



BILL C-27 [An Act to
amend the Criminal Code
(identity theft and related
misconduct)]

CBA Submission to the House of
Commons Standing Committee on
Justice and Human Rights

April 7, 2008



CANADIAN BANKERS ASSOCIATION

Introduction

The Canadian Bankers Association (CBA), on behalf of our 54 member banks, welcomes the decision by the government to address the problem of identity theft, and the criminal activities associated with it, through amendments to the *Criminal Code*. This is an issue on which the CBA has long advocated for the need to protect Canadians and we appreciate the opportunity to provide our comments to the House of Commons Standing Committee on Justice and Human Rights during its consideration of Bill C-27, *An Act to amend the Criminal Code (identity theft and related misconduct)*.

We are pleased to express our strong support for Bill C-27 and hope that it will be enacted as soon as possible. We commend the government for tabling a Bill that will make the amendments to the *Criminal Code* that are needed to combat identity theft and, in particular, will create a new offence for identity theft and deal with such related misconduct as the unlawful possession and trafficking in “identity information”. At the same time, we are suggesting some specific technical amendments that we believe will clarify the Bill and further improve its effectiveness.

General Comments

As businesses that handle personal information and the financial accounts of millions of Canadian consumers, the banks take their role in the fight against identity theft extremely seriously. The banking industry in Canada, for example, spends in excess of \$100 million annually to prevent, detect and deter fraud and other crimes against banks, including criminal activity resulting from identity theft, in addition to reimbursing bank customers who are proven victims of many financial frauds.

For many years, the banking industry has actively supported the efforts of government and law enforcement agencies to reduce the incidence of identity theft. Although the criminal activity resulting from having an individual’s identity misappropriated and used without consent is not new, identity theft has recently emerged as a particularly serious problem for individuals, who are its main target, as well as for businesses, government and law enforcement agencies. Identity theft is a criminal activity that leads to widespread harm, ranging from emotional trauma and grief to extensive financial loss for individuals and businesses. Indeed, according to the Canadian Council of Better Business Bureaus, identity theft costs the Canadian economy approximately \$2.5 billion per year. There are a number of reasons why identity theft has grown in recent years.

First, rapid technological advances in computers and reproduction technology, means that it is now a relatively simple matter to steal identities and produce counterfeit identification documents of high quality. For this reason we have advocated for several years that the identity theft problem must be addressed by going to its source; the acquisition and misuse of identification documents themselves. In Canada, however, the courts have held (most notably, the Supreme Court of Canada in *R. v. Stewart*) that the required elements for theft or fraud are not satisfied if only the confidentiality of personal information is violated.

Second, a key reason why identity theft has increased so much over the last few years is the limited scope and effectiveness of the current laws. While there are some existing offences under the *Criminal Code* and the *National Defence Act* that provide some help in addressing aspects of identity theft (or more accurately, “identify fraud” which arises from identity theft), there is currently no comprehensive set of legislative provisions that provide adequate tools to address the specific problem of “identity deception” (and related offences) which lay at the heart of identity theft.

Indeed, the approach to dealing with identity theft in Canada has been on a piecemeal basis and certainly, for the most part, has predated the 21st century technologies which are now available to criminals. For example, Section 371 of the *Criminal Code* states that individuals are guilty of an indictable offence if they fraudulently send “a telegram, cablegram or radio message” with the intent to defraud, but it does not refer to email. Yet, Western Union sent its last telegram in Canada in 2006. While Western Union has long since adopted new technologies and abandoned its telegram and commercial messaging services, the *Criminal Code* has not kept pace. In comparison, in the United States, there are now specific laws at both the state and federal levels aimed directly at this form of criminal activity.

Even where the Crown tries to use existing *Criminal Code* provisions against “identity theft” activities, it invariably means that an attempt is being made to force the proverbial “square peg into a round hole”. In particular, we note that none of the existing statutory provisions effectively deals with the following actions:

- the possession by one person of an identification document of another individual;
- the possession of personal information of another person; or
- the manufacturing or possession of “novelty” identification.

To address identity theft effectively, Canada needs a strategic and comprehensive approach to the problem, with co-operation from law enforcement agencies, government, financial institutions, other business, and the general public. Key to such an approach are legislature changes that will provide stakeholders with the tools they need to do the job of reducing identity theft.

We endorse the approach proposed in the Bill that the scope of the new measures be directed to those offences in which identifying information is intended to be used by a person to pretend to be or to pretend to have certain attributes of the person that the information actually identifies.

In our view, Bill C-27 satisfies the need for new legislative measures to address these gaps in the current laws and, therefore, we strongly endorse both the Bill and its speedy passage.

Specific Comments

As we stress above, the banking industry in Canada supports Bill C-27 and encourage Parliamentarians to expedite its enactment. We do believe, however, that some provisions in the Bill could be amended to improve its clarity and effectiveness. The details of our proposed changes, which are mainly technical in nature, are provided below.

Definition of “Credit Cards” and Proposed Offences

Section 4 amending s.342 (3) and Section 5 amending s.342.01

Issue

Bill C-27 proposes several new measures be added to the *Criminal Code* to deal with such issues as “unauthorized use of credit card data”.

It is the banking industry’s view that the wording of these proposed amendments is too restrictive and, therefore, will not capture all of the present or future payment methods that may be threatened by criminal activity. We believe that it is important to ensure that Bill C-27 has the flexibility to address the types of criminal activity that will emerge as payment methods evolve. The evolution of the financial services industry, as shaped by new technology, will lead to a corresponding evolution of financial criminal activity.

Criminal activity using counterfeit credit or debit cards, or losses due to lost or stolen credit cards, are only some of the frauds resulting from identity theft. Indeed, the skimming of debit cards and capture of “personal identification numbers” (PIN), which results in the creation and use of fraudulent debit cards, causes greater loss and reputational risk for Canadian financial institutions than credit card counterfeiting. Further, the technology is changing; with new credit and debit cards, payment is activated by embedded microchip, and credit card payments are done by the entry of a personal identification number, rather than a signature. While this represents a significant increase in security for consumers, it is to be expected that criminal elements are turning their efforts to trying to determine how to steal identities and commit fraud in this new environment. In addition to card fraud, it is expected that the criminal element will also increase its efforts to initiate other types of fraud, including mortgage and land title fraud.

Accordingly, we believe that the identity theft legislation should not be limited to combating the methods currently used today to steal the identity of an individual, and which results in such crimes as credit card fraud, but should also address all relevant types of identity theft and provide the flexibility to capture future methods.

Section 321 of the *Criminal Code* provides a definition of “credit card” that reads as follows:

“credit card” means any card, plate, coupon book or other device issued or otherwise distributed for the purpose of being used

- (a) on presentation to obtain, on credit, money, goods, services or any other thing of value, or
- (b) in an automated teller machine, a remote service unit or a similar automated banking device to obtain any of the services offered through the machine, unit or device;

This *Criminal Code* definition of “credit card” is obviously much wider than the traditional definition of the term. Nevertheless, we believe that while the broad definition of “credit card” in the *Criminal Code* covers traditional credit and debit cards, it may be insufficient to capture all possible payment methods, such as contact-less payments over the telephone, or bank or payment accounts accessed via the internet using personal computers or other devices, that will become the target of criminal groups.

Recommendation:

We recommend that the term “credit card”, as defined in section 321 of the *Criminal Code*, be replaced by the term “payment method”, which would be defined as follows:

“payment method” means any card, plate, coupon book or other device, issued, activated or otherwise distributed for the purpose of being used

(a) on presentation to

- i. obtain, on credit, money, goods, services or any other thing of value,
- ii. obtain, on payment, goods, services or any other thing of value, or
- iii. transfer funds to a third party, or

(b) in an automated teller machine, a remote service unit or a similar automated banking device to obtain any of the services offered through the machine, unit or device.

Corresponding changes would be made to sections 4 and 5 of the Bill to replace “credit card” with “payment method” in sections 342 (3) and 342.01.

Restitution

Section 11 amending s.738 (1) (d)

Issue

We are pleased to see that section 11 of the Bill amends subsection 738 (1) of the *Criminal Code* to allow for restitution to be ordered by a court and believe it is a necessary addition to the legislation. We feel, however, that it needs to be made clear in the provision that innocent parties, such as banks and retailers, if caught in an identity theft scheme, cannot be subject to a restitution order. This clarification is especially important in view of the concerns we discuss more fully below about the lack of a definition of recklessness in the Bill. Essentially, since recklessness is undefined, there may be a risk when identity theft occurs that innocent parties (such as financial institutions) may be pursued for restitution by those who claim that any theft of personal information is evidence of an undefined “recklessness” on the part of the institution, even where that institution has taken proper and appropriate steps to protect the personal information it holds.

In addition, while an individual who is the victim of identity theft faces obvious costs that deserve restitution, financial institutions and other businesses may lose money from a fraud caused by identity theft, incur costs from the investigation and detection of the fraud, as well as expenses from notifying and dealing with customers who are victims of identity theft.

Recommendations:

A restitution order against an offender that will be available under the proposed subsections 738 (1) (d) of the *Criminal Code*, for identity theft and identity fraud offences under s.402.2 and s.403, should specifically allow orders for restitution to be granted to corporations and organizations.

Suggested amendment to the proposed s.738 (1) (d) is set out below.

Subsection 738(1) of the Act is amended by striking out the word “and” at the end of paragraph (b), by adding the word “and” at the end of paragraph (c) and by adding the following after paragraph (c):

(d) in the case of an offence under section 402.2 or 403, by paying to

i. any person who, as a result of the offence, incurs expenses to re-establish their identity, including expenses to replace their identity documents and to correct their credit history and credit rating, or

ii. any organization which, as a result of the offence, incurs expenses in investigating and notifying persons about unauthorized use of their identity information, an amount not exceeding the amount of those expenses, to the extent that they are reasonable, if the amount is readily ascertainable.

In addition, it is unclear whether the list of expenses set out in section 11 is an exhaustive one.

Soliciting personal information for the purpose of committing identity fraud

The Bill does not appear to address the act of soliciting personal information for the purposes of committing identity fraud, for example, when individuals are approached by fraudsters asking them to obtain personal information and offering money for its sale. There appears to be no means to address this type of activity currently under the *Criminal Code*, or through any of the provisions proposed by Bill C-27, though it may be a problem that the government intends to address through a separate bill.

Commission of an Offence Due to “Recklessness”

Issue

Section 10 of the Bill adds new provisions to the *Criminal Code*, including proposed subsection 402.2(2) which reads as follows:

“**Everyone** commits an offence who transmits, makes available, or distributes, sells, or offers for sale another person’s identity information, or has it in their possession for any of these purposes, knowing or believing or being **reckless** as to whether the information will be used to commit an indictable offence” (emphasis added)

Section 2 of the *Criminal Code* defines “everyone” to include an “organization” and defines “organization” as including both a corporation and company.

The terms “reckless” or “recklessness” are used elsewhere in the *Criminal Code* with respect to other offences, but usually the concept that “reckless” behaviour may result in a criminal offence is restricted to very select situations which involve individual thought or action [e.g. see sections 433 (arson) and 233 (murder)], as opposed to the “mind” of an organization. There is no definition of “reckless” in the *Criminal Code* so the standard that will be applied to the “reckless” offences created by Bill C-27 is unclear and, given the wording of proposed subsection 402.2(2), raises issues for our member banks.

Most judicial interpretations of the concepts of “reckless” or “recklessness” have been applied to the actions of individuals. It is unclear whether these previous judicial definitions of “reckless” will be applied, or are even appropriate, to a charge under proposed subsection 402.2(2), since the fact situations in which recklessness may lead to committing a current *Criminal Code* offence; are very different from those contemplated by Bill C-27.

Arguably, most organizations in Canada are involved in transmitting, making available, or distributing some forms of identity information. When interpreting proposed subsection 402.2(2), the courts may decide that where a company does not use a specific data security software for securing customer personal data, it is “being reckless”. As a result, a bank (or other businesses) that has used what it feels is an appropriate and proven security system may be subject to a charge of “recklessness” if a third party makes a case that a different data security software system should have been used.

Finally, it is unclear what measures a retailer or a credit reporting agency will need to take to verify the identity of a person to ensure that they have not been “reckless”. For example, if an individual called a retailer and provided a valid SIN and name but a false address in an attempt to obtain a store credit card, and that information was then sent to a credit reporting agency, would the proposed legislation hold either the retailer or the credit reporting agency liable for acting “recklessly” if the credit card was issued?

Recommendations:

The concept of being “reckless” should not be used as a measure for the commission of a criminal offence by an organization. We recommend:

- Remove the concept of reckless behaviour as one of the measures of the commission of an offence under s.402.2 (2) or, in the alternative, restrict it to the actions of individuals.

- If the concept of recklessness is to be included as a measure of the offence under section 402.2(2), the standard needs to be defined so organizations understand what precautions need to be taken to ensure that they meet the required standard.

Conclusion

Though we have raised some technical matters in this submission, we again wish to stress our strong support for Bill C-27. Enactment of this Bill will be very beneficial for consumers and business, and will greatly improve the tools available to law enforcement to combat identity theft.