



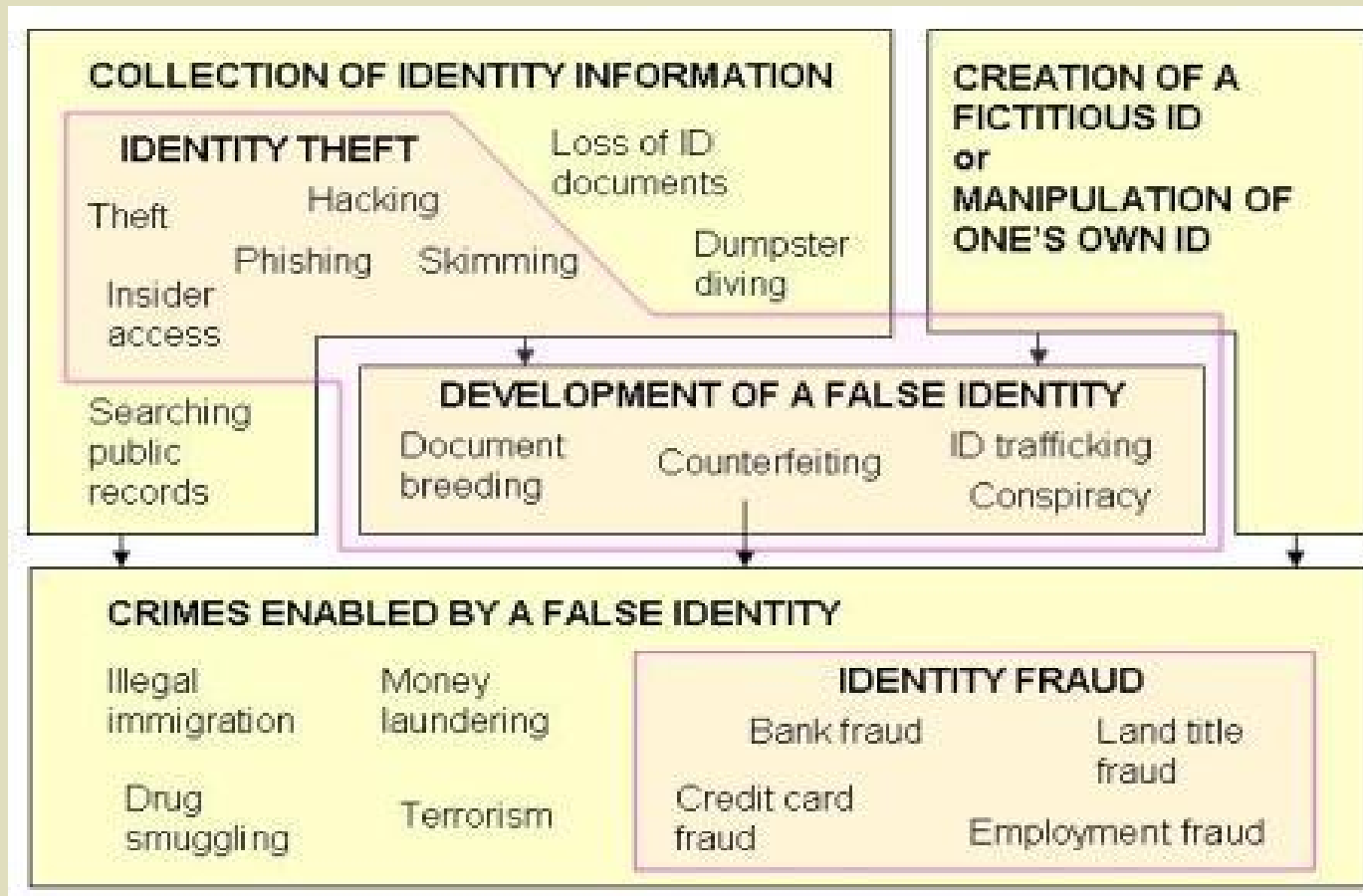
Tackling ID Theft: Legal and Policy Approaches

Philippa Lawson
Canadian Internet Policy and Public Interest Clinic
University of Ottawa
www.cippic.ca

Definitions (Archer/Sproule)

- **Identity theft:** The unauthorized collection, possession, transfer, replication or other manipulation of another person's personal information for the purpose of committing fraud or other crimes that involve the use of a false identity.
- **Identity fraud:** the gaining of money, goods, services, other benefits, or the avoidance of obligations, through the use of a false identity.

Archer/Sproule Conceptual Model



Most Useful Info

- ID documents/numbers
 - SIN, health, drivers licence, passport, birth cert.
 - employee, student, member
- Account numbers/details
 - Bank, credit card, mortgage, phone, etc.
- Credit reports
- Home address
- Date of birth
- Passwords, PINs
- Employment details
- Biometric information

Techniques of ID Theft

- taking/stealing from individuals:
 - finders keepers: trash, used computer equip, lost wallet
 - theft of wallet, chequebook, credit card, mail
 - pretexting by phone or in person
 - scams: employment, surveys, contests....
 - phishing, vishing, pharming
 - skimming - via ATMs, hidden machines
 - wireless eavesdropping
 - malware: keystroke loggers, etc.

Techniques of ID Theft

- taking from public sources:
 - personal websites, social networking sites
 - online resumes
 - employer/association websites
 - online public records (eg, court/tribunal)
 - post-disaster missing person sites
 - obituaries
 - used vehicle info package (Ont.)
 - owner's name/address used to get copy of ownership permit

Techniques of ID Theft

- taking/stealing from organizations:
 - dumpster diving
 - used computer equipment
 - corrupt employees
 - pretexting (duped employees)
 - purchase/subscribe (e.g., credit reports)
 - hacking
 - taking advantage of security holes

Intermediate Stages

- ID data trafficking
 - buy and sell personal information
- ID document “breeding”
 - create counterfeit documents
 - apply for new documents, ID numbers (forgery)
- Submit change of address to post office
 - divert victim’s mail

Iaaca.com

Enter Search Term!

Search!



Top Searches:

Credit Card Dumps

Online Dating

Gifts

Most Preferred:

Credit Report

Stolen Cards

Stolen Credit Cards

Welcome to Iaaca.com If you're looking for Credit Card Dumps, Stolen Credit Cards, Apple Store or anything similar, go ahead and browse our comprehensive resource directory. You ought to find something interesting!

Are you interested in:

- [No Annual Fee Credit Card](#)
- [Jobs](#)

- [Bank Credit Card](#)
- [Apple Store](#)

Recommended Listings:

▶ [Discover Credit Card Application](#)

▶ [Accept Visa](#)

▶ [Credit Card Applications](#)

▶ [Credit Card](#)



Popular Topics:

▶ [Credit Card Application](#)

▶ [Social Security Card](#)

▶ [Barclays Bank](#)

▶ [Computer Notebooks](#)

[Bookmark this page](#) | [Make this your homepage](#)
Copyright © 2005 Iaaca.com All Rights Reserved.

Purpose: ID Fraud

- use credit card, phone credit
- withdraw from bank account
- open new accounts (bank, utility, phone...)
- obtain loans
- mortgage/sell property (mortgage/title fraud)
- steal cars; order goods online using drop-site
- get insurance or government benefits
- get employment/hide criminal record
- create cover for other criminals/terrorists

Control Points

- Individuals:
 - limited control / ability to assess risk
- Organizations:
 - Service providers
 - Online services, electronic banking, magnetic stripe cards, wireless communications, ...
 - Software/hardware vendors/manufacturers
 - Data holders
 - Public records
 - Social networking sites

How are we dealing with
the problem?

Market Responses

- Stronger authentication mechanisms
 - more passwords, two factor authentication
 - Credit card security code
 - Smart cards
 - Digital IDs; “information cards”
 - Biometrics
- New detection tools
 - ID Alarm
 - Better account monitoring/pattern recognition
- Industry standards
 - Financial transactions (Interac, etc.)

Market Responses

- Internalize cost of fraud
 - higher service fees
 - spreads losses over customer base
 - individual victims still left to cope with non-monetary damage
- Fee-based Fraud Protection Services
 - Credit Bureaus: “ID theft protection”
 - ISPs: “anti-phishing” option
 - Insurers: ID theft insurance
- Victims left to fend for themselves

Legal & Policy Approaches

- Thieves:
 - Criminal liability
- Individuals:
 - Public education
 - Customer warnings
 - Detection tools
 - Victim assistance
- Organizations:
 - Best Practices; Guidelines
 - Data Protection legislation
 - Civil liability

Thieves

Criminal Law

- Existing ID Theft/Fraud crimes
 - fraud, forgery, personation, computer misuse
 - mere possession is not a crime; no deprivation
- Possible new ID Theft crimes
 - possession of [multiple] ID *with intent to defraud*
 - remove deprivation requirement
 - rebuttable presumption of intent (multiple ID, spec.data)
 - fraudulently obtaining personal info (Bill C-299)
 - trafficking in ID info/cards recklessly or knowingly
 - breach of trust (employee theft)
 - fraudulently redirecting mail

Caution

Beware of unintended consequences...

- shouldn't criminalize socially accepted uses of alternative identities
 - pseudonyms (eg, online privacy protection)
 - kids' use of adult ID to get cigarettes or booze
 - investigative journalism/public interest research
- mere possession is not enough
 - eroding the presumption of innocence
 - how much uncaptured crime = acceptable cost of protecting innocent individuals from prosecution?
 - “knowingly and with intent to defraud...”

Criminal Law

- Enforcement challenges
 - high cost of prosecution
 - lack of resources
 - inter-jurisdictional nature of activities
 - mild penalties (non-violent offence)
- Initiatives
 - Phonebusters - info, advice
 - RECOL: Reporting Economic Crime Online
 - international web-based partnership
 - special training; special units; hiring the best minds

Individuals

Individuals should....

- keep ID/account info secure
- shred records
- not post detailed personal information online
- not respond to questionable solicitations, emails
- keep an eye on debit/credit cards
- install up-to-date computer firewall, virus protection
- use different passwords, change frequently
- understand risk of activities and decide accordingly
- check credit report annually (detection)

Reasonable expectations of
individual behaviour?

Public Education

- Website information & Brochures
 - governments, privcoms, police, NGOs...
 - credit bureaus, service providers....
- Bill inserts
- Advertising
- Media – news stories

Customer warnings

- Notice of inherent risks of activity
 - online banking/email communications
 - marketing ignores security risks
 - social networking sites
 - participation in public proceedings
- Data breach notification
 - where risk of ID theft as a result of the breach

Detection Tools

- Unusual account activity notification
 - credit cards, debit cards, tel accounts
- Change of address notification
 - Post Office
 - Service Providers

Victim Assistance/Redress

- Existing:
 - Credit bureau fraud alerts upon request
 - Standard “Identity Theft Statement”
- Proposed:
 - Credit bureau security freeze upon request
 - Right to copy of police report
 - Process for court order establishing innocence and ordering corrected records
 - Mandatory restitution where conviction
 - Statutory right to sue negligent org’s for damages

Organizations

Governments

- tamper-proof identity documents
 - Passports, Health cards, Drivers licences
- stricter application processes
 - Passports, Birth certificates, Licences
 - Change of Address (Canada Post)
- caution in posting public records online
- avoid large databases of citizen info

Organizations

- limit collection/retention of personal information
- don't create or contribute to data warehouses
- control (minimize?) outsourcing
- minimize disclosures of personal information
 - eg., credit card receipts
- security safeguards
 - computer firewalls, access controls
 - trash: shredding docs, cleaning used computer equip.
 - validation, authentication of customers
- employee screening, training, monitoring
- warnings; notice to potential victims

Best Practices/Guidelines

- CSA Privacy Code – now law!
- Principles for Electronic Authentication: A Canadian Framework
 - <http://e-com.ic.gc.ca>
- 7 Laws of Identity (Identity Metasystem)
 - www.identityblog.com
 - www.ipc.on.ca
- Consumer Protection Codes of Practice

Civil Liability

- Common law tort of negligence
 - undeveloped law (class actions in progress)
 - problems:
 - prohibitive cost of litigation
 - applicable standard of care
 - must prove causation + damages
 - statutory regime may foreclose separate actions

Data Protection Laws

- PIPEDA + Alta PIPA, BC PIPA, Quebec
 - Fair Information Practices:
 - must employ reasonable security safeguards
 - remain responsible for outsourced data
 - must not collect more than necessary for purposes
 - must not retain longer than necessary
 - must not disclose for new purpose w/o consent
 - must provide individual access to information
 - But no data breach notification requirement....

Data Protection Laws

- PIPEDA:
 - weak enforcement regime
 - complaint based
 - Commissioner has no binding powers
 - no provision for class actions
 - remote risk of sanctions for non-compliance
 - financial or reputational
 - to get redress, individual must sue in court and prove damages

In conclusion....

- Need legal/policy action on all fronts:
 - criminal prosecutions + meaningful sentences
 - individual awareness + behaviour modification
 - recognizing limits of consumer control/abilities
 - consumer protection + victim assistance/redress
 - government and corporate data protection
 - stronger, clearer privacy laws
 - real risk of financial/reputational loss if non-compliant
 - civil liability for negligence leading to ID theft

Conclusion

- Caution that cure not worse than disease!
 - adopting privacy-invasive technologies/systems
 - criminalizing socially acceptable behaviour
 - requiring costly but ineffective measures
 - unwittingly impeding beneficial measures

www.cippic.ca