Working Together to Prevent Identity Theft

Response of the Canadian Wireless Telecommunications Association

Submitted to the Consumers Measures Committee

September 30, 2005.

130 Albert St., Suite 1110, Ottawa Ontario K1P 5G4 Tel: (613) 233-4888

September 30, 2005

Susan Gardiner
Senior Policy Analyst, Consumer Policy
Consumer Measures Committee
c/o Office of Consumer Affairs
Industry Canada
235 Queen Street
Ottawa, Ontario
K1A 0H5

Dear Ms. Gardiner:

Re: Working Together to Prevent Identity Theft

Please find attached the response of the Canadian Wireless Telecommunications Association to the Consumer Measures Committee's consultation on identity theft.

Thank you for providing us the opportunity to comment. Should you require any further information please contact me at the below coordinates.

Sincerely,

SENT VIA EMAIL

Kasia Majewski
Director, Government Affairs
130 Albert St., Suite 1110,
Ottawa Ontario
K1P 5G4
Tel: (613) 233-4888 ext. 102

General Comments

The Canadian Wireless Telecommunications Association ("CWTA"), the representative of Canadian wireless communication service providers and manufacturers, would like to thank the Consumers Measures Committee ("CMC") for the opportunity to comment on the important issue of identity theft.

In the 20 years mobile telephony has existed in Canada, the industry has grown into a sector characterised by innovation in response to customer demand. Wireless carriers provide a range of voice and data telecommunications services, including: local and long-distance telephone service; multi-media messaging, e-mail, text messaging, and paging and dispatch push-to-talk services as well as data carriage, internet connectivity, and mobile video services.

The wireless industry also plays a key role in connecting Canadians. Over 20 years, it has invested $20 billion in infrastructure build making wireless coverage available to 95% of Canadians. This investment continues at about $ 1 billion per year. As a result, Canadians are increasingly choosing wireless technologies with 46 per cent of Canadians owning a cell phone today and 44% of all phone connections occurring wirelessly. In real terms, the CWTA estimates there were about 15 million wireless subscribers at the end of 2004.

Like most industries, the CWTA believes identity theft is an increasingly larger problem, that affects both consumers and businesses. To combat it, the CWTA agrees with the CMC that "identity theft," as a term requires better clarification under the law. Indeed, the fundamental approach to address this issue is to better define what constitutes "identity theft" and clearly indicating its criminality, thereby providing law enforcement the necessary tools to tackle this activity.

As distinct from fraud, identity theft involves the illegal collection of personal information with the intent of committing a crime. While the purpose of this crime is usually for financial gain, it may also include impersonation for the purpose (for example) of facilitating cross-border travel for criminal purposes, or to carry our health or social insurance fraud.

Given the importance of this identity theft as a facilitating activity to fraud, the CWTA disagrees with the CMC that: "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." In Canada, privacy legislation, which includes instructions to business on how to manage personal information in a secure manner, has done much to decrease unwitting 'leakage' of personal information given for business purposes. Likewise, technology can, and has, increased the security of data held by organisations. However, even as technology and business processes have evolved towards better protection, criminals have continued to find increasing sophisticated ways to exploit technology in order to better impersonate individuals and commit fraud. Yet, absent the necessary criminal code provisions, Canadian law enforcement lacks a key tool which would allow for the capture of identity thieves, a subsequent recovery of the profits of this crime, and, ultimately a decrease in identity theft. As such, an approach to identity theft must firstly, address the issue of the theft of personal information, the unlawful possession of personal information, multiple identity documents and/or novelty identification with the intent to defraud in Canadian law. For example, the CWTA refers the CMC to the work being undertaken by Justice Canada to provide a comprehensive legal framework for identity theft. This work, which has been championed by the Canadian Bankers Association would include:

- A clear definition of identity theft within the *Criminal Code*
- A definition of 'personal information';
- The concept of 'misappropriation';

- A criminal offense for unlawful possession of individuals' personal information;
- A criminal offense for possession of multiple pieces of identification for a number
- of individuals without lawful excuse (to preclude those manufacturing fake identification from claiming it is "novelty id")
- A criminal offence in trafficking in personal information.

As a highly customer-focused industry, the members of CWTA take the security of their customer information seriously, and have always striven to maintain the balance between the need to verify credit and identity, while complying with relevant consumer and privacy legislation, and responding to strong consumer demands for products that are easy to purchase, allow the customer to have payment and contract flexibility and, most importantly, allow the consumer to maintain their privacy – and anonymity – by collecting only the necessary amount of personal information. This is not a matter of "convenience" as is suggested by the report, but a matter of following the law.

As an example of our industry's commitment and ongoing involvement in preventing identity theft some of our member companies, namely Bell Mobility, Rogers Wireless and Telus Mobility, are partners in the Competition Bureau's Fraud Prevention Forum. They will be working with the Bureau to put programs in place for Fraud Prevention Month in March 2006 in order to raise awareness of this important issue.

The CWTA also takes issue with the CMC's accusation that the industry chooses to ignore instances of this fraud. The report makes the following statement, attributing it to Dr. Jeff Sovern: "credit card and cell phone industries are quite profitable and at least some issuers would prefer to absorb the losses they might suffer rather then forgo the income that would have been generated by those consumers." The CWTA would like to respectfully note that this statement is a misquote. In his original work, which examines the American, not the Canadian, market, Dr Sovern states his opinion, as follows:

> Credit card customers seem to be so profitable that at least some credit card issuers prefer to swallow the losses they suffer form the occasional identity thief, instead of forgoing the income that would have been generated by offended consumers (US House Committee on the Judiciary 2002)[1].

Implicating an industry of negligence should not occur on the basis of a misquote.

Cell Phone Service Choices

Customers purchasing mobile phones in Canada have the ability to sign up for one of two payment methods: 1) a post-paid service where the customer engages in a contract with the service providers, and pays on a monthly basis; in which credit worthiness must be approved, or 2) a pre-paid service where a credit check is in not undertaken.[2] Post paid credit checks are geared towards validating the credit worthiness of the individual, not towards an exhaustive validation of the individual's identity which is not tolerated by most consumers. In fact, consumers routinely balk at having to provide personal information they consider to be in excess of what is necessary for service provision. In the pre-paid context, a credit authorization would only occur if the customer purchased pre-paid minutes with their credit card. However, consumers can use a variety of means to purchase pre-paid minutes for their cellular phone.

Personal Information Practices

The Canadian wireless industry takes the privacy of its customers, and the security of their personal information, very seriously. We follow strict privacy standards and data security policies while closely monitoring and adhering to the guidelines established in this area by the Federal Privacy Commissioner and the Canadian Radio-television and Telecommunications Commission. Additionally, wireless companies have voluntarily

[1] Jeff Sovern, "Stopping Identity Theft" Journal of Consumer Affairs, vol. 38, no. 2, Winter 2004, p 237.
[2] In the pre-paid scenario, phones are purchased without a set airtime plan or contract and customers purchase minutes on an as-needed basis, in a variety of ways.

put processes in place to help their customers who have been, or believe they have been, victims of identity theft, as detailed in our response below (Option V, Question 11).

Dr. Sovern has alleged that, in the case of the US experience, firms collect too little information for fear that "if they ask consumers too many questions, they may give offence and lose business."[3] In the Canadian case, in at least five cases, consumers have gone to the Privacy Commissioner to complain that telecommunications companies require too many pieces of identification to start an account; in four of these cases, the Privacy Commissioner ruled that the consumer complaint was not well-founded.[4] In the fifth case, the Privacy Commissioner ruled that three pieces of identification was too many, and specifically required the wireless company in question require only two.[5] These rulings affect the practices of the wireless industry, which then balances the need to validate credit and identify the customer against the need to protect customer privacy, and respond to customer demands for anonymity in their transactions.

[3] Sovern, 237.
[4] Privacy Commissioner of Canada, PIPEDA Case summaries: #217, # 56, #104, #202, and #288
[5] Privacy Commissioner of Canada, Identification requirements for cell phone services PIPEDA Case Summary #288.

CWTA Responses to Specific Questions

The CWTA has limited its responses below to questions relating to the wireless telecommunications industry. Failure to respond to any specific question should not be construed as concurrence with the question, or the direction proposed by CMC.

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.

1. Do you think this option would better protect against identity theft? Why or Why not?

Truncation of credit card numbers is already standard industry practice. In addition, the industry supports truncation of debit card number on printed receipts. These measures provide added levels of security to the protection of an individuals' personal financial information. Indeed, these practices are encouraged by privacy commissioners across the country.

2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?

The CWTA believes that wireless service providers have already implemented an effective truncation process and does not believe that a new process with additional costs should be imposed on those organizations who are already meeting the privacy needs of their customers.

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.

1. Do you think this option would better protect against identity theft? Why or Why not?

Wireless carriers already take the necessary steps to ensure only authorized personnel have access to credit reports. Access to the reports is restricted depending on the function of the employee accessing the credit bureau's records. Customer service representatives (CSR) performing a credit check on a prospective customer may only receive a yes/no response to their inquiry. The CSR will not be able to view the applicant's entire credit profile. Only fraud and security personnel with a proper user ID and password may view the entire profile.

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.

8. For retailers, real estate agencies, telecomm companies, are there any industry standards in terms of when SINs are requested?

The CWTA does not offer any comments on the practices of financial institutions.
In case of standards related to the telecommunications industry's use of the social insurance number (SIN), the Privacy Commissioner has provided clear guidance to the industry on this point. In two separate decisions, the Commissioner ruled that companies cannot make provision of the SIN mandatory to provide service.[6] As such, in signing up a customer, to try to verify the identity of the individual, and to carry out a credit check, the

[6]Privacy Commissioner of Canada, #204. See also: #288.

industry provides a choice of two identification documents. A SIN is not required. If a new customer chooses to voluntarily to provide a SIN, they may do so. The CWTA would like to note that customers often do wish to use a SIN as it is a unique identifier, which makes the credit check process faster for them.

Given consumer preferences, the CWTA believes that an effective solution in most instances is to mask the SIN on credit files rather than eliminate its use altogether. In that fashion, the SIN is protected but should instances of fraud arise, the SIN in its entirety would be available to a company potentially providing credit under fraudulent circumstances.

When voluntarily provided, the SIN plays an important role in locating credit files for credit applicants. Without it, credit providers must to rely upon other identifiers, reducing the ability to obtain the proper credit file thereby limiting their ability to provide credit to their customers.

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

1. Do you think this option would better protect against identity theft. Why or why not?

The wireless industry is not convinced that mandating disclosure in law for organisations that do not hold substantial amounts of sensitive personal information is the best option for consumers. As has been demonstrated in the US experience with California Bill 1386, disclosure "at a reasonable time" too often means disclosure before an investigation is complete, causing consumers confusion and undue stress, and absolutely not contributing

to the reduction of identity theft, and the underlying criminal activities remain unaddressed.

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.

1. Do you think this option would better protect against identity theft. Why or why not?

This practice is already in place today in many of the member companies of CWTA. The existence of such an alert is of value to vendors at point of sale – in the event credit worthiness is being checked to provide wireless telephony service.

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.

1. Do you think this option would better protect against identity theft. Why or why not?

Provided that the fraudulent debt has been confirmed or verified with the credit grantor, it is in the interest of both the consumer and credit providers to have fraudulent debt removed or suppressed from a consumer's credit file and scoring processes. Otherwise,

this would not be a true reflection of the financial risk of the customer.

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.

1. Do you think this option would better protect against identity theft. Why or why not?

The CWTA does not believe wireless service providers, and/or their retail partners should be held liable in cases of identity theft, or financial fraud committed as a result of identity theft. Businesses also are affected by identity theft, often absorbing the losses which result. As in most other criminal activity, it is the criminal who should be responsible and from whom the proceeds of crime should be recovered. As such, it is imperative identity theft be fully defined in the Criminal Code, with applicable criminal punishments.

Regarding the option that companies contact individuals at an alternate phone number, the CWTA notes that, practically speaking, in a growing number of cases, mandating that wireless services providers to contact a customer at an alternate number may not be possible; increasingly many customers choose to maintain their wireless phone as their only point of contact as opposed to having an additional landline phone. Hence, this option may not be a useful tool for addressing identity theft.