INFORMATION TECHNOLOGY
ASSOCIATION OF CANADA

ASSOCIATION CANADIENNE DE LA
TECHNOLOGIE DE L'INFORMATION

Working Together to Prevent Identity Theft

ITAC Comments on CMC Discussion Paper

September 2005

ITAC is the voice of the Canadian information and communication technology industry. Together with its affiliated organisations across the country, the association represents 1300 companies in the information and communication technology (ICT) industry in all sectors including telecommunication and internet services, ICT consulting services, hardware, microelectronics, software and electronic content. ITAC's network of companies accounts for more than 70 per cent of the 566,000 jobs, $130 billion in revenue, $5.2 billion in R&D investment, $20.7 billion in exports and $11.5 billion in capital expenditure that the sector contributes annually to the Canadian economy.

The Information Technology Association of Canada (ITAC) is the voice of Canada's information and communication technology (ICT) industry. We are pleased that the Consumer Measures Committee has turned its attention to the growing problem of identity theft, and would offer the following comments for the Committee's consideration. The responses in section A are from the point of view of telecom service providers, whose business deals with consumer relationships that are not necessarily characteristic of other sectors of our industry.

A. Questions from the Discussion Paper Workbook

Option I – Truncate (partially blank out) payment card numbers[1]

Do you think this option would better protect against identity theft?

Yes. ITAC believes that this means of limiting the amount of personal information that is routinely available through the ordinary course of business is the best option to help protect against identity theft.

We suggest, however, that it is unnecessary to require that the expiry date not be printed if the credit card number is limited to the last five digits. Absent the full credit-card number, the expiry date will be of no use to an identify thief. Requiring deletion of both the expiry date and the first digits of a credit card would impose unnecessary costs on businesses that currently indicate only the expiry date on receipts.

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

ITAC is unable to quantify the costs or savings. Businesses would be required to cover these costs themselves.

Should there be exemptions? If yes, what type?

For the reasons identified in the Discussion Paper, ITAC supports the American Approach, which limits application to electronically printed receipts by expressly excluding handwritten receipts and imprinted cards.

Should there be a penalty associated with this provision (as proposed in Option IX)?

ITAC supports a best-practices model rather than one that legislates the imposition of penalties on businesses. If penalties are introduced, they should be imposed only where there is a proven case of wilful negligence that has led to real and measurable loss or damage.

[1] Discussion Paper: "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."

For this option, who should ultimately be responsible for losses incurred from identity theft?

ITAC would point out that no rules could be applicable in all circumstances. For example, identity theft triggered by access to credit or debit card numbers on receipts can occur as a result of the misplacement by consumers of their own receipts, or their failure to dispose of receipts in a secure manner. In any event – and in all circumstances of identity theft – it should be the thief who is responsible for any loss incurred.

Are there disadvantages for consumers or industry? Please describe

ITAC is not aware of any disadvantages to either consumers or industry.

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?

There are no standards for the truncation of information on payment cards within the telecom industry. Nevertheless, most companies already truncate payment card information.

Option III – Do not disclose social insurance numbers (SINs) on credit reports or use them as a unique identifier for consumers[2]

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

There are no SIN usage standards in the telecom industry. SINs may be collected from customers on a voluntary basis, but are not demanded or required. SINs are often used in the credit-verification process for customers applying for telecom services. It has been demonstrated that successful responses from credit bureaus are more likely when a SIN is provided, thereby increasing convenience and account processing for customers. SINs may also be used to match customers applying for telecom services to accounts already existing with the same identification. This exposes potential fraud, reveals unpaid debts, or allows the telecom company to use the customer's history for setting up their new account. Telecom companies may also use the SIN at the customer's request to search the company's database for outstanding debts for which the customer does not have the account number.

Telecom companies would be very reluctant to not use the SIN for these purposes. Many telecom company customers seem more willing to provide their SIN than their

[2] Discussion Paper: "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."

driver's licence number as they know it by heart. However, most telecom companies do not use SIN as a unique identifier for consumers. Some, but not all, telecom companies may disclose SINs to collection agencies if an account is forwarded for collection and the SIN was provided to the company.

Option V – Require organisations that store personal information to notify individuals and credit bureaus in cases of security breaches[3]

Do you think this option would better protect against identity theft?

Breaches of data security are a significant issue for our industry and for the economy at large, and the need for effective responses cannot be overstated – and concern should be addressed not just to companies that store personal information, but also to companies that collect or process it.[4] While mandatory notification may seem like an obvious part of the solution, it is important to recognise that not all security breaches will be of a nature that would expose an individual to a real possibility of identity theft.

Where they are of such a nature, knowledge by the individual may help the individual take whatever further steps may be necessary to guard against identity theft. However, it will be of little constructive help to notify an individual of a security breach that is not of a nature that would expose the individual to a real possibility of identity theft, and it may do more harm than good if it causes unnecessary worry for the individual.

Depending on how it has been drafted, a legislated obligation might lack flexibility to address differing circumstances and levels of security breaches. There may also be circumstances in which a company is not aware of a security breach; imposing a legislated obligation to inform customers in these instances would place an unfair burden and responsibility on companies, and potentially subject them to unfair penalties.

Thus, a blanket legal obligation to inform individuals of all personal information security breaches could be overly broad and would not necessarily better protect against identity theft. In some cases, development of industry best practices would provide the necessary flexibility for companies to respond appropriately to the wide variety of circumstances that may arise with respect to security breaches.

However, ITAC would support a full exploration of the need for legislation addressing notification of data-security breaches, provided the concerns and limitations expressed above are taken into account. Such legislation, if properly worded, could achieve positive results by:

---

[3] "When the security of personal information held by an organisation is breached, the organisation must contact the individuals whose personal information has been compromised as well as relevant credit bureaus as soon as reasonably possible"

[4] "A Chronology of Data Breaches Reported Since the ChoicePoint Incident" - http://www.privacyrights.org/ar/ChronDataBreaches.htm - provides another perspective of the problem with a number of more recent examples that give a better indication of the scope of the problems.

- Advancing industry's adoption of comprehensive security practices as recent well-publicised security breaches have resulted from a combination of causes (not necessarily technical). Repeats of these kinds of incidents will only be prevented by the adoption of security precautions.

- Forcing industry to pay more attention to security, since incentives will exist to minimise the reputational and other risks associated with publication of disclosures.

To achieve these results, ITAC believes that the legislation should:

- **Be consistent across the country.** Organisations that operate nationally need to be able to operate pursuant to a single set of rules to the greatest extent possible. ITAC is pleased to acknowledge that that this seems to be among the CMC's objectives.

- **Require notification only in the event of a security breach that creates a significant risk.** Notification of individuals should only be necessary: a) in the event of a breach; b) when the organisation that controls the personal information knows or has reasonable grounds to believe that a disclosure of personal information to unauthorised individuals has taken place; and c) the disclosure presents a significant risk of harm to individuals (i.e., identity theft or fraud). This risk analysis required to determine whether there is a significant risk of harm would of course require the organisation to take into account the sensitivity of the personal information. In cases where the personal information at stake is not sensitive, it would be unnecessary to notify individuals.

- **Provide appropriate exemption provisions** for organisations that have taken adequate measures to protect against loss of identity. For example, an organisation which has encrypted data that later becomes lost should be able to benefit from such provisions, as data that has been encrypted or redacted generally will be of little use to recipients. Such exemptions would serve as a safe harbour to reduce defensive, unnecessary notifications.

- **Provide organisations that must notify individuals with reasonable time to do so.** While it is of the essence that individuals be notified promptly in order to reduce the risk that they may be victims of identity theft, organisations must also be given sufficient time to determine who and how to notify. Thus, it would seem reasonable to impose on organisations a duty to warn "in the most expedient time possible and without any reasonable delay".

- **Permit organisations to notify individuals through different means.** Depending on the number of people affected and the cost of notifying, organisations should be able to elect how to best notify the individuals affected by a breach.

- **Ensure the onus for notification to individuals is the responsibility of the organisation that controls the personal information**. Consistent with the Accountability principle of PIPEDA, organisations that use service providers and transfer personal information to them to be handled on their behalf should remain accountable to individuals and be responsible for notifying them. To avoid duplicative, impractical and confusing actions, service providers should have notification obligations only to their direct corporate customers and not to the end-user consumers.

B. Additional Comments

ITAC is of the view that the CMC discussion paper would have been stronger had it considered consumer-credit issues in a broader context of related initiatives, especially those related to newer technologies, such as the following.

Smart-Card Technology

Introduction of CHIP and PIN technology in Canada will have a significant impact on incidents that are broadly classified as identity theft. Sometimes it is difficult to determine if the incident should be classified as identity theft, fraud, privacy violation or all three. In any case, smart cards are often viewed as a means to mitigate the impact. Though smart cards may not be a panacea for solving identity-theft issues, the next few years will see a tremendous increase in the use of smart cards and the back-end applications and infrastructures required to support them.[5] In the US, the federal government has launched the National Personal Identity Verification Project, which is also based on smart-card CHIP and PIN technology.[6]

ITAC suspects that there will be opportunities to develop new business processes as smart cards enter the mainstream – for both the private and the public sectors. Looking into a future that will embrace advances in technologies, the CMC may wish to consider working with Industry associations like ITAC and ACT, particularly when they consider options that will involve merchants, vendors and members of the payment-card industries.

[5] See "Interac moving to CHIP" - http://www.interac.org/en_n3_42_faq.html; "VISA Canada - the road to Chip and PIN" - http://www.visa.ca/en/merchant/fraud_chip.cfm; "MasterCard Canada" - http://www.cardforum.com/$nocookies$/staticpage.html?pagename=cidchap5; and "ACT Canada - Advanced Card Technology Forum Canada" - http://www.actcda.com/.

[6] "NPIVP" - http://csrc.nist.gov/piv-program/index.html; and "National Personal Identity Verification Project Workshop" - http://csrc.nist.gov/piv-program/workshop-Jun272005/presentations.html

Phishing

Given the recent prominence of the issue in the media, ITAC is disappointed by the lack of attention given to the phenomenon of phishing, i.e., the practice of fraudulently appealing for personal information by way of spam email that purports to be – and increasingly appears to be – from a legitimate business, notably a financial institution or other commercial entity that a consumer trusts as a result of dealings in the non-cyber world. Consumers should be protected from being duped into sharing information that could result in identity theft or the disclosure of personal or financial information. Measures to reduce the amount of spam email will also reduce the number of phishing attempts that consumers receive, but won't address the full extent of the problem.