Consumer Measures Committee

Comité des mesures en matière de consommation

Working Together to Prevent Identity Theft

A Discussion Paper

Working Together to Prevent Identity Theft

A Discussion Paper for Public Consultation
July 6, 2005

Introduction

New information technologies have revolutionized business practices and made Canadian companies more efficient and competitive. However, the electronic collection and storage of personal information has, at the same time, multiplied the risk that personal information may be misappropriated and used to commit fraud or other crimes. This is called "identity theft".

The full extent of the problem is difficult to measure since affected individuals register complaints with a number of different organizations, including credit bureaus[1], banks, credit card companies, police, and government departments. And many victims of identity theft do not report the crime at all. However, household polls indicate the problem is pervasive. In February 2003, Ipsos Reid reported that nine percent or approximately 2,700,000 Canadians have been victims of identity theft at some point over their lifetime[2]. These victims suffer financial losses, a loss of reputation, emotional distress, and the often-difficult task of rebuilding their credit rating[3].

This discussion paper explores a number of options to amend federal, provincial and territorial laws to make identity theft harder to commit and to make it easier for victims to recover from the experience. Policy options related to the Criminal Code are being considered in a separate process by Justice Canada and are not included as part of this paper.

This paper is divided into four sections. The first section provides an overview of the problem posed by identity theft, including a definition of terms and specific examples of harms that can occur. The next section examines why identity theft is a growing problem and identifies those groups that can contribute to a solution. The third section provides an overview of the legislative frameworks currently in place in both Canada and the United States. Finally, the last section sets out specific options for legal reforms to combat the problem, explores the pros and cons of each option, and poses questions for consideration by the reader.

Request for Comments

The Consumer Measures Committee (CMC) is a forum of federal, provincial and territorial government representatives who cooperate to eliminate barriers to trade between provinces and territories, and to improve the marketplace for Canadian consumers. The CMC is conducting a public consultation on measures to address Identity Theft with the objective of soliciting views from stakeholders and the public on their policy and practical implications. The CMC will then revise and refine the proposals based on stakeholder feedback. A subsequent round of consultations will be held on specific proposals presented in quasi-legislative language, with an indication of which statute(s) would be affected.

By providing background on the issues and a preliminary analysis of the various options for reform, this paper is intended to facilitate public participation in the reform process

In order to assist the CMC in reviewing submissions, please structure your comments on the same basis as the consultation paper. In particular, please provide responses to individual questions, as well as any additional comments you may have. Please focus on developments that can reasonably be expected to occur over the next 10 years and provide as much detail and supporting evidence as possible.

We ask all parties to do their best to assist the CMC in achieving its challenging goal of developing recommendations for the best framework for combating identity theft – irrespective of the short-term costs and benefits for various industry players or consumer groups.

We would greatly appreciate if you would submit your comments electronically. To do so, download an electronic copy of the Consultation Workbook on our Web site at www.cmcweb.ca/idtheft, enter your responses and e-mail the workbook to us, at:

E-mail: info@cmcweb.ca

If you prefer to provide a hard copy of your submission, please send it, along with your name and contact information, to:

Fax: (613) 952-6927
Mail: Consumer Measures Committee
c/o Office of Consumer Affairs
Industry Canada
235 Queen Street,
Ottawa (ON) K1A 0H5

If you wish to submit comments on the *Discussion paper* and options, it is not essential that you use the *Consultation workbook*. You may choose to provide comments in letter form or in an e-mail and if you prefer, to limit your comments to just a few of the options outlined.

All materials or comments received from organizations may be used and disclosed by the Consumer Measures Committee (CMC) or any government body to assist in evaluating and revising the proposed options described below. This may involve disclosing materials, comments or summaries of them, to other interested parties during and after the public comment period.

An individual who provides materials or comments and who indicates an affiliation with an organization will be considered to have submitted those comments or materials on behalf of the organization so identified.

Materials or comments received from individuals who do not indicate an affiliation with an organization may be used and disclosed to assist CMC or other government bodies in evaluating and revising the proposed options. However, CMC or other government bodies will not disclose personal information, such as an individual's name and contact details, unless required by law.

Defining Identity Theft

There is a great deal of confusion about what the term "identity theft" means, especially when it comes to the misappropriation of personal information by others. Under Canadian law, in order to be considered theft, a person must take an actual "thing" and it must involve a deprivation to the owner. Therefore, with the exception of credit card and debit card data, a person who copies personal information (such as name, address, SIN number, driver's licence, birth date etc..) from a computer or official document and retains that information for future criminal use has not committed an offence under the Criminal Code. There has been no theft because the owner still has the information; all that is lost is confidentiality.[4] There is similarly no offence for selling or transferring that information to others. The limitations noted above have been characterized as gaps in the Criminal Code and other initiatives currently underway in the federal government will assist law enforcement in more effectively addressing identity theft. However, merely calling for provisions to stop "thieves" tends to neglect the more fundamental questions of how technology as well as business practices as a whole may unwittingly facilitate fraud.

For the purposes of this paper, identity theft is defined as the use of someone else's personal information, without his or her knowledge or consent, to commit a crime, such as fraud, theft or forgery. Identity theft also includes the acquisition or transfer of personal information as an instrument to commit these crimes in the future. This definition allows us to address the problem as a whole – from the collection of information to its distribution, misuse and correction – and identify measures, which can mitigate the harm to the consumer.

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) defines personal information as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization". In Quebec, an *Act Respecting the Protection of Personal Information in the Private Sector* defines personal information as "any information which relates to a natural person and allows that person to be identified". This might include such things as the individual's name, home address, age, gender, identification numbers, credit card numbers, income, employment, assets, liabilities, source of funds, payment records, personal references and health records. Personal information does *not* generally include employees' contact information at their place of work but may include the employees' e-mail addresses.

Identity theft victims report that their personal information has been used to open up a new credit card account (36%), commit insurance or payment fraud (24%), obtain government benefits (24%), open up a new phone or utility account (23%), or take out a loan in their name (22%)[5]. Personal information can also be used to commit theft or forgery. For example, an identity thief who has someone else's debit card number and personal identification number (PIN) can use the information to empty the victim's bank account (theft). Similarly, an identity thief can use someone else's information to forge a passport application or a cheque (forgery). A forged

cheque can also be deposited into the victim's account and then the funds can be withdrawn – leaving the victim on the hook for the shortfall.

It is important to remember that identity theft is not always committed for its own sake. A report submitted to the Solicitor-General of Canada and the Attorney General of the United States indicates that identity theft is commonly committed to further other criminal activity, such as organized crime and terrorism[6]. Reducing incidences of identity theft may therefore help reduce broader social harms, such as threats to national security.

Understanding the Problem

Identity theft is on the rise. Surveys in Canada and the United States indicate that approximately 3 percent of Canadians and Americans were victims of identity theft in 2003 alone[7].

While fraud and theft are not new, what is different is the scale at which the crimes are being committed. Criminals can use electronic databases to misappropriate personal information and use it to unlawfully gain access to benefits or consumer credit. TransUnion LLC, a consumer and commercial credit reporting company, reported that incidents of ID Theft increased from 4000 cases in 1999 to over 24,000 cases in 2002 (a 500 percent increase).[8]

Consumer behaviour can put individuals at risk of identity theft when, for example, people fail to protect their PIN, provide more information than necessary, or make online payments on insecure Web sites.

Corporate practices contribute to the problem. Michigan State University professor Judith Collins reports that as much as 70 percent of all identity theft can be traced to leaks that occur *within* organizations, such as employees who accept bribes or who pilfer customer information on behalf of organized crime[9]. Employees or thieves may also steal equipment for its resale value and not for the information it contains. This is what happened to Saskatchewan's Co-operators Life Insurance in January of 2003, when an employee in their data management company made off with a hard-drive containing the personal information of up to 180,000 customers. [10]

Recent data breaches in Canada have caused concern that the information stolen is used to commit identity theft. In February of 2004, the credit files of approximately 1,400 people were exposed in a security breach at Equifax.[11]

Organizations may also unwittingly release personal information to criminals who pose as legitimate businesses. This is what happened in early 2005 when the American information broker ChoicePoint inadvertently sold the personal information of at least 145,000 Americans to 50 identity thieves.[12]

In addition, certain corporate practices like printing social insurance numbers on credit reports and mailing out pre-approved credit applications encourage what the police call "dumpster diving" – sifting through garbage to find personal data which can then be used to commit crimes.

All of these practices are compounded in a highly competitive marketplace in which consumers increasingly rely upon credit to make purchases. This creates market incentives for lenders to provide quick access to consumer credit, especially since existing laws do not require that organizations take steps to ensure that the person who is requesting the credit is in fact who they say they are.

Greater vigilance on the part of credit lenders in verifying the consumer's identity could reduce identity theft. Certain lenders may not carefully vet consumers because they may be concerned that if they take up too much time or ask too many questions, consumers may take their business elsewhere. Credit card and cell phone industries are quite profitable and at least some issuers would prefer to absorb the losses they might suffer from the occasional identity theft rather then forgo the income that would have been generated by those consumers.[13] Statistics gathered by PhoneBusters in 2003 and the first half of 2004 indicate the largest number of complaints surrounding identity theft relate to credit cards or false applications for credit cards (32 percent) and cell phones or false application for cell phones (10-12 percent).

While Visa Canada and Mastercard Canada incurred losses of $134.10 million in 1999, and 163.18 million in 2004, these losses represent only a small percentage of the banks' overall sales volume (less than 1 percent).[14] Also, the lender does not bear all the losses alone. Some of those losses are shifted to consumer victims who cannot prove that they were victims of fraud. "This sets up a paradox whereby consumer victims are less able than lenders to prevent and afford the losses, and lenders find it more cost effective to process credit applications without probing applicants to authenticate their identity."[15]

Victims spend many hours trying to clear their names[16] and suffer emotional anguish throughout the process[17]. Victims also suffer from a loss of reputation, as court judgments for bad debts are registered against them and their credit rating tumbles. This, in turn, can make it difficult for victims to find employment or get access to credit when they need it. Victims may even get a false criminal record if the fraudster is convicted of a crime under the victim's name[18].

Effective responses will require cooperation among businesses, financial institutions, credit bureaus, consumers and governments. All have a role to play in making sure personal information is not available to identity thieves who want to use it to commit crimes.

The Legislative Landscape

There are a number of federal, provincial, and territorial laws that deal with some part of the identity theft puzzle. Therefore, a comprehensive response to the problem calls for action from both levels of government, and will involve a number of different pieces of legislation. To help identify potential responses, identity theft legislation in Europe, the United States and Australia was examined. American legislators have clearly been the most active. This may be the result of two factors. First, identity theft is a much larger problem in the US than it is in Europe or Australia. Second, the US is the only jurisdiction surveyed that does not have comprehensive data protection legislation.

Privacy Laws

The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) governs the collection, use and disclosure of personal information by businesses in Canada. Québec, British Columbia and Alberta have substantially similar privacy legislation, which applies to organizations operating in their jurisdictions. Personal information that travels across internal borders for commercial purposes is also subject to PIPEDA.

These information privacy laws require organizations to advise the individual as to why they want the information and only collect it with his or her consent unless collection without consent is authorized by the legislation. Organizations must limit their collection of information to what is reasonably necessary and only use and disclose the information for identified purposes or those specified in law. Organizations are also required to ensure the information is accurate, secure, and retained only as long as necessary to fulfill the identified purposes. Individuals must be able to access and correct their information except as limited by the legislation. Finally, organizations are responsible for the information they hold and individuals may complain to an independent privacy commissioner who can conduct investigations and attempt to resolve such complaints. Commissioners in Alberta, British Columbia and Quebec also have powers to make binding orders. Under the federal law, unresolved disputes relating to certain matters can be taken to the Federal Court.

Note also that Ontario, Manitoba, Saskatchewan and Alberta have health privacy legislation, which is based on the fair information principles outlined above and can apply to some businesses.

Federal Laws

PIPEDA and the federal *Bank Act* may be relevant to a number of the proposed reforms as well as other sector specific legislation. Further legal analysis will be conducted to determine how these statutes may be affected.

The federal government, in consultation with stakeholders, developed authentication principles for the electronic marketplace[19]. Although these *Principles for Electronic Authentication* do not have the strength of law, they establish benchmarks to ensure that the authentication process is based on sound business and market practises, which balance the benefits of electronic commerce against the risks to consumers. In particular, the guidelines provide that the allocation of risk should be "reasonable and fair and take into account the ability of participants to manage risk or absorb losses. It should also create incentives for those developing and implementing authentication processes to ensure that their products and services are secure and reliable"[20].

The *Criminal Code of Canada* contains provisions regarding the traditional offences of fraud and theft, as well as using, possessing and trafficking in credit card/debit card data and interference with computer data. Over the past two years, Justice Canada has examined limitations in the law regarding identity theft and is considering various policy options to address the problem.

Provincial/Territorial Laws

Provincial/territorial legislation sets out the rules and responsibilities for credit bureaus that maintain files on people's credit information. This consumer reporting legislation also regulates consumer privacy with respect to credit information, and the consumer's right not to have future financial transactions jeopardized by inaccurate credit and personal information on their record. To this end, all provinces, except New Brunswick, have legislation dealing with consumer credit reporting. These laws apply to the major credit bureaus (Equifax, TransUnion, and the Northern Credit Bureau) and to other commercial entities that hold databases of personal credit or credit-related information. The options in this paper that refer to credit bureaus or consumer reporting agencies are meant to apply to all organizations regulated under consumer reporting legislation. The provinces and territories also have jurisdiction over credit unions, certain trust companies, and Caisses populaires.

Canada's provinces and territories also have consumer protection legislation, which is generally designed to protect consumers in the marketplace and ensure a level playing field for businesses. The legislation stipulates the kind of disclosure that must be provided to consumers in various transactions, when consumers can have a cooling-off period to think over their decisions and what remedies consumers may have when transactions for various goods and services go awry.

American Laws

A number of American jurisdictions have enacted legislation dealing with identity theft. These laws contain some provisions, which may be appropriate in the Canadian context and, as such, are useful precedents to examine.

The most comprehensive law is the US government's *Fair and Accurate Credit Transactions Act* (FACTA) passed in 2003. FACTA gives consumers more control over their credit reports, including the right to place a fraud alert on their credit file in the event their personal information has been compromised. Consumers can also block false information about them (that resulted from an identity theft) from being released to creditors, and have the right to obtain a free copy of their credit report each year. Other provisions include a requirement that payment card numbers must be truncated on consumer receipts, and that credit score calculations must be more transparent to the consumer.

In addition, a number of U.S. states – including California, Illinois, Texas, Louisiana, Arizona and Connecticut – have amended their consumer reporting and consumer protection laws to implement measures to limit identity theft within their jurisdictions[21]. Many provisions are mirrored in FACTA; however, there are additional measures. For example, in some states: creditors must verify any change of address on a pre-approved credit application; credit bureaus are required to verify that persons requesting credit reports are who they say they are; and organizations must notify customers when the security of their personal information has been breached.

Solving the Problem – Possible Responses

The following section sets out a number of possible options for legal reform. There are two possible vehicles to implement the options described below in a comprehensive manner. One vehicle could be the passage of a new stand-alone Act comprised of various measures to combat identity theft (e.g. the Measures to Combat Identity Theft Act). Another could be the passage of a statute law amendment Act, which would simply amend existing statutes. Examples of statutes, which would potentially be amended to implement the proposed options are:

(a) Federal legislation such as PIPEDA; and

(b) Provincial and territorial legislation relating to consumer reporting, consumer protection, Credit Unions and Caisses Populaires, insurance companies, loan and trust corporations, municipalities, personal health information and privacy legislation similar to PIPEDA.

Regardless of the vehicle chosen, legislative action would have to be taken at both the federal and provincial or territorial levels to implement the options.

These options are divided into three sections. The first includes reforms to make it harder for identity thieves to get their hands on personal information. The second focuses on reforms that make it easier to monitor and detect identity theft at an early stage. And the third contains reforms to make it easier for victims of identity theft to clean up the damage afterwards.

(1) Stopping the Leaks

Option I – Truncate (partially blank out) payment card numbers

Persons that accept payment cards (including credit cards and debit cards) for the transaction of business must not print the expiry date or more than the last five digits of the card number on any receipt generated electronically at the point of sale or transaction.

This option would limit the amount of personal information that is routinely made available through the ordinary course of business. Account numbers and expiry dates are clearly crucial to the facilitation of fraud because they, especially when combined with the name of the individual, can be used by an identity thief to make fraudulent purchases or banking transactions. The debit card number is perhaps less vulnerable because of the use of PINs, but limiting the disclosure of debit card numbers will still make it more difficult for identity thieves to obtain crucial data about an individual

Routinely truncating payment card numbers on receipts would also entrench good information practices by underlining the importance of safeguarding personal information without detracting from the usefulness of the printed receipt. By limiting the type of information on the receipt, this option would help thwart dumpster divers and protect the payment card number at the point of sale or transaction. However, the printed receipt could still be used to verify the transaction if necessary because the individual retains the full card number for authentication purposes.

This option has been implemented in a number of American jurisdictions, including Arizona, Illinois, and California, as well as at the federal level through FACTA. Although the California and Arizona laws are limited to credit card numbers only, legislation in other jurisdictions extended the provision to debit card numbers as well. All of these laws make a failure to comply with the provision an unlawful business practice, which attracts penalties.

In addition, American legislators have limited the application of the provision to electronically printed receipts, by expressly excluding handwritten receipts and imprinted cards. This exempts very small businesses or occasional users of the credit card system (such as independent taxi cab drivers) who are less able to absorb the costs of an electronic payment system. Similarly, they

have typically delayed the implementation of this provision for two or three years if the organization is already carrying on business when the law is passed, to give existing businesses time to replace or modify existing equipment.

In the Canadian context, this is already a practice of many larger retailers on a voluntary basis. For those who do not currently truncate payment card numbers, replacing or modifying equipment would have cost consequences, especially for small businesses. To mitigate this, old equipment could be "grandfathered" – in other words, small retailers would only have to comply with this provision when they replace existing equipment with new information systems in the future. In the alternative, implementation could be delayed for a two or three-year period, to allow organizations to better absorb the costs of compliance.

This option will be in keeping with industry practice as credit card companies are already moving toward truncated numbers.

QUESTIONS FOR OPTION I:

1. Do you think this option would better protect against identity theft?
   - Yes or No
   - Why or why not?
2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?
3. Should there be exemptions? If yes, what type?
4. Should there be a penalty associated with this provision (as proposed in Option 9)?
5. Under this option, who should ultimately be responsible for losses incurred from identity theft?
6. Are there disadvantages for consumers or industry? Please describe.
7. What are the existing or planned industry standards for truncation of payment cards, and if any, what are timelines for implementation? Do the standards exclude handwritten and/or imprinted cards?

Option II – Verify the identity of persons and organizations accessing credit reports

Credit bureaus must take reasonable steps to authenticate the people and organizations that are accessing credit reports.

A consumer's credit report contains a significant amount of personal information. Credit information includes name, age, martial status, spouse's name and age, number of dependants, particulars of education or professional qualifications, current and previous addresses, social

insurance number, telephone number, date of birth and employment history, estimated income, paying habits, outstanding debt obligations, cost-of-living obligations and assets. Clearly, this information is useful to identity thieves. When a report is sold to unauthorized persons, the potential harm to individuals is significant because the report itself provides more than enough information to assume the individual's identity. In addition, an identity thief may attempt to get a copy of the consumer's credit report by posing as the individual himself or herself.

Legislation in most provinces and territories provide that no one may obtain a consumer report without the consent of the consumer or unless the consumer is given written notice that a report is about to be obtained. The Acts also require credit bureaus to have reason to believe the report is being requested for a legitimate purpose. This option would require credit bureaus to take reasonable steps to authenticate that the people requesting credit reports are who they say they are.

Stopping the release of credit reports to unauthorized persons could significantly cut back on identity theft because it would protect the confidentiality of the personal information contained in the report and make it extremely difficult for thieves to qualify for credit in the consumer's name. A standard set of authentication practices would also level the playing field in the private sector by creating incentives to ensure that authentication processes are secure and reliable, in keeping with the federal government's *Principles for Electronic Authentication*[22].

QUESTIONS FOR OPTION II:

1. Do you think this option would better protect against identity theft?
   - Yes or No
   - Why or why not?
2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?
3. Should there be exemptions? If yes, what type?
4. Should there be a penalty associated with this provision?
5. Under this option, who should ultimately be responsible for losses incurred from identity theft?
6. Are there disadvantages for consumers or industry? Please describe.
7. Should this obligation to authenticate be required of third party resellers of credit reports? If not, why not?
8. Do credit bureaus provide different levels of information in credit reports depending on the need of the organization and/or individual requesting the credit report? If so, what standards are applied?
9. What would be the costs associated with authenticating credit lenders and consumers?

Option III – Do not disclose social insurance numbers (SINs) on credit reports or use them as a unique identifier for consumers

Where it is appropriate for financial institutions to collect SINs, they should keep the numbers confidential. In particular, consumer reporting agencies and financial institutions should not use a SIN as a unique identifier for consumers, or disclose the consumer's SIN on a credit report.

Although an individual can only be required by law to disclose their social insurance number in the context of a limited number of government programs, many organizations – including financial institutions and credit bureaus – use SINs as a convenient way to identify individuals. Since the SIN is unique to each individual, it allows a lender, for example, to make a decision about a loan on the basis of a credit report, with confidence that the credit report belongs to the person who applied for the loan. The SIN is therefore a useful identifier, which is frequently used in the marketplace, especially in the context of credit transactions.

However, the use of SINs by businesses is particularly troublesome because the SIN can act as the key that opens up the victim's life to an identity thief[23]. With the individual's name and SIN, the thief could apply for government benefits, sign a lease, take out a loan or work in the victim's name. This means that protecting the SIN may be an effective way to reduce the flow of sensitive data to identity thieves.

The Office of the Auditor General of Canada reported in 2002 that the expanded use of the SIN by other levels of government and institutions has both increased the potential for SIN fraud and extended its impact. For example, once someone has established a false identity that includes a SIN obtained fraudulently from HRDC, that identity can be used to access federal, provincial, and territorial social programs, to defraud banks, and to misrepresent income to the Canada Revenue Agency[24].

This option would help protect the confidentiality of SINs by prohibiting a credit bureau from printing the individual's SIN on a credit report. Financial institutions and credit bureaus would also be required to develop an alternative unique identifier for consumers. A truncated SIN may be an acceptable alternative.

Although there is no equivalent protection in other jurisdictions, FACTA provides that consumers can request that their social security number be truncated on their credit report. This means that motivated consumers can request additional protection but the majority of people will remain unprotected.

This option would result in an increase in costs for the initial implementation of a new identifier by credit bureaus and financial institutions. It might also make it more difficult to match a credit

history to a particular individual. This could have consequences for the ease with which lenders are able to obtain credit checks on people who have legitimately applied for credit. It is unclear whether or not consumers would be willing to accept delays because of this.

QUESTIONS FOR OPTION III:

1. Do you think this option would better protect against identity theft. Why or why not?
2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?
3. Should there be exemptions? If yes, what type?
4. Should there be a penalty associated with this provision?
5. Under this option, who should ultimately be responsible for losses incurred from identity theft?
6. Are there disadvantages for consumers or industry? Please describe.
7. For financial institutions, is there an industry standard with respect to requesting the SIN? If so, when is it requested and when is it not requested? What are the grey areas?
8. For retailers, real estate agencies, telecomm companies, are there any industry standards in terms of when SINs are requested?
9. What would be the costs associated with developing a unique identifier? How long would it take to implement this?
10. Would truncating the SIN be a preferred solution? If so, how could that be implemented?

(2) Assisting in Detection

Option IV – Allow consumers to place freezes on their credit reports

> *Upon a consumer's request, credit bureaus must place a freeze on the consumer's credit report free of charge. If a freeze is in place, the credit bureau would not be permitted to release the credit report to a third party without prior express authorization from the consumer. Authorization may be obtained by contacting the consumer at a predetermined telephone number or street address.*

A freeze on his credit report would enable a consumer who is concerned about identity theft to instruct the credit bureau not to release a credit report without first contacting the consumer to get express authorization to do so. Since the consumer must be notified every time a person requests his or her credit report, he or she would be able to identify fraudulent requests for credit.

Accordingly, this option would give consumers more control over the use and disclosure of the personal information about them that is held by credit bureaus. It would also alert them to an unauthorized request for a credit report, making it much more difficult for an identity thief to

qualify for credit in their name.

Freezes on credit reports have been implemented by law in California, Louisiana and Texas. The consumer requesting the freeze is required to provide proper identification, and the credit bureau must put the freeze in place within a set period of time (between 24 hours and five days). Within 10 days, the credit bureau must also mail the consumer a password or personal identification number that can be used to authorize the release of a report or to temporarily lift the freeze. Credit bureaus that fail to comply – either wilfully or negligently – are subjected to minimum penalties ranging from $500 to $2,500 plus legal fees.

Passwords mailed after the fact to the consumer may be intercepted by identity thieves, particularly if the address in the file has been compromised. Accordingly, this option suggests the credit bureau use a predetermined telephone number to contact the consumer for authorization. Since the number is identified before the freeze on the consumer's credit report is requested, it would be more difficult for a thief to appropriate control over the account.

This option proposes that freezes should be available free of charge to ensure that there is a minimum level of protection for all consumers. This is in keeping with the authentication principle that the allocation of risk should correlate with the party's ability to manage the risk and absorb the loss.

QUESTIONS FOR OPTION IV:

1. Do you think this option would better protect against identity theft. Why or why not?
2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?
3. Should there be exemptions? If yes, what type?
4. Should there be a penalty associated with this provision?
5. Under this option, who should ultimately be responsible for losses incurred from identity theft?
6. Are there disadvantages for consumers or industry? Please describe.
7. Should this be offered as a preventive and/or post theft instrument?
8. Are there implications for monitoring of credit worthiness and other marketing activities?
9. Should there be any exceptions to the freeze on credit reports?
10. Should there be a reasonable cost-recovery fee chargeable for this service?

Option V – Require organizations that store personal information to notify individuals and credit bureaus in cases of security breaches

When the security of personal information held by an organization is breached, the organization must contact the individuals whose personal information has been compromised as well as relevant credit bureaus as soon as reasonably possible.

It is not clear whether there are sufficient market incentives to induce organizations to inform individuals when the security of their personal information is breached; individuals may not be notified that they are at a higher risk of identity theft. Accordingly, unsuspecting individuals may not be able to take swift remedial action.

This option would require that the organization who's security has been breached to inform and bear the cost of contacting all affected individuals. The ChoicePoint case indicates that legislation requiring notification of a breach has a direct impact on corporate behaviour. ChoicePoint notified California residents of the fact their personal information was released to unauthorized persons because they were required to do so under California law. The company did not intend to notify non-California residents because there was no legal requirement to do so, and only sent out notices after they were put under significant media pressure.

In the Canadian breaches suffered by Equifax and Co-operators Life Insurance, it appeared that the companies were also slow to notify the customers affected. Duty to warn legislation would go a long way to ensuring potential victims of identity theft are notified of security breaches in a timely way.

This option is also consistent with the fair information practices mandated in PIPEDA and provincial laws. Since organizations are required to keep personal information secure, notifying the individual would ensure that organizations that fail to do so remain accountable to the individual.

This option would also require that organizations inform the relevant credit bureau(s) of the names of all individuals whose information was compromised so the bureaus could place a fraud alert on their credit files (see Option 6 below).

If the organization were required by legislation to notify the relevant credit bureaus, disclosure of this personal information without the knowledge and consent of the affected individuals would be authorized under PIPEDA and provincial laws. However, to mitigate any potential harm, organizations should also be required to notify the individual that a fraud alert has been placed on their credit file (see the discussion under Option 6 below).

QUESTIONS FOR OPTION V:

1. Do you think this option would better protect against identity theft. Why or why not?
2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?
3. Should there be exemptions? If yes, what type?
4. Should there be a penalty associated with this provision?
5. Under this option, who should ultimately be responsible for losses incurred from identity theft?
6. Are there disadvantages for consumers or industry? Please describe.
7. Are there any market place incentives, i.e. contractual obligations that require organizations to disclose when they have had a breach of security? If so, what are they and do they pertain solely to breaches of specific information, i.e. financial breaches?
8. As a consumer, would you be willing to give up some control over your personal information by allowing a company to put a fraud alert on your credit bureau file in a timely way to protect you from identity theft?
9. What should be the threshold for notifying the consumer that personal information has been breached?
10. Within what period of time, and by what means, should companies have to notify consumers?
11. Should this proposal include a duty for the organization to notify PhoneBusters National Call Centre?
12. Is this a good approach to achieving a centralized reporting organization that can detect trends and compile more accurate statistics?

Option VI – Require credit bureaus to place fraud alerts on consumers' credit reports in cases of security breaches or upon the request of an identity theft victim

Upon receiving notice from an organization that the security of the victim's personal information has been breached, or upon request by an identity theft victim, a credit bureau must place a fraud alert on the consumer's credit report that his or her identity may have been used without consent to fraudulently obtain goods or services. A creditor that receives a credit report with such a notice must not give or extend credit in the person's name without first taking reasonable steps to verify the identity of the credit applicant.

Currently in the case of a security breach, if the company decides to notify affected customers, they send a letter advising the customer to contact the credit bureaus to discuss whether a fraud alert is required. The consumers must then contact each of the credit bureaus to obtain the application form to request that a fraud alert be placed on their file. The process can result in significant delays and damages during this period of time. The process could be streamlined so that the company would be required to notify the credit bureaus to place a fraud alert on the file immediately. As soon as is reasonably possible, the consumer could be notified and could then

decide whether they want the fraud alert removed.

When personal information is released without authorization, potential creditors do not have any way of knowing that the information they are relying on may be in the hands of an identity thief. This option would ensure that a fraud alert is placed in the individual's credit file when their personal information is leaked. This would let potential creditors know that there is a risk of identity theft. Accordingly, they would not be permitted to issue credit unless they first contact the consumer at a pre-designated telephone number and get authorization to do so.

A similar provision has been enacted in FACTA and by the legislatures of California, Louisiana and Texas. Under FACTA, an individual can only request that a fraud alert be placed in his/her file if s/he suspects that s/he has been or is about to become a victim of identity theft. Three of the jurisdictions provide that the alert remain on the file for 90 days (Texas calls for 45 days) but all four allow the individual to renew the alert. FACTA provides that, if a consumer submits an identity theft report, the alert can remain in place for 7 years.

American legislation also requires credit bureaus to maintain a 24/7 toll-free hotline to accept requests for fraud alerts. This ensures an individual can contact the credit bureau quickly to protect his credit report upon learning that his personal information is no longer secure. In addition, there are penalties ranging from a minimum of $500-$2,500 for credit bureaus that either wilfully or negligently fail to comply with a request for a fraud alert.

This option could be strengthened by adopting similar penalties and/or the requirement that credit bureaus maintain a toll-free hotline to accept requests for fraud alerts. In addition, there could be penalties for financial institutions that extend credit without first authenticating the identity of the consumer by calling them at the pre-designated telephone number.

This option would mean that fraud alerts could be placed on consumers' credit reports without their consent. However, any harm is likely to be minimized if consumers are notified as soon as is reasonably possible afterwards.

It is difficult to determine who should bear the cost of the alert when it is requested by an organization whose security was breached – the organization or the credit bureau. However, alerts requested by individuals should be placed on the file free of charge to ensure that there is a minimum level of protection for all consumers. This is again in keeping with the principle that risk should be allocated in accordance with those best positioned to manage it and absorb the losses.

QUESTIONS FOR OPTION VI:

1. Do you think this option would better protect against identity theft. Why or why not?
2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?
3. Should there be exemptions? If yes, what type?
4. Should there be a penalty associated with this provision?
5. Under this option, who should ultimately be responsible for losses incurred from identity theft?
6. Are there disadvantages for consumers or industry? Please describe.

(3) Cleaning Up the Damage

Option VII – Require credit lenders to disclose details of fraudulent debts to victims

Upon request, credit lenders must provide identity theft victims with details regarding the fraudulent debt that was incurred in their name.

Victims often need to know the details of fraudulent debts that were incurred, in order to help them clear their name. For example, victims may need to have the copy of the signed credit application in order to prove forgery. This information may be needed at various stages; even before a police report has been issued.

Creditors may be unwilling to release the information because they are concerned about admissions of fault or liability. While individuals enjoy general rights of access to their information under privacy legislation, such access could be denied during a police investigation. This provision would require creditors to disclose the information even if there was an investigation underway.

This option would mean that a creditor who granted credit to an identity thief in the victim's name would have to provide the victim with any information it has with respect to the debt so the victim can reverse the damage and protect his or her reputation.

A similar provision is included in both FACTA and Louisiana legislation. There, the victim is required to provide proof of his or her identity and the existence of an identity crime. The latter can be satisfied by providing the creditor with a copy of a police report and a standard identity theft affidavit.

QUESTIONS FOR OPTION VII:

1. Do you think this option would better protect against identity theft. Why or why not?
2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?
3. Should there be exemptions? If yes, what type?
4. Should there be a penalty associated with this provision?
5. Under this option, who should ultimately be responsible for losses incurred from identity theft?
6. Are there disadvantages for consumers or industry? Please describe.

Option VIII – Require credit bureaus to block information about fraudulent debts appearing on a consumer's credit report

Upon receipt of proof of identity theft, a credit bureau must block information about debts incurred in a consumer's name by an identity thief from being reported in the consumer's credit report. A credit bureau may deny or rescind a block in certain circumstances. If the block is denied or rescinded, the bureau must notify the consumer of their decision to do so and provide reasons for their decision.

Identity theft victims report that it is often difficult to correct their credit record. This option would require credit bureaus to block the information about bad debts incurred by an identity thief in the consumer's name. This would occur once the consumer has properly notified them of the situation. However, the credit bureau could remove the block if it has reasonable grounds to believe that the consumer had misrepresented the facts.

Under FACTA, consumers must provide a copy of an identity theft report and a statement that the information does not relate to a transaction by the consumer before the information will be blocked. California law requires that the consumer provide the bureau with a copy of the police report at the time of the request. In the Canadian context, the Identity Theft Statement (available on the Web sites of the CMC, the provinces and PhoneBusters), which includes a requirement for a police report, could serve as evidence that the information is the result of identity theft.

Under FACTA and California law credit bureaus also have the power to deny or rescind a block if the request was made in error, if the consumer made a material misrepresentation of fact, or if the consumer received goods or services as a result of the blocked transaction. To mitigate the difficulties that victims face when they try to clear their records, California law goes on to say that the credit bureau should believe the victim unless it has substantial reason based on verifiable facts to doubt the authenticity of the documentation submitted in support of the request to block.

This option could adopt a similar standard to ensure that credit bureaus are protected against those consumers who abuse the rules. Alternatively, a thirty-day timeline could be built into the option before the information is blocked. This would give the credit bureau time to check with the credit lender to verify the consumer's claim that s/he has been the victim of identity theft. In order to avoid uneven responses on the part of different credit bureaus to this kind of request, this option could also require that credit bureaus create a streamlined approach to resolve complaints about inaccurate credit reports that contain information about debts incurred by identity thieves. This tell one-tell all approach would significantly simplify the process for victims who are trying to clear their names as well as ensure that victims are not treated differently by different credit bureaus. So, if one credit bureau removes credit information that was incurred by an identity thief, it would inform the other bureaus who shall then similarly remove the information from the individual's credit file.

QUESTIONS FOR OPTION VIII:

1. Do you think this option would better protect against identity theft. Why or why not?
2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?
3. Should there be exemptions? If yes, what type?
4. Should there be a penalty associated with this provision?
5. Under this option, who should ultimately be responsible for losses incurred from identity theft?
6. Are there disadvantages for consumers or industry? Please describe.
7. Should information be blocked based on the consumer submitting the identity theft statement? Alternatively, should there be time for the credit bureau to verify facts with the credit lender before blocking the information?
8. Blocked information may be need to be retained on file for investigation purposes. But, at what point should information that is blocked be completely removed from the file?
9. Should blocks be streamlined such that when information is blocked at one credit bureau, it is handled in the same way at other credit bureaus? Alternatively, should there be one central clearing agency for handling consumer requests to block information about debts incurred by identity thieves?

Option IX - Make organizations liable for damages

Organizations would be liable for damages for failing to comply with the following proposals:

A. Creditors must:

(a) Contact consumers at a pre-designated telephone number before issuing credit, where there is a fraud alert on the credit file,

B. Credit bureaus must:

(a) Properly verify the identity of someone accessing a credit report, or
(b) Put a freeze on consumers' credit report in accordance with the provisions set out in Option 4,
(c) Put a fraud alert on the file where requested to do so in accordance with the provisions set out in Option 6,
(d) Block information in accordance with the provisions set out in Option 8.

C. All Organizations must:

(a) Truncate payment card numbers in accordance with the provisions set out in Option 1,
(b) Notify people affected by a security breach in accordance with the provisions set out in Option 5.

All these organizations would be legally responsible for damages suffered by identity theft victims if they fail to comply with these measures.

As discussed above, there is a mismatch in the marketplace between the costs of identity theft and the revenues generated from easily available consumer credit. This mismatch means that there may not be sufficient incentive for credit bureaus and financial institutions to aggressively monitor fraud and correct misinformation. A statutory right of action would provide the incentive for industry to be more active when it comes to identifying identity theft and correcting faulty information in their records.

Courts so far have been reluctant to hold creditors and credit bureaus liable. This option would create a civil right of action, enabling victims to sue all organizations that do not take reasonable steps to prevent identity theft. The option could also create minimum statutory damages, similar to American laws that impose minimum civil penalties between $500-$2,500 for violations of freeze on credit reports and fraud alert provisions (see Option 6 above). Minimum penalties

would relieve victims from having to prove that they suffered specific damages, and allow them to collect a minimum set amount to compensate them for mental anguish and the time they spent clearing their names.

This option could also give victims the right to get a court order prohibiting credit bureaus from selling credit reports that contain information about debts incurred by identity thieves.

This option could significantly change the responsibilities of organizations in their handling of personal information. There could be a reduction in fraud and losses associated with it. There is likely to be an increase in the costs to the credit industry, albeit, this could be proportionately negligible. The resulting uncertainty could negatively affect the credit industry and drive the cost of credit up. However, it would also provide a strong incentive for the credit industry to minimize the risk of identity theft.

Note that federal and provincial privacy laws require organizations to keep the information they hold secure from unauthorized disclosures. And while identity theft victims could claim damages for actual harm in a Federal or a provincial Court, it is a cumbersome 2-step process and does not have a streamlined option such as the minimum penalty option described above.

***QUESTIONS FOR OPTION IX*:**

1. Do you think this option would better protect against identity theft. Why or why not?
2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?
3. Should there be exemptions? If yes, what kind?
4. Under this option, who should ultimately be responsible for losses incurred from identity theft?
5. Are there disadvantages for consumers or industry? Please describe.

Option X – Inform victims of their rights

Organizations must make information about victim's rights readily available. Repairing the effects of identity theft is a costly and time-consuming process. Victims need information in plain language that tells them how to settle fraudulent debts and correct their financial and credit records.

This option would require organizations to make such information readily available to identity theft victims. Institutions should also identify any oversight or centralized reporting bodies (e.g., PhoneBusters) that can help the victim recover from the fraud.

In addition, consumers should be able to exercise their rights through the same channels they use to obtain services – over the phone, on the Internet, in writing or in person.

Under FACTA, credit bureaus are required to provide victims with a summary of their rights. In particular, victims must be told they can get copies of their credit reports and credit scores, and dispute the information contained in the reports. Under Californian law, the summary of rights must also include a toll-free telephone number the victim can use to contact the credit bureau. Summaries in Texas add information about how to place or remove a fraud alert or a freeze on the credit report.

Under PIPEDA and provincial privacy laws, organizations are required to make readily available to individuals information about their policies and practices relating to the management of personal information. These laws could be amended to make it clear that financial institutions and credit bureaus are obligated to provide this information to consumers. Changes may also be required to provincial/territorial consumer protection and consumer reporting laws, federal laws dealing with banks and provincial/territorial laws dealing with credit unions.

QUESTIONS FOR OPTION X:

1. Do you think this option would better protect against identity theft. Why or why not?
2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?
3. Should there be exemptions? If yes, what kind?
4. Should there be a penalty associated with this provision?
5. Under this option, who should ultimately be responsible for losses incurred from identity theft?
6. Are there disadvantages for consumers or industry? Please describe.
7. Should organizations be required to have a toll-free number for this purpose?
8. What type of information would be required to provide, e.g. dispute resolution process, how to prevent further ID theft (alerts, freezes, blocking of information), identity theft statement, contact names and numbers, etc?
9. Should a separate centralized agency be set up for this purpose? Should such an agency also help facilitate requests for fraud alerts following security breaches, freezes on credit reports and the blocking of negative information in a streamlined manner?

Conclusion

Identity theft is a growing problem in Canada. Identity thieves have quickly adapted to new technologies and the nation's laws have been slow to keep up. The options discussed above seek to strengthen existing laws by making it harder for identity thieves to misappropriate personal information and by making it easier for victims to detect and recover from fraud.

Some of the proposals in this paper would require appropriate resources for enforcement, such as the truncated payment card numbers, prohibition on the use of SINs and the requirement to remove bad credit information incurred by an identity thief. Other proposals, such as the duty to notify people affected by a security breach, the placement of fraud alerts, and the requirement to verify those accessing credit reports or seeking credit would simply set a standard that organizations would adhere to so they would not be liable for damages down the road.

Coordinated action between all concerned – consumers, businesses, financial institutions, credit bureaus and governments – will ensure that, together, we can address this costly problem.

We look forward to receiving your comments on any or all of the issues raised in this paper. If you have any questions, please contact info@cmcweb.ca with the subject line "Question – ID Theft".

---

[1] A credit bureau, or credit-reporting agency, collects and sells information about an individual's creditworthiness. Prospective creditors purchase a credit report to ascertain the level of risk associated with an individual prior to lending credit.

[2] Ipsos Reid, (February 28, 2003), *Concern about Identity Theft Growing in Canada.*

[3] Philippa Lawson and John Lawford, *Identity Theft: The Need for Better Consumer Protection*, (October, 2003), Public Interest Advocacy Centre. The paper cites various sources including: California Public Interest Research Group (CALPIRG), Nowhere to Turn: Victims Speak Out on Identity Theft, May 1, 2000 (http://www.calpirg.org/consumer/privacy/idtheft2000.pdf), and the Federal Trade Commission – Identity Theft Survey Report, September 2003, http://www.ftc.gov/os/2003/09/synovate report.pdf (Synovate Report).

[4] *R. v. Stewart* (1988), 63 C.R. (3d) 305, 41 C.C.C. (3d) 481 (S.C.C.).

[5] *Supra*, note 3. The total number here is greater than 100 percent because individuals reported being victimized in more than one way. In other words, some identity thieve used the same individual's personal information to open up a credit card and take out a loan, etc.

[6] Bi-National Working Group on Cross-Border Mass-Marketing Fraud, (May, 2003), *Report to the Attorney General of the United States and the Solicitor General of Canada*, <http://www.psepc-sppcc.gc.ca/publications/policing/Mass_Marketing_Fraud_e.asp>.

[7] The Canadian survey was conducted by Environics and the American survey was conducted by the Federal Trade Commission.

[8] See Canadian Bankers Association, (http://www.cba.ca/en/content/reports/English%20pamphlet.pdf).

[9] Collins, J.M. and Hoffman, S.K. (2004) Identity Theft: Predator Profiles, Submitted to Security Journal. Manuscript available from JudithCollins - judithc@msu.edu.

[10] "Vulnerability of computer info revealed," Daily Herald (Moose Jaw), February 5, 2003, p. 4.

[11] Mark Hume, *Globe and Mail*, March 16, 2004.

[12] Matt Hines, Cnet news.com, February 18, 2005

[13] Jeff Sovern, "Stopping Identity Theft," *Journal of Consumer Affairs*, vol. 38, no. 2, Winter 2004, p. 237.

[14] Canadian Bankers Association, http://www.cba.ca/en/content/stats/050210-Credit%20cards-EN.pdf.

[15] Jeff Sovern, *supra*, note 13, p. 238.

[16] There are no Canadian statistics measuring the time spent. In the American context, Synovate (in *Federal Trade Commission – Identity Theft Survey Report* [September 2003]) reports that victims spend 30-60 hours repairing the damage from identity theft, and US-based Privacy Rights Clearinghouse puts the figure at 175 hours (Beth Givens, *Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions*, (July 12, 2000), Written Testimony for U.S. Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information).

[17] Lawson & Lawford, *supra*, note 3.

[18] In the United States, some identity theft victims have been arrested for crimes committed by someone who used their personal information.

[19] In other words, these organizations must make sure someone is who they say they are before they do business with them electronically.

[20] See also the *Canadian Code of Practice for Consumer Protection in Electronic Commerce* which was developed by the federal government based on the *Principles for Electronic Authentication*. The *Code* can be found at www.cmcweb.ca/ecommerce

[21] Given American constitutional law, some provisions of FACTA have pre-empted state laws

dealing with similar subject matter.

[22] Industry Canada, *Principles for Electronic Authentication – A Canadian Framework*, (May 10, 2004), <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00240e.html>.

[23] Mastercard reports that 35 percent of its losses due to Canadian credit card fraud are caused by identity theft, compared to only 7 percent worldwide. Some analysts argue that the difference reflects the fact that social insurance numbers are used pervasively for commercial identification in Canada. In Europe, national identity cards are generally only used for in-person identification and as such do not assist

[24] 2002 Report of the Auditor General of Canada: Human Resource Development Canada – the integrity of the Social Insurance Number.