

# IDENTITY DECEPTION AND REDEMPTION AN OVERVIEW

Author Robert Bromwich

*Published and presented at the 2010 Online Networks and Communities conference sponsored by Curtin University of Technology and organised by students studying Net 204/504 Social Networks and Communities.*

## Abstract

The development of the internet and other electronic communications tools over the past 20 years has seen substantive facilitation of global commerce and service delivery for corporations, government agencies and individuals. Such facilitation has allowed the conduct of commerce across multiple locations at moderate cost.

The development of the online commerce environment has allowed those engaged with identity deception to ply their trade with near anonymity and with minimal risk of capture or prosecution. Authoritative studies by government agencies (Federal Trade Commission), private organisations (Javelin Research and Strategy) and non profit groups (Identity Theft Resource Centre) over recent years have documented the monetary and social costs associated with identity deception.

The purpose of this paper is to provide guidance on how organisations and individuals can combat identity deception and ensure that their finances and reputation will remain intact when identity criminal arrives.

---

The issue of identity management, assurance and integrity for individuals, businesses and government agencies across multiple contexts (commercial, transactional, service delivery) during the past two decades has become an increasingly complex and difficult challenge to combat. The increase of identity-related crime and deception directly impacting on individuals and businesses has impacts economically, socially and institutionally. Despite concerns over identity deception by corporations and government agencies – coupled with outright apathy by the community – no clear definition has been articulated to enable a general understanding of the issues involved and the challenges involved in combating the issue. The confusion is enhanced by the diffuse efforts by and competing interests of governmental agencies and private organisations in promoting particular products (e.g. credit reports) and general awareness of the issue.

The purpose of this paper is to provide an overview of the concepts of identity for individuals and corporations – particularly in an online environment, identity deception and its impact coupled with potential strategies available for individuals and organisations to minimise the negative effects of identity deception. Without an ongoing effort to minimise and eradicate the harmful effects of identity deception, the ability for corporations, government agencies and individuals to interact in good faith is at risk.

Identity is a challenging concept to define and articulate as academics, philosophers, religious scholars and sociologists have attempted to characterize identity on a personal level for centuries. For the purposes of this discussion, individual identity comprises three elements (Mills 2007, p. 14-18):

1. **Biometric:** Unique physical attributes (fingerprints, retina, facial profile);
2. **Attributed:** Components acquired at birth (full name, date of birth, parent names);
3. **Biographical:** Life events of an individual (employment history, education profile, governmental and financial institution interaction).

The concept of online identity has been evolving with the growth of the internet and online networking sites including Facebook, MySpace and Twitter. Such sites provide the opportunity for individuals to promote themselves to a global audience at minimal cost. The consequence of this strategy is information being archived, allowing people to access such information being accessed to cause embarrassment or other discomfort.

Corporate identity is a more artificial, legalistic concept granted by a nation-state and has been evolving over the past two centuries. The ability for corporations to exist is based solely at the behest of the nation-state, allowing a controlled, documented definition of identity (the entity's constitution or articles of association).

In Australia, identity management for individuals is generally governed by the 100 point system and the 2004 Proof of Identity Framework (POI), with both frameworks accepting similar documentation as POI (ICAC 2006, p. 9). Whilst these frameworks were initially intended to combat money laundering and other like crimes, versions of the 100 point system have been adopted by government agencies and private organisations, allowing over time for these frameworks to become an unofficial national POI standard (ICAC 2006, p. 9).

An example of the challenge of promoting awareness to companies, public sector agencies and individuals was highlighted by a 2009 study conducted by the Australian Communications and Media Authority (ACMA). The study documented various factors – including a belief that breaches were inevitable and the pace of technological change making it difficult to maintain currency in risk protection – requiring attention to ensure effective protective and remedial action (ACMA 2009, p. 3) by individuals. An anecdotal example from 2008 highlights the challenge in educating the community about identity deception ('Vox Pop', 2008). Responses to a question on the topic of identity deception and strategies to counter it include "I lock my doors"; "I have never been in that situation"; "I live in a quiet area" and "No it doesn't worry me", making awareness of the causes and effects an issue.

Recent studies sponsored by government and commercial entities have identified substantive costs to individuals, corporations and government agencies associated with identity deception. Authoritative calculations for the United States alone range in the billions of dollars annually (Federal Trade Commission; Javelin Research 2010; Aranta Jnr 2004).

The costs associated with identity deception – coupled with the dramatic surge and cost reductions in storage capability during recent years (Yao 2005) – have highlighted the essential requirement for government agencies and corporations to develop, implement and monitor information security policies covering both the strategic and operational aspects (Doherty & Fulford 2005) to secure information resources and content. For individuals, the same principles apply in ensuring that their online identity profile is effectively managed on a personal level, coupled with a rigorous attentiveness in when dealing with government agencies and corporations.

The issues of identity management and assurance within the corporate and government sectors have become a major issue for discussion during recent years with possible technical solutions from federated identity management solutions and electronic (or smart) cards have been gaining recognition during this time (Lips et al 2009, p. 717), promoted by vendors chasing revenue. The interplay with employee relations has also become a policy and legal issue for organisations as data breaches impact on staff morale (Calvasina, Calvasina & Calvasina 2006, p. 26), regulatory compliance (Anonymous 2003) and financial health.

Businesses have traditionally collected information on current and potential customers for various uses (Laudise 2008, p. 26) to assist with commercial operations. Such information can benefit the organisation in numerous ways including financial matters, product development, promotions and market identification without unnecessary staff effort or financial expenditure to correct deficiencies or to ensure regulatory compliance.

The ability for governments to levy taxation, ensure proper and effective delivery of commercial and social services coupled with national security concerns resulting from terror attacks in the United States during September 2001 and the United Kingdom during July 2005 have fuelled the need to have measures in place to identify citizens and authorised arrivals has become core to the political agenda. Government sponsored identity management programs in the United States, the United Kingdom and Australia since 2002 have reinforced this trend, resulting in controversy on political, privacy and financial grounds.

One key concept to understand in the identity deception is the data breach. A data breach occurs when there is an “unauthorised or unintentional exposure, disclosure or loss of personal information” (Peretti 2009, p. 377) to unauthorised individuals or entities. A recent high profile event the 2007 United Kingdom’s Revenue and Customs breach involving the loss of two CD-ROMs containing information on half the United Kingdom’s resident population, some 25 million people (British Broadcasting Corporation 2007).

Coupled with the data breach, corporations and government agencies need to undertake regular information security practices to physically and electronically secure information gathered during the course of business. Such information may seem innocuous at the point of collection, yet poor practices at systems and personnel levels enables nefarious elements to exploit information gained for disreputable activities/

With the development of electronic means of communication and storage during the past two decades means that data security has become increasingly crucial for companies from multiple perspectives – regulatory, public relations and operational. Information gathered in the normal course of company business is at risk of being siphoned by corrupt employees or criminals (though internal or external attacks) to fraudulently establish new accounts or to hijack existing accounts for nefarious motives (Laudise 2008, p. 26).

The most recent legal development was the enactment by California of the first data breach notification statute during 2003 that mandated reporting by organisations to affected individuals or entities in the event of serious data breaches (Laudise 2008, p. 26). Coupled with a United States-based Financial Services Technology Consortium (FSTC) review of identity management standards (Anonymous 2003) aimed at benchmarking online identity management standards, the message is being broadcast that identity assurance is becoming a political issue requiring some attention.

Current technologies handle many aspects of the identity management process with public key technology and biometrics being two of the most high profile examples being utilised. Problems that hamper efforts in assuring identity management include the lack of funding, duplication of effort and even a lack of understanding of the concept of identity in the business environment. Such problems impair the delivery of identity management strategies, cause confusion with individuals and assist those with nefarious intent.

From the organisational perspective, various strategies have been identified to address identity deception in a number of ways, including (Laudise 2008, p. 27-33; Calvasina, Calvasina & Calvasina 2006):

- The need to address the issue of the need to collect and hold sensitive data including data-flow analysis to determine how, when and where information is collected, disseminated and stored within the organisation;
- Obligation to protect from data loss independent from obligation to report data breached;
- Know what data is collected, where it is located and who (staff, contractors etc) have access to it;
- Prohibit the collection of data if it cannot be protected;
- Address obvious internal problems including password management, encryption disposal practices and the like;
- Have a documented data breach plan in place in advance of any adverse event;
- Be informed about any legal trigger notice;
- Act promptly to preserve information and related evidence;
- Utiliser opportunity to retain customers after breach event and recognise the case of when, not if, data breach event.

Individuals can contribute to minimising the effects of identity deception including investing in a shredder, maintaining an inventory of financial instruments and conducting safe electronic and technology practices (Ochlers 2004, p. 20-21).

The surge of identity deception in Western countries has become a significant legal, political, social and commercial issue that requires a concerted effort to resolve before significant economic distress occurs. Without a concerted effort to combat this issue, nothing less than the integrity of the infrastructure and marketplace generated by the globalisation expansion since the 1990s will be at stake.

To effectively combat identity deception, a concerted effort is required by individuals, corporations and governments to secure identity documents; ensure the security of collected information; conduct regular audits of the relevance and currency of information; implement protocols that effectively identify potential suppliers, customers and employees; enact processes that protects identity (birth and death certificates, driver licences) and corporate (stationary etc) documents and financial instruments (cheques, etc) coupled with an community education program targeting preconceptions over identity deception and strategies to minimise risks associated with such deception.

## REFERENCES

- Acoca, B 2008. Online Identity Theft. *The OCED Observer*. 268 July 12-13
- Adams, C 2008. No Certainty yet for Identity Assurance. *Signal* 63(1) 83-86.
- Anonymous 2003. FSTC reviews online identity management standards. *ABA Banking Journal*. 95(5) 96-97
- Australian Communications and Media Authority (ACMA) (2009). *Attitudes towards use of personal information online: Qualitative research report*. Melbourne: Commonwealth of Australia,
- Bielski, L (2003). Striving to create a safe haven online. *ABA Banking Journal*. 95(5) 53-59.
- British Broadcasting Corporation (2007). 'UK's families placed on fraud alert'. Retrieved 22 April 2010 from [http://news.bbc.co.uk/2/hi/uk\\_news/politics/7103566.stm](http://news.bbc.co.uk/2/hi/uk_news/politics/7103566.stm)
- Calvasina, G.E.; Calvasina, E.J and Calvasina, R.V. (2006). Preventing Employee Identity Fraud. *Proceedings of the Academy of Legal, Ethical and Regulatory Issues*. 10(2) 25-29.
- Chandler, J.A. (2008). Negligence Liability for Breaches of Data Security. *Banking and Finance Law Review*. 25(2) 223-273.
- Chula G King, & W Timothy O'Keefe. (2004). Online Identity Theft and Business. *The CPA Journal*, 74(4), 50-52.
- Doherty, N.F. and Fulford, H (2005). Do Information Security Policies decrease the incidence of security Breaches: An exploratory analysis. *Information Resources Management Journal*. 18(4) 21-39
- Javelin Research and Strategy (2010). *2010 Identity Fraud Survey Report Consumer Version: Prevent – Detect – Resolve*. Retrived from <https://www.javelinstrategy.com/research/complimentary-research>.
- Independent Commission Against Corruption (ICAC) (2006). *Protecting identity information and documents: Guidance for public sector managers*. Sydney: New South Wales Government.
- Laudise, T.M. (2008). Ten Practical Things to know about "Sensitive" data collection and protection. *The Computer & Internet Lawyer*. 25(7) 26-33.
- Lips, A., Miriam B., Taylor, J.A., Organ J (2009). Identity Management, Administrative sorting and citizenship in new modes of Government. *Information, Communication and Society*. 12(5) 715-734.

- Oehlers, P.F. (2004). Identity Theft: What you can do to protect your clients. *Journal of Financial Services Professionals*. 58(1) 20, 22-23.
- Mills, G. (2007). *Identity theft: Everything you need to know to protect yourself*. United Kingdom: Summersdale Publishers.
- Peretti, K.K. (2009). Data Breaches: What the underground world of “carding” reveals”. *Santa Clara Computer and High-Technology Law Journal*. 25(2), 375-413.
- Rubinstein, I.S., Lee, R.P. and Schwartz, P.M. Data Mining and Internet Profiling: Emerging regulatory and technological approaches. *University of Chicago Law Review*. 75, 261-285
- Swartz, N (2004). U.S. States disagree about online access to court records. *Information Management Journal*. 38(3), 11.
- ‘Vox Pop: A new survey says nine million Aussies are concerned about identity theft and cyber crime. Are you worried and what steps do you take to combat the crime?’ (2008) *Bundaberg News-Mail*. May 8. 4.
- Yao, D (2005). Anywhere computing opens endless possibilities ... for data loss. *International Journal for Micrographics and Optical Technology*. 23(2/3) 2-4.