Legislative Summary **LS-637E**

BILL S-4: AN ACT TO AMEND THE CRIMINAL CODE (IDENTITY THEFT AND RELATED MISCONDUCT)

Nancy Holmes
Dominique Valiquet
Legal and Legislative Affairs Division

14 April 2009
Revised 5 June 2009

Library of Parliament
Bibliothèque du Parlement

Parliamentary Information and Research Service

LEGISLATIVE HISTORY OF BILL S-4

HOUSE OF COMMONS		SENATE	
Bill Stage	**Date**	**Bill Stage**	**Date**
First Reading:	15 June 2009	First Reading:	31 March 2009
Second Reading:	17 June 2009	Second Reading:	5 May 2009
Committee Report:	8 October 2009	Committee Report:	9 June 2009
Report Stage:	20 October 2009	Report Stage:	9 June 2009
Third Reading:	20 October 2009	Third Reading:	11 June 2009

Royal Assent: October 22, 2009

Statutes of Canada 2009, c. 28

N.B. Any substantive changes in this Legislative Summary that have been made since the preceding issue are indicated in **bold print.**

CE DOCUMENT EST AUSSI PUBLIÉ EN FRANÇAIS

CONTENTS

CANADA

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

BILL S-4: AN ACT TO AMEND THE CRIMINAL CODE (IDENTITY THEFT AND RELATED MISCONDUCT)*

INTRODUCTION

Bill S-4, An Act to amend the Criminal Code (identity theft and related misconduct) was introduced in the Senate on 31 March 2009. The bill will create several new *Criminal Code* offences specifically targeting those aspects of identity theft that are not already covered by existing provisions. Essentially, Bill S-4 will focus on the preparatory stages of identity theft by making it an offence to obtain, possess, transfer or sell the identity documents of another person. The bill contains essentially the same provisions as former Bill C-27,(1) with the addition of new offences that can lead to electronic surveillance.

On 4 June 2009, the Standing Senate Committee on Legal and Constitutional Affairs made four fundamental changes to Bill S-4:

- **In clause 1, which deals with the offence of possession of and illegal trafficking in official documents:**
  - **a death certificate and an employee identity card were added to the definition of "identity document"; and**
  - **the definition of "identity document" was broadened to include any other document similar to those expressly named.**
- **In clause 4, which deals with the offence of fraudulently possessing or using credit card data or trafficking in such data, the term "personal identification number" was replaced by "personal authentication information," in order to include all future identification technology.**
- **In new clause 12, a parliamentary review of the provisions of the bill was stipulated, to take place within five years of the bill's receiving Royal Assent.**

---

* Notice: For clarity of exposition, the legislative proposals set out in the bill described in this Legislative Summary are stated as if they had already been adopted or were in force. It is important to note, however, that bills may be amended during their consideration by the House of Commons and Senate, and have no force or effect unless and until they are passed by both houses of Parliament, receive Royal Assent, and come into force.

(1) Bill C-27, An Act to amend the Criminal Code (identity theft and related misconduct), was introduced in the House of Commons on 21 November 2007, during the 2nd Session of the 39th Parliament. It reached the House of Commons Standing Committee on Justice and Human Rights study stage on 1 April 2008, and died on the *Order Paper* when Parliament was dissolved on 7 September 2008.

BACKGROUND

Identity theft has been called the crime of the 21st century. With the proliferation of personal and financial information as a result of such electronic media as the Internet and associated technology, new life has been given to an old crime. Not so long ago, assuming and using another person's identity was a relatively small-scale operation that required time and effort to execute (e.g., stealing a purse, breaking into a house, overhearing a private conversation). Today, however, perpetrators of identity theft can operate at a distance from their victims, access databases containing large amounts of personal information and transmit stolen data quickly and easily around the world.

The nature and scope of identity theft have made it not only difficult to define the term, but also to measure the extent of the problem. With respect to a definition of "identity theft," some commentators refer to identity fraud in relation to the fraudulent use of personal information, and identity theft as pertaining to the unauthorized collection of the information. This is the approach taken in Bill C-27. Others, however, apply the term identity theft broadly to encompass the preparatory stage of acquiring, collecting and transferring personal information, as well as the actual use of the information to attempt to commit, or to actually commit, a criminal offence.

Identity theft techniques can range from relatively unsophisticated methods, such as dumpster diving, mail theft and pretexting (posing as someone who's authorized to obtain information in order to get it), to more elaborate activities, such as skimming,[(2)] phishing,[(3)] pharming,[(4)] vishing[(5)] and hacking into large databases. Given the evolving nature of technology, identity thieves are constantly developing new techniques to obtain personal information. There are even online operators and underground networks that specialize in the sale of stolen personal information. Thus, identity theft can range from the stealing of credit card information to the wholesale misappropriation of an identity.

---

(2) Skimming involves stealing personal information from the magnetic strip on debit and credit cards through the use of small electronic devices called skimmers or wedges. The device copies the information stored on the card's magnetic strip to be used in the creation of additional cards often for fraudulent purposes.

(3) Phishing is a technique that uses emails from what appear to be trustworthy organizations (i.e., banks) to lure people into providing account and other personal information.

(4) Pharming is a variation on phishing in that a counterfeit website is used to entice someone to give up his or her personal information. It involves creating a false website using the correct address of the valid website and then luring individuals to provide personal information at the fake website.

(5) Vishing is similar to phishing except it uses the phone to get individuals to call what they mistakenly believe is a bank or credit card company.

Once obtained, personal information can be used to open bank accounts, obtain loans or credit cards, gain employment or transfer land title in the victim's name. Stolen or reproduced personal documents can also be used to obtain government benefits or government-issued documentation. There also appears to be a growing trend of using identity theft to facilitate organized crime and terrorism activities (e.g., to mislead or avoid detection by law enforcement officials).

Victims of identity theft may suffer significant financial loss as well as damaged reputation or credit ratings. There may also be losses suffered in terms of the time, expense and emotional stress associated with restoring reputations and recovering financial and other losses incurred. Governments and businesses may also suffer financial loss and damaged reputations, and to the extent that identity theft is used to support terrorist activities, there may be national security implications.

Given that it can take months or even years for identity theft to be detected, coupled with the fact that most cases go unreported, statistics in this area are fairly unreliable. PhoneBusters, a national anti-fraud call centre jointly operated by the Ontario Provincial Police, the Royal Canadian Mounted Police and the Competition Bureau Canada, is the principal source of data on identity theft in this country; however, its statistics are complaints-based and as such may represent only part of the problem. According to PhoneBusters, for the calendar year ending December 2008, a total of more than $9 million in losses was reported on the basis of over 11,000 complaints.(6) The Canadian Council of Better Business Bureaus points out that identity theft is the fastest growing type of fraud in North America, with the cost to consumers, banks, credit card firms, stores and other businesses estimated to be in the billions of dollars each year.(7) Of note is the fact that this is double the amount of money lost but half the number of victims from the year before, which might indicate that identity theft is becoming more profitable and that there are increasingly more ways to make money from the actual fraud related to it. The Canadian Council of Better Business Bureaus has estimated that identity theft may cost Canadian consumers, banks and credit card companies, stores and other businesses more than $2 billion annually.

---

(6) See PhoneBusters, "Statistics on Phone Fraud: Identity Theft Complaints," http://www.phonebusters.com/english/statistics_E06.html.

(7) Better Business Bureaus, "BBB and Iron Mountain join forces to fight identity theft," News release, Toronto, March 2009, http://www.bbb.org/canada/article/9314.

Calls for amendments to the *Criminal Code* to deal with the problem of identity theft have recently come from parliamentary committees as well as from individual Members of Parliament. For example, in its fifteenth report, presented during the 1st Session of the 39th Parliament, the Standing Committee on Finance recommended that the Minister of Justice take action to include the offence commonly known as "identity theft" in the *Criminal Code*.

Currently, the *Criminal Code* does not contain a specific identity theft offence. With the exception of some new offences dealing with computers (s. 342.1) and credit/debit cards (s. 342), most of the Code offences relating to property predate both the computer and the Internet. In 2004, the Department of Justice issued a consultation document to solicit views on legislative options to address gaps in the Code in relation to identity theft.(8) The paper noted that while the Code covers most fraudulent *uses* of personal information by identity thieves, it does not address the unauthorized *collection, possession and trafficking* of personal information (except for credit card data and computer passwords) for the purposes of future criminal activity.

The reason for this gap in the Code stems in large part from the fact that property offences (e.g., theft) relate to a tangible thing that the owner is deprived of. It is therefore difficult for non-physical or virtual information to be characterized as property unless it has a commercial value in and of itself, such as a trade secret. Moreover, the courts have generally held that the elements of theft and fraud are not satisfied in cases where only the confidentiality of personal information is violated. This means that copying personal information, even for future criminal use, is not an offence under the Code. Finally, the Department of Justice consultation document notes that prior to the computer and Internet, a typical case of identity fraud involved one person stealing the identification and then using it for his or her gain. Today, technology has facilitated the involvement of numerous people along a continuum of criminal activity with no one player having committed all the elements of the fraud.

(8) Department of Justice Canada, Consultation Document on Identity Theft, October 2004.

DESCRIPTION AND ANALYSIS

A. General Offences

1. Illegally Possessing or Trafficking in Government Documents (Clause 1)

The bill's first clause creates a new hybrid offence[9] involving identity documents issued by a department or agency of the federal or a provincial government or by a foreign government.

Anyone who without lawful excuse, procures to be made, possesses, transfers, sells or offers for sale such an identity document that relates to another person is liable to a term of imprisonment not exceeding five years. (Clause 1 of the bill adds subsections 56.1(1) to 56.1(4) to the *Criminal Code*.)

The new subsection 56.1(3) of the Code lists the identity documents covered by the new offence. They are the following official documents:

- Social Insurance Number card
- driver's licence
- health insurance card
- birth certificate
- **death certificate**
- passport
- any document that simplifies the formalities of entry into Canada
- certificate of citizenship
- document indicating immigrant status in Canada
- certificate of Indian status
- **employee identity card bearing the employee's photograph and signature**
- any other similar document issued by **a federal or provincial government department or agency or** a foreign government.

With respect to official documents issued by the various levels of government in Canada, it would appear that this list is **not** exhaustive. Any new government identity document that might be issued in the future would **thus be covered** by the offence of possessing or trafficking in government documents provided for in the bill.

---

(9) A "hybrid" offence is one that can be prosecuted either by way of indictment or by way of summary conviction.

The new offence does not require that the prosecution prove the intent to use an identity document in a dishonest or fraudulent manner or in the perpetration of a crime (as is the case, for example, for the new offence of identity theft in clause 10).

However, the bill does provide that a person can have a lawful excuse for procuring to be made, possessing, selling or offering for sale a government identity document related to another person (clause 1 of the bill, adding new subsection 56.1(1) to the Code). For example, a person would not be found guilty of the offence if he or she had acted:

- in good faith in the ordinary course of his or her business, employment or office;
- for genealogical purposes;
- with the consent of the person to whom the identity document relates or of a person authorized to consent on behalf of the person to whom the document relates, or of the entity that issued the document; or
- for a legitimate purpose related to the administration of justice (new subsection 56.1(2) of the *Criminal Code*).

2. Forgery and Similar Offences (Clauses 8 and 9)

Clause 8 adds to the current offence of using a forged document[(10)] those of trafficking in forged documents (new section 368(1)(*c*) of the Code) and possessing a forged document with intent to use it (new section 368(1)(*d*) of the Code). All these offences are punishable by a term of imprisonment not exceeding 10 years.

Clause 9 stipulates that the offence of making, selling or possessing an instrument or device intended for the making of a forged document[(11)] includes the repair, purchase, exporting our importing of such an instrument or device (new section 368.1 of the Code). This offence is punishable by a term of imprisonment not exceeding 14 years.

a. Exceptions (Clauses 7 and 9)

Clauses 7 and 9 provide for exceptions for undercover work carried out by law enforcement agencies.

(10) S. 368(1)(*a*) and (*b*) of the Code.

(11) S. 369(*b*) of the Code.

Clause 7 protects from prosecution for making a forged document[12] people who do so at the request of a police force, the Canadian Forces or a department or agency of the federal or a provincial government (new subsection 366(5) of the Code).

Clause 9 allows public officers to create and use covert identities in the legitimate performance of their duties or employment. They could thus not be found guilty of making a forged document,[13] using a forged document,[14] trafficking in forged documents,[15] or possessing a forged document with the intention of using it,[16] or of an offence relating to instruments intended for the making of a forged document[17] (new section 368.2 of the Code).

3. Identity Theft (Clause 10)

Clause 10 adds a new section to the *Criminal Code* under the heading "Identity Theft and Identity Fraud." Under its provisions, identity theft refers to the preliminary steps (e.g., the collection and possession of another person's identity information) and identity fraud constitutes the subsequent deceptive use of such information in connection with crimes like personation, fraud or abuse of credit card data.[18]

Clause 10 thus creates a hybrid offence targeting the obtaining or possession of identity information: identity theft (new subsection 402.2(1) of the Code). The new offence is punishable by a term of imprisonment not exceeding five years (new section 402.2(5) of the Code).

a. Identity Information

For someone to be found guilty of identity theft, the prosecution would first have to prove that the person had knowingly obtained or possessed another person's "identity information."

---

(12) S. 366 of the Code.

(13) Ibid.

(14) S. 368(1)(*a*) and (*b*) of the Code.

(15) New s. 368(1)(*c*) of the Code.

(16) New s. 368(1)(*d*) of the Code.

(17) New s. 368.1 of the Code.

(18) See Department of Justice, "Identity Theft: Distinction between Identity Theft and Identity Fraud," Backgrounder, http://www.justice.gc.ca/eng/news-nouv/nr-cp/2007/doc_32179.html

The bill defines identity information as “any information – including biological or physiological information – of a type that is commonly used, alone or in combination with other information, to identify or purport to identify an individual” (clause 10).

This definition differs from the definition of “personal information” in the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[19] The PIPEDA definition states that “personal information” means “information about an identifiable individual.” This definition may thus include information that does not permit identification of an individual, but rather information about an identifiable individual (for instance, his or her shopping preferences).[20] The definition of “identity information” in the bill is more restrictive, because such information must “identify or purport to identify” an individual.

Moreover, under the definition in the bill, information that on its own might not identify an individual (for example, an address) can be considered “identity information” if it could be combined with other information (for example, a birth date) for the purposes of identification.

The new section 402.1 of the Code gives examples of identity information:

- name
- address
- date of birth
- written, electronic or digital signature
- Social Insurance Number, health insurance or driver’s licence number
- credit or debit card number
- number of an account at a financial institution
- passport number
- user code
- password
- fingerprint or voice print
- retina or iris image
- DNA profile

---

(19) Under the PIPEDA, “personal information” means “information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization” (S.C. 2000, c. 5, s. 2(1)).

(20) See House of Commons Standing Committee on Justice and Human Rights, *Evidence*, 1st Session, 39th Parliament, 22 February 2007, 0910 (William Bartlett [Senior Counsel, Criminal Law Policy Section, Justice Canada]).

Some information, such as a Social Insurance Number, fingerprint or DNA profile, is unique, in that it is sufficient in itself to identify an individual.

b. Indictable Offences Including Fraud, Deceit or Falsehood

Second, to obtain a conviction for identity theft the prosecution would also have to prove that the accused had obtained or possessed another person's identity information *in circumstances giving rise to a reasonable inference that the information was intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence*. Under the new subsection 402.2(3) of the Code, this would include the following indictable offences:

- forgery of a passport or uttering a forged passport
- fraudulent use of a certificate of citizenship
- personating a peace officer
- perjury
- theft, forgery, etc., of a credit card
- false pretence or false statement
- forgery
- uttering, trafficking in or possession with intent of forged documents
- fraud
- identity fraud.

4. Trafficking in Identity Information (Clause 10)

Clause 10 creates another hybrid offence, trafficking in identity information (new subsection 402.2(2) of the Code). It involves the transmission, making available, distribution, selling or offering for sale, or possession of another person's identity information. The definition of "identity information" provided in the new section 402.1 of the Code applies to this new offence as well.

To obtain a conviction for trafficking in identity information, the prosecution would have to prove that the accused had trafficked in another person's identity information knowing that, or being reckless as to whether the information would be used to commit an indictable offence that included fraud, deceit or falsehood as an element of the offence. The examples of indictable offences set out in the new subsection 402.2(3) of the Code apply to trafficking in identity information as well.

This new offence, like identity theft, is punishable by a term of imprisonment not exceeding five years (new subsection 402.2(5) of the Code).

5. Identity Fraud (Clause 10)

The bill replaces the current offence of "personation with intent"[21] (i.e., pretending to be another person to gain an advantage for oneself or cause a disadvantage to someone else) with "identity fraud" (clause 10 of the bill amending section 403 of the Code).

Clause 10 also adds to the existing offence the fact of pretending to be another person to avoid arrest or prosecution or to obstruct the course of justice (new section 403(1)(*d*) of the Code).

Clause 10 further specifies that the expression "personating a person" includes pretending to be that person or using that person's identity information as if it pertained to the person using it (new paragraph 403(2) of the Code). The definition of "identity information" in the new section 402.1 of the Code applies to the offence of identity fraud as well.

The maximum sentence for identity fraud is the same as that currently provided for personation, 10 years in prison (new section 403(3) of the Code).

B. Specific Offences

1. Personating a Peace Officer (Clause 2)

At present, personating a peace officer is an offence punishable on summary conviction,[22] which means that the maximum sentence is a fine of not more than $5,000 or six months' imprisonment or both.[23]

Clause 3 makes it a hybrid offence and increases the maximum sentence to five years in prison (new subsection 130(2) of the Code).

(21) S. 403 of the Code.

(22) S. 130 of the Code.

(23) S. 787(1) of the Code.

2. Use and Copying of Credit Card Data (Clauses 4 and 5)

Section 342(3) of the Code currently governs the offence of fraudulently possessing, using or trafficking[24] in credit card data. Clause 4 stipulates that such data include **"personal authentication information" in order to take into account any future identification technology. This term includes "a personal identification number or any other password or information that a credit card holder creates or adopts to be used to authenticate his or her identity in relation to the credit card."** The definition of a credit card already includes debit cards.[25]

Section 342.01(1) of the Code currently provides for the offence of making, selling, exporting, importing or possessing an instrument for falsifying or forging *credit cards*. Clause 5 adds a similar offence for instruments used to copy credit card *data* (new section 342.01(1) of the Code).

The maximum sentence for all these offences is a term of 10 years' imprisonment.

3. Mail-related Offences (Clause 6)

The postal system is a gold mine of personal information. Through it pass bank and credit card statements, a wide variety of government documents, and pre-approved credit applications. The theft of mail is thus becoming a favourite activity for those who want to obtain identity information illegally.

At the present time, section 356(1)(*a*)(i) of the Code deals with the theft of any thing sent by post, after it is deposited at a post office and before it is delivered. Under clause 6(1), a person will also be committing a theft of mail if he or she steals a thing *after it has been delivered* but before it is in the possession of the addressee (new section 356(1)(*a*)(i) of the Code).

In addition to stealing mail, some criminals will illegally divert another person's mail. They do this by submitting a forged change of address notice to a body that has sent out a statement (for example a bank or credit company) or by using Canada Post's general change of address (forwarding) service. In addition to obtaining a host of personal data, such criminals can

(24) Under s. 342(4) of the Code, to "'traffic' means … to sell, export from or import into Canada, distribute or deal with in any other way."

(25) S. 321 of the Code.

also gain time for pursuing fraudulent activities without the victims' knowledge. Clause 6(1) tackles this problem by creating the offence of fraudulently redirecting mail (new section 356(1)(*c*) of the Code).

This provision also creates the offence of making, possessing or using a copy of a Canada Post mailbox or other key with intent to commit a mail-related offence (new paragraph 356(1)(*a.1*) of the Code). The Code already covers the theft of such a key.[26]

The mail theft offences in the Code are treated as indictable offences. Clause 6(2) makes mail-related offences hybrid offences. The maximum sentence remains 10 years' imprisonment.

C. Interception of Private Communications (Clause 3)

Legal authorization to proceed with the electronic interception of private communications can be obtained only for the offences listed in section 183 of the *Criminal Code*. Clause 3 of Bill S-4 adds to this section new offences created by the bill, such as identity theft and trafficking in identity information. This means that law enforcement agencies will be able to use electronic surveillance in investigations of these new offences.

D. Restitution Order (Clause 11)

When an offender has been found guilty of identity theft, trafficking in identity information, or identity fraud, the court can order that he or she compensate the victim. The offender must reimburse the victim for reasonable expenses incurred to re-establish his or her identity, including expenses to replace identity documents and to correct credit history and rating. This is a discretionary order that can be added to any sentence.

E. Parliamentary Review (Clause 12)

Within five years of the legislation receiving Royal Assent, a comprehensive review of its provisions and operation must be undertaken by a parliamentary committee.

(26) S. 356(1)(*a*)(iii).

COMMENTARY

Generally speaking, police associations, business organizations, credit reporting agencies and privacy advocates were pleased with the introduction of Bill C-27, the predecessor to Bill S-4, as an enforcement measure that sought to detect, prosecute and convict identity theft offences. Indeed, the Canadian Association of Chiefs of Police and the Canadian Bankers Association had for some time been calling for amendments to the *Criminal Code* to deal specifically with the crime of identity theft.

However, privacy advocates and consumer groups were quick to note that the bill was but one piece of a larger identity theft toolkit. They maintained that there was still the need for a comprehensive framework involving law enforcement agencies, consumer organizations, businesses and financial institutions that would address the broader issues associated with identity theft (e.g., strengthening and enforcing data protection laws, consumer protection and victim redress and public education). The case for this broader framework was made by witnesses before the House of Commons Standing Committee on Access to Information, Privacy and Ethics in the spring of 2006. The Committee held several preliminary hearings on the issue of identity theft prior to the prorogation of Parliament on 14 September 2007.(27)

(27) House of Commons Standing Committee on Access to Information, Privacy and Ethics, 1st Session, 39th Parliament, http://www2.parl.gc.ca/CommitteeBusiness/CommitteeMeetings.aspx?Cmte=ETHI&Stac=2047692&Language=E&Mode=1&Parl=39&Ses=1.