House Standing Committee on Communications Inquiry into Cyber Crime

Submission on Cyber crime

Version 1.1

Lockstep Technologies
June 2009

FOR PUBLIC RELEASE

Lockstep Technologies

Submission on Cyber Crime

Version 1.1

[Lockstep Submission - Cyber Crime Parliamentary Inquiry June09 (1.1).doc]

FOR PUBLIC RELEASE

Table of Contents

1. Executive Summary

It is no exaggeration to characterise the theft of personal information as an epidemic. Personal information in digital form is the lifeblood of banking and payments, government services, healthcare, a great deal of retail commerce, and entertainment. But personal records—especially digital identities—are stolen in the millions by organised criminals, to appropriate enormous financial assets, as well as the fast growing intangible assets of "digital natives". The Internet has given criminals x-ray vision into peoples' details, and perfect digital disguises with which to defraud business and governments.

Credit card fraud over the Internet is the model cyber crime. Childs play to perpetrate, and fuelled by a thriving black market in stolen details, online card fraud represents 50% of all card fraud, is growing at 50% p.a., and cost A$71 million in 2008. The importance of this crime goes beyond the gross losses, for some of the proceeds are going to fund terrorism, as recently acknowledged by the US Homeland Security Committee.

Yet there is a deeper lesson in online card fraud: it needs to be seen as a special case of digital identity theft. ID theft is perpetrated by sophisticated organised crime gangs, behind the backs of the best trained and best behaved users, aided and abetted by insiders corrupted by enormous rewards. No amount of well meaning security policy or user awareness can defeat the profit motives of today's online fraudsters.

We have reached the point where cyber crime is to crime as the digital economy is to the wider economy. And yet the e-business environment can be accurately compared to the Wild West of old: it's everyone for themselves! There is no consistency in the gadgets foisted upon consumers to access online businesses and services; worse, most are flawed and readily subverted by hackers. We could build security deep into our transaction platforms to prevent identity theft, phishing, web site spoofing and spam, but instead, almost all attention turns to user education. Most everyone now knows they need a firewall and anti-virus software; what very few people appreciate is that their identities are stolen in other channels utterly beyond their control. The predominant technology neutral policy position of government and the banking industry has not fostered market driven innovation as hoped but instead has created a leadership vacuum, leaving consumers to fend for themselves.

Lockstep submits that to really curtail cyber crime we need the sort of concerted balanced effort that typifies security in all other walks of life, like transportation, energy and finance. Bank customers don't need to install their own security screens; bank robbers are not kept at bay by security audits alone. The time has come, now that we're constructing the digital economy, to embrace a new breed of intelligent security technologies that can actually prevent identity theft and cyber crime.

2. Preamble: Are we serious about online security?

This section is an edited version of Stephen Wilson's October 2008 column in Online Banking Review "Many hands make security work".

If one thinks about online security, all sorts of parallels emerge with other fields. A good comparison is road safety, which depends on a blend of user education, standards, processes and technological innovation.

Cyber safety policy is preoccupied with user education. Governments and industry groups have developed volumes of reasonable security advice[1] but for the average user, this material is probably overwhelming. There is a subtle implication that security is for experts, and that the Internet isn't safe unless you go to extremes. Moreover, the most recent cyber criminal attacks show that even if consumers do their best online, their personal details can still be taken over in massive raids on merchant databases.

We believe that too much onus is put on regular users *protecting themselves* online, creating a blind spot as to potential preventative responses to cyber crime. In other walks of life, we accept a balanced approach to safety, and governments are less reluctant to impose standards. For example, road safety rests evenly on enforceable road rules, certified automotive products, traffic management systems, and driver training and licensing. Education alone would be nearly worthless.

In the aftermath of the TJ Maxx data breach (where tens of millions of credit card numbers were stolen by a gang that infiltrated department store networks), a column was headlined provocatively: "Preventing data breaches not a technology issue".[2] It may be politically correct play down technology, but it is ridiculous to ignore it. Nobody would ever assert that preventing bank robbery is 'not a technology issue'.

Credit card fraud and ID theft in general are in dire need of concerted technological responses. Consider that our Card Not Present payments processing arrangements were developed many years ago for mail orders and telephone orders. It was perfectly natural to co-opt the same processes when the Internet arose, since it seemed simply to be just another communications medium. But the Internet turned out to be more than an extra channel: it connects everyone to everything, around the clock.

The Internet has given criminals x-ray vision into peoples' banking details, and perfect digital disguises with which to defraud online merchants. There are opportunities for crime now that are both quantitatively and qualitatively radically different from what went before. In particular, because identity data is available by the terabyte and digital systems show no respect for originals versus copies, identity takeover is child's play.

[1] See for example www.protectfinancialid.org.au and www.staysmartonline.gov.au.

[2] See http://www.networkworld.com/columnists/2008/062308insider.html.

You don't even need to have ever shopped online to fall foul of CNP fraud. It is now apparent from TJ Maxx and other cases that most stolen credit card numbers might be obtained en masse by criminals invading databases at merchants' back-ends. These attacks go on behind the scenes, out of sight of even the most careful online customers.

So the standard cyber security advice increasingly misses the point. Consumers are told earnestly to look out for the SSL padlock that purportedly marks a site as secure, to have a firewall, to keep their PCs patched and up-to-date, to only shop online at reputable merchants and to avoid suspicious looking sites (as if cyber criminals aren't sufficiently organised to copy legitimate sites in their entirety). But none of this advice touches on the problem of coordinated massive heists of identity data.

And yet the Internet now is absolutely indispensible to Australian business. The latest ABS figures show that in FY 2008 Australian companies took over $80 billion worth of orders online (up 20% from FY07).[3]

Merchants are on the hook for unwieldy and increasingly futile security overheads. In order to process credit cards online, shopkeepers now have to sign up to onerous PCI requirements that in effect require even SMEs become IT security specialists. But to what end? No audit regime will ever stop organised crime. To stem identity theft, we need to make stolen IDs less valuable.

All this points to urgent public policy matters for governments and banks. It is not good enough to put the onus on individuals to guard against attacks on their credit cards. Systemic changes and technological innovation are needed to render stolen personal data useless to thieves. It's not that the whole payments processing system is broken; rather, it is vulnerable at one point where stolen digital identities can be abused.

Digital identities are literally the keys to our valuables. As such they really need to be treated as seriously as, say, house keys and car keys, which have become very high tech indeed. Modern car keys cannot be duplicated at a suburban locksmith; some office and filing cabinet keys even carry government security certifications. And we never use the same keys for our homes and offices; we wouldn't even consider it (which points to a basic oddity in the current craze for Single Sign On and identity "federation").

In stark contrast to car keys, almost no attention is paid to the pedigree of digital identities. Technology neutrality has led to a bewildering array of ad hoc authentication methods; at the same time we've done nothing to inhibit the re-use of stolen IDs. It's high time that government and industry got working together on a uniform and universal set of intelligent identity tools to properly protect consumers online.

[3] See http://tinyurl.com/kmlrta.

3. Introduction

Addressing the inquiry terms of reference

This submission is structured as a number of major sections that map onto the terms of reference[4] as follows:

a) Nature and prevalence of e-security risks including financial fraud and theft of personal information:	Part 4 of this submission examines the common thread in most important cyber crime today: the vulnerability of digital identities to theft and abuse.
b) The implications of these risks on the wider economy:	Part 5 presents recent data on the impact of identity theft, and the implications for future digital economy initiatives of enormous importance, such as e-health.
c) Level of understanding and awareness of e-security risks within the Australian community. *d) Measures currently deployed to mitigate e-security risks faced by Australian consumers: Education, Legislative and regulatory, Cross-portfolio and inter-jurisdictional coordination, and International co-operation.*	Part 6 canvasses the ever declining effectiveness of public understanding as a weapon against cyber crime.
e) Future initiatives that will further mitigate the e-security risks to Australian internet users. *f) Emerging technologies to combat these risks.*	Finally, Part 7 argues for a coordinated effort to secure digital identities. Lockstep does not advocate any single identity system; in fact we actually oppose Identity Cards. Instead we argue for a uniform approach to handling and conveying diverse digital identities, each fit for purpose in a rich array of domains: commerce, healthcare, government services, employment, education, social networking and so on.

[4] See http://www.aph.gov.au/house/committee/coms/cybercrime/tor.htm.

About the Lockstep Group

Lockstep Technologies researches and develops new solutions to prevent identity theft and enhance privacy online. Sister company Lockstep Consulting provides independent research, analysis and advice on policy and strategy for cyber security and privacy.

Our recent government clients include the Australian Government Information Management Office (AGIMO), the Victorian Department of Justice, Australia Post, the National eHealth Transition Authority (NEHTA), Medicare Australia, and the federal Office of the Privacy Commissioner.

Lockstep founder and Managing Director Stephen Wilson recently served as an invited member of the Australian Law Reform Commission's Emerging Technology Subcommittee. He is currently a member of the Australian Industry Group (AiG) Digital Technologies Forum, Standards Australia IT Security Subcommittee IT-12-4, and the IT Testing Accreditation Advisory Committee of the National Association of Testing Authorities (NATA). He is a past chair of the international OASIS PKI Adoption Technical Committee.

In October 2007 Lockstep Technologies was awarded an AusIndustry Commercialising Emerging Technologies (COMET) grant in support of our privacy and identity security R&D.

We have published widely on cyber security policy, privacy, e-health and related topics, and have previously made detailed submissions to government inquiries into the Human Services Access Card, the Privacy Act, spyware, and the draft national health privacy code. In March 2007, Stephen appeared before the Senate Finance and Public Administration Committee in its inquiry into the Access Card.

See also www.lockstep.com.au/library.

4. The predominant nature of e-security risks

A common thread runs through the most important cyber crimes: the vulnerability of *digital identities* to abuse. By "digital identity" we mean a data item or data set, unique in a particular context, that represents an individual or other entity. Common examples of digital identities are customer reference numbers, account numbers, employee numbers, government identifiers, US social security numbers, avatars, online social networking profiles, and biometric templates.

Digital identities act as handy proxies for actual identities of natural persons or legal entities. An important axiom of most modern thinking in identity management is that it is natural and indeed preferable for people to use multiple digital identities. See for example the influential *Laws of Identity* [2] as well as the academic work of Jøsang and Pope [3].

Stolen identity data is traded on a thriving black market, and used in a range of criminal enterprises including terrorism [4]. The most overt identity crime is Card Not Present (CNP) payment fraud, where stolen account details are replayed against unsuspecting e-merchants.

Looking at how it's perpetrated, online CNP fraud is the *model* identity crime, the exemplar of the ease with which digital identities can be taken over and used without the permission of their owners. Many other cyber crimes at heart are very similar:

— Medical Identity Theft[5]

— Social networking identity theft, such as that suffered by James Packer when his LinkedIn profile was taken over and used apparently to collect contact details for hundreds of his associates[6]

— Avatar theft (when an attacker takes control of a digital persona in an online game or virtual world) is now an important device in financial fraud, as we shall see in the next section.

While Lockstep acknowledges that the Australian Government has done a great deal of work on a National Identity Security Strategy [7], we are concerned that little attention to date has been given to *digital identities*. The NISS is focused on the integrity of evidence of identity documents, and does not consider the entirely separate array of risks that people face after they have obtained digital identities and are using them in purely online settings.

[5] See *The Medical Identity Theft Information Page* of the World privacy Forum http://www.worldprivacyforum.org/medicalidentitytheft.html.

[6] *How James Packer's LinkedIn page was stolen, and how to protect yours* Smartcompany 2 December 2008; http://www.smartcompany.com.au/internet/how-james-packer-s-linkedin-page-was-stolen-and-how-to-protect-yours.html.

5. Impacts of digital identity crime

Recent research sheds light on the financial impact of the digital identity crimes canvassed in the previous section:

— Card Not Present fraud is the fastest growing and now most prevalent form of payment fraud. CNP fraud in 2008 cost A$71M p.a. in Australia [5], and £328M in the UK [8]. If we scale these figures according to share of global GDP, a worldwide CNP fraud estimate of at least US$5 billion is reasonable.

  The European Commission's Fraud Prevention Expert Group (FPEG) reported in 2008 that ID fraud has reached the point that it "undermines the general confidence in payments systems" [6].

— Medical Identity Theft is a particular problem in the USA [10] where the nature of their health system creates extra incentives for fraudsters to avail themselves of actual treatments as well as drugs and money.[7] While not as prevalent in Australia, we must heed the American lessons because as national health identifiers are issued here, their susceptibility to theft and replay by attackers seeking various rewards must be evaluated. In any event, certain types of Medicare fraud may be regarded as digital identity crimes if they are perpetrated by faking Medicare numbers, and/or by redirecting payment to illicit bank accounts.

— Avatar theft can lead to real losses now that players are investing significant sums of money in virtual worlds and online games. The European Network and Information Security Agency (ENISA) last year conservatively estimated real money sales of virtual world assets at over US$2 billion annually, and acknowledged it could be as high as US$5B p.a. [9] Almost all of these assets are vulnerable to cyber crime; ENISA rates avatar theft as the number one risk.

Beyond the dollar value of cyber crime lies the deeper issue of confidence in participation in the digital economy. We are on the verge of a new wave of e-government programs that promise to transform the way that Australians live and work. Perhaps chief amongst these is Electronic Health Records (EHRs) including Personal Health Records (PHRs). It is widely believed that EHRs and PHRs will be key to improving health outcomes via participatory patient-centric preventative care, improving health policy implementation with the help of better public health data collection, and cutting cost. These hugely important benefits depend

[7] "[A] digital black market for the fraudulent use of stolen health data is thriving ... there's big money in medical identity theft". *Identity Thieves Target Medical Records*, PC World, 20 June 2009; http://www.pcworld.com/article/166879/identity_thieves_target_medical_records.html.

squarely on cyber security, privacy and trust. Even if cyber crime had no direct impact on e-health, its very existence and its remarkable growth rightly undermine public confidence in new digital assets that are perceived to be far more valuable and perishable than mere finances.

Lockstep would also like to highlight two other strategic e-government objectives that will prove difficult to realise unless public confidence in cyber space is bolstered:

— **The desire to engage electronically with the populace**, especially in the human services portfolios. It is well known that perhaps 100 million letters are mailed to citizens every year; to transition even a small proportion of these to e-mail and SMS would present a huge cost saving, not to mention enhanced service delivery and flexibility. Yet the fundamental challenge is that thanks to spam, everyone has been trained not to open unsolicited e-mail from government! National anti-spam measures should be contemplated in this light.

— **Electronic-voting** in the medium term is an important policy objective for Australian defence force personnel and other workers stationed overseas. In the longer term, e-voting may bring deeper benefits across the board, in respect of improved reach and participation, and efficiencies in tallying. Internet e-voting brings several challenges in confidentiality and integrity, none insurmountable given a national investment in protecting digital identities.

6. Public understanding & current initiatives

The limits of education

Lockstep's considered position on the question of public understanding is that as a weapon against cyber crime, user education has reached its limit. Frankly, "understanding" is now almost moot.

The dominant modus operandi of CNP fraudsters is to go behind customers' backs and steal their IDs *en masse* from payment processors, department store databases and so on. In this way, organised cyber criminals negate almost all of the online security advice given to consumers. A credit card holder *might have never used their card online* and still fall foul of cyber crime if their details have been acquired from a merchant's database or payment gateway.

In Australia's technology neutral regulatory environment, the overwhelming approach of governments to public cyber security has been to focus on education and awareness campaigns. Sites like www.staysmartonline.gov.au provide plenty of worthwhile guidance about the SSL padlock, passwords, anti-virus software and personal firewalls, but all this advice has been rendered obsolete. We believe the time has come for policy makers to confront the fundamental limitations of trying to train lay people to behave safely on the Internet.

The medium itself is a big problem. There are really no reliable cues by which people can gauge real from fake online. For most people, surfing the Internet is much like watching a cartoon show on television. The human-machine interfaces of PC and TV are almost the same. The images and actions on the web are just as synthetic; crucially, *nothing on a web browser is real*. Almost anything goes: just as the Roadrunner defies gravity in besting Coyote, there are no laws of physics that moderate the way one web screen leads to the next. So it is inevitable that people lose their bearings in synthetic cyber space; without realising it, they are taken in by a virtual reality, and become fatally vulnerable to social engineering.

Using the Internet "safely" today requires deep technical knowledge in order for the user to be able to abstract the different layers where threats may lurk. The requisite knowledge level seems to us to be comparable to the level of expertise needed to operate an automobile circa 1900. Back then a driver needed to know first hand how the machine worked so they could repair it for themselves in the back blocks. They had to maintain the engine (which we compare to configuring a PC operating system and firewall), and watch out for dangers on the emergent road network (as often noted, there's no driver licensing on the Internet, nor any road rules).

The Internet is so critical now that we need to move towards ways of working that don't require us to all be do-it-yourself experts, fending for

ourselves as if the digital economy is the Wild West. The sad truth is that no amount of understanding now can protect citizens against the newer forms of attack. "Understanding" is moot when the consumer is powerless to prevent their personal details being abused behind their backs. The time has come for payment service providers to re-engineer their systems with better resistance to identity theft. Likewise, those that are planning online services in government need to take heed of how ID theft operates in the finance sector, consider carefully the consequences for near term and medium term e-government programs, and evaluate preventative measures to preserve the community's digital confidence.

Reflections on current initiatives

The inquiry's terms of reference indicates interest in measures to mitigate e-security risks under the headings *Education*, *Legislative and regulatory*, *Cross-portfolio and inter-jurisdictional coordination*, and *International co-operation*. For reasons outlined above, we believe that policy and awareness based measures are limited. Government's response to cyber crime—as with its response to traditional crime—ought to include a greater proportion of preventative technological measures.

To really curtail digital identity theft, steps must be taken to render stolen personal data useless to thieves, thus removing the profit motive for organised ID theft and neutralising the identity black market. If the digital economy is crucial to the wider economy, then the ability of citizens to protect their own digital identities is critical. A level of infrastructure investment is indicated, not dissimilar to what we're familiar with in other important spheres of commerce and government such as road safety, air traffic control, telecommunications and energy.

We can draw lessons from various current programs and proposals:

— **Chip-and-PIN**. In international banking, plastic card fraud is being redressed by the deployment of Chip-and-PIN smartcard technology. Smartcards supersede magnetic stripe cards with vastly better protection of cardholder data against skimming, copying, cloning and counterfeiting. The advanced cryptography built into Chip-and-PIN cards—at first intended to be used in retail terminals—can also be applied via web browsers to protect digital identity data in e-commerce settings against theft and abuse.

— **US Government Personal Identity Verification (PIV)**. The US government is deploying a new smartcard standard as part of a program to improve the identification of federal employees and contractors. The so-called PIV standard (technically referred to as "FIPS 201") is now being co-opted across industry[8] because it provides an interoperable suite of powerful tools for managing digital identity. It is important to note that FIPS 201 has been

[8] See for example "PIV in the enterprise" at http://www.smartcardalliance.org/articles/2009/03/19/piv-in-the-enterprise-latest-physical-access-technologies-focus-of-smart-card-alliance-at-isc-west-2009.

adopted here in Australia by the Department of Defence in its current project personnel identity management project JP2099.

Intelligent personal identity devices such as the FIPS 201 chip card embody encryption techniques adjudged by experts to be uniquely equipped to deal with contemporary cyber crime threats. The head of cryptography at the US National Institute of Standards & Technology (NIST) describes these sorts of smartcard as "the only practical solution today [account hijacking and eavesdropping]" [11].

Lockstep's own peer-reviewed research has taken up these technology themes and developed a vision for wider application of intelligent technologies for protecting digital identities [12].

— **Smart Medicare card concept**. From time to time, the concept has been floated of upgrading the magnetic stripe Medicare card to incorporate a chip. The headline benefit for doing so is often said to be prevention of Medicare fraud using fake cards, a proposition that fails to ignite public support for it tends to cast aspersions on *all* Medicare recipients. Additional benefits are sometimes claimed around streamlining of government services by joining them up through a single card, at which point the argument for a new card tends to be lost on privacy grounds.

  Recent press reports have introduced a much more worthwhile angle on the idea of a smart Medicare card: protection of the new Unique Health Identifier.[9] Lockstep appreciates that these have been false reports and that the government has no plans to introduce smartcards. Nevertheless we are encouraged by the evident appreciation that protection of identifiers is a distinct benefit of the technology. If a new Medicare smartcard did nothing other than protect Unique Health Identifiers against theft and misuse, then it might be a valuable development to protect the emerging e-health records system.

— **National Broadband Network**. Last but not least, the most notable infrastructure development is surely the NBN, for it signals the government's appetite to build lasting national foundations for the digital economy. Lockstep advocates evaluation of appropriate cyber crime fighting technologies for integration into the NBN infrastructure.

[9] See "Medicare cards to become smarter", The Australian, 16 June 2009; http://www.theaustralian.news.com.au/story/0,25197,25642642-5013945,00.html.

7. Emerging technologies and future initiatives

We advocate a coordinated effort across business and government to treat all digital identities more seriously. Lockstep does not advocate any single identity system; in general we actually oppose Identity Cards (for in and of themselves they cannot solve the problem of digital identity theft). Rather, we favour all sectors adopting a uniform approach to how they handle and convey diverse digital identities, each fit for purpose in its own specific domain: banking, commerce, healthcare, government services, employment, education, social networking and so on.

We submit that the most important new technology for preventing digital identity theft and therefore cyber crime in general is to be found in smartcards and related intelligent personal authentication devices such as smart phones, advanced SIMs, and USB crypto keys.

These devices are called "smart" because *they can tell what's going on around them.* They can act as proxies for their users, protecting them against misadventure and cyber crime. A few simple examples serve to illustrate the capabilities of these technologies:

— A smart credit card can tell if it is being used in an unusual location, or being used in excess of the daily spending limit. These rules can be enforced in off-line merchant locations, without needing to defer to a central mainframe or payment gateway.

— A smart health & welfare card can tell if it is being used to obtain excessive services (i.e. doctor shopping), or unusual quantities of prescription drugs. These rules can be enforced in real time by software running entirely inside the chip, and without needing to centrally log and data-mine all transactions, which would be an affront to privacy.

— Such cards can also be used to prevent provider fraud, by indelibly marking each public health insurance claim with a unique digital patient code (which, to protect privacy, need not be the same as any other identifier) thus making it impossible for providers to lodge repeat claims, create fake claims, or doctor claim amounts.

— Smartcards can be used by individuals as secure "containers" to hold one or more personal identifiers, pseudonyms, log-on credentials and so on. When accessing a particular service, the card can work out precisely which identifying information is relevant in that context; the card will then release just the right amount of information to authenticate the user, and no more. Controlling the release of identity information is an important key to privacy, and limits exposure of personal data to identity thieves. Lockstep's own AusIndustry-backed R&D in this area has demonstrated ways to

remove all identifying information from such sensitive transactions as electronic health record entries, e-voting, and anonymous proof-of-age.

— When accessing secure websites, it is important that the security "master" keys sitting behind the SSL padlock mechanism have not been tampered with by fraudsters. Smart devices can hold trusted copies of the master keys to prevent web site spoofing and phishing.

— Finally, smartcards can be used to automatically encrypt separate transactions, making them immune to tampering and "replay" attacks favored by cyber criminals.

Smartcards are associated by many with national identity schemes, and dubious past efforts to re-engineer social security services. Yet intelligent personal authentication technologies can provide powerful privacy protections as outlined in these simple examples.

Please note carefully that what we propose is that Australia can implement digital identity security measures nationally *without any semblance of a national identity system*. To avoid a national identity, intelligent technologies should be deployed according to principles such as:

— existing purpose-specific identifiers and relationships with service providers should in general be preserved

— different digital identities should be dedicated to different domains: banking, commerce, healthcare, government services, employment, education, social networking and so on

— no new multi-purpose identifiers need be created

— businesses and agencies should remain autonomous in deciding how they transact with their customers and users

— no new central registries are necessary to improve the pedigree of digital identities

— all smartcard software should be subject to independent inspection and audit to ensure it follows these and other privacy principles.

The possibilities for combating cyber crime using these technologies are many and varied, and we believe should be studied further as part of the government's ongoing work on identity security and online safety. There may be opportunities for state and federal governments to lead by example when deploying smart technologies like new driver licences and entitlements cards.

8. Conclusions & recommendations

Lockstep contends that industry and government alike need to move beyond the current focus on user education, security policy and audit, and adopt a more blended approach to combat organised cyber criminals. We recommend that the government look closely at sophisticated new intelligent authentication technologies that mitigate digital identity theft and render stolen IDs useless to criminals. Such devices can act as proxies for their users, protecting them from cyber crime, controlling the release of personal ID data, and automatically detecting risks like spoof web sites.

The National Identity Security Strategy should broaden its scope to consider also the integrity of digital identities. There is little point focusing only on the security of original identity documents like birth certificates and driver licences when the modus operandi of cyber criminals is to subvert digital identities after issuance, like account numbers, government IDs, health identifiers, and social networking profiles.

Government must be prepared for identity theft to migrate into its own services, especially with the advent of Unique Health Identifiers. Countermeasures ought to exceed those seen in Internet banking. Banks are able to cover losses from financial identity theft, and can precisely compensate the victims, but governments don't have that luxury. The intangible losses arising from fraud against government services, and from health privacy breaches are inestimably harder to redress.

Government should lead by example, deploying state-of-the-art digital identity technologies to safeguard its citizens in coming generations of online services, such as health identifiers, electronic health records, social security services, and e-voting. There are examples in state and federal government where the latent ability to better protect digital identities may already be emerging, in such programs as smart driver licences.

We hope that the National Broadband Network provides the investment vehicle, the policy precedent and the motivational drive for government to invest in digital identity security for the nation.

9. References

[1]. Stephen Wilson *Many hands make security work* Online Banking Review, October 2008 http://www.lockstep.com.au/library/online_banking_review/obr-lockstep-200810-many-hand

[2]. Kim Cameron *The Laws of Identity*, Microsoft 2005; http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

[3]. Audun Jøsang and Simon Pope *User Centric Identity Management*, AusCERT Conference 2005; http://conf.isi.qut.edu.au/auscert/proceedings/2005/josang05user.pdf

[4]. Yvette Clarke *Prepared Statement to Homeland Security Committee Hearing: "Do The Payment Card Industry Data Standards Reduce Cybercrime?"* (Chair) Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, 31 March 2009; http://hsc.house.gov/SiteDocuments/20090331141915-60783.pdf

[5]. Australian Payments Clearing Association *Payment Fraud Statistics - Summary of Results; Fraud Perpetrated on Australian Issued Payment Instruments 1 January 2008 - 31 December 2008* http://tinyurl.com/APCA-fraud-CY2008.

[6]. European Commission Fraud Prevention Expert Group *Report on fraud regarding non cash means of payments in the EU: the implementation of the 2004-2007 EU Action Plan*, 22 April 2008; http://ec.europa.eu/internal_market/payments/docs/fraud/implementation_report_en.pdf.

[7]. *Report to the Council of Australian Governments on the elements of the National Identity Security Strategy* April 2007 http://tinyurl.com/reportNISS

[8]. *Press release: 2008 fraud figures announced by APACS*, UK Payments Administration Ltd (formerly APACS); http://www.apacs.org.uk/09_03_19.htm

[9]. European Network and Information Security Agency (ENISA) *Virtual worlds Real money*, 2008; http://tinyurl.com/VW-RealMoney

[10]. Booz Allen Hamilton *Medical Identity Theft Final Report* For the US Department of Health and Human Services, 15 January 2009; http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848096_0_0_18/MedIdTheftReport011509.pdf

[11]. Bill Burr *Electronic Authentication in the U.S. Federal Government* National Institute of Standards and Technology, Asia PKI Forum,

Tokyo, 2005;
http://www.asia-pkiforum.org/feb_tokyo/NIST_Burr.pdf

[12]. Stephen Wilson *A new manifesto for smartcards as national information infrastructure* 5th Homeland Security Summit – 2006 Security Technology Conference, Canberra, 21 September 2006;
http://www.lockstep.com.au/library/smartcards/a_new_manifesto_for_smartcard.

[13]. Lockstep Consulting *Towards a uniform solution to identity theft* White paper 2006
http://www.lockstep.com.au/library/identity_authentication/towards_a_uniform_solution

[14]. Lockstep Consulting *What's so smart about smartcards?* "Babystep" No. 10, 2007
http://www.lockstep.com.au/library/babysteps/lockstep_bs10_what_makes_smar