Brief to the House of Commons Standing Committee on Access to Information, Privacy and Ethics on the subject of Identity Theft

Canadian Internet Policy and Public Interest Clinic (CIPPIC)
University of Ottawa
Philippa Lawson, Director

May 15, 2007

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) is a legal clinic hosted by the University of Ottawa's Faculty of Law. We work with students and faculty on a variety of legal issues arising from new technologies, including privacy, free speech, copyright, and consumer protection. The clinic's mandate is to fill voids in public policy debates, and to thereby ensure greater balance in policy and law reform initiatives. The clinic's director, Philippa Lawson, is a lawyer with over 16 years experience as a consumer advocate on the national and international stages.

CIPPIC is part of a multi-institution research project on Identity Theft funded by the Ontario Research Network on Electronic Commerce (ORNEC), a public-private partnership including four major Canadian banks. Over the past year, we have been researching legal and policy approaches to identity theft, while colleagues at four Ontario Universities have been examining issues involving the definition and measurement of ID Theft, management approaches to ID Theft, and technical solutions to ID Theft.

We have published a series of Working Papers on various aspects of the ID Theft problem: an Introduction and Backgrounder, Techniques of Identity Theft, Legislative Approaches to Identity Theft, and Caselaw on Identity Theft. Working Papers on Enforcement of ID Theft Laws and on Policy Approaches to ID Theft are forthcoming. We have also published, as you know, a White Paper on Security Breach Notification. All of these documents are available on our website, www.cippic.ca (under "Publications"). We have also posted a webpage on Identity Theft, with Frequently Asked Questions and Resources for the public.

Our intention, after further research and analysis this summer, is to issue a White Paper with specific recommendations for law and policy reform by the end of the year.

We understand that this committee has launched "a study of identity theft that addresses types of and trends in identity theft, measures to increase consumer protection and that could reduce and eliminate identity theft, and measures to increase public awareness of

and provide better education with respect to identity theft." This study is being conducted in light of the impending Justice Canada 'White Paper' on the criminal justice aspects of identity theft.

Identity Theft: Types and Trends

The term "identity theft" is somewhat misleading insofar as it covers not just the unauthorized collection (or "theft") of data, but also the fraudulent use of someone else's identity information. Some experts use the term "identity fraud" to refer to the second stage of this two-stage crime. We use the term "identity theft" as it is commonly used, to refer to both stages of the crime: unauthorized collection and fraudulent use.

Identity theft can take many different forms, from fraudulent credit card use (for which individual victims are generally compensated) all the way to fraudulent real estate transactions and impersonation in the course of committing a crime. Once they have enough information about a given person, ID thieves typically use it to take over existing accounts (bank, credit card, cell phone, etc.), create new accounts, obtain loans, transfer land title, or engage in other fraudulent acts for their own financial benefit, in the victim's name.

Identity thieves use a number of techniques to gather personal information, from relatively unsophisticated methods such as dumpster diving, mail theft, insider bribing and pretexting (posing as someone who is authorized to obtain the information) to more sophisticated techniques such as skimming, phishing, pharming, keystroke logging, and hacking into large databases.

A single individual may be repeatedly victimized before he or she knows it. Indeed, victims of ID theft are often unaware of it until they apply for credit from a lending institution or start getting calls from a debt collection agency. By this point, their credit rating has been destroyed and they will likely experience great difficulty restoring it. Victims experience a myriad of difficulties restoring their reputations and recovering losses suffered, often as a result of no negligence on their part.

Another, apparently growing, phenomenon is known as "synthetic identity theft". This occurs when the thief combines identifying information about a real person (e.g., SIN or Drivers Licence) with a fictional name or other fabricated personal information, in order to apply for credit. While individual victims may or may not suffer financial loss or reputational damage in these cases, all consumers end up paying for the costs of this fraud, as they do with fraudulent use of credit cards generally.

In the United States, medical ID theft is becoming a serious issue, as fraudsters impersonate insured patients in order to obtain privately-insured medical services. A recent report by the World Privacy Forum highlights the dangers of this form of ID theft, pointing out that it can result in death when incorrect information is added to a victim's health record. This does not appear to be an issue in Canada, due to our system of publicly-funded medicare.

Another trend worth pointing out is the use by ID thieves of the internet to gather and trade in stolen information. While some attempts are made to keep this activity out of reach of law enforcement agencies, it's not hard to find websites offering credit card data for sale, or sales on eBay of computer hard drives with personal data. Although most ID theft activity still likely occurs offline, there is a thriving trade in personal information, facilitated by the internet, making ID theft all the more easy.

"Phishing", "vishing" and "pharming",[1] while no longer new phenomena, continue to be lucrative scams through which ID thieves fool unsuspecting consumers into handing over their account information, by cleverly disguising themselves as banks or other trusted institutions in email messages, phone calls, and on websites that look as official as the real ones.

Statistics on Identity Theft

Unfortunately, there are few reliable statistics on the incidence and cost of identity theft in Canada. Phonebusters, a collaboration between the RCMP, OPP and Competition Bureau, publishes statistics based on the complaints it receives, but these represent only a fraction of the problem. Some public opinion surveys have attempted to estimate the extent of the problem, but this data is suspect insofar as respondents may under- or over-report depending on their understanding of what is meant by "identity theft". In order to be useful, statistics should distinguish among different types of ID theft.

Our colleagues Dr. Norm Archer and Susan Sproule of McMaster University have been researching statistics and definitional issues around ID theft, and have recently completed a consumer survey on the issue.

In contrast to the dearth of information on ID theft in Canada, there is much more data being generated on ID theft in the U.S., where the Federal Trade Commission has been tasked with gathering statistics and reporting on the problem in that country. Even there, however, data is incomplete as it is based on complaints and surveys. **We need a concerted national strategy for gathering reliable, reasonably comprehensive data on the incidence, types and costs of identity theft in Canada.**

ID Theft Prevention

Our research suggests that identity thieves are benefiting as much, if not more, from unnecessary collection, storage, and trading of personal information by organizations as they are by deficiencies in criminal law enforcement or by consumer credulity and carelessness. **If we are to attack this problem successfully, efforts are needed in four**

[1] "Phishing" refers to the fraudulent acquisition of personal information by masquerading as a trusted entity such as a bank in an email communication. "Vishing" is the same sort of activity conducted over the phone, through the use of automated messages, call-back numbers, and interactive voice systems. "Pharming" is a type of computer attack that redirects legitimate website traffic to bogus sites imitating the legitimate website. All three practices are designed to gather account and other personal information from unsuspecting consumers.

key areas: strengthening and enforcement of data protection laws, prosecution of ID thieves, consumer protection and victim redress, and public education.

PIPEDA needs teeth

We have a reasonably good data protection law: the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). This law prohibits organizations from collecting more personal information than they need, from retaining it longer than necessary, and from using or disclosing it for purposes other than those to which the individual has consented. It also requires that organizations put in place reasonable security measures to protect against unauthorized access and identity theft.

The most significant problem with PIPEDA is not any particular substantive deficiency (many of which this Committee has identified in its recent report on PIPEDA), rather it is that **PIPEDA lacks an effective mechanism to encourage industry compliance.** As a result, many organizations are collecting, retaining, and trading far more personal information than they need to, thereby exposing individuals to a greater risk of identity theft. They are also failing to secure the personal data that they hold, through effective encryption, careful employee screening, and other measures. CIPPIC's 2006 study of 64 online retailers, *Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?*, confirms anecdotal evidence of widespread non-compliance with even the most basic requirements of the Act.

As the Privacy Commissioner stated in her Submission to this Committee last week, "the risk of identity theft in the private sector would be significantly reduced if organizations engaged in commercial activities simply follow the dictates of PIPEDA and use common sense when dealing with personal information."

A data breach notification requirement holds some promise for creating incentives for compliance, but only if (a) such notification is made public, and (b) breaches are not so frequent and widespread as to diminish the reputational damage of publicity. Even so, breach notification rules need to be supplemented with an enforcement regime that creates a real risk of financial penalty for over-collection of personal data or other violations of PIPEDA that contribute to the ID theft problem.

In its November 2006 submission to this Committee on PIPEDA reform, CIPPIC made a number of recommendations for strengthening PIPEDA's enforcement regime. These included:

- giving the Privacy Commissioner order-making powers;
- requiring the Privacy Commissioner to name non-compliant organizations in her findings;
- allowing for class actions against organizations that violate PIPEDA;
- removing financial disincentives for individuals to pursue lawsuits against organizations for breaches of PIPEDA; and
- including punitive damages as a possible remedy for violation of PIPEDA.

Disappointingly, none of these recommendations was adopted by the Committee. Yet, addressing the incentive problem - the most important deficiency of PIPEDA and a key factor in the growing problem of ID theft – is critical if we want to make any real headway on ID theft.

More public education and awareness initiatives are needed

While there are many excellent websites and brochures explaining these schemes and offering tips for avoiding ID theft, individuals continue to fall prey to "social engineering" schemes such as phishing that are designed to extract their personal information for fraudulent use. Financial institutions could do more to warn their customers about such schemes. Young people should be educated about the risks of posting detailed personal information on web forums such as Facebook and MySpace. More consumers, especially the elderly and other vulnerable populations, could be reached through mass media communications.

The federal government could take action in this area by including educational inserts in government cheque mailings, by posting information and brochures in government offices serving the public, and by using the mass media.

We recommend that the Financial Consumer Agency of Canada (FCAC) be mandated to undertake a national public education campaign on ID Theft, in consultation with lending institutions, credit bureaus, law enforcement agencies, and consumer organizations. Such campaign should focus on the most common scams used by ID thieves to gather information directly from individuals.

Consumers can help prevent and prosecute ID fraud if given more rights

Currently, victims of ID theft usually have no way of knowing that the theft has occurred until the damage is done. Moreover, they have limited rights to stop the continued flow of credit information based on fraudulent transactions. Even the most able, educated and motivated victims encounter tremendously frustrating obstacles as they attempt to stop the damage and regain their reputations. If such obstacles were removed, individual victims would be able to mitigate the damage and take preventative actions more quickly. They could also, in some cases, assist the police in identifying and prosecuting criminals.

Measures needed to empower consumers in this context include, but are not limited to:

- requiring organizations to notify individuals of security breaches that put their personal information at risk of unauthorized and fraudulent use;
- requiring lending institutions to provide consumers with access to the version of their credit reports relied upon by the lending institutions, upon request (rather than the much more abbreviated version provided to consumers by credit bureaus);
- providing consumers with the right to a "credit freeze" upon request to credit bureaus (such that no credit information can be disclosed without the consumer's explicit permission for that specific disclosure);

- providing victims with a standard affidavit that is accepted by all major credit-grantors and identity document grantors; and
- giving victims of ID theft the right to obtain, without unreasonable effort and within a reasonable time, a police report on their complaint, and an official process for clearing their name.

Victims of ID theft are an important source of information about the problem, and should be treated as the valuable resource that they are, rather than as complainers, or worse, suspects. They should be given the tools they need to help stem the tide of ID theft.

Attacking the Problem

There are many different players dealing with ID theft in Canada, largely on their own without much coordination. The Consumer Measures Committee has done some good work, but it is limited in scope. Law enforcement agencies, courts, credit-granting institutions, credit bureaus, issuers of official documents, Canada Post, consumer protection agencies, and victims of ID theft are all key stakeholders in the effort to combat ID theft. There needs to be much more coordination both within sectors and among different stakeholders if we are to make significant progress on this issue.

We recommend the establishment of a federal/provincial/territorial Task Force with representation from all major stakeholders (e.g., law enforcement agencies, consumer protection agencies, lending institutions, credit bureaus, consumer groups) to investigate the problem of identity theft in Canada and to develop a strategy such as that proposed below. The recent federal Task Force on Spam provides a good model for this kind of work.

Conclusion: Summary of Recommendations

CIPPIC recommends the development of a national strategy for combating ID theft, which strategy should include:

- **amending PIPEDA so as to create meaningful incentives for compliance, based on real risks of financial and/or reputational damage due to non-compliance with the Act;**
- **appointment of a lead agency responsible for gathering and reporting ID theft statistics and for coordinating efforts to combat ID theft across Canada;**
- **mandating the Financial Consumer Agency of Canada to undertake a national public education campaign on ID Theft;**
- **establishment of a national ID theft victim assistance bureau with a mandate of gathering statistics, analyzing the problem, educating the public, and making recommendations for legislative and policy reform;**
- **requiring credit-granting institutions to report on incidents of ID theft (by type; amount of loss suffered or avoided);**
- **providing consumers with rights that improve their ability to detect, prevent and mitigate the effects of identity theft, which rights should include:**

    - **allowing consumers access to the version of their credit report relied upon by lending institutions; and**
    - **allowing consumers the right to a "credit freeze" upon request to credit bureaus;**
- **a thorough review of legislation governing credit bureaus, lending institutions, and police agencies with a view to identifying other ways in which these agencies could assist in the prevention, detection and mitigation of ID theft.**

We further recommend the establishment of a Task Force with representation from all major stakeholders to develop this strategy.

*** END OF DOCUMENT ***