Australian Government
Australian Institute of Criminology

Veda: *Fraud Focus Group Forum*

Identity Crime Trends, Risks and Solutions

Dr Russell G Smith
Principal Criminologist

Outline

Identity crime concepts

- The scope of identity crime
- Identity crime taxonomies and measurement categories
- Methods used to obtain personal information

Quantifying the extent of identity crime

- Crime victimisation surveys and business surveys
- Official crime statistics

The Australian National Identity Security Strategy

- Key elements of the Commonwealth Strategy

Risks arising from online verification of evidence of identity

- Online verification processes (e-Authentication) and risks
- Database, data capture and data matching irregularities

Developing solutions to address emerging risks

- Legislative, policy and technological solutions

The scope of identity crime

Public sector

- Income tax, customs duty and GST fraud, superannuation fraud
- Obtaining welfare and health care benefits in false names
- Immigration fraud and taking English language tests for someone else

Private sector

- Opening bank accounts in false names and obtaining finance
- ATM, online and mobile banking and payment card fraud
- Funds transfer fraud and securities and investment fraud

Consequential activities

- Money laundering – ARS, SVCs, virtual worlds, trade-based
- Motor vehicle re-birthing; art and antiquity fraud
- Obtaining security guard, motor vehicle, boat and shooters' licences
- Avoiding driving demerit points and local government fees
- Avoiding detection and prosecution for violent crime

Identity crime taxonomies

ACPR-AUSTRAC Proof of Identity Steering Committee 2006

- *Scope* – living and deceased individuals, and corporations
- *ID fabrication* – creation of a fictitious identity
- *ID manipulation* – alteration of an identity or evidence of identity
- *Lent IDs* – use of another person's identity with their permission
- *ID theft* – assumption of a pre-existing identity without authority
- *ID fraud* – gaining benefits or avoiding liabilities using identity info.
- *ID crime* – generic term for criminal activities using identity info.

Categories of methods used to obtain personal information

- *Semantic* – social engineering to obtain personal information
- *Syntactic* – fabrication and alteration of documentary evidence and other high-tech methods – hacking, skimming, cloning, spoofing
- *Blended identity crime attacks* – spamming via botnets, phishing

Quantifying the extent of identity crime

SIRCA (2003)

- Direct loss from identity fraud in Australia 2001-02 was $420 million
- Total cost of identity fraud $1.1 billion (including prevention & recovery)

Personal identity fraud (ABS)

- Total personal fraud in 2010-11 – 713,600 victims ($1.4b); 6.7% pop'n
- ID theft – 124,000, 0.8% (2007); 44,700, 0.3% (2010-11) [-64%]
- Card fraud – 383,300, 2.4% (2007) ; 662,300, 3.7% (2010-11) [+73%]

Official dishonesty offence statistics recorded by police

- 24% decline in offences; 35% decline in rate/100,000 pop'n since 2000

Australian Government
Australian Institute of Criminology

Trends in officially recorded fraud in Australia

Rate per 100,000 popn, recorded by Australian police (1953/54 – 2011/12)

Source: Australian Police Services

Quantifying the extent of identity crime

SIRCA (2003)

- Direct loss from identity fraud in Australia 2001-02 was $420 million
- Total cost of identity fraud $1.1 billion (including prevention & recovery)

Personal identity fraud (ABS)

- Total personal fraud in 2010-11 – 713,600 victims ($1.4b); 6.7% pop'n
- ID theft – 124,000, 0.8% (2007); 44,700, 0.3% (2010-11) [-64%]
- Card fraud – 383,300, 2.4% (2007) ; 662,300, 3.7% (2010-11) [+73%]

Official dishonesty offence statistics recorded by police

- 24% decline in offences; 35% decline in rate/100,000 pop'n since 2000

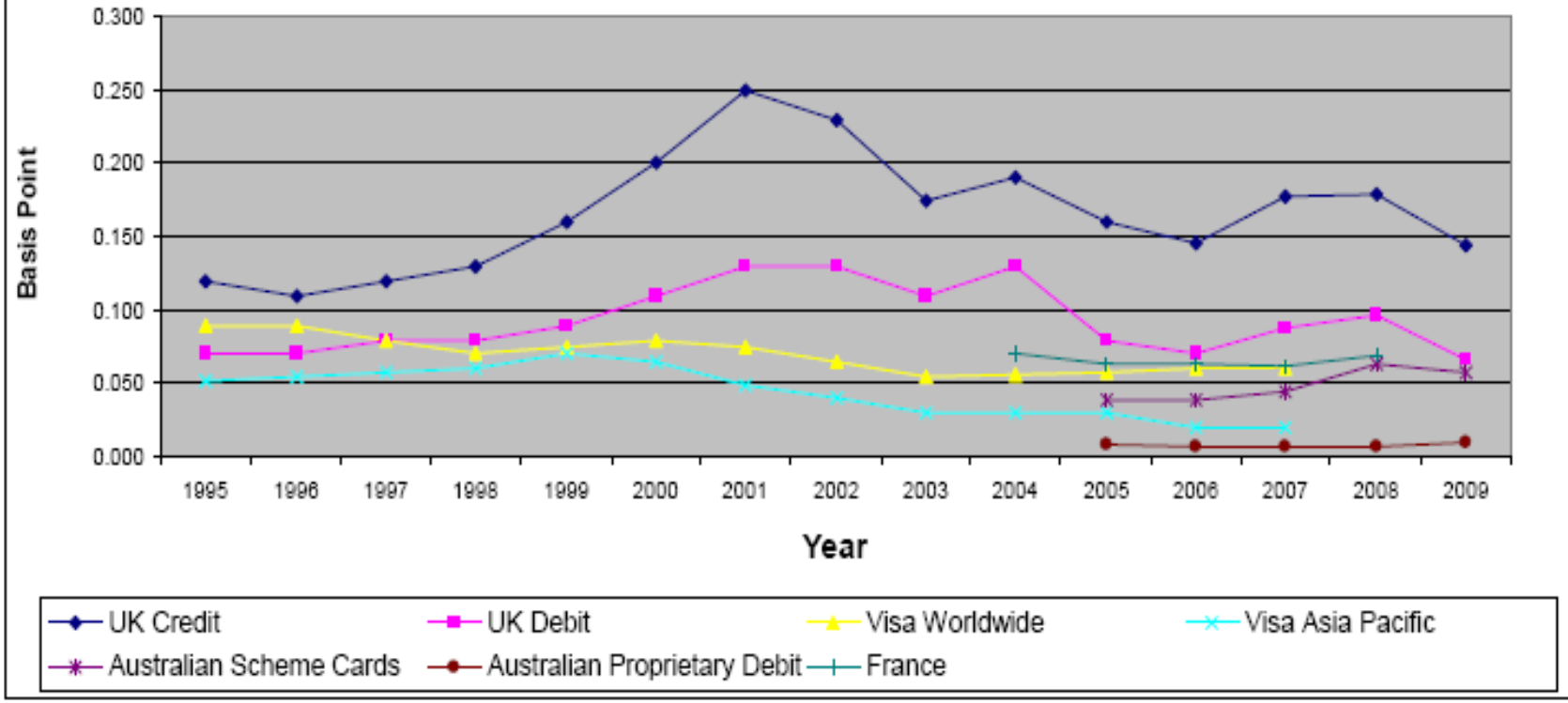
Plastic card fraud (APCA)

- 0.015% of card transactions fraudulent in 2006; 0.052% in 2011(Aust)
- Card-not-present fraud losses increased: $31.8m (2006) $198m (2011)
- Sept 2012 – 15,000 false cards worth $37.5m seized by police

Australian Government
Australian Institute of Criminology

Payment card fraud trends

Plastic card fraud losses in basis points for selected countries



Sources: APCA, UK Payments Association, Observatory for Payment Card Security (France) and Visa Inc.

Quantifying the extent of identity crime

SIRCA (2003)

- Direct loss from identity fraud in Australia 2001-02 was $420 million
- Total cost of identity fraud $1.1 billion (including prevention & recovery)

Personal identity fraud (ABS)

- ID theft – 124,000, 0.8% (2007); 44,700, 0.3% (2010-11) [-64%]
- Card fraud – 383,300, 2.4% (2007) ; 662,300, 3.7% (2010-11) [+73%]

Official dishonesty offence statistics recorded by police

- 24% decline in offences; 35% decline in rate/100,000 pop'n since 2000

Plastic card fraud (APCA)

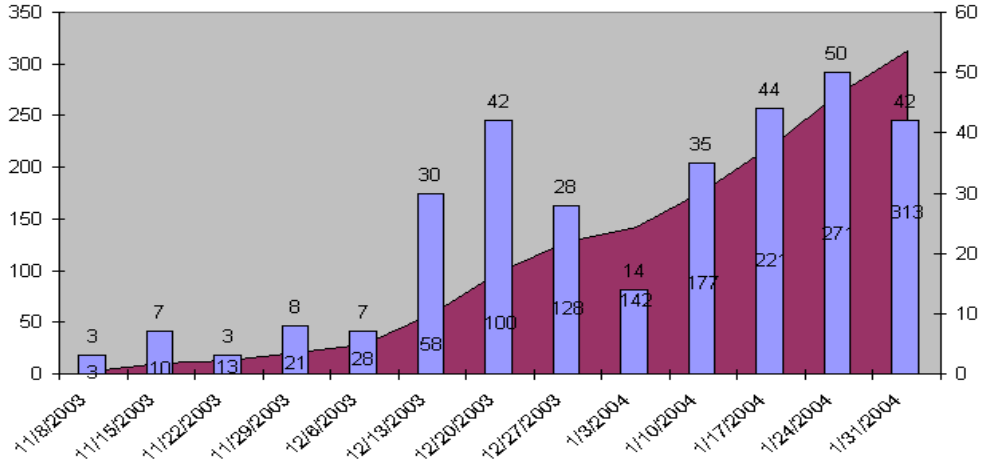
- 0.015% of card transactions fraudulent 2006; 0.052% in 2011(Aust)
- Card-not-present fraud losses increased: $31.8m (2006) $198m (2011)
- Sept 2012 – 15,000 false cards worth $37.5m seized by police

Cybercrime

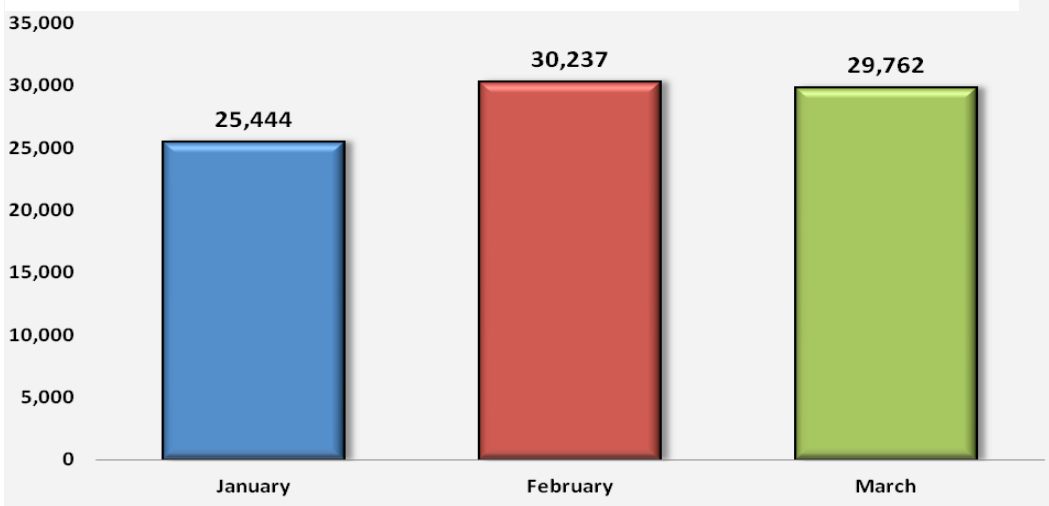
- Verizon – 621 data breaches involving 44 million records in 2012
- APWG – Phishing attacks – 176 (Jan 2004); 25,444 (Jan 2012)

Anti-Phishing Working Group Data

January 2004
- 176 unique attacks



January 2012
- 25,444 unique attacks



14,000% increase over 8 years

Source: http://www.antiphishing.org/phishReportsArchive.html

Australian Government
Australian Institute of Criminology

Commonwealth identity-related fraud 2009-10

Internal fraud

- 5% of agencies reported internal fraud involving misuse of identity

External fraud

- 11% of agencies reported external fraud involving misuse of identity
  – 1,153 incidents of creating and/or using a fictitious identity / forgery
  – 2,859 incidents of unauthorised use of another person's TFN/ABN

Australian Federal Police

- AFP recorded 41 offences of identity fraud in 2009-10 (85 in 2008-09)

Examples of Commonwealth identity-related fraud

- Receipt of $125,463 in social security in 3 false names over 8 years
- Receipt of $200,000 for mother's pension for 22 years after her death
- Pharmacist submitted fraudulent prescriptions worth $400,000

Source: Australian Institute of Criminology *Commonwealth Fraud Survey* data (2010)

National Identity Security Strategy

1. Enrolment standards

- Registration and enrolment standards for use by agencies which enrol individuals to issue government documents (*Gold Standard Enrolment Framework* and *National e-Authentication Framework*)

2. Document security and verification standards

- Security standards for such documents to reduce the possibility of forgery or unauthorised alteration of documents (*Security Standards for Proof of Identity Documents*)

3. Document verification

- Improved ability for Government agencies across jurisdictions to verify information on such documents (*National Document Verification Service)* – includes drivers' licences, passports, visas and citizenship certificates – extending to 17,000 private sector organisations on a fee-for-service basis

National Identity Security Strategy 2005

4. Recording identity data

- Standards in the processing and recording of identity data to improve the accuracy of existing records (where appropriate) and to prevent the creation of inaccurate identity records in future (e.g. *Better Practice Guidelines for Recording Names*)

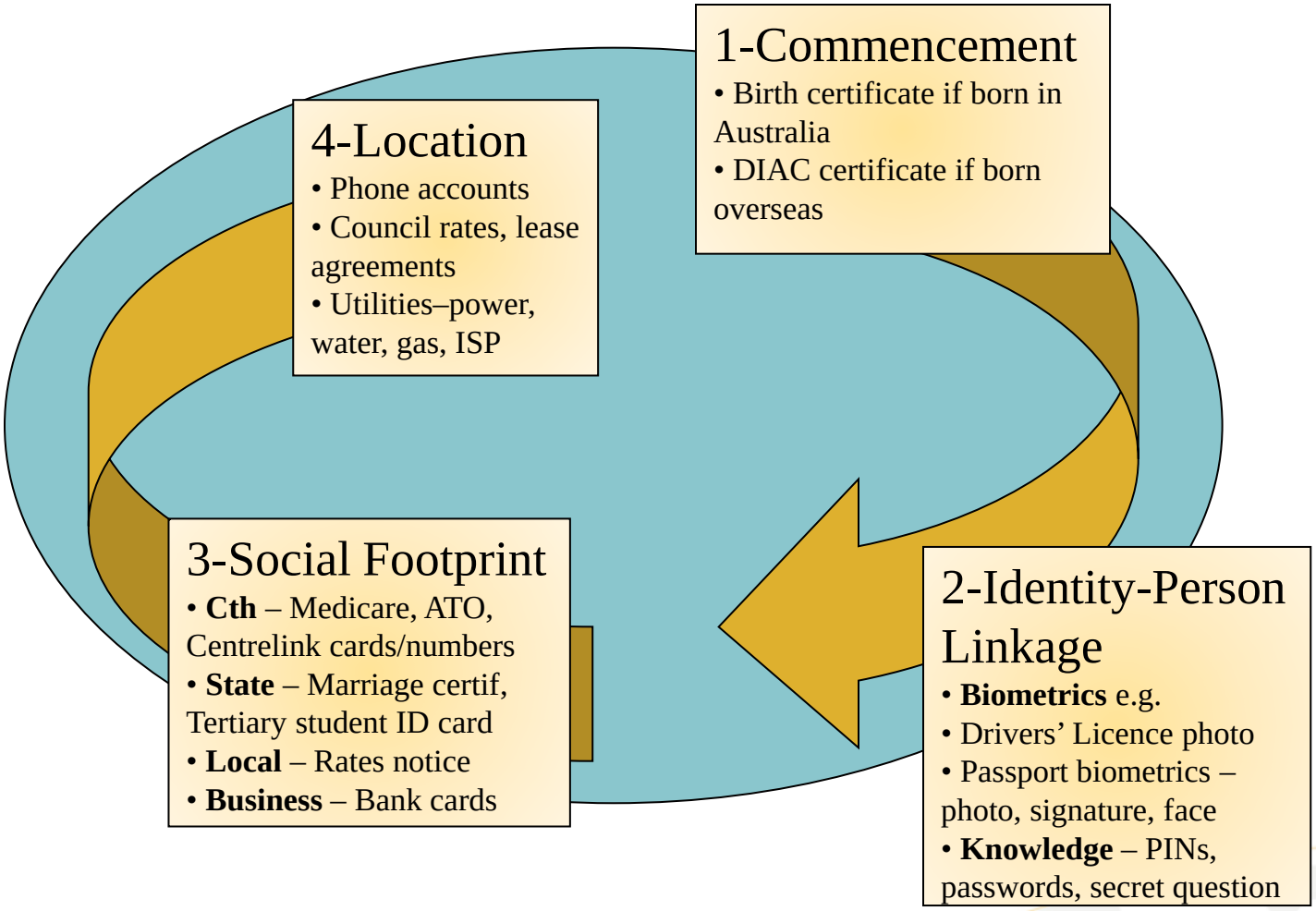
5. Agency service provision

- Standards for Government agencies to apply where they provide services to a person whose identity needs to be verified and there are significant risks associated with the wrong person getting access to a service

6. Biometric interoperability

- Measures to enhance the national interoperability of biometric identity security measures (e.g. Standards Australia *Committee on Biometric and Identification Technologies* - IT-032)

Proof of identity framework



Source: Derived from *Report to COAG on NISS* (2007)

Online verification (e-authentication)

Credential checking

- Gold standard credentials are read electronically using Public Key Infrastructure – identifier protected by a digital certificate

Two-factor authentication

- *Something you have* – USB token, password generator, PKI key
- *Something you* know – PIN, password, secret question, transactions
- *Something you are* – Facial image, voice, fingerprint

Delivery channels

- Post, phone, SMS, online

Data security

- Adhere to government standards on e-authentication, smartcard and token security, PKI Gatekeeper for digital certificates, ICT security

Online verification risks

Database irregularities

- Failure due to inaccurate personal information in legacy databases
- Mistakes in enrolment of new personal information
- Intentional manipulation of database entries
- Accidental, negligent or intentional data leakage

Online verification risks

Database irregularities

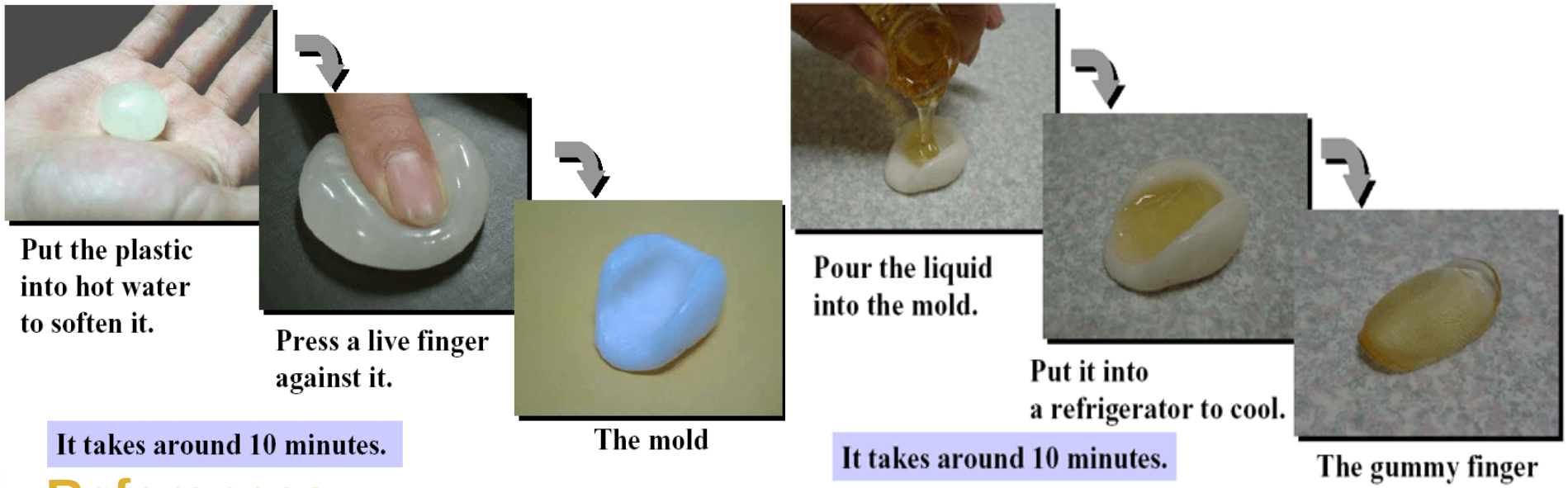
- Failure due to inaccurate personal information in legacy databases
- Mistakes in enrolment of new personal information
- Intentional manipulation of database entries
- Accidental, negligent or intentional data leakage

Data capture irregularities

- Submission of false proof of identity credentials / e-counterfeiting
- Spoofing biometric capture systems

Spoofing biometrics

Voluntary finger cloning – 'gummy fingers'



References

- Thalheim et al. - http://www.larc.usp.br/~pbarreto/Leitura%202%20-%20Biometria.pdf
- Rick Smith - http://www.cryptosmith.com/
- *The Register* -http://www.theregister.co.uk/2002/05/23/biometric_sensors_beaten_senseless/

Online verification risks

Database irregularities

- Failure due to inaccurate personal information in legacy databases
- Mistakes in enrolment of new personal information
- Intentional manipulation of database entries
- Accidental, negligent or intentional data leakage

Data capture irregularities

- Submission of false proof of identity credentials / e-counterfeiting
- Spoofing biometric capture systems

Data matching irregularities

- Technological errors creating false positives and false negatives
- External manipulation of data flows – active network attacks; trawling
- Internal corruption of staff within agencies
- Coercion of individuals to provide information under duress

Legislative and policy solutions

Legislation

- Global normative approaches and harmonisation (UNODC)
- Criminalisation of identity fraud and possession of equipment
- Procedural and evidentiary reforms to aid prosecution
- Assets confiscation, unexplained wealth laws and AML/CTF regime

Policy solutions

- Using multiple solutions rather than one
- Ensuring cooperation between Commonwealth & states and territories
- Ensuring cooperation between public and private sectors
- Improving education – coordination (e.g. ACFT), computer security, risks of social media, enhanced standards – computer driving licence
- Improving victim support – reporting, loss recovery, counselling, identity fraud court victimisation certificates

Technological solutions

Document security and verification

- Document security solutions; RFID blocking
- Electronic document verification
- Chip/PIN card roll-out; PC smart card readers for home and business

Industry responses

- Secure data transmission and storage using PKI
- ATM anti-skimming technologies – BNZ liquid encryption numbers, radio jamming, shields, vibration sensors, touch screens, voice recog.
- Enhanced security of online personal information
- Transaction monitoring, notification and blocking

Biometrics

- e-passports (facial scanning)
- Biometric ATM/POS (fingerprints)

Australian Government
Australian Institute of Criminology

Russell.Smith@aic.gov.au