

Identity Theft: Managing the Risk



A white paper by
Insight Consulting

Why identity theft has become the UK's fastest growing type of fraud and the controls that can be used to reduce its impact

Identity theft occurs when someone steals and misuses an individual's personal data such as their name, address or passport number. Whilst this theft of identity is, by itself, not a crime under UK law, misusing the identity information to fraudulently obtain goods or services is.

Identity theft has most commonly arisen from physical attacks such as burglary or pick-pocketing where identifying information is stolen from credit cards, passports or driving licences. More recently, though, identity theft has enveloped the online world as a result of:

- Increasing numbers of consumers surfing or shopping on-line
- More online sources of personal information often derived from the Electoral Register
- Increased use of credit and information exchanged with banks and retailers.

This white paper is primarily aimed at corporate audiences and examines identity theft in relation to the risks associated with eCommerce and the Internet. It also covers issues relating to personal identity theft and will, therefore,

be of interest to individuals themselves as well as organisations that offer online services to such individuals.

Impact to individuals and businesses

Identity theft has become the fastest-growing type of fraud in the UK and already costs Britain £1.3bn a year.

For individuals, the main impact of identity theft is likely to be unauthorised use of one or more of their existing credit card accounts. Such crimes can normally be detected by the identity owner within a matter of weeks following receipt of their next statement – assuming that the individual regularly checks it.

However, in the event that the stolen identity information is used to create a new account, it may not be possible for the identity owner to detect any offence for some time. In many such cases, account statements will have been redirected to an address selected by the thief. The owner will only become aware of the activity when either the credit card company debtors or bailiffs contact them to settle the debt-ridden account – or when legitimate future credit applications

SIEMENS

Global network of innovation

Insight Consulting

made by person fail.

Whilst credit card customers are generally only liable for the first £50 of unauthorised transactions, the harm to person's credit reputation, their inability to carry out domestic business – as well as efforts to put things right – can be far more damaging and long lasting to the individual.

The cost of identity theft – in terms of paying for fraudulently obtained goods – is most likely to be claimed against the relevant retailers by the credit card issuer. Indirect costs to business include reduced levels of sales through eCommerce channels due to continuing concerns over security and privacy of the Internet and, when news about identity thefts are published, any named company may have its reputation damaged as a result.

In the UK, the Home Office reported identity theft statistics that included over 3000 driving tests which were terminated due to concern over the identity of candidates, 1500 fraudulent passport applications, and over 500 cases of identity fraud identified by the Benefits Agency.

In more extreme cases of identity theft, such as identity cloning, the importer uses the victim's information to establish a new life. Examples include illegal immigrants, criminals avoiding warrants, people hiding from abusive situations or other instances where becoming a 'new individual' would be advantageous to them.

Corporate identity theft allows criminals to order goods or obtain services from suppliers on company accounts or to conduct industrial sabotage. For the company that becomes the target of this activity, there would be an impact of direct financial losses of misappropriated services or goods, possible fines resulting from breach of regulatory rules and, significantly, loss of actual and potential customers resulting from harm to the company's reputation.

Company directors have a duty to exercise control and, in the event they breach their responsibilities, they may be liable for disqualification from being a director. In the case of stolen corporate

identity being used to obtain confidential company information, there could be a loss of competitive or marketing advantage, loss of staff morale and also public confidence. It's important to note that 'insiders' carry out the majority of identity theft and fraud involving companies.

Threats and vulnerabilities

There are a number of threats and vulnerabilities to systems that have given rise to the increase in significance of identity theft.

Internal attacks on systems The storage of large numbers of individual's personal records on eCommerce sites presents a clear risk to the identity of the customers or subscribers involved. Credit card details – including expiry dates which can allow 'card not present' purchases to be undertaken – as well as passwords and other personal identifying information offer the identity thief a variety of opportunities for misuse.

Earlier this year, bulk disclosure of personal information from the computer system of a North American insurance company followed the theft of a computer disk drive. The paperback-sized, 30-gigabyte drive went missing from the organisation's supposedly secure computing facility. The drive was recovered but the data it contained has been overwritten. Police believe an employee of the company stole the drive for personal use.

One of the largest known and published incidents of identity theft involved an employee of a US company that supplied banks with credit reports from many of the large credit agencies. He used confidential computer passwords and subscriber codes to access and download the credit reports of over 30,000 consumers during a three year period. The employee provided the stolen codes to external co-conspirators who were willing to pay up to \$60 per credit report.

Increased use of mobile devices Many millions of people now rely on PDAs for electronic scheduling and address books as well as storing passwords and codes for their online banking accounts. However, very few individuals carry sufficient security protection to prevent identity theft if the hand held device is lost or

stolen – and such loss is commonplace.

Of the users who store their bank account details on a PDA, it has been estimated that around two thirds do not encrypt this information, with just under a quarter failing even to implement password protection. Further revealing statistics indicate that around 6 per cent of users have lost PDAs in the past, but 32 per cent of those still continue to use them without a password.

Online scams There have been a great many reported cases where individuals have been enticed, by email, into disclosing sensitive information such as passwords by using clever social engineering trickery. The substantial torrent of spam now produced worldwide has included a number of such scams.

In a recent case, a teenager was charged with using spam emails and a fake web page from a well-known ISP to trick people into divulging credit card information. The emails told recipients they needed to update their ISP billing information and instructed them to click on a hyperlink connected to a billing centre. In fact, the link diverted people to a fake web site - similar in appearance to the legitimate one - containing the company's logo and links to real ISP web pages. The targets of the scam were instructed to enter their credit card numbers, along with mothers' maiden names, billing addresses, social security numbers, personal identification numbers and ISP logon names and passwords. The information that was derived was subsequently used to steal thousands of dollars.

Poor password management A username and password required to access a free website, such as an online news site, is of limited immediate value in itself. But many users tend to re-use passwords, and those same credentials may be valid for giving access to confidential, web-based email and providing access to information at electronic banking and other eCommerce sites.

There's even a good chance that the password is identical to the user's corporate network login. So, identity

information obtained from one source may provide a much bigger impact to its owner when used in different circumstances.

Loss of privacy online Individuals who register or subscribe to services from web sites, or who run file or plug-in downloads run the risk of giving away more personal information than they realise - and to parties that they are not even aware of. Any activity in which identity information is shared or made available to others creates an opportunity for identity theft.

The majority of these risks relate to loss of privacy - revealing interests and purchasing trends for the benefit of marketing organisations. In some cases, however, theft of identity can result when information submitted to a web site run by an unscrupulous organisation is passed on to a dishonest third party.

Web mechanisms including cookies, adware and web bugs may all be misused to achieve this loss of privacy, and ultimately identity theft. For more information on this subject, see Insight's white paper entitled *Spyware – The Risks Facing Businesses*.

Confidential documentation theft

Dumpster diving – involving the searching of waste for confidential information that has been discarded – has been identified in a recent survey to be a major source of identity theft. The survey, which interviewed local councils in the UK, revealed a significant number of incidents involving the practice and which specifically targets individuals at home where the use of paper shredders, for example, is still relatively uncommon and where awareness of the associated risk is similarly low.

The survey also identified many cases of information that could be used to instigate identity theft such as utility bills, bank statements and blank cheques together with household documentation that included samples of individual's signatures.

Corporate security measures

A number of regulatory requirements that affect organisations now encompass risks such as corporate identity theft. The guidance contained in the *Turnbull*

Report, for instance, states that a board of directors is responsible for a company's system of internal controls, and that they consider the nature, extent and likelihood of the risks faced by their company.

It also requires that a company's annual report includes a statement on the effectiveness of internal controls and non-compliance with the Turnbull code. Whilst this guidance is mandatory for companies listed on the London Stock Exchange, it does also provide sound business advice for smaller organisations as well.

Some of the controls that specifically address corporate identity theft and the risks described above include:

- Recruitment security checks on new staff
- A clear desk policy and use of secure storage for sensitive documentation
- Ensuring personal data is adequately secured with access limited to named individuals
- Secure disposal of confidential information
- Segregation of duties, ensuring that not one person is solely depended upon to carry out a business process
- Secure procedures for exchange of personal information
- Ensuring the personal and sensitive data stored on websites and other vulnerable systems is encrypted for additional protection
- Documented procedures for verifying the identity of individuals
- Effective access control measures for password management, user registration and de-registration procedures (with the ability to examine historical data access records)
- Restricting corporate desktop configurations such as browser settings for accepting cookies or downloading active code.

Recommendations for individuals

Individuals, whether operating in a corporate or domestic environment, have a responsibility to take measures to minimise the risk of identity theft.

Online precautions Users should ensure that any web sites they are looking to register with, or subscribe to, have a privacy policy. Credible policies should be both easy to find and to understand. Most reputable organisations include a link to a privacy policy on the home page of their web site.

The policy should reveal what information a web site collects and what it is used for. If the web site shares the information with anyone else it should tell the user and give them the option of restricting such use. A privacy policy should also describe the security used to protect personal information.

There are a number of organisations that now provide privacy seals designed to provide assurance that a web site is abiding by its posted privacy policy. The presence of a seal indicates that the company has implemented privacy mechanisms and procedures and that ongoing checks are implemented to ensure that this remains the case.

The use of seals provides some advantage over the more automated privacy checks performed by sites complying with Platform for Privacy Preferences (P3P) standards.

Browsers that are compliant with P3P will notify the user if a website does not have a privacy policy – or if it does not meet the level configured in the browser. What P3P cannot do, however, is ensure that a site that claims, for instance, not to disseminate personal data to third parties does indeed comply with this stated policy.

Other measures Many of the guidelines for individuals to help prevent identity theft are similar to those that underpin any good information and password security policy. Users should ensure that waste paper placed in recycling trays does not include personal or sensitive data. The owner, preferably using a shredder if one is available, should take care to securely destroy all such information.

Individuals should also be cautious about giving personal information to someone who is not personally known to them but who claims to have a legitimate need to know personal data. Most corporate

information security policies prohibit users divulging passwords to anyone, and there should never be a legitimate need to share a personal account and password.

Individuals should maintain a clear desk policy in the office – visitors who do not have authorisation to read corporate data may well occupy the same office area. Similarly at home, family, friends or cleaners may not realise the sensitivity of information and may inadvertently possibly pass it on to someone else who does.

Future developments

In the UK, the Home Office is proposing new measures that could mean that a fraudster could be arrested for mere possession of a false document. This would mean that criminals who were caught with stolen documents – such as fake passports or driving licences – could face up to two years in prison. In the US, identity theft is already a crime under *The Identity Theft and Assumption Deterrence Act*.

And, in a move to further improve the privacy of online activities, IBM has unveiled an open-standard privacy language designed to provide a method of automating the enforcement of privacy policies. The Enterprise Privacy

Authorisation Language (EPAL) is a means to express data-handling policies inside the enterprise and goes one step further than the existing P3P privacy specification.



Insight Consulting is the specialist security, compliance and continuity unit of Siemens Communications.

We offer a complete, end-to-end portfolio encompassing:

- Research
- Consultancy
- Testing
- Implementation
- Training
- Recruitment
- Managed services

Insight is BS7799 certified, is a GCat and S-Cat (Category 7) supplier and subscribes to the CESG Listed Advisor Scheme (CLAS) and CHECK services.

If you'd like to discuss how Insight could help you manage risk in your organisation, email us at insight@insight.co.uk or visit www.insight.co.uk

Insight Consulting

Churchfield House
5 The Quintet
Churchfield Road
Walton on Thames
Surrey KT12 2TZ
United Kingdom
Tel: +44 (0)1932 241000
Fax: +44 (0)1932 244590