



Inhibiting Enterprise

Fraud and Online Crime Against Small Businesses



Federation of Small Businesses
The UK's Leading Business Organisation

Foreword

Fraud and online crime is on the rise and is a growing concern for small businesses particularly in the current economic climate. In volume terms, instances of low level crime against a business such as vandalism or criminal damage are more frequent, however, the issue with fraud and online crime is that one event can be highly disruptive and even force a business to close.

It is of huge concern that 54% of businesses have been a victim of fraud or online crime and a significant 26% of businesses are deterred from buying and selling online because of the fear and risk of online fraud. Small businesses make up over half of UK GDP, are the primary job creators and are more likely to be able to respond flexibly to the current downturn in the economy. Small businesses need to take steps to protect themselves but are also relying on an effective response to fraud and online crime from the police, banks and other relevant organisations.

The survey results give interesting feedback on the instances and impact of fraud and online crime in small and micro businesses which we trust will inform intelligence in this area and support work around setting up a National Fraud Reporting Centre (NFRC) (to give businesses a central mechanism through which to report fraud) and the Police Central e-Crime Unit (PCeU), which will more effectively coordinate the work of police forces in this area.

Success in addressing fraud and online crime effectively in the future lies in a joined-up partnership approach with government, industry and law enforcement coming together to pool expertise, share information and best practice.

This report contains our positive proposals for future action in order to support small businesses that make up 58% of the private sector workforce



Mike Cherry
Home Affairs Chairman

Contents

1	Foreword	2
2	Key findings	4
3	Background	5
4	Fraud and online crime in small businesses	7
	Reporting of fraud and online crime.....	8
	Improving the response to fraud and online crime	9
	Fraud reporting centres.....	10
	Fraud prevention	11
	Cost of online crime and fraud	12
5	Corporate identity fraud	13
	Improving the response to corporate identity fraud.....	14
6	Card-not-present (CNP) fraud	15
	Improving the response to CNP fraud.....	17
	3D Secure.....	18
7	Data Security	19
	Payment Card Industry Data Security Standard (PCI-DSS)	19
8	Summary of recommendations	21
9	Useful links and advice for small businesses	22

Key findings

- A significant 54% of businesses have been a victim of fraud or online crime in the last twelve months: 37% had an issue with phishing emails, 15% were victim to card not present fraud and 15% experienced IT system issues (such as viruses, hacking etc)
- One third of businesses currently do not report fraud or online crime to the police or banks, 23% believe that it would not achieve anything
- Businesses are positive about the options for improving the response to fraud: 53% want clearer information about how and where to report these types of crime, and 44% want a specifically named contact in their local police force responsible for tackling fraud and online crime
- Overwhelmingly, 85% of businesses in England and Scotland said that they would report fraud if a designated reporting centre was set up which would gather data and use it to fight fraud (Wales already has a reporting centre)
- Businesses understand that the best form of protection is prevention with 84% opting for a firewall between the computers/network but only 6% accessing guidance and training on prevention through regional fraud forums or websites such as www.getsafeonline.org
- In over half of cases (54%), the cost of online crime and fraud was negligible to businesses. However, fraud also seems to hit businesses between the £500 - £4999 brackets (12%), which, over a twelve month period, are significant sums to small businesses
- Only 6% of businesses have had their corporate identity stolen, however 60% believe that there should be more awareness raising and education on how they can protect their business
- A significant 29% of businesses have been a victim of card not present fraud where 22% had received a chargeback (most frequently below £1000). 52% think that the bank/payment company should take greater responsibility for the chargeback fee, particularly where authorisation has already been given
- Where it is relevant to their business, 13% are implementing the Payment Card Initiative Data Security Standard (PCI-DSS) (which ensures that businesses securely store information on their customers and clients) but the most common feedback was that the initiative was not well tailored to small businesses

Background

The FSB carried out a survey in 2008 on the impact of crimes against business which showed that crime overall is on the rise: up to 64% of businesses were a victim (compared with 57% in 2006)¹. The FSB wanted to delve deeper into the issues raised around fraud and online crime and how it is affecting small businesses and decided to carry out its first survey in this area.

The survey was made available online for a two week period and elicited 1823 responses. The respondents to the survey were, in the main, self employed (32%) or micro businesses with 1-4 employees (42%) or those with 5-9 employees (15%) and 10-25 employees (8%). In terms of their location, survey respondents were spread across England, Scotland and Wales but with strong representation from the South East (22%) and South West (18%). Responses spanned a whole range of industry sectors but the largest response was from the retail sector in particular at 17%.

¹Putting the Economy Back on Track: Crimes against business, FSB (2008)

Table 1: Number of people employed in the business

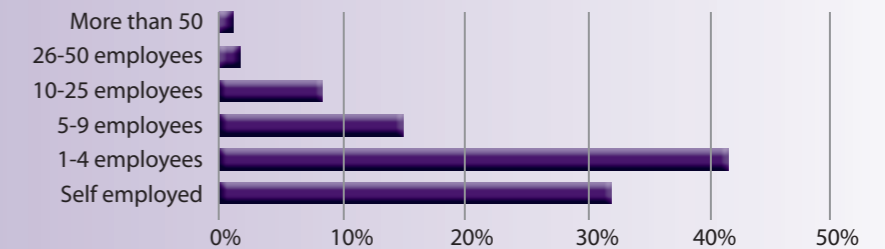


Table 2: Responses by Region

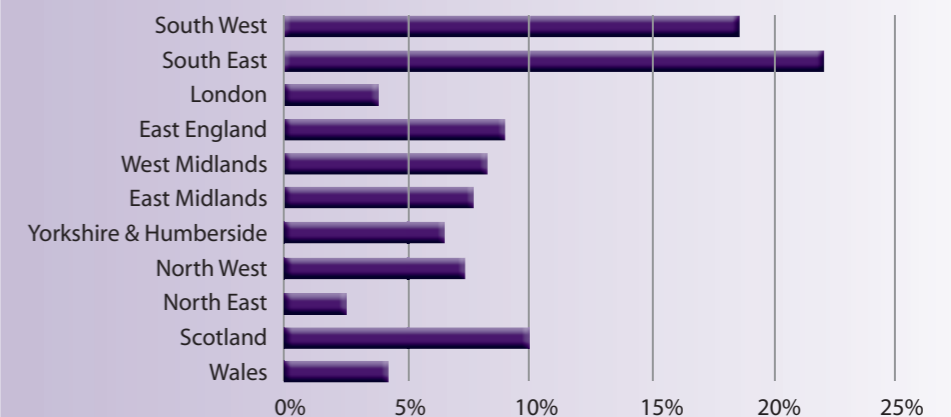
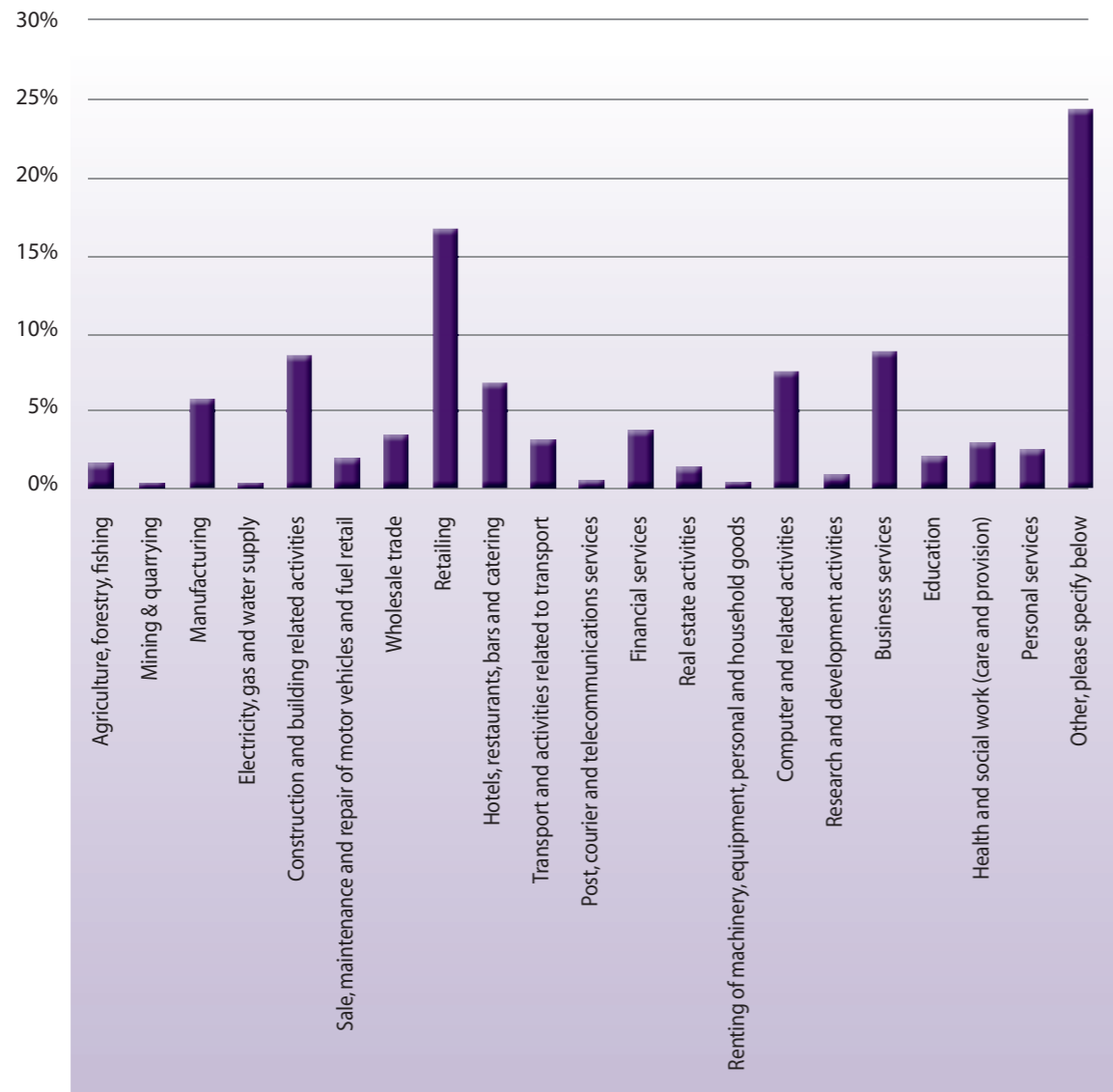


Table 3: Responses by sector



“Small business quotes”

It is clear that in some instances fraud can result in huge losses: ‘We had an order placed against paperwork from a Dutch bank supposedly backing a venture that turned out to be totally fake and resulted in the loss of approximately £40,000 plus losses by other contractors.’

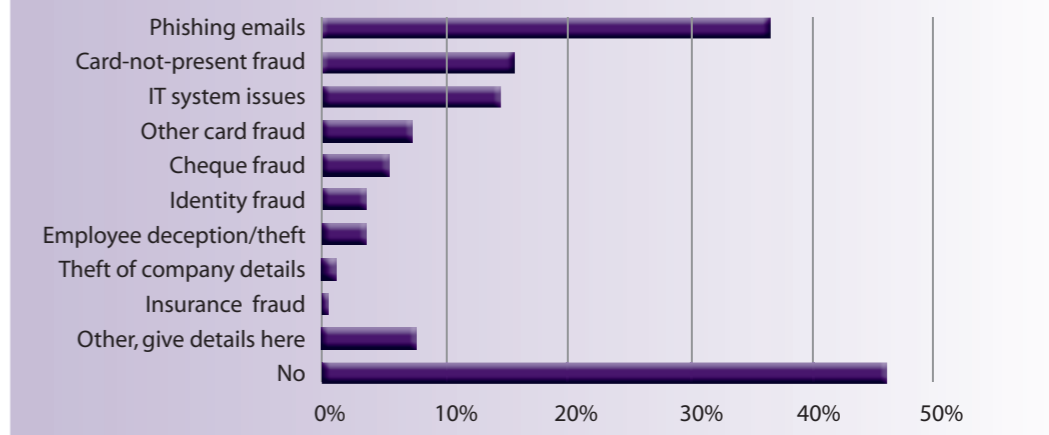
Small businesses are also vulnerable to scams to avoid payment: ‘A large corporate rescue and recovery business bounced a cheque on us because they knew it would cost more to pursue through the courts.’

Fraud and online crime in small businesses

Key findings:

- 54% of businesses have been a victim of fraud or online crime over the last twelve months
- A significant 37% said that phishing emails had been a problem (where a fraudster poses as a legitimate organisation fishing for personal or financial information²)
- 15% had been targeted by card-not-present fraud (where card details are fraudulently used for transactions over the phone or internet)
- 15% said that IT systems issues (such as viruses, hacking, denial of service attacks) had been an issue

Table 4: Experience of fraud or online crime over the past 12 months



Businesses were invited to give further comments on the types of crime they were victim to which revealed that phishing attacks are a regular annoyance but that businesses are becoming ‘more savvy’ and are now able to recognise such emails and press delete.

The diversity of the small business community means that they are victim to fraud across the board: from forged cash, bounced cheques and invoices for work not done to fraud via online banking, as well as unauthorised direct debits/standing orders, the sale of eBay fake goods and scams through Skype and Paypal. Businesses also fall victim to scams for charity support, rogue door to door traders and advertising in fake magazines. On some occasions businesses have also been lured by boiler room scams (a boiler room is a business that attempts to peddle worthless shares to unsuspecting investors).

²Note: it is difficult to determine whether the phishing email is merely a nuisance email or whether businesses are actually taken in by the fraudsters

“Small business quotes”

Small businesses see the value in preventing fraud in the first place and having good backup systems:

‘I prevented any fraud occurring through the proper use of security software and knowing how to discern the difference between a legitimate email and a phishing email.’

‘A hacker on my business PC was sorted by my online protection service; their team took 4 hours to resolve it’.

Reporting of fraud and online crime

Key findings:

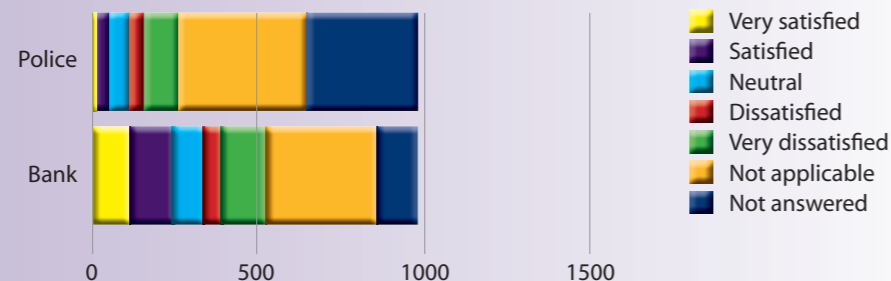
- Of those businesses that had experienced fraud or online crime: 50% said that they had reported it to their bank or relevant financial institution, 20% said they had reported it to the police or Crimestoppers and 33% said that they did not report it
- Businesses said that the main reasons for not reporting fraud or online crime were that it ‘would not achieve anything’ (23%), that the ‘police would not be interested’ (14%) and that they would ‘not be able to find the fraudsters’ (8%)
- Businesses also did not report because they thought the crime was not serious enough (10%) and that they were not sure who to contact (7%) and were concerned that the police would not even want to accept the report

When businesses were asked for further comments as to who they reported to, many businesses said that they would not report viruses on their system or phishing emails which are common. Businesses also reported to Ebay, PayPal, the Office of Fair Trading (OFT), Amazon, Companies House, CIFAS, HM Revenue and Customs and their Service Provider. In some instances, the bank had actually flagged up the instance of fraud to the business.

Response from the police and banks

When asked how satisfied businesses were with the response they received, in general support for banks was much higher than support for the police. Businesses were much more likely to be ‘very satisfied’ with the response from banks. Although where support had failed, businesses seemed to be ‘very dissatisfied’ in equal number with police and banks alike.

Table 5: Satisfaction levels with response from police/banks



“Small business quotes”

Better communication between police and businesses is necessary in order to catch repeat offenders:

‘We have regular attempts made on us for credit card fraud and stolen cheques. We have told the police and they say that until goods are received no crime has been committed. I have offered to “accept an order” and provide a delivery address so police can pick up fraudsters but they are not interested.’

Issues around employee fraud:

‘There was a long delay between reporting of the theft and the initial interview by the police of the employee. This had two effects: i) The employee was very visible locally which caused embarrassment to my business and anger amongst my other staff who were outraged on my behalf, ii) The CPS felt that the investigation had gone on too long (six months) and it was not appropriate to move to a prosecution. This was despite strong evidence.’

When asked for further comments on the response to fraud and online crime, businesses were very vocal about the lack of reporting mechanisms, follow up and support available, particularly from the police. This is particularly the case, even where fraud worth £1000s is involved. Businesses report that the police seem reluctant to get involved and criminals act in the knowledge that they will get away with it.

Improving the response to fraud and online crime

Business owners were positive about the range of options proposed to improve the response to fraud and online crime:

- 61% favoured tougher penalties for offenders
- 53% wanted clearer information as to how and where to report fraud and online crime
- 47% asked for more information from the police/banks about how they tackle fraud/online crime
- 44% opted for a specific named contact in the local police to tackle fraud and online crime
- 43% wanted a more effective response and follow up from the police

Table 6: Improving the response to fraud and online crime



“Small business quotes”

‘Most online crime is internationally based. The data needs to identify sources quickly, probably by recipients forwarding that email to a Government spoof email, where the sender can be blocked. Also automatic identification when one visits an identified fraudulent website: someone like Google could add this feature to a browser features with ease.’

‘Only if I could see some sort of response. Have been reporting ‘phishing’ e-mails to reports@banksafeonline.org. uk, we’ve now stopped using it because we got absolutely no feedback whatsoever.’

21% of businesses call for discounted rates for small businesses joining fraud forums. Unfortunately 97% of businesses said that they were not a member of a regional fraud forum, 90% said that they have never heard of them, and 15% said they were not sure there was any benefit to their business. The FSB is involved with Regional Fraud Forums across the country but there is clearly a role for these Forums to reach out more effectively to small businesses and specifically target them with accessible information about prevention.

When asked for further comments, businesses recognise that fraud and online crime is an international issue which requires effective international cooperation but also effective UK law for prosecuting offenders. There are also clearly issues about ‘place’ from a national point of view which can lead to cross border disputes between police forces about which force will take ownership of the crime or fraud in the first place. Businesses also called for ISPs to take more responsibility for their networks and ensure a far more effective level of security.

Fraud reporting centres

Overwhelmingly, 85% of businesses in England and Scotland (Wales already has a reporting centre) said that they would report fraud if a designated reporting centre was set up which would gather data and intelligence and use it to fight fraud. This bodes well for the National Fraud Reporting Centre to be set up later in 2009.

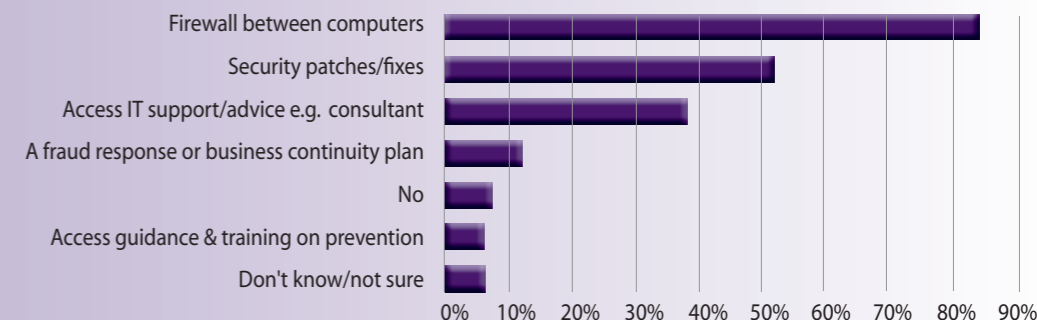
Recommendations

- Businesses need a central, accessible and well-advertised reporting centre for both fraud and online crime to enable them to report these types of crime in a straightforward way
- The National Fraud Reporting Centre and Police Central e-Crime Unit (PCeU) must work hand in hand in order to set up an effective system of gathering intelligence which feeds into investigation and prosecution
- Businesses that report fraud would appreciate feedback on how the information is being used to tackle fraud and online crime with information about successes
- Businesses are keen to have access to a local police contact for fraud and online crime to answer queries. There is clearly a need for the National Fraud Strategic Authority and Police Central e-Crime Unit to work on rolling out effective training to all police forces.
- All Regional Fraud Forums should devise effective strategies to engage and communicate with small businesses and offer advice on fraud prevention

Fraud prevention

Businesses were asked about how they prevent fraud and online crime. The most common answer was a firewall between the computers/network (84%), security patches/fixes (52%) and access to appropriate IT support/advice through a consultant (38%). Businesses were less supportive of a fraud response through drawing up a business continuity plan (12%) or accessing guidance and training on prevention (6%) through regional fraud forums or websites such as www.getsafeonline.org. Where businesses had not ticked any of the options given, this was because they perceived that they do not have the technical skills (9%) or they are concerned about costs (7%).

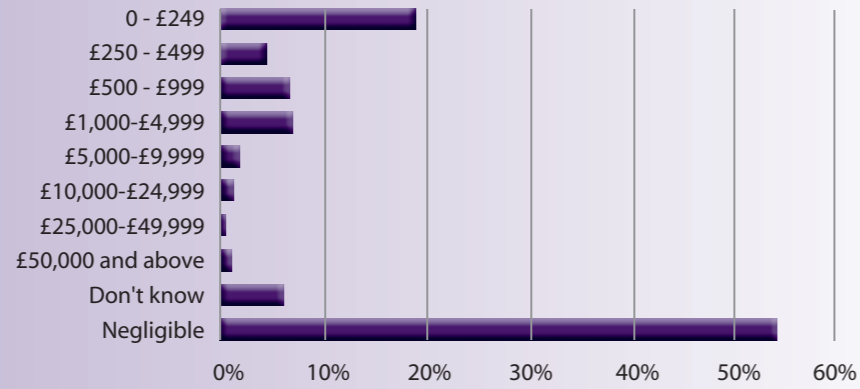
Table 7: Fraud prevention measures



Cost of online crime and fraud

The cost of online crime and fraud was negligible to over half (54%) of businesses. However, 19% of businesses said that it cost them up to £249 a year and 12% that it had cost them between £500 - £4999 which are still significant sums to a small business. According to these figures, conservative estimates are that fraud and online crime costs a small business, on average £768 per year.

Table 8: Estimated cost of online crime/ fraud to a business over the past 12 months



Corporate identity fraud

Corporate identity fraud is not huge in volume terms with 93% of businesses saying that their company identity had not been stolen. However, worryingly 6% of total respondents said that their business identity had been stolen.

Businesses were asked for further details on their experience and the comments received illustrate the multitude of ways in which corporate identity fraud can happen. A particular concern is the issue of theft of domain names, bought or used fraudulently by criminals and competitors. Spam emails are also sent by fraudsters using a legitimate business email address to seek out information from clients or simply to tarnish the reputation of the business.

Businesses tell us how their identity had been stolen:

- 'Fraudulent use of our mailbox address and registrations at Companies House'
- 'Imposters presented themselves as co-directors, changed the company name and the first we knew about it was when the bank issued us with new cheque books (due to name change)'
- 'Our company name and address was taken from our website and an email sent to various people in the USA offering a job collecting money raised from sales. A false email address and a false phone number (pay-as-you-go mobile) was used and the clear intention was to get peoples' personal details'
- 'Mortgage application made purporting to have come from my firm but using wrong address: fraudulent direct debit mandate sent to bank'
- 'Competitors using company names as tags on search engines to direct the customers elsewhere'
- 'Trojan virus used to steal IP identity and commit crime under business identity'
- 'Impersonating companies and opening an account on eBay to sell fictional items using company name but false email address, business then gets billed'

"Small business quotes"

'Someone tried to impersonate me and cancelled my hosting/ domain for my website. I managed to get it back before anything too bad happened, but it cost me one contract (c.£5000) and my time.'

'A person pretending to be me opened an account on eBay and began selling fictional items. He insisted the buyers pay by cheque or money transfer to an account in my name. I realised the fraud was taking place when a buyer called me after getting my number off the internet to let me know he had sent a cheque to me for £800. I checked on eBay and found the seller who was using my name and displaying my address, using a different email. I immediately contacted the police and eBay. The police were a waste of time. eBay were not listening. They did not even cancel the bogus sellers account until I threatened them with legal action.'

Improving the response to corporate identity fraud

Businesses were asked how they think the response to corporate identity theft should be improved:

- 60% said more awareness raising and education on how to protect your business
- 44% said that more effective security procedures for registering and updating details with Companies House were necessary. Companies House have tightened up their security mechanisms in recent years but clearly there is more scope for communicating this to businesses.

Businesses also thought that the ISPs must do more to prevent access through the internet system and that there should be greater control over the issuing of domain names similar to those of existing companies.

“Small business quotes”

‘I have launched an internet business as a subsidiary of my main business and this does, by necessity, rely on CNP card transactions. It is frustrating that there is not enough information and seems to be no protection against fraudulent transactions for me, and subsequently I am the one that is out of pocket, even where a card issuer has provided an authorisation code for a transaction. More action needs to be taken to support entrepreneurial businesses that are helping to expand and develop the economy on a local and national level.’

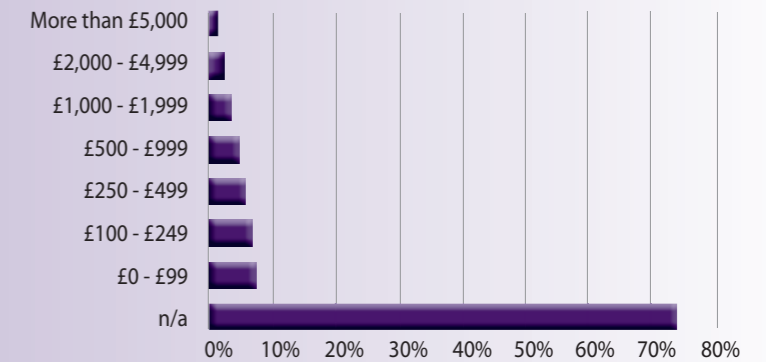
‘We offer consultancy services to online stores and all of our

Card-not-present (CNP) fraud

Card-not-present fraud (when card details are fraudulently used over the phone, fax or internet) is on the rise and a big problem for retailers and small businesses relying on the internet to sell products online to national and international markets.

- A significant 29% of businesses have been a victim of CNP fraud
- Of those businesses that had been a victim of CNP fraud, a significant 22% said they had received a chargeback (i.e. the transaction went through at the time but the bank later charged the business back for the cost of the item)
- Where chargebacks happened, these were most frequently below £1000

Table 9: Value of the chargeback



Improving the response to CNP fraud

When asked how businesses thought the response to CNP fraud could be improved:

- The majority of businesses (52%) thought that the bank/payment company should be made responsible for the chargeback
- 50% gave their support to the use of the new generation of pocket-sized handheld card authentication devices that take a PIN and generate a one-time number
- 47% said that clearer information should be available on how businesses can protect themselves

clients are hit by CNP fraud on an almost continual basis. The police will no longer investigate as it is now the jurisdiction of the banks. The banks will not investigate as they then have to record a crime which demonstrates what a poor job they are doing. End result - nothing is done. Even in cases when we have in depth and complete evidence of who committed the crime nothing happens. CNP fraud is increasing and the reason is that the fraudsters have close to zero chance of being caught.

'Bottom line is when a card is fraudulently used, the penalty is applied to the small business, not the criminal or the financial institution. This is a real barrier to online commerce.'

CNP fraud case study

Elly runs Airbossworld.com a retail outlet selling extreme kites and has recently suffered from a few fraudulent transactions.... 'I am concerned that the banks put all the emphasis on the retailers so we lose out if the item has shipped to a fraudster.

I took a phone order from a person who gave me all the correct details, home address, card details including the security code, the name of the person on the card and a delivery address which they said was a friend's they were staying at whilst going to do the kite sports activity. I have a proof of delivery signed by the card holder, the details of the order that was taken, home address and delivery address.

I then heard back from the bank two months later saying this has been charged back and the money we had (£900) had been taken from us. The bank asked us to send over the details of the order and the proof of delivery so they could fight this case for us, but we later had correspondence from them to say that we didn't win the chargeback as the apparent real customer had said this was not his purchase. We are out of pocket and have not only lost the £900 out of our bank, but also the cost of the kite, so a total of £1,350.

It seems wrong that we take all the information the bank needs for the card systems and we are still the party that loses out. Is this right, and should shops have the responsibility if we have taken all the right details, it surely can't be our fault if we are deceived?

We take orders via the phone, via visitors in the shop and internet sales, we have had fraudulent transactions through the phone once and a couple through our internet banking system. Which in effect would mean that we should only take transactions face to face, but that wouldn't be very economical in the long run as we have to stay competitive in our market and to do that mail order and internet sales are a huge part of our service.'

"Small business quotes"

Small businesses on improving the response to CNP fraud

'Banks and payment companies should shoulder more of the responsibility of fraud by using better and stronger encryption and anti-fraud measures rather than trying to pass the buck to the retailer or member of the public.'

'Forced implementation of 3D across the board'

'New generation of pocket-sized handheld card authentication devices but for the PERSON not the card so we don't have to carry one device for every card/bank account'

'A consistent policy on use of the three digit security code (CVV) on back of card'

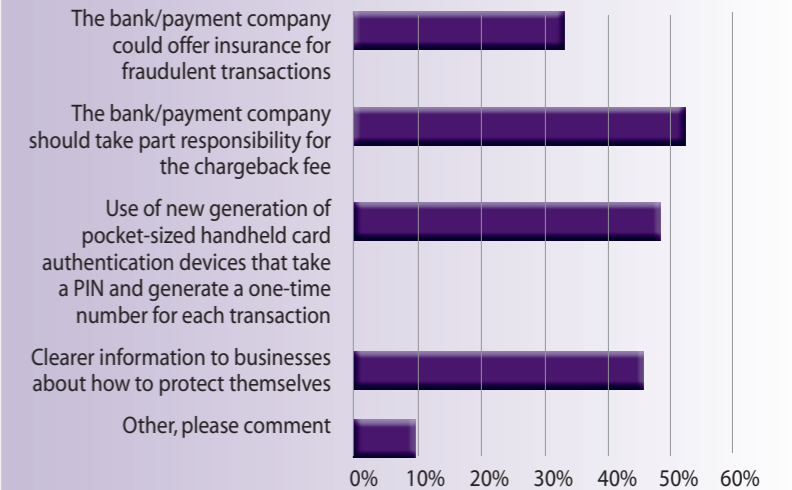
'Direct bullet points with information and guidance are much more useful than long-winded booklets'

'For transactions over £100 the card holder receives a text message confirming the sale. Therefore if someone has used their card they know about it straightaway and do not have to wait for the credit card statement - possibly a month later'

'Each card has a password attached as with online/ phone banking, then when doing a card not present the PDQ has to request one or more of the letters, i.e. letter 4 from your password. This is in addition to the current address numbers having to be keyed in.'

'Every PC should have built-in chip and pin card reader'

Table 10: How banks/card payment companies could improve the response to CNP fraud



Recommendations

- Banks should take greater responsibility for the chargeback and businesses should be told up-front that authorisation does not guarantee payment, rather than this being hidden in the small print
- Information about how to protect the business from card-not-present fraud should be more effectively communicated to small businesses

“Small business quotes”

Small business quotes - MasterCard Secure Code & Verified by Visa

‘The adoption of MasterCard SecureCode and Verified by Visa whilst welcome, has been a complete botch with many consumers completely unaware of their benefits/risks of registering and at least 30% of our online sales now failing to complete at the secure code password stage because of the poor communication about these systems. In addition it is frankly ridiculous to have the security registration process handled at the time of a transaction - this should clearly be handled by the card issuers to provide consumers with absolute confidence that the registration process isn't in itself a scam by the online retailer to obtain personal information’

‘MasterCard SecureCode and Verified by Visa is a great initiative but has been so poorly advertised by the banks it is a hindrance to our business rather than an aid. Plus the system is unreliable, and not fully implemented (despite many businesses being told they have to implement it, this is not being done consistently, it should be compulsory for all transactions)’

‘It's a no-win situation for businesses. Fees for internet transactions are higher, supposedly due to the 'increased risk'. However, due to the chargeback process, businesses still pay if there is a fraudulent transaction. Ludicrous. In addition, only the first payment is covered by the Verified by Visa/ MasterCard SecureCode system - continuous authority payments are apparently not covered. Information on these aspects is minimal and not easily available’

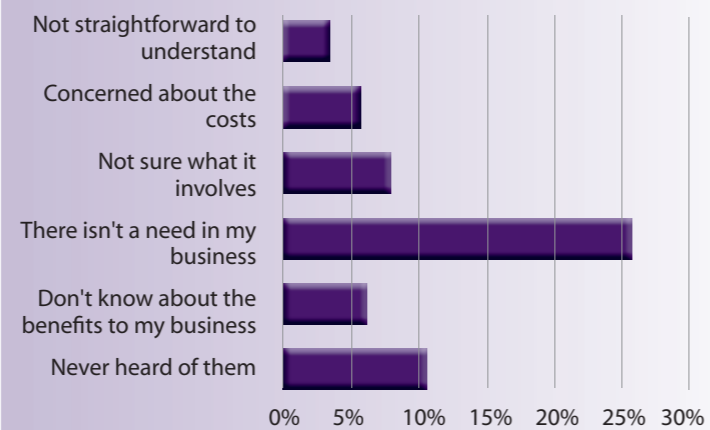
3D Secure

Verified by Visa/MasterCard SecureCode

Businesses were quite split on their use of payment security systems such as MasterCard SecureCode or Verified by Visa used for online transactions:

- 48% said that they did use these systems but 48% said that they did not
- One quarter (26%) said that there is not a need in their business
- 10% said that they have never heard of them and 8% that they are not sure what it involves.

Table 11: Reasons for not using VerifiedbyVisa/MasterCardSecureCode



“Small business quotes”

‘PCI DSS What a joke! I refused to pay for their assessors because we don't store credit card data on our computers. In the end, after phone calls and letters, they told me that they were re-assessing the self-assessment forms. Half of my calls were to people who had no idea what the self-assessment form was. We don't offer online booking so customers must call with their credit card details and yet I was still asked to submit a hopelessly complicated self-assessment form.’

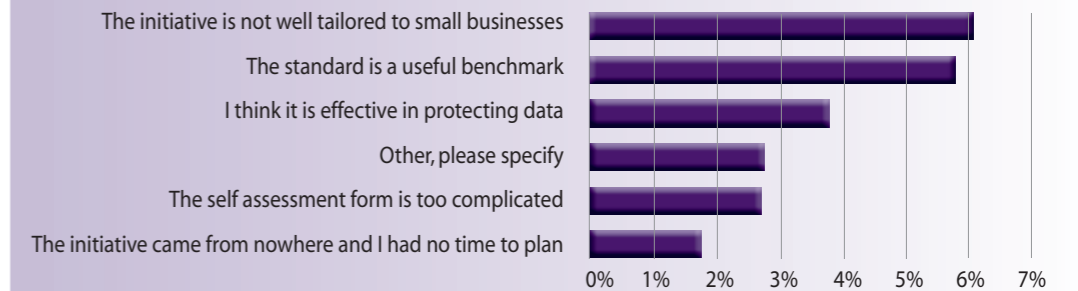
Data security

Payment Card Industry Data Security Standard (PCI-DSS)

The PCI-DSS is a security standard which encourages businesses that are processing, transmitting or storing card holder data on customers or clients, to protect that sensitive information. Small businesses are usually required to fill in a self-assessment questionnaire. When asked whether they were complying with the PCI Data Security Standard 62% of businesses said that they didn't know what it was, 20% said no and only 13% said that they were complying with the standard.

Out of those that were using the standard, the most common view was that the initiative was not well tailored to small businesses but 6% also said that it is a useful benchmark. 3% thought that the self assessment form was too complicated.

Table 12: Views on the PCI-DSS



Summary of recommendations

PCI-DSS case study

Jerry, running a business called Aquila Media, has had many conversations with his Merchant account provider and his Security Assessors with regard to PCI-DSS.

'The whole thing seems very complicated for individuals like me. It may be fine for large organisations with large budgets and their own IT people, but the requirements for this seem to be excessive for a small business.

Most of it is fairly straightforward but the main issue I have is with the requirement to perform Internal Vulnerability scans four times a year. The QSA (Qualified Security Assessors) will perform the external scan as part of their annual fee so that is easy enough. There are companies that will do the Internal Vulnerability scans for you at £1,000 per day, but £4,000 a year is a heavy price to pay for this.

I have completed the questionnaire and am therefore compliant however, I did find that the Security Assessors' staff seemed to have different opinions as to how to satisfy the criteria needed to answer the questions in order to become compliant. The whole system just seems too complicated and not properly managed, especially for small businesses.

Recommendations

- The benefits of security initiatives such as MasterCard Secure Code and Verified by Visa need to be more effectively communicated to the public and small business community, to improve take up
- The Payment Card Initiative Data Security Standard (PCI DSS) needs to be more effectively communicated to businesses and better tailored to their situation rather than the same template applying to businesses of varying sizes

“Small business quotes”

Tackling fraud and online crime

'The industry should circulate details of scams as they arise. A major task but this could be related to a particular industry e.g. book selling, building industry, medicines etc. What is happening in medicine frauds may not be relevant to building materials and vice versa'

'It's amazing what the ISPs can do to counter music piracy. It's high time they did far, far more.'

'ISPs must be made accountable for passing through unmistakably fraudulent e-mail traffic to users' inboxes. International agreements must be enforced to restrict fraudulent card usage across all countries as laxity in many places sustains the value of stolen and cloned cards. It is a global issue that needs globally supported action. Would High Street banks knowingly close their eyes to daily bank robberies? Why aren't they taking effective action to stop online robbers?'

'Having also spent the last two years working in the PCI / Internet security arena, it is clear to me that a number of financial institutions in Europe are not taking their roles in preventing fraud as seriously as they should, and that the second generation IT security tools that are evolving very rapidly at this point in time are able to provide more effective security monitoring at significantly reduced cost, the problem being that large companies that are selling into the corporate finance sector are not implementing the most effective technologies based on the best practise as discussed in the Jericho Forum www.opengroup.org/jericho'

Summary of recommendations

- Businesses need a central, accessible and well-advertised reporting centre for both fraud and online crime to enable them to report these types of crimes in a straightforward way
- The National Fraud Reporting Centre and Police Central e-Crime Unit (PCeU) must work hand in hand in order to set up an effective system of gathering intelligence which feeds into investigation and prosecution
- Businesses that report fraud would appreciate feedback on how the information is being used to tackle fraud and online crime with information about successes
- Businesses are keen to have access to a local police contact on fraud and e-crime to answer queries. There is clearly a need for the National Fraud Strategic Authority and Police Central e-Crime Unit to work on rolling out effective training to all police forces.
- All Regional Fraud Forums should devise effective strategies to engage and communicate with small businesses and offer advice on fraud prevention

Card-not-present fraud

- Banks should take greater responsibility for the chargeback and businesses should be told up front that authorisation does not guarantee payment, rather than this being hidden in the small print
- Information about how to protect the business from card-not-present fraud should be more effectively communicated to small businesses

3D Secure/ PCI-DSS

- The benefits of security initiatives such as MasterCard SecureCode and Verified by Visa need to be more effectively communicated to the public and small business community, to improve take up
- The Payment Card Initiative Data Security Standard needs to be more effectively communicated to businesses and better tailored to their situation rather than the same template applying to businesses of varying sizes

Useful links and advice for small businesses

www.getsafeonline.org

www.banksafeonline.org

www.cardwatch.org.uk

www.becardsmart.org.uk

www.identitytheft.org.uk

www.stop-idfraud.co.uk

www.bcrc-uk.org (Business Crime Reduction Centre)

www.fraudadvisorypanel.org

www.keepyour.co.uk/ (Nominet domain name advertising campaign)

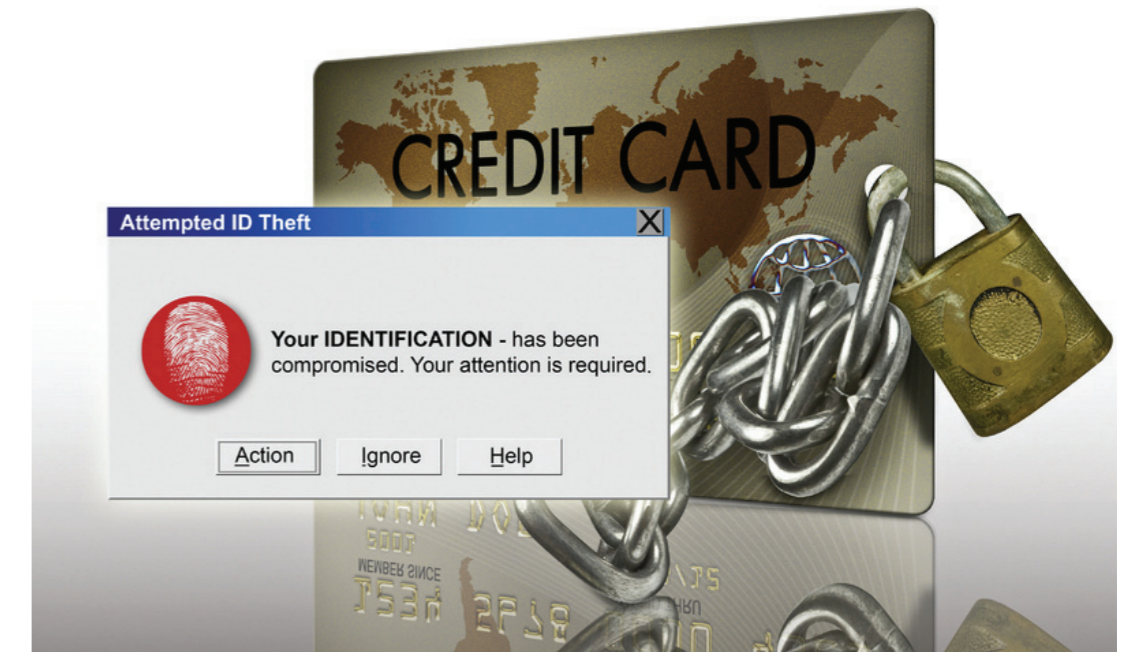
www.met.police.uk

www.attorneygeneral.gov.uk/nfsa

The Police Central e-crime Unit (PCeU)

The Police Central e-crime Unit (PCeU), to be launched in spring 2009, is intended to provide businesses and the public with a more effective means of reporting e-crime. The PCeU aims to provide specialist officer training and co-ordinate cross-force initiatives to crack down on on-line offences.

The Unit will come into operation alongside a new National Fraud Reporting Centre (NFRC), and National Fraud Intelligence Bureau (NFIB), which will come under the control of the City of London Police. The model is that businesses will report fraud and e-crime to the NFRC, the data will be analysed by the NFIB for strategies to be developed, then the law enforcement response will be coordinated through the e-Crime Unit. The PCeU will collaborate with SOCA (Serious Organised Crime Agency), and will have staff embedded at the NFRC. There will be a PCeU website, and an effort to raise awareness of e-crime at the local police station level with an e-Crime contact in every police force and regional hubs to share information.





ISBN Number 978 0 906779 95 8
February 2009

©Federation of Small Businesses
Copies of this publication may be obtained by writing to:
Federation of Small Businesses
2 Catherine Place, London SW1E 6HF
Telephone: 020 7592 8100
Facsimile: 020 7233 7899
email: london.policy@fsb.org.uk
website: www.fsb.org.uk

D i s c l a i m e r

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the Federation of Small Businesses (FSB). While every effort has been made to ensure the accuracy of the facts and data contained in this publication, no responsibility can be accepted by FSB for errors or omissions or their consequences. Articles that appear in the book are written in general terms only. They are not intended to be a comprehensive statement of the issues raised and should not be relied upon for any specific purposes. Readers should seek appropriate professional advice regarding the application to their specific circumstances of the issues raised in any article.

Designed on behalf of the Federation of Small Businesses by
Hutton Design, Long Road, Paignton, TQ4 7BB
Telephone: 01803 668718 Fax: 01803 557148
email: luke@huttondesign.net

