, Cofidis, Cofinoga, Diners Club, Finaref, Franfinance, S2P and Sofinco.
- Issuers of the electronic purse Moneo.

The French statistics therefore include some private-label cards as part of the coverage of three-party card networks.

The Observatoire supplements the data from the banks, card issuers and card networks with statistics compiled by the Fédération du e-commerce et de la vente à distance (Fevad), which consults a sample of 33 companies representing 38% of the turnover of distance selling to individuals.

In addition to domestic transactions involving French cardholders and French merchants and international transactions between French cardholders and foreign merchants, the Observatoire report includes statistics on transactions between foreign cardholders and French merchants. These are excluded from the analyses and comparisons in this report, which is focused on fraud from an issuer perspective.

Of the 84.7 million cards in circulation in 2008, 58.2 million were four-party cards ("CB" and Moneo) and 27.2 million were three-party cards (around 530,000 cards were reported lost or stolen in 2008). However, the four-party cards accounted for approximately 92% of purchases and 99% of withdrawals by value in 2008.

Four-party cards accounted for approximately 95% of fraud losses by value in 2008. There are some notable differences in the profile of fraud losses between French four-party and three-party cards:

- While almost all the domestic losses on four-party cards are due to lost/stolen cards and stolen card numbers, approximately half of the domestic losses on three-party cards fall under the "Other" category. According to the Observatoire, this category covers, particularly for three-party cards, fraud resulting from the fraudulent opening of accounts with a false identity.

- International losses by value account for a higher share of total losses on four-party cards. This is unsurprising given the greater international utility of "CB" cards. Though three-party card issuers include American Express and Diners Club, they also include the French private-label card issuers.

Netherlands

The data for the Netherlands has been supplied by Currence, the organisation that oversees payments in the Dutch market. Currence is the owner of the Dutch uniform payment products PIN (debit card plus PIN code), Chipknip (electronic purse), Incasso (direct debit), Acceptgiro (giro collection forms) and iDEAL (online payments). Currence sets rules for its payment products, issues licences and certificates to banks and other firms wishing to offer Currence payment products or to provide support services, and monitors compliance with the rules. It also works closely with all interested parties to prevent fraud.

The figures for Bankpas only cover domestic turnover and domestic fraud losses on Dutch debit cards (ie domestic PIN debit card transactions).

The figures for total card losses cover PIN debit card transactions plus use of Dutch debit cards internationally (which are treated as Maestro transactions), plus domestic and international transactions on Dutch credit cards.

Spain

The statistics for Spain mainly cover the ServiRed network. In addition, some of the commentary draws on statistics available for the Sistema 4B network.

ServiRed reported 40.5 million cards (credit and debit), 708,902 merchants and 32,648 ATMs as of 2008. According to ServiRed, its cards accounted for 61.6% of the total monetary volume of purchases made with Spanish cards, and for 63.1% of total card purchase transactions. They were also used for 56.4% of all cash withdrawals from ATMs with cards issued in Spain, for 55.1% of total withdrawals.

ServiRed presents its fraud statistics in the form of loss ratios. Where needed for the analysis, actual values have been calculated by applying these ratios to the statistics available on the value of purchases and cash withdrawals on ServiRed cards.

According to ServiRed's 2008 annual report: "In terms of issue fraud, ServiRed continues to post a lower incidence than the industry average."

UK

The UK figure of 168.7 million cards in issue for 2008 includes 19.4 million ATM only and 0.4 million cheque guarantee only cards. There were 148.8 million UK cards with a payment function as of 2008, of which 66.1 million were credit cards, 6.4 million charge cards and 76.3 million were debit cards. The UK statistics do not include private-label cards.

The UK fraud statistics by card type (credit, charge, debit, etc) and method of compromise (lost/stolen, mail non-receipt, etc) cover both domestic and international transactions. However, the breakdown by place/type of misuse (ATM, MO/TO/internet, etc) covers only domestic transactions.

The UK breakdown of domestic losses by place/type of misuse includes losses of £11.3 million in 2008 from UK cash withdrawals at bank counters in addition to £45.7 million of losses at UK ATMs. The UK domestic fraud loss rate on withdrawals quoted in Section 4 includes the losses from UK cash withdrawals at bank counters.

Eurostat

The Eurostat data quoted in Section 2 on use of the internet to order goods and services is taken from the Eurostat bulletin: Data in Focus 46/2008, Internet usage in 2008 Households and individuals, available free of charge in pdf format on the Eurostat web site. The full set of data can be found in the dedicated section: <http://ec.europa.eu/eurostat/ict> under "Data".

Gross and net losses

The fraud loss statistics for the UK from 2000 onwards are explicitly specified as recording gross rather than net losses, ie the gross value of fraudulent transactions before any recoveries. It is assumed that the statistics for France, Netherlands and Spain are recorded on the same basis, though it has not been possible to confirm this.

In addition to the value of fraudulent transactions, there are of course significant additional costs associated with card fraud, notably the staff and other costs associated with processing fraudulent transactions and liaising with cardholders and merchants, the costs of developing, purchasing and maintaining fraud prevention systems, and the opportunity cost of lost card business. An analysis of these costs by Visa Europe is included in the supplement.

Card-not-present (CNP) fraud

CNP fraud can refer both to the method of compromise (theft of card details) and to the place/type of misuse (use of card details in MO/TO/internet transactions, sometimes called distance payments). The two uses are not identical. As the French data shows, while the theft of card details results mainly in MO/TO/internet losses, there are also some MO/TO/internet losses from lost/stolen and counterfeit cards. For example, the French statistics for 2008 show losses from appropriated card numbers of €91.0 million in 2008. Almost all of this was in the form of MO/TO/internet losses. However, total MO/TO/Internet losses were €134.5 million because there were also significant losses from the use of lost/stolen cards, counterfeit cards, etc, in a MO/TO/internet environment. ■

France – four-party and three-party cards compared 2008

	"CB" cards	Three-party cards	Total
Number of cards	58.2 million	27.2 million	84.7 million
Value of purchases	€303.7 billion	€25.7 billion	€329.4 billion
Value of withdrawals	€109.2 billion	€1.0 billion	€110.3 billion
Fraud losses	€237.0 million	€12.2 million	€249.2 million

Notes: 1. Four-party cards include 1.3 million Moneo electronic purses. 2. Statistics on value of purchases and withdrawals, and on fraud losses cover both domestic and international transactions on French cards. They do not include transactions in France on non-French cards. 3. Around 530,000 cards reported lost or stolen in 2008. Source: Observatoire de la sécurité des cartes de paiement

France – domestic fraud losses on four-party and three-party cards 2008

€ million	Four-party cards	Three-party cards	Total
Domestic losses (cards):			
Lost or stolen	53.4	2.4	55.8
Intercepted	0.3	0.6	0.9
Forged or counterfeit	2.6	0.5	3.1
Appropriated numbers	66.6	0.6	67.2
Other	-	3.9	3.9
Domestic total	122.9	7.9	130.9
International losses	114.1	4.3	118.3
Total	237.0	12.2	249.2

Source: Observatoire de la sécurité des cartes de paiement



Tailored research

Payments Cards and Mobile Research offers comprehensive, targeted research into topics which are relevant and tailored to your needs – billed in a tiered structure allowing maximum efficiency for a reasonable budget.

Bulletins and reports – Payments Cards and Mobile Research publishes both short bulletins and longer research reports on current topics to a worldwide audience. Topics range across the measurement of efficiency and performance to the impact of non-banks such as retailers on the financial services and mobile financial services market.

Targeted Research – we also research targeted aspects of banking, card payments, financial services and the mobile financial services market. For example, information on a particular market or a pan-European comparison of a particular segment.

For more information, visit our website or email research@paymentscm.com

paymentscardsandmobile.com/research

Payments
CARDS&MOBILE



IRIS[®]

Real-time decision making for better fraud and risk control

Fraud losses out of control? Too many false alarms and unhappy customers?

The IRIS fraud prevention solution combats fraud and controls risk for all types of card based payments, online banking, transaction banking (e.g. Faster Payments, SEPA Direct Debits) and mobile payments. IRIS is your best choice when it comes to boosting system profitability, securing customer confidence and protecting your brand value.

To learn more, visit www.iris.de

