THE UKCARDS ASSOCIATION

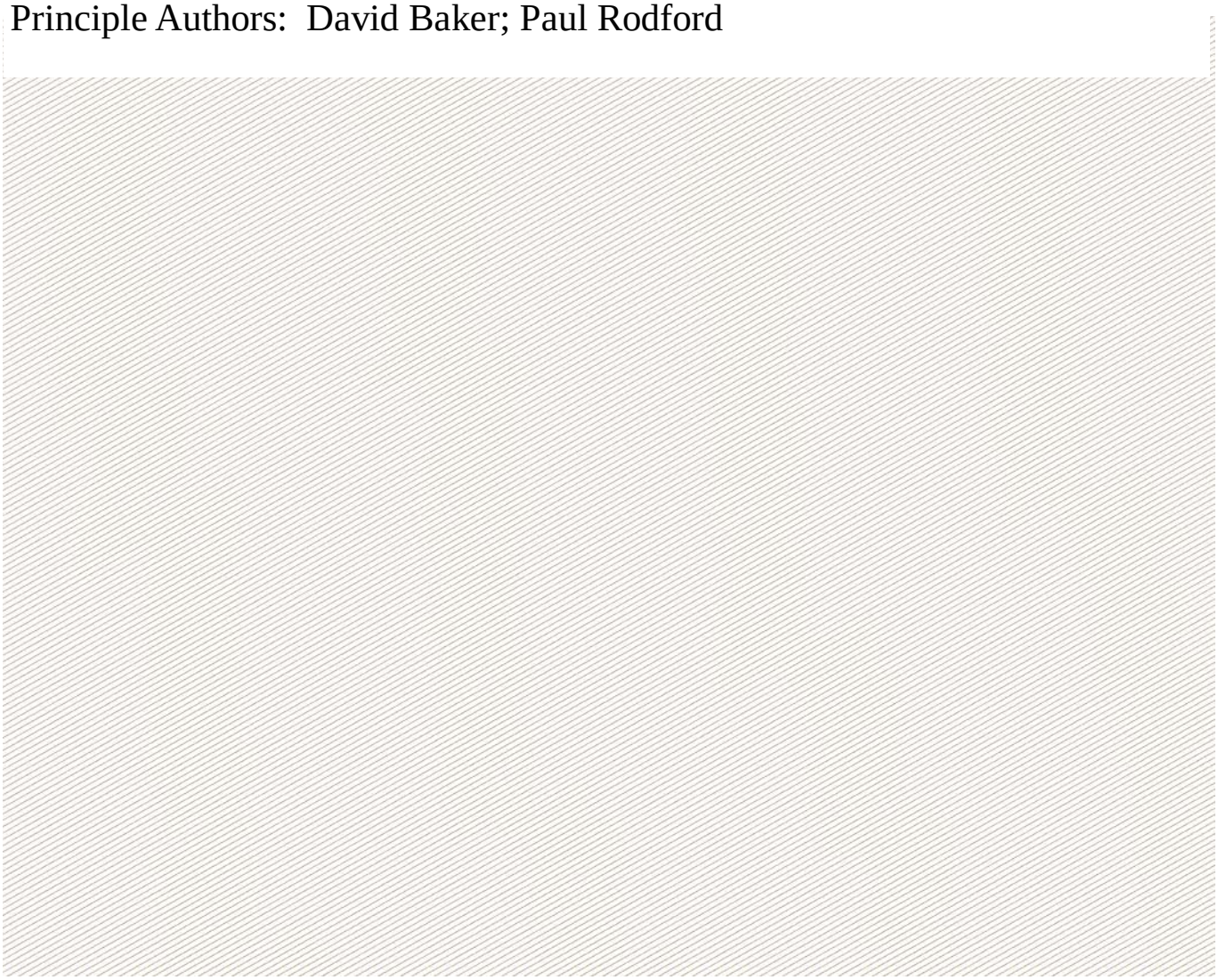
European Central Bank Paper

Recommendations for the Security of Internet Payments

Response from The UK Cards Association

June 2012

Principle Authors: David Baker; Paul Rodford



MANAGEMENT SUMMARY

1. Key Points and Themes of The UK Cards Association Response

The UK Cards Association welcomes the opportunity to comment upon the European Central Bank paper entitled *Recommendations for the Security of Internet Payments* and has provided a comprehensive response, reflecting the importance it attaches to the issues raised.

We fully support the objectives set out in the paper, namely that:

- The establishment of harmonised, minimum security requirements will contribute to fighting internet payment fraud (*though we believe that maximum harmonisation is unlikely to be appropriate*);

- Securing internet payments will enhance consumer confidence in this important business channel.

However, we have some concerns with the proposed approach which we believe has the potential to create unfair market conditions where those not bound by requirements may be able to operate more freely in the internet payments space. The ECB acknowledge that the safety of internet payments depends on the responsible behaviour of all actors, yet proposes to place the bulk of the burden of policing the environment on PSPs. In particular, acquirers are singled out as having to enforce the ECB's requirements on e-merchants, a body of actors over whom central bankers and national supervisors have no direct jurisdiction.

2. Background

The ECB asserts that the internet payments are subject to higher rates of fraud than traditional payment methods but acknowledges that publicly available information is limited. This therefore largely unsubstantiated assertion leads the ECB into proposing a regulatory framework without presenting its clear economic justification.

From a cards industry point of view the proposals appear to be based on the fact that card-not-present fraud is the most prevalent type of payment fraud and thus fails to recognise the good work that the industry has already done to address internet payment fraud which in the UK has declined from a peak of £182 million in 2008 to £140 million in 2011. Initiatives such as the introduction of 3D Secure and the compliance programmes associated with Payment Card Industry Data Security Standard (PCI-DSS) have shown that the industry takes the issue of fraud seriously and is addressing it without the need for regulatory intervention.

In addition, retailers have contributed to the reduction with their own sophisticated fraud screening tools. The UK Cards Association suggests that the ECB should assess the adequacy of these programmes (to ensure they cover the main recommendations) and their effectiveness before considering the introduction of additional requirements that may conflict with, and potentially require the unravelling of, existing legislation and/or industry initiatives.

The proposals also fail to recognise the global nature of internet payments in the cards space and suggest that European regulation will be sufficient to address fraud and enhance consumer trust. There is no evidence to suggest this is the case and, with an increasing amount of international trade, one could argue that only global initiatives will be truly effective. There is a genuine risk that by focusing on European regulation the European market would be placed at a disadvantage. This would lead to the conclusion that controls implemented by the global payment schemes will be more effective.

The ECB assumes an ideal world where all issuers, acquirers, schemes, e-merchants, consumers and transactions are homogenous and that a one-size-fits-all set of information security requirements can be implemented equally across all actors. In implementing the PCI-DSS the card industry has found that this is an unrealistic aspiration and that setting strict requirements can cause greater problems than those they are attempting to address.

For example, PCI-DSS compliance requirements assume a particular implementation model which is not always matched by real world experience. Where such cases exist, enterprises have had to enter complex negotiations with the schemes to understand which of the requirements apply to them and which don't. Delays in resolving issues have unnecessarily increased the overall cost of compliance programmes for some. Unless regulators are very clear about the ECB recommendations a similar situation is likely to result.

Finally, page 4 of the ECB paper makes it clear that its recommendations are applicable to all Payment Service Providers (PSPs) as defined in the Payment Services Directive (PSD). We understand that this definition exempts e-money institutions including, for example, PayPal. No explanation or justification is given for this exemption which will inevitably create an uneven playing field, skewing the market in favour of e-money institutions. No assessment is made in the paper of the payment volumes or fraud experience of such alternative payment methods, despite the fact that we know that 35% of UK adults use Paypal for making e-commerce transactions[1].

Overall, whilst the paper's intentions are in the right place, the overall impression is of a document that is, to date, under-researched and is therefore an insufficient basis for introducing profound and far-reaching regulation. In many cases the paper is written as if the industry has not considered the issues discussed which is simply not the case.

[1] During 2010 35% of online shoppers (around 13 million UK adults) used PayPal online and a smaller number (around 3 million) used other methods such as cheques, vouchers, Neteller and Nochex or charged items to their internet service provider account. Over the first half of 2011 just over 15 million UK adults (or 41% of online shoppers) had used PayPal to purchase goods and services over the previous year.

3. Conclusions and Recommendations

The UK Cards Association welcomes the opportunity to comment on the ECB's recommendations but believes that the current analysis of the market and the scope for improvement has not been subjected to the required level of analysis to enable firm recommendations to be made and regulations developed.

In particular the ECB needs to give careful consideration to striking an appropriate balance between security and consumer convenience in order that internet commerce is not made too cumbersome for consumers and that recommendations do not result in an economic setback, especially during harsh economic times.

It would therefore seem sensible to us for the ECB to:

- gather more information about the state of play across the whole of Europe;
- take a considered view on the effectiveness of existing self-regulatory regime embodied in card scheme requirements and establish the level of non-compliance;
- engage more fully with the card payments industry, e-commerce retailers and consumers in order to assess the need for regulation;
- conduct consumer research to establish consumers' reaction to the recommendations and the changes to the customer experience that would result;
- use this information to help build a cost/benefit case for each of the recommendations;
- in the event that regulation is required, should consult with stakeholders on setting realistic timescales (to avoid the need for widespread waivers);
- carry out further investigations into the emerging mobile payments marketplace in order to understand better the complex relationships between wallet providers, consumers and their payment service providers.

4. A Positive Agenda for European Payments

It is timely that the ECB should issue these recommendations at the same time as the European Commission (EC) is considering responses to its recent Green Paper on cards, internet and mobile payments[2]. In our response to the EC Green Paper we raised a number of issues that are also relevant to the ECB recommendations. It is appropriate that we share these with the ECB in order that it might consider joint initiatives with the Commission. It is important that any regulatory intervention in this area fosters an environment where market growth and innovation thrive and are not hindered through the inadvertent consequences of well-intended regulation.

The UK Card Association's suggestions in response to the recent EC Green Paper are shown in the box below.

Recommendations from The UK Cards Association's response to the EC Green Paper on cards, internet and mobile payments (April 2012)

The following extract from our response to the EC's Green Paper are relevant to both the ECB and the Commission as both institutions have a pivotal role in ensuring that Europe is at the forefront of payment innovation.

"We have identified the following supporting activities where the European Commission could be of assistance, and would suggest that, in priority order:

- *the Commission should urgently engage with the payments industry to review existing legislation such as the Payment Services Directive (PSD) and the Consumer Credit Directive (CCD), with the objectives of (i) accommodating a mobile payments world and (ii) identifying and removing any aspects that are inadvertently inhibiting the development of e-commerce and m-commerce;*
- *the Commission should assess the risk to the integrity of the payment system of (new and emerging) PSPs who may have a lesser regard for, or focus on, credit and fraud risk and what measures might be necessary to ensure that PSPs do give due regard;*
- *the Commission should seek parallel commitments to 'SEPA for cards' from other relevant industries and players who may be instrumental in delivering m-payment products and services;*
- *the Commission should set out guidance on the appropriate scope for collaboration of different sectors to deliver against a vision for e-commerce and m-commerce;*
- *the Commission should undertake research to fully understand why consumers and retailers in other member states have not yet embraced e-commerce as much as the UK, Australia and the US, including what products and services they might be interested in purchasing cross-border online;*
- *the Commission should undertake research to fully understand consumers' propensity to make payments beyond Europe;*
- *the Commission could evaluate how merchants in different sectors with cross-border reach adapt their business models and websites to local conditions.*

[2] http://ec.europa.eu/internal_market/consultations/2012/card_internet_mobile_payments_en.htm

Contents

A. The UK Cards Association

The UK Cards Association is the leading trade association for the payment card industry in the UK. The Association is the industry body of financial institutions who act as card issuers and/or merchant acquirers in the UK payments market.

The Association is responsible for formulating and implementing policy on non-competitive aspects of card payments. Members of the Association account for the majority of debit and credit cards issued in the UK, issuing in excess of 54 million credit cards and 86 million debit cards at the end of 2011, and covering the whole of the plastic transactions acquiring market.

The Association promotes co-operation between industry participants in order to progress non-competitive matters of mutual interest and seeks to inform and engage with stakeholders to advance the industry for the ultimate benefit of its members' consumer and retail customers. As an Association we are committed to delivering a card industry that is focused on improved outcomes for the customer based upon robust evidence.

This document contains a detailed response to the ECB's *Recommendations for the Security of Internet Payments*.

The UK Cards Association is an evidence-based organisation which believes that policy decisions and proposals should always be based on the strongest possible evidence. It seeks to provide evidence to back up its points and is wary of anecdote and unsubstantiated assertion. Hence there is an underlying concern regarding the absence of detailed analysis and quantifiable evidence provided by the ECB which would have helped discussion of the issues raised and assisted responders in responding.

The UK Cards Association works in partnership with Financial Fraud Action UK, the name under which the financial services industry co-ordinates its activity on fraud prevention, on industry initiatives to prevent fraud on credit and debit cards.

Given The UK Cards Association and Financial Fraud Action UK's role and lengthy track record in card fraud prevention (dating since the early 1990s) it is disappointing that we were not among the bodies consulted in the preparation of the ECB paper mentioned on page 4, which mentions a fact-finding exercise and consultation with PSPs, technical service providers and e-merchants (despite FFA UK being mentioned in footnote 1 on the same page).

B. Comments on the ECB Recommendations for The Security of Internet Payments

General Part

ECB Introductory Notes

In the general introduction the ECB sets out its justification for recommendations which aim to improve the security of internet payments and ultimately to improve consumer confidence in the payment channel. These are welcome aims and are supported by the cards industry in the UK which has sought to be at the leading edge in the fight against fraud. This has been achieved by providing consumers with secure payment services that offer the appropriate balance between usability and security.

As part of the justification for the ECB paper, footnote 1 on page 4 paper states that card-not-present fraud has become the most prevalent type of payment fraud, but fails to acknowledge that this type of fraud, in common with card fraud more generally in the UK, is in decline and reducing as a proportion of turnover.

The UK Cards Association would, however, suggest that a number of the arguments and assumptions made by the ECB, in this paper, may rely on incomplete and potentially inaccurate analysis. To address these, and therefore validate the ECB's proposals, The UK Cards Association would propose that the following would assist the ECB in validating its proposals:

- Scale the size of any problem to show that regulatory intervention is justified or necessary;
- Provide an impact assessment either on the levels of fraud or wider business implications;
- Provide a cost/benefit analysis which would help assess the proportionality of the recommendations to the size of the problem;
- Present evidence as to the opinions of merchants or consumers on the recommendations sourced from, for example, consultation or market research;
- Describe or explain the shortcomings that the ECB perceives to exist in how the market currently manages risk and fraud;
- Consider the appropriate balance between security and consumer convenience and usability;
- Quantify the use, and fraud experience, of alternative e-commerce payment methods (such as PayPal) who are exempted from the recommendations and who stand to benefit from any skew in the market.

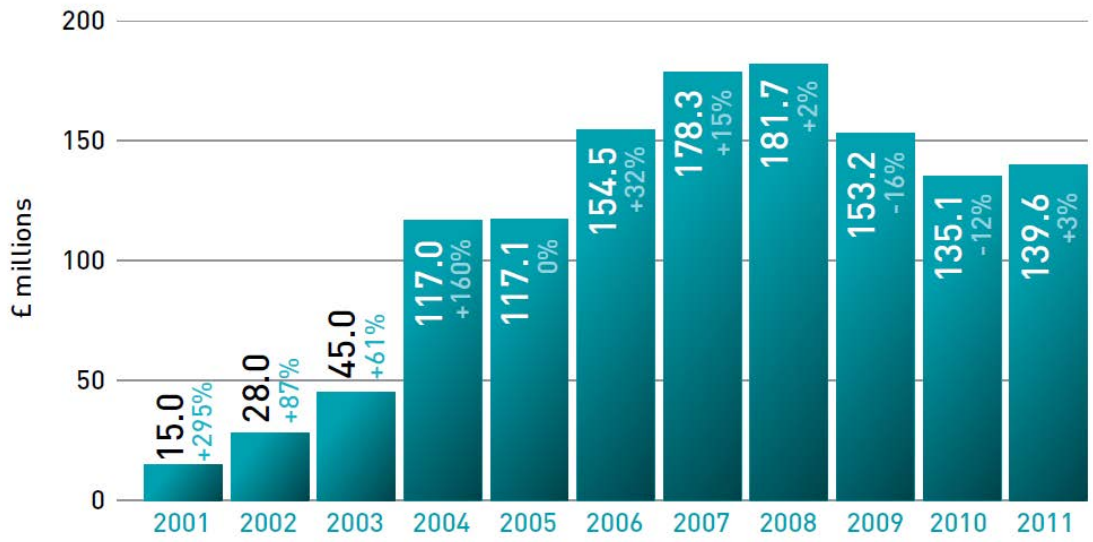
The assumption that internet payments made using cards are subject to major weaknesses and vulnerabilities is therefore unproven and not a point of view with which we would agree. The ECB acknowledges that EU-wide data on fraud is limited and cites the UK and French examples where Card-Not-Present fraud (CNP) has become the most prevalent type of fraud. Without a more rigorous collection of data and evidence it is difficult to regard the recommendations as anything other than a list of ideas, some of which may be good, some of which may be bad, but none of which have been, in our view, adequately justified.

Card-Not-Present (CNP) Fraud In the UK

CNP fraud is indeed the single largest fraud type in the UK but the total figure reported includes mail and telephone order fraud which would be unaffected by the implementation of the ECB recommendations. Estimates suggest that of the £220.9 million CNP fraud reported in 2011, £139.6 million (63% of the total) was attributed to internet payments (see table below). This proportion has been declining in recent years as the industry's anti-fraud initiatives, including the continued growth in use of 3D Secure, takes effect.

INTERNET/E-COMMERCE FRAUD LOSSES ON UK-ISSUED CARDS 2001-2011

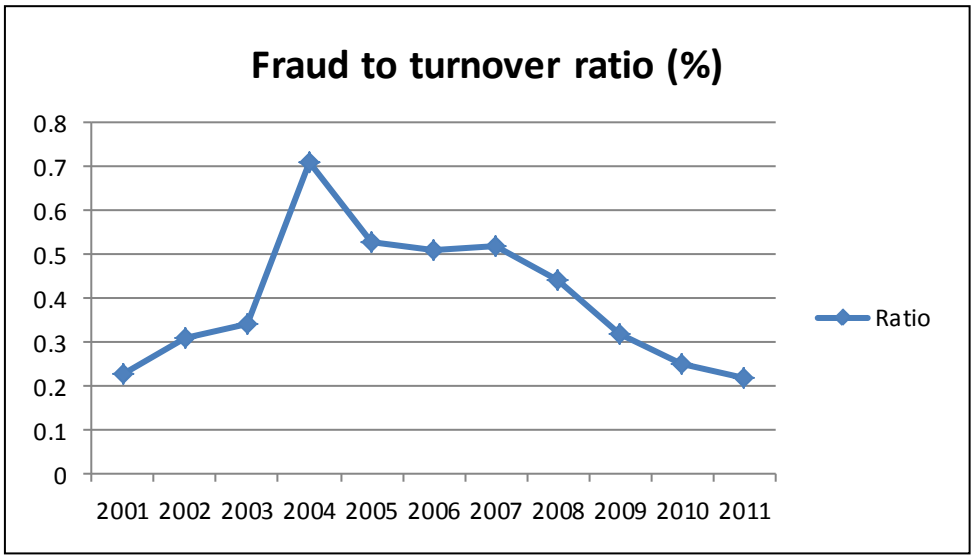
Tinted figures show percentage change on previous year's total. All figures estimated.



These figures should also be considered in the context of the increased use of internet card spending by consumers which has risen ten-fold from £6.5 billion in 2001 to £63.2 billion in 2011 (see Appendix 1 Charts 5 & 6).

In common with overall card fraud, the fraud to turnover ratio for internet/e-commerce transactions (using UK Payments Council figures for e-commerce turnover[3]) has been in sharp decline in recent years, falling from a peak of 0.707% in 2004 to 0.221% in 2011, as shown in the following table.

Fraud to Turnover Ratio for Internet / E-commerce Losses on UK-Issued Cards 2001-2011



According to Barclaycard[4], the fraud-to-turnover ratio varies markedly between 3D secure and non-3D secure transactions. Barclaycard's advice to merchants is as follows:

> *"To improve your fraud to sales ratio in the e-commerce space, think about authentication through 3D Secure. As at September 2010, Verified by Visa (VbV) penetration in the UK was 53.3% and 90% of the UK VbV volume was fully authenticated. This reduced the fraud-to-sales ratio on fully authenticated transactions to 0.08%, compared to 0.25% for non VbV traffic."*

This information alone shows the effect of 3D Secure as it is currently implemented and raises questions over the case for stronger authentication.

[3] NB: the e-commerce turnover figures used in the above are calculated and published by the UK Payments Council. Given this different source the resulting fraud-to-turnover ratio may not be directly comparable with fraud-to-turnover ratios quoted elsewhere. However, it is the long term trend that is important.

[4] Barclaycard Payment Security Newsletter – Issue 1 – January 2011

It is our understanding that the recommendations are not intended to apply to e-money institutions, including PayPal. However, no assessment or comparison has been made between cards, PayPal or other alternative online payment methods, despite the fact that in 2010 PayPal was used by 35%[5] of UK adults to purchase online (41% for the first half of 2011) and a smaller number (around 3 million) used other methods such as cheques, vouchers, Neteller and Nochex or charged items to their internet service provider account. No assessment is made of fraud associated with non-card online payment methods.

[5] Source: UK Payments Council Internet Monitor XVII June 2011

UK Card-Not-Present Fraud in Context

In the broader context the UK's National Fraud Authority estimated there to be a total of £73.0 billion of fraud losses in the UK, according to its Annual Fraud Indicator 2012[6].

- Of this total, some £3.5 billion (less than 5% of the £73.0 billion) was accounted for by the financial and insurance industries;
- Of this, £341.0 million was related to plastic card fraud (2011 figures) (see Appendix 1 Charts 1 & 2);
- Of this, £220.9 million (65% of the £341.0 million) was related to card-not-present (CNP) fraud in 2011 (see Appendix 1 Chart 4);
- Of this, £139.6 million (63% of the £220.9 million) was attributable to internet payments, in the UK, a country that leads Europe in terms of the number of adults purchasing online and the amount spent per adult purchasing online (see chart on page 9);
- The £139.6 million of online card fraud accounts for less than 0.2% of the total £73.0 billion of fraud in the UK.

Total fraud losses on UK cards fell by seven per cent between 2010 and 2011 to £341.0 million. This is the lowest annual total since 2000 and follows on from a fall of 17% in the previous year and 45% from the 2008 peak.

Card-not-present (CNP) fraud encompasses phone, internet and mail-order fraud. The crime most commonly involves the theft of genuine card details that are then used to make a purchase. The vast majority of CNP fraud involves the use of card details that have been fraudulently obtained through methods such as skimming, hacking into retailers' data connections, or through unsolicited e-mails or telephone calls. The card details are then used to undertake fraudulent CNP transactions over the internet, by phone or by mail-order.

CNP fraud accounts for 65% of all card fraud but these losses have to be seen in the context of a massive growth in CNP spending over the past ten years especially over the internet. The estimated total value of internet spending in 2011 was £63.2 billion – an increase of 18% on the previous year (£53.6 billion in 2010).
In light of this growth it is all the more impressive that CNP fraud has fallen for the third successive year.

So whilst card usage and transaction volumes continue to grow, card fraud losses against total turnover – at 0.06% - continue to decrease (see Appendix 1 Chart 3) and have now fallen by 33% in the past two years.

The reasons behind the continued decrease include the increasing use of sophisticated fraud screening detection tools by retailers and banks, as well as growth in the use of American Express SafeKey, MasterCard SecureCode and Verified by Visa by both online retailers and cardholders. These online fraud prevention initiatives add an extra layer of protection to shopping online. Cardholders simply register their card when prompted and create a password that they will be asked to provide at participating retailers. More than half of all cards issued in the UK have been registered to date.

The UK card industry's BeCardSmart Online campaign[7], launched at the end of 2008, provides UK consumers with straightforward practical tips to help them shop safely on the internet.

It does not seem to be an area where there are major weaknesses and vulnerabilities to address. It would seem sensible for the ECB to gather more information about the state of play across the whole of Europe before introducing additional regulatory requirements.

[6] http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/annual-fraud-indicator/annual-fraud-indicator-2012?view=Binary
[7] http://www.financialfraudaction.org.uk/Consumer-be-card-smart-online.asp

Experience of the implementation of PCI-DSS suggests that the cost of compliance can, in some cases, be greater than the fraud it is designed to address, hence the importance of a detailed cost/benefit analysis.

For card payments many of the ECB requirements are already included in compliance programmes from the international card payment schemes. The ECB should first establish the level of non-compliance in order to assess the effectiveness of self-regulation. It is The UK Cards Association's view that card issuers and acquirers are already subject to sufficient control in the internet payments space.

Scope and Addressees

The ECB makes it clear that the recommendations, key considerations and best practices are applicable to PSPs as defined in the Payment Service Directive 2007. Limiting the scope to the PSPs alone seems to ignore the important role played by other actors in the ecosystem – including those who may provide internet payment services to consumers such as PayPal, Neteller and Nochex. This seems to create an uneven playing field and place PSPs at a disadvantage, as well as being in contradiction of the comment on page 6 of the ECB's paper that says that "*the recommendations are formulated as generically as possible to accommodate continual technological innovation*".

Placing the burden of policing internet payments on PSPs alone ignores the potential for others to provide weaker payments solutions that will perpetuate the fraud problem and undermine consumer confidence in the payments channel. It is The UK Cards Association's view that, should regulation be required, it must apply equally to all actors in the internet payments ecosystem to have any worthwhile impact and to not skew the market.

Guiding Principles

Four guiding principles are listed as the basis for the recommendations that follow. All are broadly accepted by the cards industry.

Risk Assessment – The ECB calls upon PSPs to carry out regular risk assessments on the specific issue of internet payment services. The ECB fails to acknowledge that, from a business point of view, looking at one business process in isolation may not be appropriate and that the provision of internet payment services must be looked at in the context of the wider business relationship that PSPs have with their customers.

Almost every financial institution conducts risk assessments in order to develop their business and information security strategies. It is not clear why the ECB feels it is necessary to intervene in what could be a competitive area of a PSP's business.

Strong Authentication – The ECB defines strong authentication as requiring two of three authentication factors or 'elements' (knowledge, ownership, inherence). In the guiding principles it suggest that 'elements' must be mutually independent – i.e. "*the breach of one does not compromise the other(s)*". It is also suggested that "*At least one of the 'elements' should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet*".

The wording also discusses elements as though they are interchangeable and as though "two or more" can be combined in an ad hoc manner.

These definitions are not ideal and it seems over-optimistic to call two or three factor authentication 'strong'. It is important that the right combination is chosen. There are many variables – such as tokens and biometric choice – that can affect security. Also, not all examples of the 'possession' factor are equal. A mobile phone is given as an example of 'something only the user possesses', but mobile phones are not secure devices and cannot be directly compared with, say, smart cards or tokens.

The ECB should recognise that mutual dependence is not necessarily undesirable. Authentication solutions such as a biometric match-on-card, and offline Chip & PIN (EMV as implemented in the UK), might be forbidden if the wording of this principle is taken at face value.

Equally the ECB should recognise that 'elements' are not as interchangeable as the wording suggests. For example, if the two factors were a secret and a biometric, how could one of them be non-reusable and non-replicable? And (for internet payment) how could they be input and protected if not through a token?

The definitions for 'strong' authentication need to be more carefully considered.

The principle also suggests that PSPs relying on weak authentication procedures cannot, in the event of a dispute, provide proof that the customer has authorised the transaction. No attempt is made to define 'weak' authentication (as opposed to 'weaker' authentication), nor why, for example, static passwords are no longer considered acceptable by the ECB. There is danger in such a loose statement and the crossover with PSD liabilities will need to be considered.

Authorisation – The ECB's requirement for authorising transactions and monitoring for abnormal activities is well understood and accepted. Scheme requirements expressly require card based internet payments to be authorised by the issuer.

Customer Awareness – The ECB suggests that PSPs should engage in customer awareness and education programmes on security related issues (though provides no detail on what this might mean or how effectiveness might be monitored). We agree with this principle but would draw attention to the fact that industry level communications can be most effective.

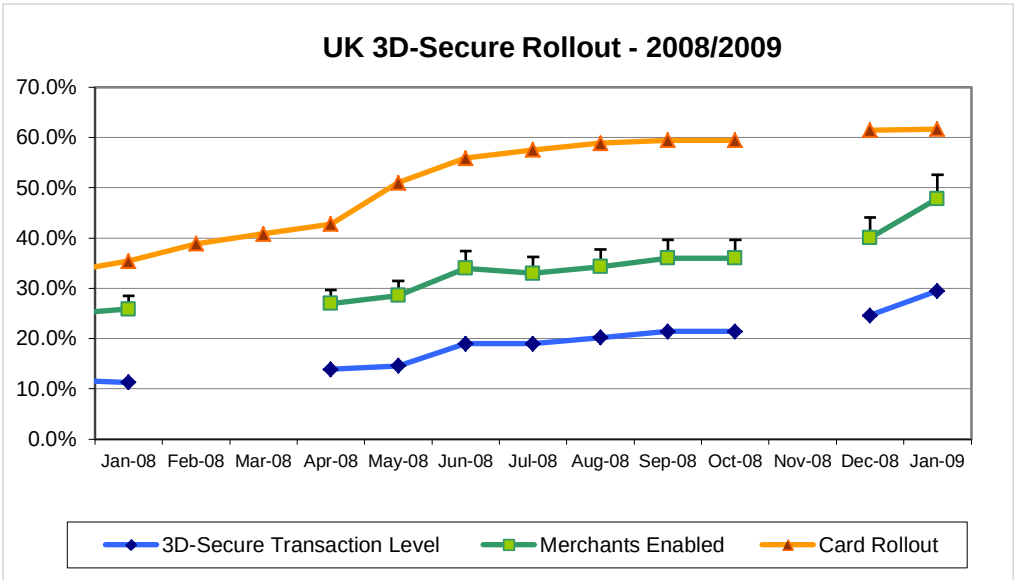
The UK is fortunate to have bodies such as The UK Cards Association and Financial Fraud Action UK through which such campaigns can be managed on behalf of the entire industry and has a history of successful educational campaigns such as that around chip & PIN (2004-2006); BeCardSmart[8] (2008 onwards); and The Devil's in Your Details[9] (2012) (see Appendix 2).

Implementation

The paper indicates the need for regulation to promote security of internet payments but makes no case to justify such measures. The card industry is sceptical of the need for regulation (especially where there is no precedent) and can point to the measures that it has already implemented to secure card based payments as evidence of a self-regulatory regime that is already addressing the core issues.

To provide stronger authentication, 3D Secure solutions are gaining greater market penetration and compliance with the PCI-DSS addresses many of the recommendations included in the recommendations. However, mass adoption by merchants and consumers, both of which are needed, cannot be achieved overnight.

By way of example, the table below shows the rate at which 3D-secure was adopted in the UK during the period 2008/2009, in terms of the numbers of cards 3D-secure enabled, the number of merchants enabled and the impact of 3D-secure transaction levels and shows that, even with the will to do so, adoption of such initiatives in mass markets is inevitably a gradual process.



NB: gaps in the above time series are due to data not being available

[8] http://www.financialfraudaction.org.uk/Consumer-be-card-smart-online.asp
[9] http://www.financialfraudaction.org.uk/consumer-protecting-your-personal-information.asp

The ECB should engage more fully with the card payments industry and e-commerce merchants in order to assess the need for regulation.

It is proposed that implementation of the recommendations be through national authorities using domestic legislation. It is difficult to imagine that this will result in a consistent implementation or enforcement across European member states, something which is more realistically achieved by the international card schemes.

Requiring implementation of all the recommendations by 1 July 2014 is challenging and probably unrealistic. To avoid the need for widespread waivers the ECB should consult with stakeholders on setting realistic timescales.

C. Recommendations

Recommendation 1 – Governance

It is unclear what purpose the ECB sees in a separate internet security policy unless it is expected that this would be subject to specific review and approval by regulators, who would need appropriate resource and expertise to evaluate such policies.

The provision of internet payment services should not be seen as a stand-alone function but as part as a PSP's overall relationship with its customers and the product portfolio they offer. Risk assessments should therefore be carried out with due consideration for a PSP's overall business model and risk appetite.

In KC 1.2 the ECB suggests an independent risk management function should be responsible for internet payment services and for managing sensitive payment data. There is no justification presented for this and, in most cases, it is more desirable that integrated risk management functions take a more holistic view of a PSP's risks.

No assessment is made of how domestic regulators would view a formal pan-European internet payment services policy or how it is envisaged that there would be consistent enforcement or sanctions, the lack of which would risk the flight of merchants and/or acquirers to countries where enforcement was considered weaker.

Recommendation 2 – Risk identification and assessment

We support the regular review of changing threats and vulnerabilities in the internet payments space and certainly welcome the call for changes to internet security measures in light of any significant changes to the threat landscape.

The ECB should recognise the difficulties PSPs have in enforcing changes across the ecosystem and therefore the effectiveness of any proposed changes or interim measures, in particular for card payments, where the changes require global support.

Recommendation 3 – Monitoring and reporting

KC 3.2 – The requirement for the immediate reporting of major security incidents should be considered in light of the potential for separate data protection legislation currently being considered by the European Commission and not introduced as an independent part of a payments-related compliance programme. There is potential crossover of recommendations here with existing and proposed data protection legislation, with no explanation given as to the shortcomings of the existing regime that would justify additional requirements relating to internet payments.

Recommendation 4 – Risk control and mitigation

Whilst it is not unreasonable to expect PSPs to implement security measures in line with their own internet payment services policy, it is often the case that measures need to be tempered in light of market conditions and the availability of user friendly products and services. For PSPs engaged in the cards business it is desirable that, for the sake of interoperability and usability, common solutions are deployed.

The ECB presents a series of key considerations that are specific in their nature but may not be applicable in all cases. For example, in KC 4.2, the ECB assumes a particular architecture and suggests the use of firewalls and proxy servers to protect against man-in-the-middle and man-in-the-browser attacks without saying how.

The same key consideration suggests the use of extended validation certificates drawn up in the name of the PSP to enable customers to check a website's authenticity, assuming that it is a realistic expectation.

KC 4.6 calls for PSPs and card payment schemes who are outsourcing 'core functions' to include provisions requiring compliance with the ECB recommendations in contracts. The ECB would need to provide greater clarification of what it defines as 'core functions' in order to ensure correct application of this key consideration.

KC 4.7 is the first of a series of suggestions that, in the cards space, acquirers should 'require'[10] that e-merchants implement security measures equal to those required of the PSPs. This appears to be an attempt by regulators to achieve jurisdiction over e-commerce merchants through an already regulated third party i.e. the acquirers. The UK Cards Association disagrees with this approach as a matter of principle.

In many cases e-merchants have implemented fraud control and management routines in accordance with their own risk profile and fitting with their own customer service proposition. In some cases these may be at odds with the expectations of the ECB. It is not clear how PSPs can implement these recommendations without threatening their business. Whilst other actors are able offer alternative internet payment services e-merchants are likely to turn to them to maintain the user experience. Merchants such as Amazon rely on the ease of use of one click services to attract and maintain customers[11].

[10] E.g. see also BP 5.1 and KC 11.3

[11] Although The UK Cards Association does not have such information, we believe that online merchants will have statistics on the rates of abandoned transactions attributable to cumbersome secruity, something merchants will be keen to avoid.

It is not clear what consequences or sanctions might arise as a result of KC 4.7. If it is intended that European acquirers are to be unable to provide services to a merchant because the merchant is regarded as not implementing sufficient security measures (such as Amazon) then the potential impacts are that (i) the merchant will source acquiring services from outside of Europe or perhaps (ii) move the location of their business outside of Europe whilst still serving the European consumer market.

Where PSPs 'require' e-merchants to have specific measures in place, no consideration is given to the effort or additional cost of auditing compliance. If a merchant falsely self-certifies that they are compliant – self-certification presumably being the cheapest and most tempting option – it would not become evident that they were not compliant until a breach occurs. If they are unable to audit compliance, is it again meant that acquirers do not offer services to such e-merchants?

Ultimately, e-merchants should be accountable to themselves when it comes to protecting themselves against fraud.

Recommendation 5 – Traceability

These recommendations need more careful consideration. The unnecessary storage of transaction information runs contrary to advice included in other security standards. The PCI-DSS, for example, encourages actors to reduce the risk of data loss by not storing data unless absolutely necessary (Requirement 3). The ECB recommendation should be considered against an organisation's data retention and disposal policies.

With regard to BP 5.1, in recommending that e-merchants have such processes in place the ECB runs the risk of perpetuating a problem that the PCI-DSS compliance process has gone a long way to eradicating i.e. the unnecessary retention of sensitive data. Acquirers should not be expected to reverse existing advice and guidance, especially if it means a lowering of standards.

Recommendation 6 – Initial customer identification, information

From a cards point of view these recommendations are vastly onerous with no tangible benefit to be derived. They are likely to be costly and, in some cases, would be unworkable. For example, in BP 6, it suggests that consumers should sign a dedicated service contract before being able to transact on-line. The ECB does not suggest how the retrospective enrolment of over 40 million consumers in the UK and many millions more across Europe might be achieved. In all likelihood, inertia will mean many millions of consumers failing to enrol, resulting in a setback to internet commerce and significant inconvenience to consumers and merchants alike, with unquantifiable economic implications.

No assessment has been made of how consumers might react to this recommendation and the impact on e-commerce through the shifting of the current balance between security versus convenience towards increased security. KC 6.1 essentially means that consumers need to have their PSP's permission to shop online, something which would not happen in respect of high-street retailers (where non-CNP fraud, through counterfeit, lost & stolen fraud, card ID theft and mail non-receipt, still accounts for £108.7 million of card fraud, compared to the £139.6 million of CNP online fraud).

Recommendation 7 – Strong customer authentication

The need to strengthen authentication processes commensurate with the risk associated with a transaction is understood. The ECB suggests that **all** internet payments require 'strong authentication' – a view that could be ultimately be an inhibitor of internet commerce with unquantifiable economic implications. A number of existing e-commerce transaction processes will be disallowed under these recommendations, for example the 'one-click' processes requiring pre-registration of accounts, arrangements which are extremely popular with consumers. E-merchants offering such convenience would be non-compliant. It is not clear what business justification the ECB sees in requiring strong authentication for all internet payments.

Requirements for cards make no allowance for the legacy environment that most PSPs work in. KC 7.3, for example, would require the re-issue of cards in order for them to be pre-registered and issuers would need to seek permission from their customers prior to the customer being allowed to use online services. No assessment is made of how consumers might react to such requirements which place security over convenience.

In KC 7.6 the ECB suggests liability shifts from e-merchant to issuer across European markets. This fails to recognise the global nature of internet payments. Before proposing such changes the ECB should engage with international counterparts in order to ensure that they do not disadvantage European stakeholders by inadvertently favouring merchants that are not bound by these recommendations.

KC 7.7 places requirements on providers of wallet solutions without considering the impact on an emerging technical implementation. For example, it is unclear whether a CVx2 would even be available in a wallet solution. The ECB should carry out further investigations into the emerging mobile payments marketplace in order to understand better the complex relationships between wallet providers, consumers and their payment service providers. For example, it is not clear how, unless the industry comes up with a common method of providing strong authentication, a wallet provider (who may not be a PSP) can be expected to support all of the possible options for providing strong authentication.

Recommendation 8 – Enrolment for and provision of strong authentication tools

The recommendation suggests an incomplete understanding of the variety of means of delivering security tools or credentials to consumers. For example, KC 8.1 would rule out internet or e-mail delivery where, in fact, there are secure processes in common use today. This same requirement would require a stateless card reader used for chip authentication to be delivered securely when in fact they contain no security credentials or secret key data. We believe that the delivery mechanisms used by PSPs should be a risk-based decision made against an assessment of individual market conditions.

The UK Cards Association proposes that the ECB carry out a more detailed investigation into the current state of the market in order to better understand what is and is not viable before enforcing requirements on the market.

The economic argument for strong authentication over weaker authentication remains to be proven given the fraud-to-sales ratio for fully authenticated Verified by Visa transactions of 0.08% (mentioned on page 10).

Recommendation 9 – Log-in attempts, session time-outs & validity of authentication

Such measures are implementation specific and should not be subject to regulation. It should be left to the PSP to establish their own rules based on their customer base, their risk assessment and their risk appetite.

Recommendation 10 – Transaction monitoring and authorisation

The need for real time or near-real time monitoring is recognised but such monitoring should always be proportionate to the level of risk associated with the transaction or the strength of the security measures used to execute the transaction. The ECB recommendations should make allowance for PSP's differing risk appetites and control frameworks before suggesting a one-size-fits-all approach.

KC 10.2 suggests the use of harmonised e-merchant categories without saying why they are required or how they would be monitored in use. There are already international standards for merchant categories.

Recommendation 11 – Protection of sensitive information

In the cards industry, requirements to protect sensitive data are already covered by the application of the PCI-DSS. It is not clear why the ECB sees any additional requirements as being necessary as the paper does not define what data is considered to be sensitive in the context of this recommendation. It is essential that these be better explained in order that the market can get a better understanding of what is being required and its potential impact.

Recommendation 12 – Customer education and communications

The idea that consumers would agree a secured channel for on-going communications with each of their PSPs, be it a (presumably costly) letter with acknowledgement of receipt signed by the customer, a dedicated mailbox on the PSP's website, or a secured website to receive information regarding the correct use of internet payment service appears to us to be unrealistic. No assessment is made of whether consumers would see any benefit in such communications, especially if there are barriers to be overcome in accessing it, or of the costs associated with obtaining such agreement retrospectively.

The ECB recommends that PSPs should initiate customer education and awareness programmes without defining what it thinks such communications might involve. For example, no explanation or consideration is given to the scale of such communications or how often, which are critical factors, nor how this might be embodied in regulation. No consideration is given as to whether or how it might be established that such communications are effective, however 'effective' might be defined.

The ECB should not ignore the potential for centralised customer communications and education to be effective in raising customer awareness of security issues. The UK Cards Association and Financial Fraud Action UK have a history of leading highly successful industry-level campaigns including 'BeCardSmart, and 'The Devil's in Your Details' (see earlier comments under 'Customer Awareness' and Appendix 2).

Consumer awareness and understanding of online security and how they might protect themselves is relevant to all online activity covering all types of products and services, including social networking, not just payments. Obliging one business sector to take responsibility for such activity in isolation does not make sense to us.

Communications in an area such as online security should not simply be a matter of meeting regulatory obligations. Strategies aimed at conditioning consumers *en masse* to adopt different behaviours (e.g. to stop smoking; to wear a seat belt) often take many years and represent long term investments. To suggest that obligations to make one-off tactical communications will achieve such conditioning is to misunderstand consumer communications which, in this instance, might be regarded as a form of public information provision.

Recommendation 13 – Notifications, setting of limits

As with Recommendation 9, the ECB is straying into the competitive space where PSPs should be left to manage spending limits based on their own risk assessment and appetite. Such measures should not be subject to regulation.

No assessment is made of whether consumers would see any benefit in setting spending limits within an already agreed credit limit or overdraft limit; whether they would understand or appreciate it; how this might be achieved retrospectively (in the UK, for around 147 million credit and debit cards already in circulation); how much this might cost; what benefit it delivers; or what impact this would have on consumer spending and the wider economy.

Further, no consideration is given as to how consumers might judge for themselves an appropriate online limit within their credit limit or the implications should they wish to change the limit or find it insufficient for a purchase they are considering.

Recommendation 14 – Verification of payment execution by the customer

The provision of timely information to allow customers to check payments is important. PSPs should be allowed the freedom to select the most appropriate delivery channel based on a balance of risk and usability. It is unlikely that customers will choose to check payment data if it involves complex security procedures to obtain access it.

D. Conclusion

Regulatory interest in the security of internet payments is understood and ensuring adequate security and protection for consumers is a valid goal. In documenting these recommendations the ECB appears to have drawn on sensible security good practice but makes an assumption that all requirements should be implemented equally regardless of the stakeholder's or the consumer's perception of risk.

Whilst the paper recognises the fact that securing internet payments is the responsibility of all stakeholders the ECB aims its recommendations at PSPs alone and, in particular, singles out the acquiring PSPs as being responsible for policing e-merchant compliance. This position seems to place PSPs at a disadvantage when compared to other stakeholders. It has the potential to favour other players in the ecosystem who will be able to offer services more akin to the existing customer friendly processes that would be outlawed for cards under these recommendations.

The ECB view that European regulation will have a significant impact on fraud and security fails to recognise the global nature of internet payments and does not acknowledge the likelihood that customer confidence in the channel can be undermined by major security incidence in markets not bound by these regulations.

It is the opinion of The UK Cards Association that, to be truly effective, any regulation in the internet payments ecosystem must apply to ALL players and it is preferable that any such regulation be applied globally.

Before any further steps are taken, regulators should seek a clearer understanding of existing and emerging market conditions and be able to articulate clear explanations and justifications for any requirements.

Key Contacts

For further information on the content of this document please contact:

David Baker, Head of Technical
+44 (0)20 317 8297
david.baker@ukcards.org.uk

Paul Rodford, Head of Card Payments
+44 (0)20 317 8238
paul.rodford@ukcards.org.uk

The UK Cards Association
2 Thomas More Square
London
United Kingdom
E1W 1YN

Visit our websites at:

www.theukcardsassociation.org.uk

www.financialfraudaction.org.uk

APPENDIX 1

Chart 1 – Fraud Losses on UK-Issued Cards 2001-2011

FRAUD LOSSES ON UK-ISSUED CARDS 2001-2011

Tinted figures show percentage change on previous year's total

Chart 2 – Annual Fraud Losses on UK-Issued Cards 2001-2011

ANNUAL FRAUD LOSSES ON UK-ISSUED CARDS 2001-2011

All figures in £ millions

Fraud type	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	+/- change 10/11
Card-not-present	95.7	110.1	122.1	150.8	183.2	212.7	290.5	328.4	266.4	226.9	220.9	-3%
Counterfeit	160.4	148.5	110.6	129.7	96.8	98.6	144.3	169.8	80.9	47.6	36.1	-24%
Lost/stolen	114.0	108.3	112.4	114.4	89.0	68.5	56.2	54.1	47.7	44.4	50.1	+13%
Card ID theft	14.6	20.6	30.2	36.9	30.5	31.9	34.1	47.4	38.2	38.1	22.5	-41%
Mail non-receipt	26.8	37.1	45.1	72.9	40.0	15.4	10.2	10.2	6.9	8.4	11.3	+34%
TOTAL	411.5	424.6	420.4	504.8	439.4	427.0	535.2	609.9	440.0	365.4	341.0	-7%
Contained within this total/breakdown by location												
UK	273.0	294.4	316.3	412.3	356.6	309.9	327.6	379.7	317.4	271.5	261.0	-4%
Fraud abroad	138.4	130.2	104.1	92.5	82.8	117.1	207.6	230.1	122.6	93.9	80.0	-15%

Chart 3 – Fraud to Turnover Ratio 2001-2011

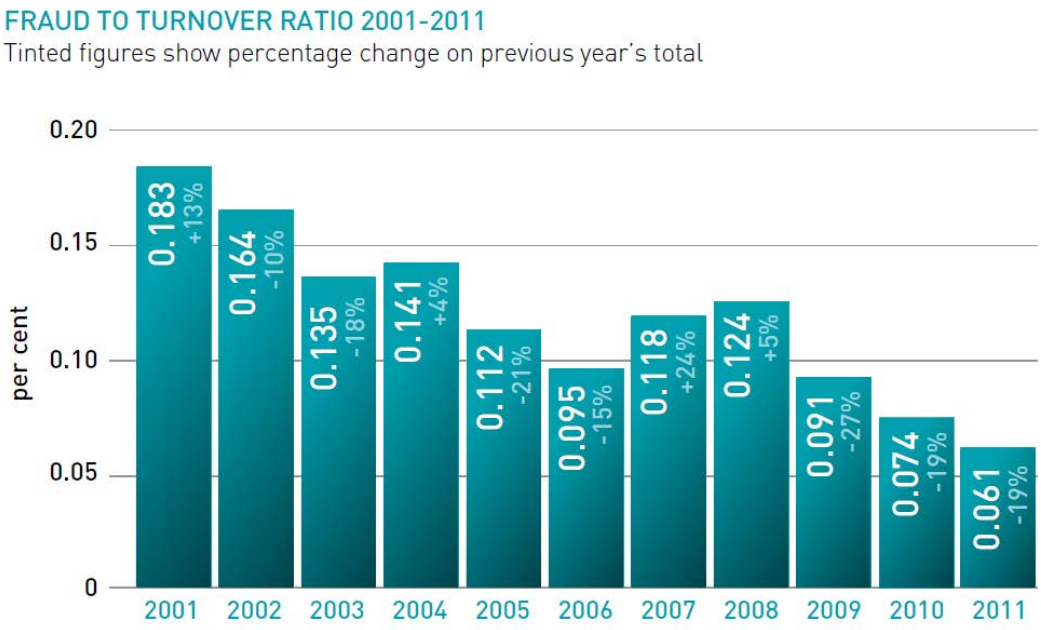


Chart 4 – CNP Fraud Losses on UK-Issued Cards 2001-2011

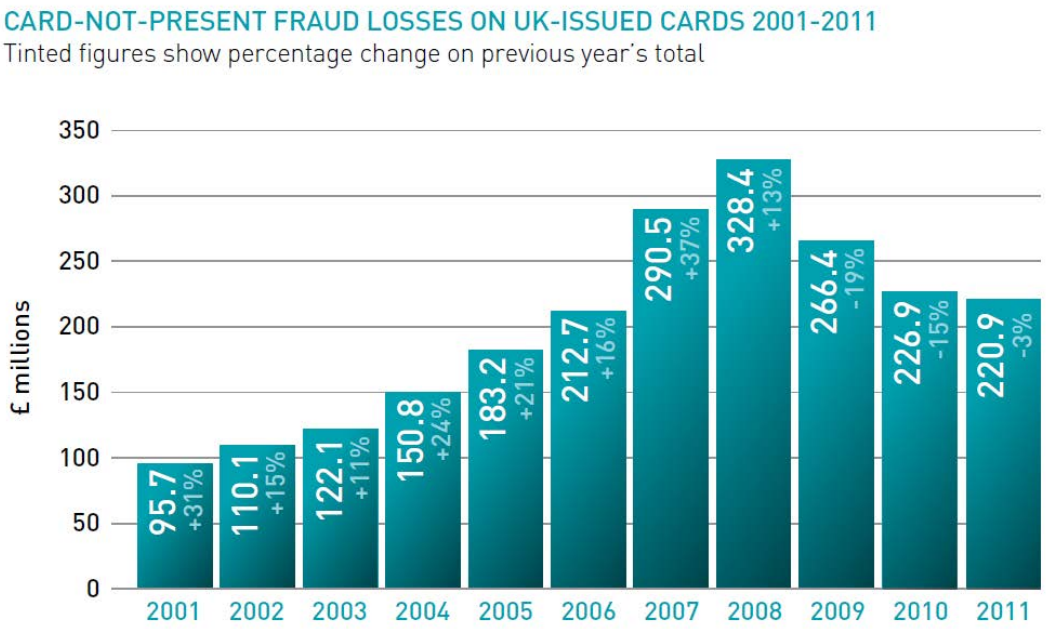


Chart 5 – UK online card payments spending volume 1999-2011

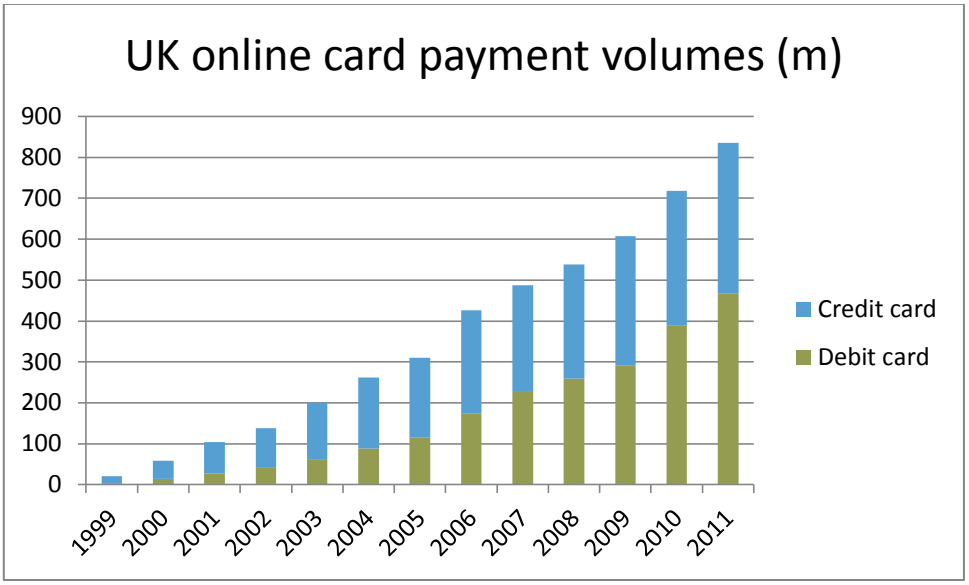
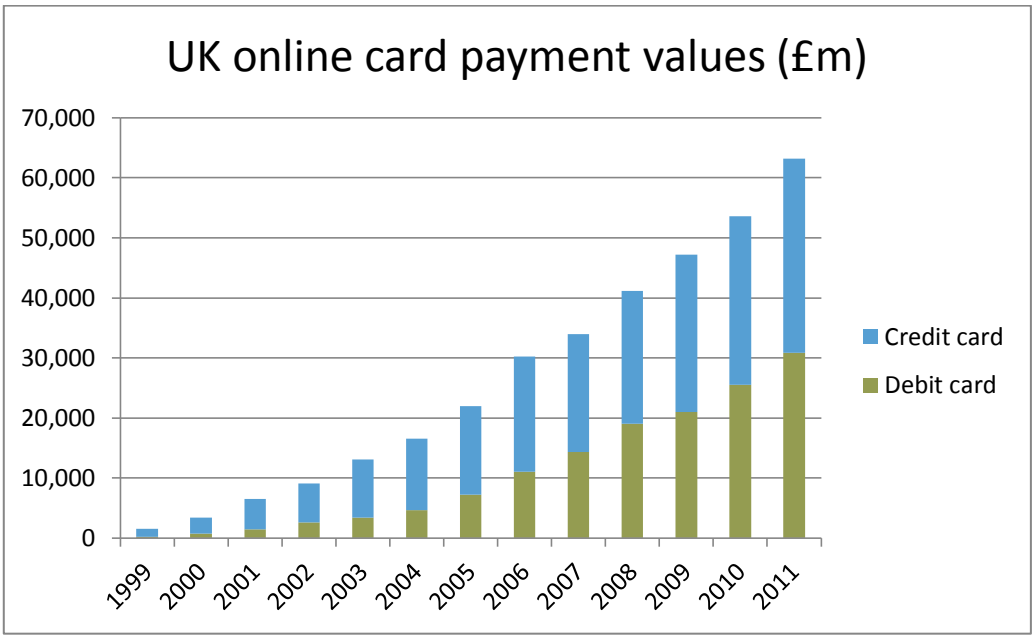


Chart 6 – UK online card payments spending values 1999–2011



Appendix 2

UK Industry-Level Consumer Education Campaigns Relating to Online Security

BeCardSmartOnline (2008–2011)

The Devil's In Your Details (2012)

http://www.actionfraud.police.uk/thedevilsinyourdetails

In partnership with Action Fraud, the UK's national fraud and internet crime reporting and support centre, and the Telecommunications UK Fraud Forum (TUFF), Financial Fraud Action UK developed 'The Devil's in Your Details' fraud awareness campaign which ran during March-May 2012.

The hard-hitting campaign was aimed at increasing public awareness of the importance of protecting personal information and to remind them to check that who they share their details with is genuine, whether this be on the phone, in person or online.

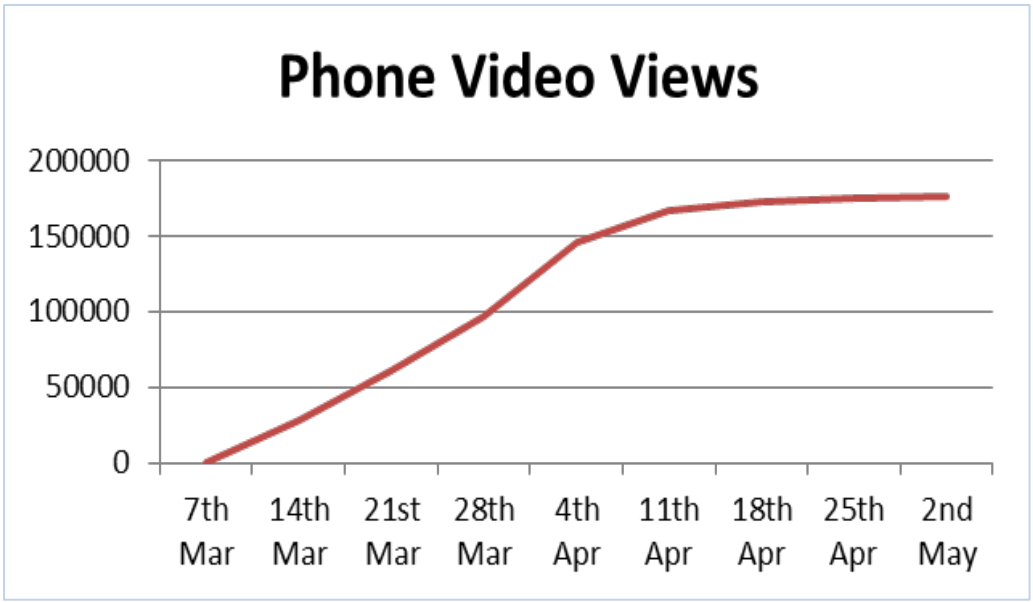
The campaign consisted of two viral videos and a Facebook app designed to highlight what to look out for and where to go to find advice. The actor and writer Stephen Fry backed the campaign on Twitter, making his own personalised video and tweeting about it to his four million followers.

It also provided some memorable tips on keeping SAFE from fraud:

- **S**uspect anything or anyone you don't know – no matter what or who they claim to be.
- **A**sk questions. Whatever a fraudster tries, you have the power to stay in control.
- **F**ind out for certain who you're dealing with. Challenge anything that seems suspect.
- **E**nd situations that make you uncomfortable. If you feel threatened, contact the police.

THE DEVIL'S IN YOUR DETAILS – Phone Fraud (2012)

http://www.youtube.com/watch?v=0N4MgKN3pkE



Soundbites from consumers

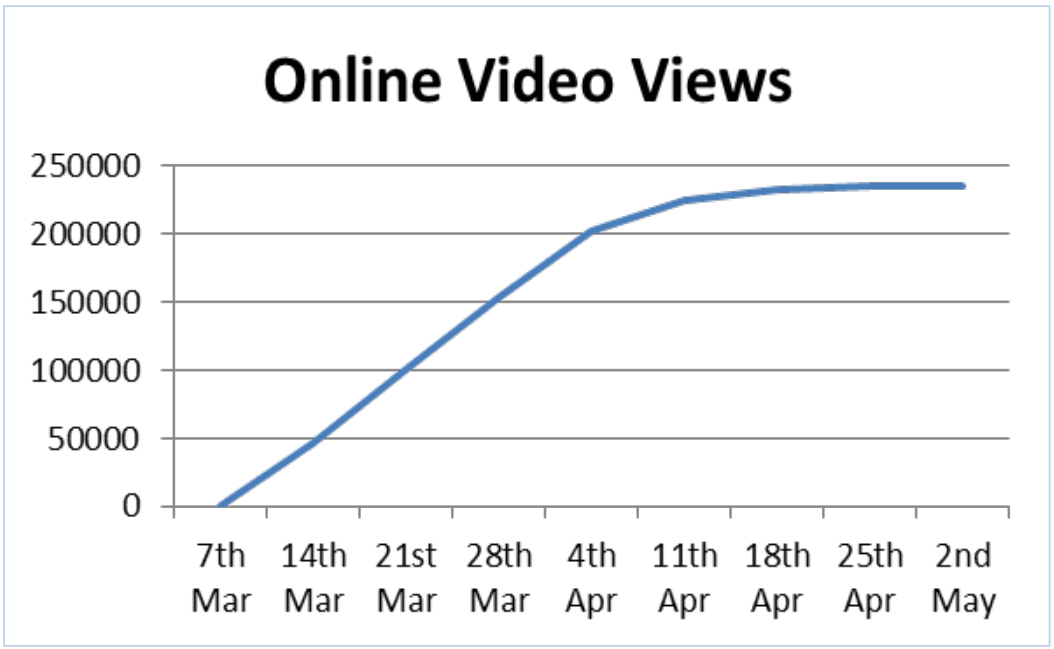
- *'Great vid, never give ur details to anyone no matter who they say there are, ur bank will always ask u to pop in if there is a problem'*

- *'As many as 4 people sent this video to me at the same time. interesting :p'*

- *'Crazy to think that this is what actually happens on the phone – get calls like this all the time, how can you be sure?!!'*

THE DEVIL'S IN YOUR DETAILS – Online Fraud (2012)

http://www.youtube.com/watch?v=Ugl8bmZF9Pc



Soundbites from consumers

- *Great video and the campaign is awesome. About time we cracked down on these scammers and understood how we can prevent this happening.'*

- *'I was sent a link in a text from O2, I and don't usually read them but this one said 'who do you trust? So I read on and watched the film'*

- *'Wish they were that easy to spot! It was a very humorous video, but nothing funny about fraud, thanks for the alert'*