

Combating Identity Theft

Article by Folajimi F Akinsuyi (LL.B, BL, MSc, LLM)¹, April 2005

Introduction:

Identity theft has taken up new grounds in the debate about the protection of personal information. High profile successful unauthorised and fraudulent access to databases where personal information is stored have more recently also called for speedy enactment of stringent legislation to assist in the curtailment of the phenomenon.

Identity theft was initially thought to affect the individuals whose personal information has been hijacked. It can however be seen that organisations whose primary business involves obtaining and selling personal information are falling prey to sophisticated criminals. These criminals are willing to go the extra length to obtain as many instances of personal information at one fell swoop, rather than having to hunt for individual pieces of information risking being caught out at each attempt.

Organisations that have made a business out of the brokerage of personal information have also learnt first hand that identity theft can lead to damaged reputation and a drop in share value². This can be illustrated with Choicepoint and Lexisnexis³ both of which have been hit by large scale identity theft of personal information stored on their databases.

¹ Folajimi F Akinsuyi is a Partner at DataLaws Ltd an information technology law consultancy

² See Nearly 3,200 Washingtonians Affected By ChoicePoint Breach reported 23rd February 2005 by komo news available at www.komotv.com/stories/35405.htm

³ See Security breach at LexisNexis now appears larger: Article by Heather Timmons and Tom Zeller JR NewYork Times April 13, 2005

Why is identity theft on the increase?

It has been identified in recent surveys⁴ on both⁵ sides of the Atlantic that identity theft has increased over the years at an exponential rate costing individuals and companies billions. Indeed in the study on the issue for the United Kingdom it has been estimated that identity theft is responsible for the economy losing out on an estimated £1.3 billion. While in the United States of America, the figure has been estimated by the Federal Trade Commission to be in the region of \$48 billion. Given the above stats coupled with the growing numbers of people using the Internet to carry out commercial and personal activities, it can be determined that these numbers will accelerate over the next three years if nothing is done to curtail its progress.

The reasons for this can be attributed to a number of reasons:

1. Huge margins for little effort and risk on the part of criminals

The rise in identity theft can be attributed to the relative ease in which it is possible to gain access to personal information along with the process used by merchants and suppliers of services in verifying such information in return for goods and services. Key attributes utilised by most organisations in the United Kingdom to verify a person's identity are their: name, date of birth and mother's maiden name.

An identity thief will look to environments where this information can be obtained typically:

- Call centres of utility service providers or financial institutions.
- Opportunist identity thieves using their place of work to gain unauthorised access to personal information,
- Others taking the less sophisticated route of trawling through bins.

Whatever route is used, once the information is obtained they typically set about creating accounts in the name of the victim to obtain goods and services or in more sinister cases commit serious crimes.

⁴ See <http://www.ftc.gov/opa/2003/09/idtheft.htm> for the United States of America

⁵ See http://www.homeoffice.gov.uk/docs/id_fraud-report.pdf for the United Kingdom

Once they have obtained their objective with the identity they move on leaving the victim and organisations that have been hit to sort out the wake they have left behind.

A reason why it appears as if identity theft is growing is that there does not appear to be a concurrent rise in the number of criminals being arrested and jailed for identity theft. This can be attributed to the guile and sophistication of the criminals.

2. No appropriate legislation or punishment to deter identity thieves

A fundamental loophole at the moment is that legislation has not kept up with the manner in which identity theft is being perpetrated. As has been stated in the introduction, in the United States it has only been the recent Choicepoint and LexisNexis breaches that have led to the clamour for federal legislation on the issue. In the United Kingdom while there is a drive by the department of trade and industry⁶ to make people aware⁷ of the issues thus making them more cautious about their personal information, there is no offence for identity theft. It can also be identified that there is no appropriate legislation to sanction organisations which have been careless or negligent in their handling of personal information.

When an individual makes a fake claim for goods or services, more often than not they will be turned down rather than be prosecuted for their actions as such they will keep trying different methods until they succeed knowing that they are not technically committing an offence.

3. Organisations not deploying appropriate security measures

While it has been well publicised that implementing information security is crucial to the reduction of breaches to systems, it is surprising that many organisations are not adopting appropriate security measures on systems which are used to store, process, transmit and destroy personal information. How often have we been informed that personal information

⁶ See <http://www.dti.gov.uk/bestpractice/assets/security/frauds-scams.pdf>

⁷ See www.consumerdirect.gov.uk

has been found on systems that have been discarded by organisations⁸, personal information being compromised by online break-ins⁹, internal staff gaining unauthorised access to personal information¹⁰ or indeed organisations losing personal information of customers¹¹?

4. The Victims

A common denominator in this equation is individuals themselves, many people make it easy for their personal information to be compromised by offering the information without a thought for the consequences, this can be in the form of

- Filling out questionnaires when replying to mailshots,
- Providing the information to unsolicited callers without verifying who they are or whether indeed the organisations they claim to work for actually exist,
- Carrying too much information on their person such that if they misplace their wallets, or handbags, opportunists can use the information to obtain goods and services in their names.

5. Items used to prove ones identity

Let us take a look at the components that make up a persons identity, typically, it constitutes their name, date of birth, social security number, or mothers maiden name. Each of these is used when applying for documents that are used to identify an individual, for instance driver's license or passport and for the provision of services, bank accounts or utility services. The problem lies in the manner in which these documents are issued and also the verification process used to gain access to such services. It has been identified that the process for issuing passports and driving licenses are not secure¹². It has been well documented that

⁸ See San Francisco Chronicle Thursday, August 23, 2001 where it was identified that a laptop purchased at an auction still contained personal information on employees of the purchasers former employer

⁹ See Washington Post Thursday, January 13th, 2005 where a hacker obtained Social Security numbers, names and other personal information from as many as 30,000 students and employees in a break-in discovered Jan. 3 by the George Mason Universities computer management workers

¹⁰ See US V Luckey where a former credit union employee admitted releasing confidential personal customer information to the defendant. She also pled guilty, to obtaining financial information contained in the credit union computer. More information about this case can be viewed at <http://www.usdoj.gov/criminal/cybercrime/LuckeySent.htm>

¹¹ See Japan Times 31 March 2005 where it was reported that Mizuho Bank lost data on as many as 270,000 of its customers

¹² See Identity Theft : A study p22 available at http://www.homeoffice.gov.uk/docs/id_fraud-report.pdf

criminals have been able to successfully produce counterfeit passports¹³ and licenses. When this is coupled with stolen personal information it is plain to see why it is easy to forge a person's identity to obtain goods and services or use it to commit criminal activity.

Possible Solutions:

While it must be stated that it may never be possible to put a stop to identity theft, there are ways in which it can be curtailed. This can in my view be achieved by the following:

1. Implementing appropriate legislation:

As has been stated in the beginning of this article, in the United Kingdom identity theft is not an offence. It may be used to show it fuelled other offences such as theft or deception. In the United States personal information compromise at Choicepoint and LexisNexis have only now led for the clamour for federal legislation on the matter even though studies prior to this pointed to the rise in identity theft.

For any legislation on identity theft to be effective, it needs to take into account the elements and entities which make up the aspects of an identity theft.

Let us take a look at these further:

- The Identity thief

The identity thief is the major element in the equation, any legislation enacted needs to define the offence such that where an individual obtains goods or services in another persons name without that persons consent or knowledge using a form of identity that they know not to be their own with the intention of obtaining goods or services for themselves or with the intention of carrying out a crime, the offence of identity theft is committed. It is to be noted that it should not only be restricted to the obtaining of goods and services, but also to the obtaining of documents used to verify an individual such as passports and driving licences.

¹³ See <http://thisiscostablanca.com/index.php?option=content&task=view&id=387&Itemid=>

The legislation should also make it an offence to gain unauthorised access to personal information with the intent of using the information to obtain, goods, services or creation of another identity.

The legislation must also mete out appropriate penalties for those found guilty of the offence such that it at least serves as a deterrent.

- Organisations

Organisations both public and private are aware of the phenomenon of identity theft and as such the onus of proving that they have not been negligent or careless where an individual's personal information has been compromised should fall on them. Legislation must recognise that individuals place their trust in organisations to keep their personal information confidential and secure. As such, identity theft legislation as a minimum must place mandatory obligations on organisations to implement appropriate vetting and security measures around systems where personal information is held. Where it is determined that they have not, appropriate penalties must be meted out.

Legislation should also provide that where an organisation has detected a breach to personal information under its control, affected individuals must be notified immediately so that they can inform necessary parties of their plight, failure in doing so should also be punished with appropriate penalties.

- The Victim

Where it can be determined that the victim has not been careless or negligent in the handling of their data, the legislation should afford for appropriate compensation

2. Organisations handle personal data appropriately

In the United Kingdom, the Data Protection Act¹⁴ provides that " Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes."¹⁵ Unfortunately when systems are being tested to identify if they integrate with other systems, many organisations instead of using

¹⁴ The Data Protection Act 1998

¹⁵ Schedule 1 part1section 2 Data Protection Act 1998

dummy or anonymised data¹⁶, actually use personal data derived from their production systems. The risk this brings is that the personal information can be printed out either in the form of screen shots or to verify the data meets test script criteria. The printed out material may then be left lying around before it is disposed of. This presents an easy avenue for opportunistic identity thieves to strike.

As has been mentioned call centres are ideal places for identity thieves to thrive, as they are personal information rich environments. Organisations customer relationship management systems are used to identify their customers and call centre staff have access to all this information, access to these systems by calling parties and staff should be monitored closely. There should also be stringent vetting procedures for staff using, developing and making upgrades to these systems.

Another area where organisations can help in the reduction of identity theft is the in the implementation and management of appropriate security. The UK Data Protection Act also provides that “appropriate technical and organisational measures must be implemented on systems utilised to process personal information.”¹⁷

The importance of implementing appropriate security cannot be over-emphasised. Information security here is not limited to technology such as access control, authentication, authorisation monitoring, and auditing of systems, but also includes policies, procedures and processes.

Many organisations have subsidiaries, partners and third party organisations to which they may transfer personal data. In these situations, appropriate contractual agreements should be put in place to ensure any such data transferred is given the same levels of security which the original organisation places on the personal data.

3. Utilisation of technology to assist in making identity theft more difficult

The components that make up personal information can easily be obtained from various open sources. This is one of the reasons why identity theft is on the rise. In order to curtail the success of identity thieves, a different set of identifiers will need to be built into personal information components used for

¹⁶ Anonymised data should exclude the name, address and full post code, and any other information which when combined with other information could allow the individual to be identified.

¹⁷ Schedule 1 part1section 7 Data Protection Act 1998

identifying an individual. The method used to identify people should be reviewed for the long run. As it stands, without a change in the manner of identifying persons from personal but readily available information, the identity thief will always be in business!!

Technology can be an enabling factor in achieving this aim. In the United Kingdom one of the current methods in combating credit card fraud is the introduction of chip and pin on all new debit and credit cards.

Such technology should also be used in providing harder to forge passports and driving licences.

In my view, it would be harder for identity thieves to steal and use an identity if there are a number of other factors placed in the identification process. This could include entering a password for online transactions, along with the expiry date or some form of biometric authentication and validation.

In relation to online purchases, web cam and videoconferencing technology has been in use for a number of years, as a means to reduce customer not present transaction fraud, the authentication and verification process could include adapting these technologies with biometrics.

To conclude:

The rise in identity theft can be attributed to the ease of access to and the simplicity of components that make up an individual's personal information.

Without appropriate legislation, technological advances in the authentication and verification process in conjunction with better handling of personal information by organisations in their processing of personal information there will be no let-up in the phenomenon.

Awareness campaigns on a global scale need to be adopted to ensure people are made aware of the significance and the imperative necessity of safeguarding their personal information.

The technology to drastically reduce the occurrence of identity theft is available likewise legislation can be pushed through to categorise identity theft as a serious offence.

Once these are implemented and given appropriate prominence, we may see a drastic reduction in identity theft.

© Folajimi F Akinsuyi 2005