The Step Method – Battling Identity Theft Using E-Retailers' Websites

Marion Schulze, Mahmood H Shah

University of Central Lancashire, Lancashire Business School, PR1 2HE Preston, UK
MSchulze@uclan.ac.uk, MHShah@uclan.ac.uk

Abstract. Identity theft is the fastest growing crime in the 21st century. This paper investigates firstly what well-known e-commerce organizations are communicating on their websites to address this issue. For this purpose we analyze secondary data (literature and websites of ten organizations). Secondly we investigate the good practice in this area and recommend practical steps. The key findings are that some organizations only publish minimum security information to comply with legal requirements. Others inform consumers on how they actively try to prevent identity theft, how consumers can protect themselves, and about supporting actions when identity theft related fraud actually happens. From these findings we developed the **S**upport – **T**rust – **E**mpowerment – **P**revention (STEP) method. It is aimed at helping to prevent identity theft and dealing with consequences when it occurs. It can help organizations on gaining and keeping consumers' trust which is so essential for e-retailers in a climate of rising fraud.

Keywords: Identity Fraud; Identity Theft; Customers' Behavior; Websites; Security; Privacy; E-retailer

1 Introduction

This paper aims to investigate how e-retailers in the UK communicate identity theft on their websites, and what can be considered as promising practice. Identity theft related fraud is a growing problem and can be seen as the fastest growing type of fraud in the UK (CIFAS, 2008).

We distinguish between identity theft and identity theft related fraud. Identity theft is "… the misappropriation of the identity (such as the name, date of birth, current address or previous address) of another person, without their knowledge or consent." (CIFAS, 2008) Identity theft is often followed by identity fraud which "… is the use of misappropriated identity in criminal activity, to obtain goods or service by deception." (CIFAS, 2008) e-Retailers become victims of identity fraud when fraudsters take over customer accounts, e.g. after getting hold of user name and password by "phishing" (Myers, 2006). Fraudsters may also set up new accounts with stolen identities and stolen payment card details. Internet fraud clearly damages internet businesses. (Lindsay, 2005; SOPHOS, 2007) Not only trading goods are lost, also the trust of consumers, damaging the Internet economy as a whole (Tan, 2002;

Berkowitz and Hahn, 2003; Sullins, 2006; PITTF, 2007; Acoca, 2008). Therefore it is important for e-retailers to find ways to gain consumers' trust in times of rising fraud.

Publishing information on websites is one way of achieving this. Collins (2005) points out that legal requirement about what to publish are merely superficial. She suggests an e-business website that is perceived by customers as secure. In addition, it should offer information on how customers can help secure their own privacy. She recommends that organizations should perform a website security assessment to measure the performance of their website in terms of how security is perceived by customers.

Collins' recommendation how to communicate identity theft on websites focuses on perceived security. Our analysis aims to investigate if this approach is enough and how it is used in practice on websites of well-known e-retailers in the UK. The next section describes our research methodology. The findings section outlines what UK e-retailers are communicating on websites regarding identity theft and related fraud. The discussion section proposes what can be considered as promising practice, we call it the STEP method. The final section concludes with a critical evaluation of the results.

2 Research Methodology

The nature of this research required an analysis of organizations' websites. This paper is an analysis of websites of ten large online retailers in the United Kingdom, shown in appendix one and table one. All of them sell consumer goods online. One of these retailers is the sponsor of this research.

Table 1. Chosen sample of retailers

No	E-retailer	Industry	E-retailer
A	Computer Supermarket.com	Computer	http://www.computersupermarket.com/
B	Bodyshop	Body care	http://www.thebodyshop.co.uk/
C	Laura Ashley	Furniture, Home	http://www.lauraashley.com/
D	Multizoneav.com	Computer	http://www.multizoneav.com/
E	PC World	Computer	http://www.pcworld.co.uk/
F	Amazon.co.uk	Miscellaneous	http://www.amazon.co.uk/
G	Sainsbury's	Supermarket & miscellaneous	http://www.sainsburys.co.uk/home.htm
H	Debenhams	Miscellaneous	http://www.debenhams.com/
I	Marks & Spencer Plc	Cloths & Grocery	http://www.marksandspencer.com/
J	Shop Direct (Littlewoods)	Miscellaneous	http://www.littlewoods.com/

We identified all possible actions companies mention or perform on their websites that are related to identity theft and identity fraud. Based on a first sample we developed an analysis sheet, containing five categories of information that will be presented separately in the findings section: Accreditation, prevention of identity

theft, prevention of identity fraud, empowerment of customers, and reaction when fraud occurs.

3 Findings

3.1 Trust-building Information

It is important to publish security and identity theft related information on websites because consumers have the legal right to be informed. Consumers may also gain trust if they get the impression that a company takes these issues seriously.

We found that e-retailers try to establish trust on websites by letting customers know what they do to battle the crime: accreditation, prevention of identity theft, and prevention of identity fraud. These attempts are described here and evaluated in the discussion section.

3.1.1 Accreditation

One way of gaining trust is demonstrating an accreditation with companies who check the safety of internet pages. Information on different accreditation programs can be followed up by links given in appendix 2. The following table shows how our sample of e-retailers makes use of it.

Table 2. Information given about accreditation of data security

	A	B	C	D	E	F	G	H	I	J
Participant of the Safe Harbor Framework						x				
ISIS accredited by IMRG										x
Certified Tier 1 PCI DSS Compliance			x							
SafeBuy Web Code of Practice	x									
VeriSign SSL certificate				x						
IMRG member (e-retail industry body)										x
Link to accreditation website	x		x							x

When a website links to an accreditation program, it does not always mean that the organization is accredited, e.g. the ISIS link on Laura Ashley's (C) website. Half of the e-retailers of our sample do not mention accreditation at all.

3.1.2 Prevention of Identity Theft

A second way of gaining trust is to demonstrate how much the organization does to prevent identity theft. The statements we found on the analyzed websites are described in following table three.

Most of these points reflect the requirements of the Data Protection Act 1998 (ICO, 2009). Organizations in the UK are legally obliged to protect customers' data from

identity theft and publish a security statement on their websites. The security statement should inform consumers about who is collecting their personal information, which data are stored, what the data are used for, their rights of accessing the data and refusing their storage and usage, and finally the use of cookies and other tracking systems. Additionally the Data Protection Act 1998 demands a transcription-based transmission system. Sensitive personal information should be secured by encryption or similar techniques on a website operator's server.

The analysis of organizations' websites in table three reveals that some of the organizations just mention the minimum requirements of the Data Protection Act 1998; others put a lot of effort in to show how serious they are about data security.

Table 3. E-retailers' actions to prevent identity theft

	A	B	C	D	E	F	G	H	I	J
Protect customers' data when they are transferred or stored										
Secure online data transfer										
Secure sockets layer (SSL) software is used	x		x	x	x	x			x	x
E-retailer only accept orders using SSL software					x					
Encryption is used	x		x			x		x		x
Secure storage of data										
Encrypted sensitive data when stored (e.g. credit card data)								x		
Stored data on separate server / secure server	x			x		x		x		
Payment card data are deleted when account has not been used for a while							x			x
Secure transfer of data										
Onward transfer of data only to reliable sources or not at all				x		x				
Choice of established delivery firm										x
Only part of the debit or credit card is revealed when confirming the order					x	x				

3.1.3 Prevention of Identity Fraud

There are no legal obligations in the UK about how companies should inform consumers on websites about identity fraud.

Table 4. E-retailers' actions to prevent identity fraud

	A	B	C	D	E	F	G	H	I	J
Fraud-monitoring systems in place										
Data checked with fraud prevention agencies										x
Credit Card checks - details passed to credit reference agencies	x		x		x					
Procedures in place to detect fraud						x	x			x
Automated decision making systems in place when assessing customers										x

	A	B	C	D	E	F	G	H	I	J
Authentication systems in place										
Multi-factor authentication for customers' accounts										
Ask for password and postcode										x
Additional protection for payment cards										
3D Secure Schemes (MasterCard SecureCode, Verified by Visa)	x							x	x	x
Information for customers what happens when identity fraud is detected										x

The Data Protection Act 1998 (ICO, 2009) only obliges organizations to publish their physical address on their website. This enables consumers who are victims of identity fraud to ask for relevant information. Nevertheless the website analysis, shown in table four, reveals that some organizations describe other means to protect customers from becoming fraud victims.

3.2 Empowering Information – How Customers can Protect Themselves

Apart from gaining customers' trust as shown above, organizations use websites as well to inform customers how they can secure their own privacy, illustrated in table five. Again, some of the organizations mainly focus on the minimum requirements of the Data Protection Act 1998; others put a lot of effort into providing information for customers.

Table 5. E-retailers' information for customers to deal with data security

	A	B	C	D	E	F	G	H	I	J
Information about legal requirements										
Give notice how data are handled	x	x	x	x	x	x	x	x	x	x
Tell customers that they have the choice of submitting data or not	x		x	x		x	x		x	x
Let customers know how they can access their data	x			x	£10	x	x		£10	£10
Mention that data are used in accordance with legal requirements	x	x	x	x	x	x	x	x	x	
How to protect personal information										
Contribution to secure data transfer										
How to recognize secure websites				x	x			x	x	
Inform customers about secure versions of internet software					x					
Account protection										
How to create safer passwords						x			x	
Remind customers to keep password safe						x			x	
Prompt customers to sign off						x				

	A	B	C	D	E	F	G	H	I	J
before leaving the website										
Prompt customers to close browser when finished on public computers						x			x	
Protect customers from Spoof/false e-Mails and false phone calls										
Explain the nature of spoof/false e-mails						x			x	
Let customers know how you do not contact them					x	x	x		x	x
Advise customers never to enter sensitive data into an email						x	x	x	x	x
Let customers know how you contact them						x		x		
Inform customers about data security and secure online shopping in general										
10 Tips of ISIS			x							x
Data transfer via internet is never 100% safe	x								x	
Explain what is identity theft										x
Advice to check security of linked websites before entering data		x				x	x		x	
Advice to ensure that customers' personal details are kept confidential										x
Advice to destroy documents with personal details by using paper shredders										x
Advice to check payment statements regularly for unknown transactions										x
Advice to fully close accounts when customers do not need them anymore										x

3.3 Supporting Information - What Companies do when Identity Fraud occurs

Finally we found some information that has not been considered by Collins' (2005). Three e-retailers of our sample communicate on their websites what they do when identity fraud occurs, shown in table six.

Table 6. E-Retailers' Information what happens when Identity Fraud occurs

	A	B	C	D	E	F	G	H	I	J
In case of unusual orders, drivers can reserve the right to query the order										x
Identity theft team - Personal case worker										x
Inform fraud prevention agencies										x
Pay for up to £50 of damage if payment card is fraudulently used						x				
Information for customers how to apply for a personal credit report										x
FAQ - what do I do when my card has been used fraudulently?								x		
Security and identity theft as help topic										x

3.4 Types of Information Policies on Websites

We can summarize that we found three main approaches in battling identity theft on e-retailers' websites. The minimalist approach just fulfils legal requirements and does not seem to put much emphasis on trust-building, e.g. the website of Bodyshop (B). This finding supports Collins' hypothesis that the minimalist approach is still used by practitioners. The prevention approach aims to gain customers' trust by highlighting how securely data are handled and by informing customers of how they can protect themselves. It has been recommended by Collins (2005) and is used by most e-retailers of our sample. Finally there is a holistic approach, e.g. the website of Shop Direct / Littlewoods (J), which combines the prevention approach alongside giving additional information of what happens after identity fraud occurs. In the following section we will discuss the components of these approaches and develop promising practice which we call the STEP method.

4 Discussion

Because of legal requirements all organizations have to follow at least the minimalist approach. Should e-retailers do more on their websites? We are proposing the STEP method which stands for **S**upport – **T**rust – **E**mpowerment – **P**revention (STEP).

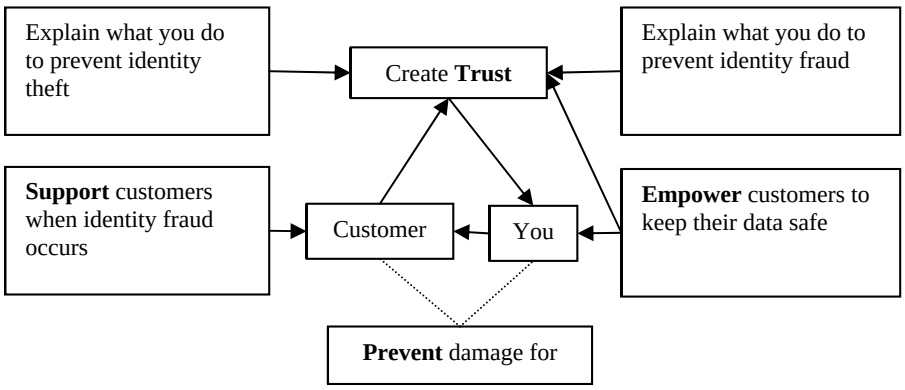

Fig. 1. The STEP Method

This holistic approach is based on the promising practice of the findings' section above.

4.1 "S" for Support

Support means that organizations should provide the best possible support for consumers when the latter become victims of identity fraud. Identity fraud does not only cause financial losses, it can have tremendous impacts on consumers' health. Collins (2005) points out that identity fraud can cause an emotional component comparable to the effects of rape and calls the crime "identity rape". Therefore we suggest E-retailers should not only provide fast support for victims but also make this support visible on their websites. Promising practice is described in table six. We recommend positioning this information in the Help or Customer Services menu and under frequently asked questions. It should contain information about who to contact when identity fraud happens; and provide general information about the first essential steps the consumer needs to take, e.g. how to contact credit reference agencies for credit reports. A fully trained personal case worker seems to be a promising way of dealing with the emotional upset of victims. A good example for this kind of support is the website of Shop Direct / Littlewoods (J) in table six.

We recommend on top of this to inform customers on e-retailers' websites in more detail about the nature of identity fraud, how it usually occurs, and its impact on victims.

Figure one shows that support prevents damage for customers. Victims are not necessarily customers when a fraudster has set up a fraudulent account in their name. E-retailers can see this as an opportunity to win victims of such crimes as new customers by supporting them in a best possible way and winning their trust.

4.2 "T" for Trust

Trust means that consumers should have evidence that they can trust the website. For many well-known companies trust is implicit given their long-standing reputation. Younger and less well-known companies may benefit from some form of accreditation. Research (cited by Safebuy, n.d.) suggests that consumers are more likely to buy when they find accreditation symbols on websites. Our sample shows in table one that larger well-known e-retailers might not need this kind of confirmation of their trustworthiness.

As shown in figure one, trust can be as well obtained or reinforced by describing what else organizations do, apart from following legal requirements, to keep customers' data safe and to prevent identity fraud. Examples are given in table three and four.

Promising practice of communicating prevention of identity theft above legal standards is e.g. the choice of a reliable delivery firm or showing only parts of the debit or credit card on the order confirmation. Some e-retailers emphasize how secure their data transfer and storage is, selling the legal standards very well.

Amongst our research sample, two e-retailers avoid mentioning identity fraud related prevention methods on their websites, Bodyshop (B) and multizoneav.com (D). Firstly they miss out on informing customers and creating more trust. Secondly fraudsters may be more likely to target a company when such information is not provided. Therefore we recommend including it on websites. 3D secure schemes, credit card checks and procedures to detect fraud are the most popular prevention methods mentioned in our sample. We recommend additionally implementing multi-factor authentication and communicating it on websites as this seems to be one of the safest prevention methods.

Finally there is an expected positive effect on trust when e-retailers support victims of identity fraud. Trust is, as shown in figure one, beside prevention one of the two central themes of the STEP method.

4.3 "E" for Empowerment

Empowerment stands for informing the customers of how they can avoid identity theft and fraud. We regard it as good practice to inform consumers about the real risk of identity theft and identity fraud. They need to take it seriously in order to be prepared to actively prevent it. The empowerment of customers to deal with data security has two main advantages, as shown in figure one. Firstly consumers are more likely to protect themselves when they are aware of the risk of identity theft and know how they can minimize it. This reduces the damage for the e-retailer. Secondly consumers will be more interested in the security statement when it applies to them and probably gain the impression that this organization takes their security seriously.

Table five gives an overview what kind of information can be given. We find it especially useful to inform customers about "phishing" and ways how they can avoid becoming a victim of this crime. This includes spoof / false e-mails. The websites of Amazon (F) and Marks & Spencer Plc (I) are good examples. Customers should be made aware how they can protect there payment card details, how important it is to

logoff their accounts, and how they should choose their passwords to make them more secure. The more information is given, the better the empowerment. The only exception is the legal requirement that does not seem to be helpful to prevent identity theft.

4.4 "P" for Prevention

As shown in figure one, support, trust, and empowerment ensure that the e-retailer heads for a better level of prevention than with the minimalist approach or the prevention approach that has been proposed be Collins (2005).

The likelihood for the e-retailer of becoming a victim of identity fraud can be reduced. If prevention methods are communicated on websites fraudsters may be less likely to target this company. Customers are more likely to prevent crime when they are empowered and know how. We would expect less account takeovers and cases of application fraud for an e-retailer who provides such information, and therefore less related costs.

The support within the STEP method adds one additional preventative point; as arrows demonstrate in figure one. Negative effects of occurred identity fraud on customers, especially emotional damage, can be better prevented when supportive information is in place. Customers are more likely to stay customers when they are treated with care, and when trust is created through this experience. The advantage for the e-retailer might be the prevention of lost revenues or even a gain of more customers.

Therefore we can summarize that prevention is beside trust-building one of the two strength of the STEP method. It outperforms the prevention method in both aspects.

5 Conclusion

We reached our aim and identified three approaches of communication on websites in practice regarding identity theft and identity fraud, the minimalist approach, the prevention approach, and the holistic approach. We favor the holistic approach and recommend the STEP method that combines different ways of good practice we have found on the reviewed websites. The outcome of this paper can be used by e-retailers to review their current websites and their identity theft risk management approaches. It proposes plenty of options of how to inform customers on websites not only to gain trust, but also to better prevent crime. It is as well a good starting point for further research.

This paper will be followed by primary research testing the pros and cons of the holistic approach compared to the more popular prevention approaches. The result of this paper is based on a limited sample of organizations and needs to be confirmed by extending the sample size. It is also limited by using websites as the only source of gathering information.

References

1. Acoca, B.: Online Identity Theft. OECD Observer 268, 12--13 (2008)
2. Berkowitz, B., and Hahn, R. W.: Cyber Security: who's watching the Store. Issues in Science & Technology 19 (3), 55--63 (2003)
3. CIFAS: Identity fraud and identity theft. CIFAS Online, http://www.cifas.ork.uk/default.asp?edit_id=561-56
4. Collins, J. M.: Preventing Identity Theft in Your Business: How to Protect Your Business, Customers, and Employees. John Wiley & Sons, Hoboken, pp. 156—161, 173--177 (2005)
5. ICO, Data Protection Act 1998 - Data Protection Good Practice Note for collecting personal Information using Websites, Information Commissioner's Office's Data Protection Guide, http://www.ico.gov.uk/home/for_organisations/data_protection_guide.aspx
6. Lindsay, N.: E-Commerce: Boom or Bust? Computer Weekly, (Jan 25, 2005), 18--19 (2005)
7. Myers, S.: Introduction to Phishing. In: Jakobsson, M., Myers, S. (eds.) Phishing and Countermeasures, pp. 1-29. John Wiley & Sons, Hoboken (2006)
8. PITTF, 2007: Combating Identity Theft: A strategic Plan. The President's Identity Theft Task Force, http://www.idtheft.gov/reports/StrategicPlan.pdf
9. SOPHOS, 2007: Phishing, phaxing, vishing, and other Identity Threats: The Evolution of Online Fraud. A SOPHOS White Paper, http://ithound.vnunet.com/view_abstract/1181?layout=vnunet
10. Sullins, K. L.: "Phishing" for a Solution: Domestic and international Approaches to decreasing Online Identity Theft. Emory International Law Review, 20 (1), 397--433 (2006)
11. Tan, H. S. K.: E-Fraud: Current Trends and international Developments. Journal of Financial Crime, 9 (4), 347--354 (2002)

Appendix 1: Websites of the Analyzed Sample

Amazon.co.uk. (March 10, 2009), http://www.amazon.co.uk/
Bodyshop, (March 24, 2009), http://www.thebodyshop.co.uk/
Computer Supermarket.com, (March 24, 2009), http://www.computersupermarket.com/
Debenhams, (March 24, 2009), http://www.debenhams.com/
Laura Ashley, (March 24, 2009), http://www.lauraashley.com/
Marks & Spencer Plc, (March 24, 2009), http://www.marksandspencer.com/
Multizoneav.com, (March 24, 2009), http://www.multizoneav.com/
PC World, (March 11, 2009), http://www.pcworld.co.uk/
Sainsbury's online, (March 10, 2009), http://www.sainsburys.co.uk/home.htm
Shop direct group: Littlewoods, (March 24, 2009), http://www.littlewoods.com/

Appendix 2: Websites for Accreditation

Certified Tier 1 PCI DSS Compliance by venda, (March 24, 2009), http://www.venda.com/
IMRG, (March 24, 2009), http://www.imrg.org/
ISIS, (March 24, 2009), http://isisaccreditation.imrg.org/
Safebuy, (March 24, 2009), http://www.safebuy.org.uk/
US-EU Safe Harbor Framework, (March 10, 2009), http://www.export.gov/safeharbor/
VeriSign SSL, (March 24, 2009), http://www.verisign.co.uk/ssl/