Online & mobile payments:

New opportunities & threats

Autumn 2013

ogone
An ingenico company

Contents

01 Introduction

You don't have to go too far to find information to show that card-not-present payments online and mobile devices are on the rise, year after year, across Europe. e-Commerce Europe expects the European B2C e-Commerce market to double in size by the end of 2016 to reach €625bn, driven by increased confidence and a growing number of people buying online. Almost half (47.6%[1]) of all Europeans have a smartphone, which means that consumers are already always connected; they can search and purchase wherever and whenever they want.

Buying goods and services online has become a natural part of the customer journey and with the increase of mobile-optimised websites, one-click payments and free returns; it has never been so quick or convenient for consumers to purchase online – whether it be on their laptop, smartphone or tablet.

Brands are now waking up to the opportunity to increase sales and brand engagement through online and mobile because they know that their customers are using online and mobile more, then visiting their store. Domino's Pizza in the UK recently released sales statistics that showed that the revenue gained through mobile last year was the same amount as the entire revenue the business achieved in 1999. It's growing at an exceptional rate.

So it would seem, on the surface, that the world of online and mobile payments is providing businesses of all sizes across Europe the opportunity to increase revenue and engagement with their customers – but there are some clear risks attached.

Europol[2], The European Union's law enforcement agency that handles criminal intelligence, reported that in 2011, around 60% of total payment card losses were caused by card-not-present fraud – which equates to a staggering €900m. They report that the main sources of online payment fraud came from data breaches and malicious software. A key barrier to addressing online payment fraud, Europol state, is the lack of proper regulations for reporting data breaches to police authorities. Though the European Central Bank (ECB) have recently stated that card fraud is actually on the decline since 2007, online payment fraud remains the largest category of fraud – with 73% of card-not-present fraud taking place online.

With the threat of online payment fraud ever-present, how are businesses, of all sizes, protecting themselves and their consumers against the threat of fraud?

Ogone have recently completed depth qualitative research with businesses selling online across UK, Germany, France, Belgium & The Netherlands to understand what they are currently doing to guard against online fraud as well as understand what they expect from a fraud management solution[3]. The survey highlighted e-Commerce businesses' focus on adapting to the demand for more online payment transactions, and found that, even where e-Commerce businesses have not installed specific software to detect potential fraudulent transactions, they all had procedures in place to protect their online payment sales. The level of resource required – and the issues they face – correlates with the number of transactions, their retail sector and 'speed to market' of the sale.

E-Commerce businesses with fast-growing online payments, particularly those dealing with new sales channels (such as mobile phones and tablets) are especially aware of the issues and shortcomings of existing processes as well as the business trade-off between making the purchase process easy for the customer whilst ensuring that the fraud 'firewall' they have in place is as effective as possible in identifying fraud attempts.

1. Data taken from www.thinkwithgoogle.com/mobile planet
2. https://www.europol.europa.eu/sites/default/files/publications/1public_full_20_sept.pdf
3. Ogone's research, carried out in Q2 2013, comprised 253 telephone interviews with merchant clients in the UK, Germany, France, Belgium and The Netherlands, ranging from those who handled fewer than 100 transactions per month, to those processing in excess of 1,000. The survey included merchants who already use Ogone's fraud detection service as well as those who have no 'built-in' module to detect fraud automatically

02 Setting the scene

The opportunity & the threat:

The growth of online/mobile payments

According to a recent European Commission report[4] more than half (53%) of European consumers have made at least one purchase online in the last twelve months from September 2012. Of the countries investigated in this research, The Netherlands had the highest rates of online purchase with around three quarters of consumers (74%) purchasing something online in the last 12 months – UK (71%); Germany (63%); France (58%) and Belgium (44%).

When investigating cross-border purchasing, the numbers are lower with only 15% of EU consumers purchasing something from another EU country in the last 12 months. This may have something to do with the fact that only 36% of EU consumers are confident about purchasing goods via the internet from retailers in another EU country.

The European e-Commerce industry is dominated by the UK (€96bn), Germany (€50bn) and France (€45bn). The total of €191bn of these three countries together represents 61% of the total European B2C e-Commerce sector and 69% of the EU28.

European B2C e-Commerce, including online retail goods and services such as online travel bookings, events, tickets and downloads, grew by 19.0% to reach €311.6 bn. The EU28 countries reached sales of €276.5bn, or 88.7% of total European e-sales, a growth of 18.1%.

Without a doubt, online payments are here to stay and will continue to rise over the coming years as consumer confidence increases and new technological payment solutions make it easier and safer for people to buy online.

One area of payments that is also growing is mobile payments. By 2017, eMarketer predicts that smartphone penetration in Europe will hit around 90% - the highest predicted penetration rate than anywhere else in the World. Smartphones are changing consumer behaviour in a similar way that the Internet impacted in the early 2000's. We now use our smartphones to do nearly everything: research products, consumer media and content, play games, travel, redeem vouchers and coupons, shop in-store and purchase goods and services.

The growth of payments via mobile is clear to see. Last year, Amazon stated[5] that 5% - 8% of sales is generated on mobile – a staggering $3bn last year. Google's statistics on mobile usage[6] in the countries analysed in this study (UK, Germany, France, Belgium & The Netherlands) states that 50% of all smartphone users in those countries have purchased something on their phone in the last month with payments using a debit / credit card being the most popular method.

In the countries that we analysed in this study, there is, however, clear consumer apprehension to purchase via their mobile. Again, Google's statistics show that the second most cited reason for not purchasing via their smartphone is because they do not feel it is secure enough (44% of UK smartphone owners do not purchase online because they feel it isn't secure; France 29%; The Netherlands 24% and Germany & Belgium 23%).

So, it would seem that with online and mobile payments on the rise, the future is bright for e-Commerce businesses around Europe. But with the increased opportunity comes the increased threat of fraud and security issues.

With the growing threat of online and mobile payment fraud ever-present, Ogone wanted to investigate in more detail how e-Commerce businesses across UK, France, Germany, Belgium and The Netherlands protect against fraud.

4. http://ec.europa.eu/public_opinion/flash/fl_358_en.pdf
5. http://allthingsd.com/20130104/eight-percent-of-amazons-sales-are-coming-from-mobile/
6. Data taken from www.thinkwithgoogle.com/mobile planet

03 Merchants

How are merchants protecting against the threat and what do they want from a fraud management tool?

Ogone's European survey

Ogone's research was carried out earlier this summer, and comprised 253 telephone interviews with e-Commerce businesses the UK, Germany, France, Belgium and The Netherlands, ranging from those who handled fewer than 100 transactions per month, to those processing in excess of 10,000. The survey included e-Commerce businesses who already use a fraud detection service as well as those who do not have an automatically built-in fraud detection product.

The research found that, even where e-Commerce businesses have not installed specific software to detect potential fraudulent transactions, they all had procedures in place to protect their online payment sales. The level of resource required – and the issues they face – correlates with the number of transactions, their retail sector and 'speed to market' of the sale.

The typical problem areas they identify are:

- Region-specific fraud: particularly arising from US cards, UK credit cards, and cards from outside Europe
- Ability to investigate and authorise non credit card payments, more prevalent in specific countries (for instance, direct debit fraud in Germany, and debit cards in France)
- Chargebacks: especially last-minute claims from customers which do not allow merchants enough time to collate evidence of purchase
- Verifying customer details in order to establish authentic payment details
- 3-D Secure: while this is valued highly as an effective fraud management tool it is restrictive for a large volume of e-Commerce businesses/mobile payment channels and some have moved away from it
- Cards outside the 3-D system (e.g. corporate cards)
- Speed of authorisation: for instant purchases, real time response is required
- Cost of insuring against fraud

Our research revealed that e-Commerce businesses for whom online payment is still in its infancy and/or with low online payment sales typically feel confident of their fraud management procedures and are able to prevent fraud successfully: the process of manually checking each transaction against black lists, customer history and any other source of data available to them is not onerous on staff time. Whilst they can contain and control fraud the issue of fraud management is not high on their list of priorities. However, as their businesses grow (with an implicit increase in online payment sales) they will have to face the impracticality of trying to authenticate a significant share of their transactions manually.

Regional differences reflect levels of activity in the specific markets, as well as different payment systems in place, but the results also indicate that cultural attitudes may be influencing e-Commerce businesses views to some extent.

Managing the risk of online payment fraud country by country analysis:

UK

In the UK, where e-Commerce and m-commerce are both growing fast, online payment fraud is understandably a high priority for e-Commerce businesses. Of the five countries covered in this research, UK e-Commerce businesses were most likely to regard fraud management as a business priority and be on the alert for innovations that help to combat the ever-increasing sophistication of fraudsters. And because e-Commerce businesses are 24/7, businesses need to be supported by an equivalent 'fit for purpose' fraud management tool.

The statistics show that UK e-Commerce businesses are managing to contain fraud to some extent as this is not growing as fast as overall online payment business, but e-Commerce businesses in our research were clear that their aim was to eliminate fraud altogether.

"Online payment fraud is a high priority for UK e-Commerce businesses whose aim is to eliminate fraud altogether."

Germany

Online payment business is relatively new in Germany and e-Commerce businesses in our research (with some exceptions) felt in control of stopping any fraudulent attempts by means of manual checks for each transaction. These procedures are likely to be extremely thorough (and time consuming) but the net result is successful for them, as few e-Commerce businesses in the research had experienced fraud. Because of the evolution of payment structures in Germany there is a strong direct debit culture: although these present their own challenges, online payments may well be made via the customers' bank as well as credit cards and are arguably easier to control.

E-Commerce business attitudes to fraud management tools (typical of businesses elsewhere with the same profile) are therefore more measured: the decision whether or not to implement such a tool is based on a cost benefit analysis, weighing the financial gain (usually viewed in relation to chargebacks rather than fraud per se) against the cost of the tool itself. Even among the largest e-Commerce businesses, attitudes toward fraud management are more pragmatic than those expressed elsewhere: their objective is more likely to be containment and management of the most obvious fraud rather than complete elimination.

"Attitudes toward fraud management are more pragmatic than those expressed elsewhere: their objective is more likely to be containment and management rather than elimination."

France

Online payment business is growing strongly in France and it could be argued that the e-Commerce businesses in our research are playing 'catch-up' with the ability to stem the amount of fraud that comes with such growth. Certainly, respondents in France were more likely (than those in other countries) to have experienced fraud in the last twelve months and felt the pain of lost business. Their estimates of lost business were twice as high – 1.4% of total online payment turnover compared to 0.6% elsewhere.

Understandably, French e-Commerce businesses see fraud management as a business priority, and believe that any tool has to offer, as basic functionality, 3-D Secure customer authentication and the ability to control who buys their products/ services (by country blocking, and customer ID checks).

At this point in time, their appetite for fraud management is very high, albeit at a relatively simple, functional, level.

Belgium

In Belgium, online payment fraud is a high priority; the e-Commerce businesses in our research were typical of those in other countries: they were not likely to have experienced much fraud to date but do recognise that this is a business priority that they need to focus on. If they implement a fraud management tool, they believe it needs to be as comprehensive and efficient as possible, in order to minimise their own involvement and resource in managing the process.

"Online payment fraud is a high priority; a fraud management tool needs to be as comprehensive and efficient as possible, in order to minimise resource in managing the process."

> Only 1 in 3 Dutch e-Commerce businesses sees online payment fraud as a high business priority. With such limited exposure to fraud, they are unlikely to be equipped to tackle fraud as their businesses grow.

The Netherlands

In our research, the e-Commerce businesses in The Netherlands were least likely to have experienced any fraud at all and so concerns about managing fraud are not yet on their radar: only 1 in 3 businesses sees this as a high business priority. Perhaps it is not surprising that, across the five countries, the e-Commerce businesses here were least interested in paying for a tool to manage fraud, which they feel they can control successfully themselves. They certainly do not view the cost of such a tool as an investment to protect their business. It may well be that education and support from their financial providers have a role to play in convincing Dutch e-Commerce businesses of the benefit of 'prevention rather than cure': with such limited exposure to fraud, they are unlikely to be equipped to tackle fraud as their businesses grow.

"The largest businesses lose an estimated 1.2% online payment turnover to fraud versus 0.8% overall"

Generally, while there is an acceptance that fraud management is important, the respondents in our research said there is a trade-off between the cost of implementing a fraud management system and chargeback loss. At the same time, e-Commerce businesses want control but not necessarily involvement.

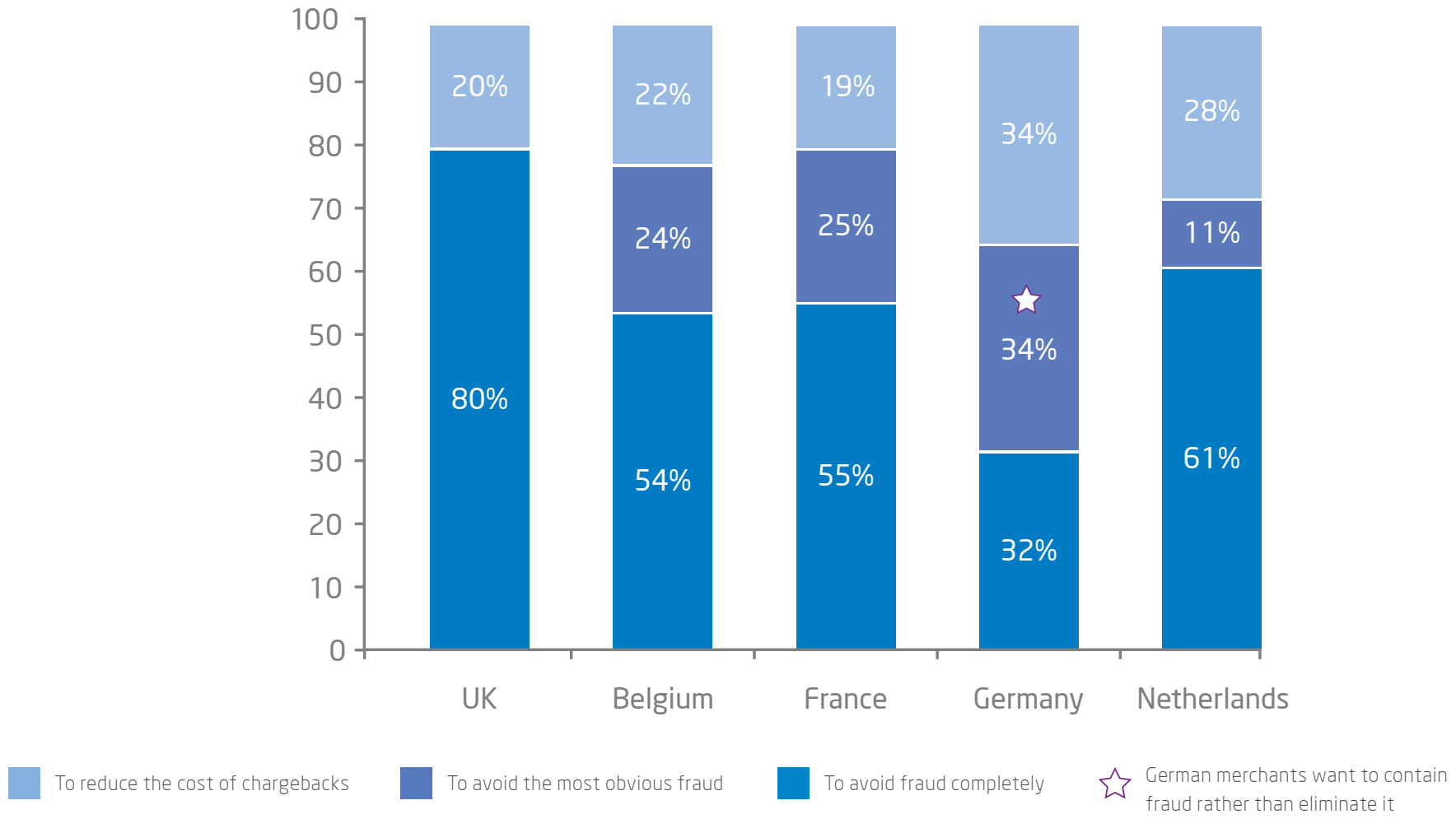
"There is a trade-off between the cost of implementing a system and chargeback loss. E-Commerce businesses want control but not necessarily involvement."

E-Commerce businesses have slightly different motivations for, and expectations of, the fraud detection measures they put in place, but overall, the main desire is to eliminate fraud completely.

The largest e-Commerce businesses in this study were pragmatic about the ability to avoid fraud completely: they want to control fraud and reduce the costs of chargebacks. Other e-Commerce businesses hold an ideal of complete fraud avoidance. Alongside the various fraud detection measures in place are e-Commerce businesses' own 'in house' methods, such as: individual customer research, making customers pay in advance, and 3-D Secure.

Main motivator for implementing fraud detection measures.

Across the UK, Germany, France, Belgium and The Netherlands, e-Commerce businesses have slightly different motivations for, and expectations of, the fraud detection measures they put in place but generally, the main desire is to eliminate fraud completely.



Only 14% of e-Commerce businesses in the survey did not have any specific fraud management process in place. The key reason given for this was a lack of need but it is clear from this research that education and cost are key factors in their decision-making, and that even those e-Commerce businesses with fraud management systems in place are not always aware of the scope of functionality.

Typically, these e-Commerce businesses are not inclined to consider fraud management tools until, or unless, they are confronted with the problem as their business grows.

Regardless of the protocols in place, the great majority of e-Commerce businesses feel that their procedures are adequate. Even those e-Commerce businesses who do not have fraud management software run thorough and time-consuming checks, the most basic of which are visual checks to ensure that the nationality/country of origin of the cardholder is acceptable to them.

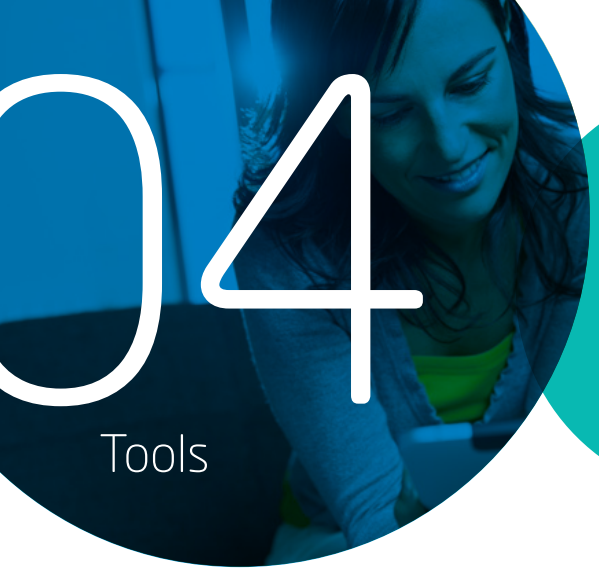
From then on, they may check for suspicious behaviour based on, for example:

- number of payment attempts
- number of payment defaults/credit history.

Only 11% of e-Commerce businesses surveyed felt that their fraud management tools are not 'fit for purpose', and that there was scope for improvement in fraud detection and prevention. In some cases, particularly the smaller e-Commerce businesses (handling fewer than 100 transactions per month), this is because they do not have the human and technical resources necessary to run the protocols more efficiently. Some e-Commerce businesses are also basing their decisions on outdated blacklists.

Others have adopted an incremental approach, opting for low security levels, to see where the main fraud problems stem from, and to ease the shopping process for honest customers, which over time they have increased where necessary, without introducing hurdles for acceptable customers.

While the cost of detecting fraud is felt by some respondents to be high, the potential loss from fraud is considered potentially "enormous – thousands of euros – this is a real issue", a view held especially strongly by respondents in France.



04 Tools

What do e-Commerce businesses want from a fraud management tool?

"It is essential that if there's a suspicion of fraud, there will be no clearance at all, so the transaction is stopped."

Belgian e-Commerce business

E-Commerce businesses are clear about what they need a fraud management tool to deliver in order to be effective and appealing to them. When asked for their (unprompted) views on what it should provide, the check list was comprehensive:

- 100% watertight: giving black & white decisions rather than potential risk (particularly for small & medium e-Commerce businesses)
- Detailed levels of information to better assess and control risk
- Include basic customer and card ID checks/ IP addresses – which they would do manually anyway
- The ability to block certain countries which are prone to fraudulent activity (deemed to be a basic protocol)

"Blocking countries is extremely important, because from this, one can infer a lot. For example, when there is a Mexican email together with a US credit card in an order, we know roughly with 99% certainty that this is fraud."
(German e-Commerce business)

- Blocking based on black lists/historical offenders
- Must deliver fast results

"It should work swiftly, so that we quickly can check the customer and send out the goods in time. In the past we have sent goods and got the message (too late) that the buyer was a fraud/not trustworthy."
(German e-Commerce business)

"It has to be instant, in real time, especially when dealing with flights on daily basis."
(UK e-Commerce business)

- Include past spend behaviour/frequent failed payment attempts
- Work efficiently with little manual intervention

"Everything that makes sure that manual intervention isn't necessary anymore would be essential for me."
(Belgian e-Commerce business)

- Enable the e-Commerce business to create his/her own template of transaction levels/product type protocols
- Prevention rather than cure
- Unobtrusive for customers

"It's essential that our customers don't have too many obstacles to order their tickets. Otherwise the protection constricts the actual use of online payment."
(NL e-Commerce business)

- Cost effective

"The cost-benefit balance: what can I win or lose if I implement the system? Up to a certain degree I'd rather regulate the fraud cases I have rather than buy specific fraud detection tools."
(Belgian e-Commerce business)

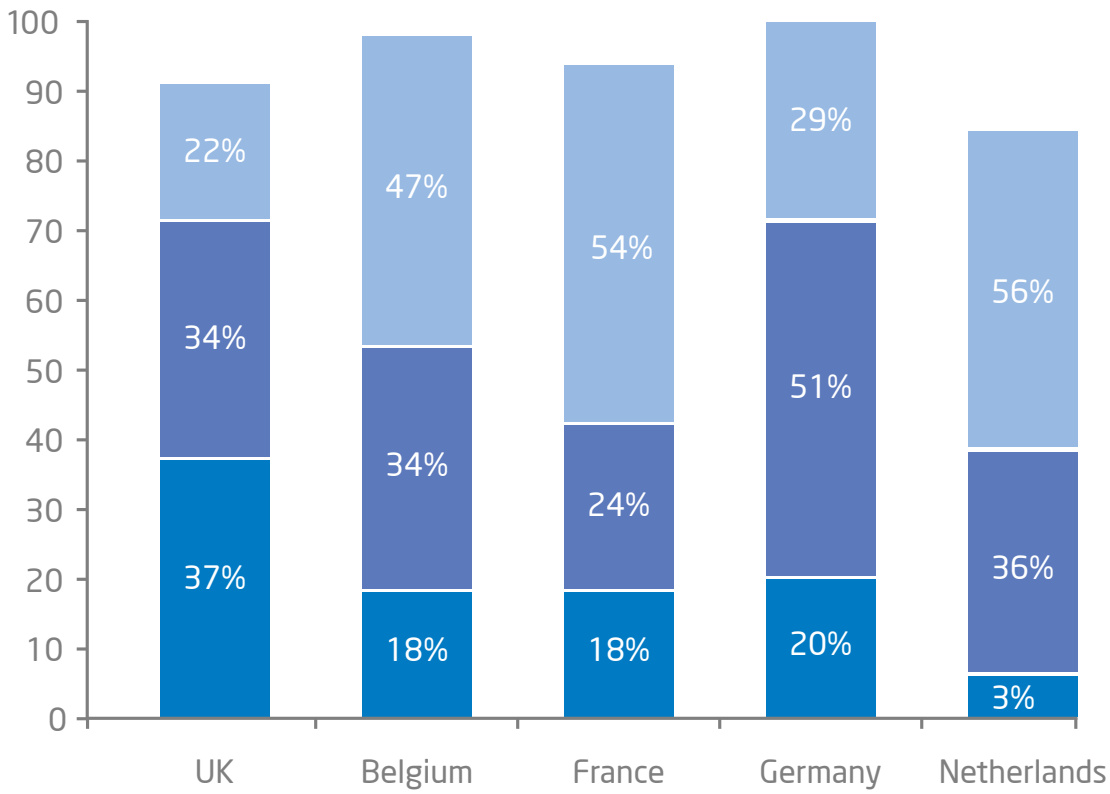
In the research, we asked e-Commerce businesses about the importance of specific features. The findings show that the single most important feature is 3-D Secure. Interestingly, 3-D Secure has a polarising effect on those we interviewed. Smaller to mid-volume e-Commerce businesses consider 3-D Secure customer authentication to be the central element of any fraud management process, larger businesses are more likely to consider it to be cumbersome, inflexible and not user-friendly.

We found that it's quite common for large businesses to switch off the 3-D functionality altogether. It is only useful to them if they can specify the trigger points for invoking 3-D Secure (eg. size of transaction, transaction type, visitor type, etc.).

What features are essential in your ideal fraud management tool?

The differences between the countries are highlighted by the businesses perceptions of what they consider most appropriate for their needs.

UK e-Commerce businesses are more likely to want the most comprehensive tool possible and the ability to develop bespoke solutions. German e-Commerce businesses are more pragmatic and accept the possibility of complex fraud slipping through the net. At the other extreme, it's the norm for French, Belgian and Dutch e-Commerce businesses to perceive that the 3-D Secure functionality is sufficient for their needs.



05 Conclusion

The main purpose of this report was to spend time talking to our customers to understand how online payment fraud affects them and what they're doing to prevent it – and most importantly, how we can help protect their businesses and their customers.

All the data that we have featured in this report shows that the future for online payments across online and mobile is set to grow across Europe – and this is good news. It gives consumers new, faster and more convenient ways to pay and it allows our e-Commerce businesses to sell their goods and services online and around the world.

But with that comes the added administration and threat linked to fraudulent activity linked to online payments. It's clear that the issue is one of scale for our e-Commerce businesses. The bigger your business is, the higher the risk is and as is the requirement for proper fraud management processes and platforms. Though the motivations to prevent fraud maybe different for e-Commerce businesses across the countries we analysed in this study, one thing is clear, all sizes of businesses are susceptible to online payment fraud and it's up to payment service providers to ensure that the new opportunity of online and mobile payments for our e-Commerce businesses remains, along with safeguarding them against the new threats.

06 Appendix

Online and mobile payments profile: across UK, Germany, France, Belgium & Netherlands:

UK

In 2012, the United Kingdom posted impressive online sales to consumers, the task for e-merchants looks likely to become increasingly complex as the market matures. UK online shoppers are the highest spenders of all, reaching €2,466 per capita in 2012. UK online sales of technical consumer goods grew 8.1% in 2012, whereas traditional retail sales dropped -0.4%. The growth of mobile-commerce is equally buoyant in the UK: 12% of all e-sales were made with a mobile phone, up from 4% in 2011 and 0.9% in 2010.

"Sales made via mobile phones in the UK have seen 300% growth per annum in the last three years. 12% of all e-sales were made with a mobile phone, up from 4% in 2011 and 0.9% in 2010."

Germany

With 37 million online shoppers, Germany has a well-developed market for e-Commerce. Its turnover in 2012 amounted to €50bn in total, 22% more than in 2011. The annual average amount spent per e-shopper exceeds €1,300. Online retail goods represented 6.4% of the German retail market. Items that sold best are clothing, electronics and books. Total distance selling of goods, including traditional mail-order (catalogue) sales and online retail goods, reached €37.5bn, up 15.6%, of which the share of online retail was 70%. German online sales of technical consumer goods grew 6.1% to €7.3bn in 2012. Traditional sales also grew to €25.3bn (1.5% in 2012).

"Germany has 37 million online shoppers; turnover in 2012 amounted to €50bn in total, 22% more than in 2011."

France

France is among the leaders in e-Commerce, occupying third position amid the internet's top ten European countries. With over 50 million internet-users, France follows Germany and the UK, which hold the second and third positions respectively. France has 42 million active internet-users and 31.7 million e-shoppers, reflecting 76% of the total number of active users, a growth of over 500% since 2000. French companies have reaped the rewards of rapidly growing broadband amongst already widespread coverage. Online sales of technical consumer goods grew by 7.0% to € 3.6bn in 2012. Traditional sales dropped -7.4% to € 19.2 bn. The annual amount spent per e-shopper exceeds €1,400, almost double the amount spent in 2007, just five years ago.

"In France, e-shoppers spent more than €1,400 p.a. each – almost double the amount spent in 2007, just five years ago."

Belgium

E-Commerce activity is increasing in Belgium. Over 78% of households now have access to the internet (compared to 60% in 2008). Belgian e-Commerce of goods and services reached €4.8bn, up 20% compared to 2011. Over 30% of e-shoppers purchased over €150 per month last year. Belgian online retailers are looking towards the future with confidence.

The vast majority of traders expect the number of online purchases to increase in 2013 and that the number of online businesses will continue to increase. Two-thirds of the online retailers intend recruiting more staff this year. This success is partly due to the tripling of the number of purchases via smartphone. The top five items purchased online is hotel bookings, fashion, event tickets, transport tickets and books.

The Netherlands

94% of Dutch households (the second highest percentage just after Iceland) now have access to the internet at home. Over 80% of the population between 16 and 74 years use the internet every day, not only at home, but also at work or school and increasingly, while out and about. In the course of just one year, access to mobile internet via smart phones has risen from 31 to 42%, and via tablets from 10 to 27%. Online sales grew 8.9% in 2012 to reach €9.8 bn.

Online shopping has become an important sector in the Netherlands. With a struggling economy and low consumer confidence, e-Commerce makes an increasingly positive contribution to the Dutch economy. The number of e-shoppers reached 10.6 million, a growth of 5% compared to 2011 and more than 20% up since 2009. In 2013, online consumer spending is expected to grow by about 9% to a value of €10.7 bn. As the increase in new e-shoppers is levelling off, growth will have to be generated by more purchases by experienced buyers.

"In 2013, online consumer spending is expected to grow by about 9% to a value of €10.7bn."

ogone

An ingenico company

www.ogone.com