Are You Sure You Want to Continue?
Consumer Authentication at the Crossroads

Written By: Janet Lo and John Lawford
Additional Research: Neida Gonzalez
Public Interest Advocacy Centre
1204 - ONE Nicholas St.
Ottawa, Ontario
K1N 7B7

September 2008

With Funding from Industry Canada

The Public Interest Advocacy Centre
(PIAC)
Suite 1204
ONE Nicholas Street
Ottawa, ON
K1N 7B7

Canadian Cataloguing and Publication Data

Are You Sure You Want to Continue?
Consumer Authentication at the Crossroads

ISBN – 1-895060-84-2

Acknowledgement

Financial support from Industry Canada to conduct the research on which this report is based is gratefully acknowledged. The views expressed in this report are not necessarily those of Industry Canada or of the Government of Canada.

EXECUTIVE SUMMARY

This report looks at the consumer experience with electronic authentication. Authentication is the process that is used to ensure that a person is who she or he reports to be. Electronic authentication systems are increasingly widespread in our information society.

Authentication systems are often discussed in terms of three factors: something that is known by the individual, something that the individual has, and something that the individual is. Consumers encounter authentication in banking and online retail services. For transactions conducted in person, the most common consumer authentication solution is two-factor authentication by a card in the customer's possession and a PIN that the customer knows. The most common consumer authentication solution for online transactions is single-factor authentication by a username and password, as both authenticators are known to the customer. Some authentication systems add extra layers of security by asking security questions known to the individual. As well, there are an increasing number of portals through which the consumer can access a number of services after a single authentication process.

Despite the widespread use of electronic authentication systems in consumer transactions, a number of studies have shown that consumers are still resistant to authentication services and frustrated with the lack of security provided by online bank services and online retailers. In a survey constructed by PIAC, the majority of respondents felt that there were security and privacy risks inherent in online banking and retail transactions. In particular, consumers are concerned about hackers, identity theft, monetary fraud and the loss of privacy. Phishing is a type of attack that targets weak authentication systems. As phishing threats increase in frequency and become more complex, widespread consumer adoption of authentication systems will only occur if individuals trust strong security and privacy protections built into authentication systems.

Industry Canada convened an Authentication Principles Working Group to study the issue of authentication in Canada. The Working Group published six principles for electronic authentication in May 2004. These principles have not been updated since, though there have been various international and national government initiatives to address authentication.

The Principles fail to provide adequate protection for consumers, as they are too broad to provide guidance for the design and implementation of authentication systems that promote strong security and respect consumer privacy. Secure authentication systems that respect user privacy will boost consumer trust and confidence in electronic commerce. At the same time, authentication systems should be user-friendly such that they are not overly cumbersome for the average consumer.

This report makes several recommendations to improve the electronic authentication framework for consumers. The recommendations are summarized below.

Assure consumers of their security when using authentication systems

- Multi-layer single-factor authentication should not be used for sensitive consumer transactions such as online banking.
- For online banking transactions, solutions such as out-of-band authentication and true two-factor authentication by OTP tokens could be utilized to enhance consumer security. However, additional research should be undertaken to assess the effectiveness and acceptability of these authentication technologies before they are implemented.
- Consumers should never be required to use a biometric to authenticate. Where biometric authentication systems have already been rolled out, consumers should be able to choose an authentication process that does not require a biometric authenticator.
- The industry should document standards and protocols for consumer authentication systems, which should be continually reviewed to respond to changing threats.
- Authentication standards should promote strong authenticators that are non-linkable and non-traceable. Consumers should be able to choose which pieces of personal information they wish to use as authenticators.
- Organizations that offer a portal of services behind a single authentication process must avoid risk creep by ensuring that the strength of the authentication system matches the risk level of offered transactions.

Clarify who bears the liability for losses related to authentication

- Legislation should clarify who bears the liability for losses in the event of unauthorized transactions that relate to authentication.
- The provider of the payment system and financial services should be liable for losses, not consumers. Banks and retailers are in the best position to ensure that their authentication systems are secure and protect consumer privacy.
- Financial institutions and businesses should not be able to shift their liability for losses to consumers through standard form contracts. Furthermore, organizations should be required to highlight clauses in standard form contracts that discuss the apportionment of liability so customers are aware of the terms buried within the contract.

Protect consumer privacy in authentication systems

- Industry Canada's Principles for Electronic Authentication should be reviewed to integrate specific fair information practices mandated by the *Personal Information Protection and Electronic Documents Act*.
- Organizations that authenticate their customers should minimize the amount of personal information collected, as is required by *PIPEDA*. Similarly, compliance with the prohibition on secondary use of

authentication information should be better monitored so that consumers cannot be profiled or tracked.

- Consumer accounts should expire if they are not used regularly, and consumers should be able to terminate their accounts if they do not plan to have an ongoing relationship with the bank or retailer. Organizations should purge their databases regularly of personal information in expired accounts.
- Consumer choice should be promoted in three areas:
  - Consumers should be able to choose to authenticate for the transaction in person, especially for essentially and widely performed commercial transactions.
  - When using a single sign-on portal that offers access to a multitude of services, consumers should be able to choose which services they want activated or de-activated after assessing their level of comfort with the service portal's authentication system.
  - Consumers should be able to choose which pieces of personal information they wish to use as authenticators so that they can retain control over their personal information and choose how to best protect their own privacy against perceived risks.
- As often as possible, consumers should be able to complete transactions while anonymous or using pseudonyms.

<u>Mandate full public disclosure and consumer education about authentication systems</u>

- Consumers should be fully informed about the risks of electronic authentication before initiating a transaction or registering for an online account.
- Consumers must be provided with clear notice when a service is added to an online portal that is accessible by a single authentication process. The service and additional authentication requirements should be described in the notice. Consumers should be able to opt in to the added service or strengthen the security of the authentication process.
- A legislative requirement should allow a federal regulatory body such as the Office of the Superintendent of Financial Institutions Canada to audit the authentication systems of financial institutions.
- A similar audit requirement should be implemented at the provincial level to address authentication in the retail environment.
- Banks and retail businesses must fully disclose the results of authentication audits to their customers and the public.
- A positive obligation should be placed on organizations to notify their customers when their authentication system is affected by a security breach and to detail the nature and extent of the breach.
- Consumer education about authentication should be provided by the Financial Consumer Agency of Canada, detailing practices on how consumers can effectively protect their personal privacy when using authentication systems. The Retail Council of Canada and the Canadian

Marketing Association could draft similar consumer education documents about the authentication systems of in-person and online retailers.

- Financial institutions and online retailers should also provide their customers with specific consumer education regarding the security features of their authentication systems. In particular, financial institutions should educate their customers about phishing threats and the limited circumstances and methods through which banks would attempt to contact their customers.

<u>Guarantee consumer protection by improving the regulatory framework for electronic authentication</u>

- A voluntary set of principles for electronic authentication do not provide adequate consumer protection.
- Financial institutions should be subject to stricter authentication regulation because they host a vast collection of sensitive financial and personal information. Authentication by financial institutions can be best regulated under the *Bank Act*.
- Regulation of authentication under the *Bank Act* should set minimum security standards for in-person and online banking transactions and clarify the extent to which consumers bear liability for losses related to authentication.
- Consumers must have mechanisms for recourse. The Financial Consumer Agency of Canada should issue guidelines for the handling of consumer complaints about authentication systems.
- The Ombudsman for Banking Services and Investments should investigate complaints made about authentication.
- A similar complaint mechanism should exist for retailers companies.
- The Financial Consumer Agency of Canada should compile statistics on the number of complaints made about authentication systems.
- The regulation of authentication for retailers and payment systems is more challenging as regulation lies within provincial jurisdiction. As well, there are a range of retail transactions that may require authentication.
- In conjunction with better regulation of banks and retailers, the federal and provincial privacy commissioners should be mandated to oversee authentication practices. Privacy commissioners can adapt their audit and complaint investigation requirements to oversee authentication by financial institutions and retail organizations while protecting consumer privacy.

Table of Contents

INTRODUCTION

While used frequently in a variety of contexts, there is no common definition for "authentication."[1] Technology-focused groups define authentication as "the process of establishing confidence in the truth of some claim"[2] whereas authentication guidance documents use the definition: "a process that attests to the attributes of participants in an electronic communication or to the integrity of the communication."[3] Ultimately, "authentication" is simply the process that is used to ensure that a person is who she or he reports to be.

Electronic authentication has become widespread in our information society, with daily transactions performed through electronic services and the internet, as new online services require remote electronic authentication. Everybody uses electronic authentication – businesses, government and consumers. New technologies for authentication make online transactions more seamless, tying together information on multiple devices and offering services to consumers that were previously unimaginable, moving closer to full realization of the internet's potential. As electronic commerce grows, the ability to optimize success in this new market is dependent on consumer confidence.[4] However, many authentication systems collect and use the personal information of its users, creating privacy and security risks. Phishing has become a prevalent online threat directed at weak authentication systems and is often performed as part of a larger identity theft or monetary fraud scheme. To mitigate these risks, it is essential that authentication systems are designed to give consumers greater control over their personal information and promote user security and effective privacy protections.

Recognizing that electronic authentication is a shared interest, Industry Canada brought together consumer groups, industry and government agencies to develop the *Principles for Electronic Authentication – A Canadian Framework* (Authentication Principles), which came into effect in May 2004. The Authentication Principles are a voluntary code of conduct for those developing, implementing or using electronic authentication products and services in Canada.

The topic of electronic authentication easily segues into a philosophical discussion about identity management, raising controversial questions about national identification cards, radio-frequency identification and biometrics. While these issues are important and have been discussed by PIAC in detail

[1] Privacy Commissioner of Canada, "Policy Scan Survey: Identification & Authentication Issues in Canada Summary Report" (February 2005), online: http://www.privcom.gc.ca/information/survey/2005/ps_050404_e.asp.

[2] Authentication Privacy Principles Working Group, "Privacy Principles for Authentication Systems" (May 2003), online: http://www.cdt.org/privacy/authentication/030513interim.shtml.

[3] *Principles for Electronic Authentication: A Canadian Framework* (Industry Canada, May 2004) at p. 7 ("Authentication Principles").

[4] Federal Trade Commission, *Proof Positive: New Directions for ID Authentication* (Washington, D.C.: April 2007), online: http://www.ftc.gov/bcp/workshops/proofpositive/index.shtml.

elsewhere, they are broader questions that are not within the scope of this paper.[5]

The purpose of this report is to examine how consumers use electronic authentication and to recommend how Canada's electronic authentication framework for consumer transactions can be strengthened. While issues in authentication for business-to-business or government-to-citizen transactions are important, they are not within the scope of this report. The report will restrict its focus to daily consumer transactions with financial services and online shopping. The research methodology consists of literature review in the area of electronic authentication, canvassing government documents, multilateral agreements, security reports, consumer surveys and legal and policy articles. As well, this report is based on a large-scale online survey constructed by PIAC and conducted by survey research firm Pollara. In total, 2414 surveys were completed.

This report begins by describing the consumer experience with authentication using specific examples and describing the results of PIAC's survey. We also discuss authentication trends in the marketplace. Next, the report reviews the Authentication Principles developed by the Industry Canada Working Group and more recent initiatives following the publication of Authentication Principles. The report will then examine how the Authentication Principles address consumer concerns with electronic authentication in Canada, focusing on the areas of authentication security, liability for losses and consumer privacy. Finally, this report advances recommendations to strengthen legislation and regulations to protect consumers who use electronic authentication products and services in Canada.

[5] See PIAC report, "National Identity Cards, Biometrics and the Consumer: Displacing the Personal from the Person" (26 February 2007), online: http://www.piac.ca/privacy/piac_report_national_identity_cards_biometrics_and_the_consumer_displacing_the_personal_from_the_person/.

CONSUMER EXPERIENCES WITH ELECTRONIC AUTHENTICATION

What is authentication?

Many definitions have emerged since policymakers began discussing authentication. At its simplest, authentication refers to "insuring [*sic*] that a person is who she or he reports to be."[6] An important distinction must be drawn between identification and authentication. According to the Office of the Privacy Commissioner "Guidelines for Identification and Authentication," identification involves a claim or statement of identity, such as "I am John Doe" or "I am the customer associated with this account." Authentication is the verification of that claim.[7]

Some offline consumer transactions can be conducted in anonymity and without identification or authentication, such as retail cash transactions. However, businesses increasingly need to identify and authenticate their customers to ensure that a customer's transactions are associated with the correct account and so that a customer's records are retrievable. Sometimes, the identity of the customer need not be associated with the customer's "real world" identity or name, but can be an identity created for the purposes of the business relationship, such as "Customer 4523."

Factors of authentication

Authentication is often discussed in terms of the three factors that can be used to authenticate an individual, also called "criteria" or "authenticators." The three factors are:

(1) something that is ***known*** by the individual (such as a password, a personal identification number, an account name or number, favourite colour, make of their first vehicle);

(2) something that the individual ***has*** (such as a bankcard, token, identity card, digital certificate; and

(3) something that the individual ***is*** (usually a biometric such as a facial image, retina scan or voice print) or ***does*** (a person's signature).

The most common electronic authentication solution is single-factor authentication, where a system requires the user to provide an authenticator in one of the categories outlined above. True two-factor or three-factor authentication requires elements from two or three of the above categories.

[6] Federal Trade Commission, *Proof Positive: New Directions for ID Authentication* (Washington, D.C.: April 2007), transcript, online: http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/042307_sess1.pdf at p. 1

[7] Privacy Commissioner of Canada, "Guidelines for Identification and Authentication" (October 2006), online: http://www.privcom.gc.ca/information/guide/auth_061013_e.asp.

Where authentication is based on more than one authenticator from the same category, the authentication system is more appropriately referred to as “multi-layer authentication.” A new method of authentication is multi-channel or “out-of-band” authentication which may use single-factor or multi-factor authenticators. Out-of-band authentication generally refers to “any technique that allows the identity of the individual originating a transaction to be verified through a channel different from the one the customer is using to initiate the transaction.”[8] Verification can occur through callback or voice verification, e-mail approval or notification and cell-phone based response processes.[9]

PIAC’s survey results on authentication

Research methodology

PIAC constructed a survey to examine consumer experiences with authentication systems. The survey was conducted by research firm Pollara. Online surveys were conducted with Canadians aged 18 and over between May 7 and May 13, 2008. In total, 2,414 surveys were completed. A comparable telephone survey would have an overall margin of error of ± 2.0%, 19 times out of 20.

Survey respondents were representative of gender and regional demographics across Canada. Regionally, 38% of respondents were from Ontario, 24% from Quebec, 14% from British Columbia and the territories, 10% from Alberta, 7% from Atlantic provinces and 6% from Prairie provinces Saskatchewan and Manitoba. 52% of respondents were female, and 48% of respondents were male.

Key findings

In our survey, we asked a range of questions about how consumers used online banking and online retail services. Not surprisingly, the majority of respondents bank online (86%) and made online purchases within the past 12 months (81%). As well, the majority of respondents reported that their online purchasing increased or stayed the same in the past year.

Most respondents (58%) noticed that banks and retailers were asking for more than a login and password for authentication. The majority of those who noticed stated that the extra step increased their confidence in the system’s security (67%).

The majority of respondents felt that there was a risk involved in online banking (62%) and in purchasing goods online (77%). We asked respondents who stated that there was a risk to identify the level of risk they associated with conducting online banking and retail transactions on a scale from 1 to 10, where 1 was not at

[8] Federal Financial Institutions Examination Council, “Authentication in an Internet Banking Environment” (October 2005: Arlington, VA) at p. 11, online: http://www.ffiec.gov/pdf/authentication_guidance.pdf.

[9] *Ibid.* at p. 3.

all risky and 10 was extremely risky. Generally, respondents found purchasing online goods to be slightly more risky than online banking. A sizable minority labeled the risk level for online banking and online retail transactions to be fairly risky (6 or above on a scale of ten). This suggests that a number of consumers still do not fully trust and do not feel fully comfortable with online banking and retail transactions.

The majority of respondents (87%) believed that banks and retailers should bear the loss if their account was accessed without their permission. Even where the bank or retailer added two-factor authentication systems, the majority of respondents still believed that banks and retailers should bear the loss (75%).

As well, the majority of respondents (55%) indicated that they never had a problem using authentication systems before. However, a sizable minority (38%) had problems when using authentication systems. While the majority of respondents were able to contact the bank or company to resolve their issue in a satisfactory manner, 21% of respondents who had issues were not able to contact the bank or retailer about authentication issues.

Finally, we asked a series of questions to gauge consumer understanding and comfort levels with online banking, online retail and seal programs. Approximately half of respondents (46%) had cancelled a purchase attempt or online banking session because they were confused, with most of those respondents citing unfamiliar questions or steps and requests for too much personal information as reasons for canceling the transaction. Similarly, a number of respondents (44%) had previously cancelled a purchase attempt or online banking session because they felt uncomfortable, citing a number of reasons including identity theft, requests for too much information and unsecured websites or hackers. Respondents were indecisive as to whether a seal of approval would bolster their confidence in the security of an authentication process. As well, when asked about how they felt about a common look and feel for authentication products, 38% of respondents stated that they would feel more comfortable, compared to 35% whose level of comfort would not be affected and 5% who would be less comfortable with the transaction.

Results of the survey are also incorporated into our analysis below examining how Canadian consumers use electronic authentication. To see the full survey and the results that were collected, please see Appendix A.

Survey limitations

While the results of our survey were helpful to our understanding of the consumer experience with authentication, their usefulness was limited. For PIAC's questions asking consumers to assess and quantify their level of risk, comfort and confusion while banking and shopping online, respondents provided answers based on their own perceptions and experiences with authentication. Authentication is a highly technical issue and most consumers lack the technological knowledge to truly differentiate between weak and strong authentication systems. This is a problem that will be addressed later in this report when criticizing the Authentication Principles.

Additionally, PIAC's survey focused exclusively on authentication for online transactions. The survey neglected to ask consumers about their experiences with authentication in real-world or point-of-service business-to-consumer transactions.

How Canadian consumers use electronic authentication

As stated above, this report restricts its focus to electronic authentication of consumer financial transactions. Consumers authenticate in everyday transactions, and authentication is particularly important in banking and retail transactions. The following are examples of daily transactions that require consumers to electronically authenticate.

Banking and financial services

More Canadians bank online than with a bank teller.[10] This was confirmed in PIAC's survey, in which 86% of respondents indicated that they bank online, most doing so on a weekly basis.[11] When banking online, most customers check their balance (95%) and pay bills (93%). Some customers use their online account to e-mail money transfers (33%), purchase investments or stocks (17%) or perform account transfers (6%).[12]

When a customer logs on to their bank's website to check their balance or pay bills, they use the bank's online authentication system to verify that they are who they claim to be. Most bank authentication systems in Canada require the customer's account number and a customer-selected password. Some banks will also ask security questions that are highly personal in order to confirm the person's identity, such as "What is your mother's maiden name?" or "What was the make of your first car?" This is an example of multi-layered single-factor authentication, as all of these criteria are things that the customer ***knows***.

When a customer goes to an automated teller machine (ATM) to withdraw cash or perform a financial transaction, the ATM's authentication system requests the customer's account card and PIN. This is an example of true two-factor authentication, as the consumer is required to provide something he or she ***has*** and something he or she ***knows***.

[10] EKOS survey in 2005, cited in Electronic Commerce Branch presentation, "Consumer Trust and Business Confidence in the Online Environment: Status Update" (14 June 2006). In the survey, 24.7% of respondents indicated that they bank online compared to 23.3% of respondents who bank with a teller.

[11] In PIAC's survey at Q2, 62% of respondents bank weekly, 22% bank daily, 14% bank monthly, while 2% bank less frequently than a month.

[12] In PIAC's survey at Q1AN, less than 1% of consumers also indicated that they used online banking for purchases, to monitor investments, loans, purchase checks, foreign exchange or currency, mortgage rates, credit cards, deposits, to set up a new account, withdrawal, or direct deposit.

Airport check-in

At the airport, consumers can conveniently check-in at automated kiosk machines. The kiosk offers the consumer two authentication options: the consumer can enter their flight confirmation number or scan the credit card that they used to purchase the ticket. This is a simple single-factor authentication process, requesting either something the consumer ***knows*** or something the consumer ***has***.

Online shopping

In PIAC's survey, 81% of respondents stated that they made an online purchase in the last year. Most people made two to five online purchases within the last year (54%), compared to 20% who made six to ten purchases, 17% who made more than ten purchases, and 8% who only made one purchase within the last year.[13] Most consumers spent less than $500 in online purchases within the past year, though over a quarter of respondents spent between $500 and $1500 and 17% spent over $1500 online within the past year.[14]

Most online retailers require consumers to authenticate using a log-in ID and password. For example, Amazon and Best Buy use a consumer's e-mail address as the log-in paired with a password, while eBay, Expedia and Apple require the customer to select a username and a password. Expedia also allows customers to sign in using their Microsoft .NET passport information.[15] The Microsoft .NET passport is an online personal authentication service that allows users to use their e-mail address and a single password to sign in to websites and online services that have adopted the Microsoft .NET passport system.[16] These are all examples of multi-layer single-factor authentication.

Once the customer has authenticated, he or she must perform a payment transaction in order to receive their desired goods or services. Many retailers only accept major credit cards – Visa, MasterCard or American Express. Customer accounts with a retailer retain the customer's personal information: their name, e-mail address, home or office address and shipping address. In addition, many retailers offer to retain credit card information for the convenience of the customer's future transactions.

[13] See PIAC's survey at Q4.

[14] In PIAC's survey at Q5, 54% of respondents spent under $500, 28% spent $500 to $1500, and 17% spent over $1500 in online purchases in the last month.

[15] We selected these companies as examples because according to comScore, a research company that analyzes online consumer behaviour, these companies are consistently ranked in the top 25 online properties according to the number of unique Canadian visitors. See "comScore Releases Top Canadian Web Rankings for March 2008" (28 April 2008), online: http://www.comscore.com/press/release.asp?press=2200. eBay is consistently ranked the fifth most popular online property in Canada, Amazon often ranks 9th or 10th and Apple often ranks 10th or 11th. Best Buy and Expedia are popular among Canadian consumers based on seasonal trends. For example, Best Buy is very popular in December, presumably due to Christmas shopping, and Expedia is popular in winter months, when people begin to book summer travel.

[16] For more information, see online: http://www.microsoft.com/oem/passport.mspx.

Recently, some credit card companies rolled out services that merchants can implement to further authenticate credit cards for online transactions. An example of this is the Verified by Visa (VbV) service, where Visa cardholders are prompted to enter their registered VbV password at online shopping check-outs where the service is implemented. The password is then verified by their Visa card issuer. Visa encourages online merchants to subscribe to this service by denying protection to non-VbV-subscribing retailers against "fraudulent purchases," disputes and chargebacks.[17] MasterCard has a similar program called MasterCard SecureCode.[18]

Credit card payment options can be overly complex and costly for smaller online retailers as online credit card processing requires merchant accounts, bank security deposits and secure websites.[19] Many online retailers will use third party credit card processing companies that reduce merchant costs by offering processing services on a per transaction basis and fraud screening.[20] As well, a number of online merchants are increasingly using third-party payment options as alternatives to credit card payments. The best known of these companies is PayPal, a popular eBay payment option. PayPal customers can decide how they wish to pay for their product or service – they can pay directly from their PayPal balance, debit from their bank account or charge the transaction to their credit card. The recipient merchant receives the money without seeing the customer's financial details, such as credit card or bank account numbers.

Industry trends in electronic authentication

In Canada, the number of electronic payments continues to increase through the use of debit and credit cards. For example, point-of-service debit transactions in

[17] Verified by Visa Service, Merchant FAQs, online: http://www.visa.ca/en/merchant/products/vbv/faqs.cfm.

> ***What if I don't implement VbV?***
> Without VbV, you will not be protected against "fraudulent purchaser" disputes and chargebacks.

[18] For more information, see MasterCard SecureCode, "Credit Card Security: Safe & Secure Online Shopping," online: http://www.mastercard.com/us/personal/en/cardholderservices/securecode/index.html.

[19] To become a merchant that accepts credit card payments, businesses need to set up a merchant account with a financial institution that is partnered with the credit card company. For example, see the list of Visa member financial institutions, online: http://www.visa.ca/en/merchant/acceptingvisa/becomemerchant.cfm. See also, TD Canada Trust, "Payment Power for Merchants", online: http://www.tdcanadatrust.com/merchantservices/pdf/TDMS-PaymentPower.pdf . Justin Whitney explains the myriad of details for setting up merchant accounts to process credit cards: "Setting Up Merchant Accounts for Credit Card Processing" AllBusiness, online: http://www.allbusiness.com/banking-finance/banking-lending-credit-services-payment/7129539-1.html. For a discussion of alternatives to processing credit cards online, see Paul Lima, "Credit Cards, Online Payment, E-commerce – Canadian small businesses need to know how to collect money online" Canada One (April 2001), online: http://www.canadaone.com/ezine/april01/ecommerce_revenue.html.

[20] Some examples of third party credit card processing companies include InternetSecure Inc., PSiGate, WorldPay, iBill, visage, CCNow and ClickBank.

2007 increased to more than 2.7 billion transactions with a cumulative value of just under $127 billion compared to 1.95 billion point-of-service debit transactions valued at nearly $88 billion in 2002 and 806 million point-of-service debit transactions with a cumulative value of $36 billion in 1997.[21] The growth of electronic payments can be partially attributed to e-commerce, as parts of the economy move online. According to Statistics Canada, internet sales in Canada continue to grow in 2007 to $62.7 billion, up 26% from 2006.[22] The connectivity of Canadian business reached 82.8% in 2007.[23] The Canadian Payments Association added a ledger to account for online debits (payments initiated by a customer online for the purchase of goods or services) in 2005. Since 2005, there has been significant growth in the volume and value of online debits, increasing from four thousand transactions valued at $153,000 in 2005 to over 331,000 transactions with a cumulative value of $21 million in 2007.[24]

The most common online authentication solution is single-factor authentication with a username and password.[25] Requests for authentication are increasingly widespread, as online users are encouraged to create accounts for various services that do not necessarily have a commercial purpose, such as informational catalogues and news services. In retail, consumers are encouraged to sign up for "frequent shopper" cards with promises of rewards and discounts. In these ways, consumers are routinely asked to give away pieces of personal information in the retail environment as they create more accounts and digital identities on today's internet.

Another trend is the industry focus on strengthening existing single-factor authentication solutions by adding layers of the same factor. For example, a number of Canadian banks have added security questions to the authentication process for online banking services that ask details about a customer's personal background or preferences. Some financial institutions also added a

[21] See Canadian Payments Association, Statistics: "Annual Flow of Payment Items Through the Automated Clearing Settlement System (ACSS)", online: http://www.cdnpay.ca/publications/acss_ann.asp.

	2007	2002	1997
Volume	2,736,665,268	1,951,684,943	806,284,752
Value	$126,887,350,000	$87,907,751,000	$36,004,528,000

Note that statistics compiled by the Canadian Payment Association (CPA) for payment items through ACSS do not include transactions performed with credit card, as these do not clear through CPA systems but through the credit card networks' own clearing systems.

[22] Statistics Canada, "Electronic Commerce and Technology" (24 April 2008), online: http://www.statcan.ca/Daily/English/080424/d080424a.htm.

[23] Statistics Canada, "Electronic Commerce and Technology" (20 April 2007), online: http://www.statcan.ca/Daily/English/070420/d070420b.htm.

[24] See Canadian Payments Association Statistics.

	2007	2006	2005
Volume	313,323	71,025	4,086
Value	$21,808,000	$2,166,000	$153,000

[25] Duncan Consulting, "Authentication: Environmental Scan & Assessment of Market Trends," (31 March 2006) Industry Canada at p. 5.

confirmation of the customer's computer internet protocol (IP) address along with their log-in and password to the authentication process.[26] Online retailers are also introducing added layers of authentication for online purchases with credit cards through the Verified by Visa and MasterCard SecureCode programs, which require customers to enter a PIN to authenticate their credit card number.[27]

There are many instances of true two-factor authentication for in-person consumer transactions in Canada. Interac transactions at automatic banking machines and point-of-sale transactions are examples of two-factor authentication. Though two-factor authentication is prevalent for in-person transactions, there is limited use of two-factor authentication in business-to-consumer transactions that occur online.

A number of business groups and industry associations have introduced new authentication technologies, such as chip debit and credit cards with PINs.[28] In 2007, TD Canada Trust announced the first chip debit card in Canada.[29] Chip-enabled point-of-service terminals prompt chip debit and credit cardholders to enter a PIN, which claims to provide an extra level of security against fraudulent and unauthorized use. Many other countries have already migrated to chip technology, but Canada has just begun, expecting a critical mass of cards, automatic banking machines (ABMs), and point-of-sale terminals in the market by 2010. The chip debit card represents the first Canadian financial transaction technology that adheres to EMV standards. EMV is the global technology standard developed by Europay, MasterCard, and Visa for chip-based debit and credit cards to replace existing magnetic strip cards.[30] The chip-based debit and credit card is still an example of two-factor authentication, though it is unclear how the chip card will be used in an online environment.

Migration to chip technology may lead to single-factor authentication as the Canadian Payments Association considers implementing a new framework for electronic funds transfers in Canada, particularly the point-of-sale PIN-less debit transactions. In this framework, point-of-sale PIN-less debits would merely require the possession of some token for authentication. This would be accomplished by radio frequency identification (or RFID) technology on the token, likely a card, which would be tapped on a reader to make a payment. Point-of-sale PIN-less debits would be an example of single-factor authentication. PIAC has several concerns with the proposed framework for PIN-less point-of-sale debit transactions and has submitted comments to the Canadian Payments Association.[31]

[26] *Ibid.* at p. 6.
[27] *Ibid*. Verified by Visa and MasterCard SecureCode are discussed earlier in this paper on page 16.
[28] *Ibid.* at p. 7.
[29] "Canada's First Transaction with a Chip Debit Card" (9 July 2007) The Frontier Times.
[30] EMVCo, online: http://www.emvco.com/.
[31] Public Interest Advocacy Centre, "Comments regarding the framework proposed for PIN-less POS debits in Canada" (August 2008).

Retailers and banks are also beginning to implement out-of-band authentication. For example, Visa and Chase have partnered on mobile phone coupon redemption by their customers. This out-of-band authentication technique sends Visa customers coupons and offers that are customized to their personal interests via SMS text message, redeemable at the point-of-sale or website of participating merchants. The technology is said to be cheaper than paper campaigns and provides one-to-one marketing, as mobile coupons have a higher conversion rate and reduce fraud.[32]

In the global payment and financial services industry, new systems have been unveiled that pair mobile banking with voice biometrics. In August 2008, Voice Commerce and Nuance Communications announced a new system that uses a biometric voice authenticator, Voice Transact, stating that they expect to announce a partnership with a "large U.S. bank" in September.[33] The consumer sets up a "voice signature" biometric to authenticate for payments and other transactions. Only two weeks later, Canada's TD Waterhouse Discount Brokerage announced that they plan to implement Nuance's voice biometric authentication in the summer and early fall of 2008, targeting their telephone client base. TD Waterhouse is the first discount brokerage in Canada to implement voice biometric authentication.[34] We will discuss the broader implications of using biometrics in authentication later in this paper.

Another trend is the development of enterprise-wide authentication solutions, also known as the "single sign-on."[35] A number of financial institutions are adopting these online portals as they allow their customers to access a wide range of financial services with a convenient single sign-on. Industry Canada has noted an inherent increased risk with this approach, as an instance of failed or improper authentication would grant an imposter access to several financial services. This risk will be discussed in detail later in this report.

Consumer concerns with electronic authentication

A 2002 Gartner study found that consumers are growing more resistant to authentication systems and that the majority of consumers who registered for an online authentication service only did so because they were required to in order to use a particular online service.[36] A 2004 Gartner study showed that online

[32] "Chase teams with Visa on mobile coupon pilot" finextra (21 August 2008), online: http://www.finextra.com/fullstory.asp?id=18885.

[33] Michael Sisk, "Yin and Yang? Mobile Banking and Voice Biometrics" American Banker (1 August 2008), online: http://www.americanbanker.com/printthis.html?id=20080728F2BZVI6.

[34] "TD Waterhouse Discount Brokerage launches voice biometric identification system – First discount brokerage firm in Canada to use technology" Yahoo! Finance (13 August 2008), online: http://biz.yahoo.com/cnw/080813/td_voice_recognition.html?.v=1.

[35] *Supra* note 25 at p. 7.

[36] "Gartner Group finds consumers wary of online authentication" (29 April 2002) Telecomwire, online: http://findarticles.com/p/articles/mi_m0ECZ/is_2002_April_29/ai_85180252.

consumers are growing frustrated with the lack of security provided by online bank services and online retailers.[37]

Various surveys have examined how risky Canadians perceive online banking. In PIAC’s survey for this report, 62% of respondents felt that there was a risk involved in online banking. The majority of respondents (70%) who indicated that there was a risk in online banking identified hackers as the risk. Other respondents noted identity theft, loss of personal information, credit card theft and fraud as risks in online banking.[38] An April 2005 study conducted by Forrester reported that 74% of Canadian online consumers have concerns about e-mail fraud, a concern that is affecting their online financial behavior.[39] Another 2004 survey found that 80% of American, Canadian, German and British consumers are specifically concerned about identity theft and imposters accessing their online bank accounts.[40] Canadians who believe that there are serious risks associated with online banking are not likely to fully trust and take advantage of online banking services.

Consumers are more wary of online retail transactions, with 77% of respondents to PIAC’s survey stating that purchasing goods online is risky. Respondents generally felt that purchasing goods online was more risky than online banking.[41] In addition, respondents who felt there was a risk inherent in online retail transactions were more concerned about lost product or money than hackers. Some respondents also indicated that credit card fraud, identity theft and loss of personal information, and lack of security and security breaches were additional risks in the online retail arena.[42] A 2005 study found that Canadians were more

[37] Paul Roberts, “Gartner: Consumers Dissatisfied with Online Security: consumers feel passwords no longer enough protection for online transactions” (6 December 2004) IDG News Service, online: http://www.pcworld.com/article/118841/gartner_consumers_dissatisfied_with_online_security.html. According to the article, 60% of those surveyed were concerned about online security.

[38] In PIAC’s survey, 70% of respondents who indicated there was a risk in online banking stated that hackers posed a risk to online banking, compared to 16% who stated identity theft or loss of personal information and 11% who stated credit card theft or fraud. See Q12N.

[39] Forrester survey in April 2005, cited in Electronic Commerce Branch presentation, *supra* note 8.

[40] “Survey Finds Identity Theft Negatively Impacting Consumer Use of the Internet: Entrust Commissioned Survey Finds that Organizations That Take Steps to Protect Consumer Identity are More Likely to Attract New Customers and Online Users of Services” (19 October 2004) Entrust Security, online: http://www.entrust.com/news-archives/2004/archive2004_6026.htm.

[41] In PIAC’s survey, respondents were asked to identify the level of risk they associated with banking and purchasing goods online on a scale of 1 to 10, where 1 is not at all risky and 10 is extremely risky in Q10A and Q11A.

	1 (not at all risky)	2	3	4	5	6	7	8	9	10 (extremely risky)	Don’t know
Online banking (N=1503)	<1%	7%	19%	15%	15%	13%	15%	9%	4%	3%	1%
Purchasing goods online (N=1880)	<1%	4%	11%	12%	16%	13%	16%	17%	7%	4%	<1%

[42] In PIAC’s survey, respondents who indicated that online retail transactions were inherently risky were asked to identify those risks. 31% of respondents stated loss of product or money, 28% stated credit

concerned about security and privacy than Americans: 40% of Canadians avoided online shopping over security concerns, compared to 24% of Americans.[43]

The Privacy Commissioner of Canada has noted concerns with the trend of increased collection, use and “ever-expanding retention” of personal data. Increased collection of personal information seems to go hand in hand with data warehousing, matching, mining and profiling.[44] As data mining and profiling proliferate, these databases become valuable targets for online fraudsters and phishing attacks.

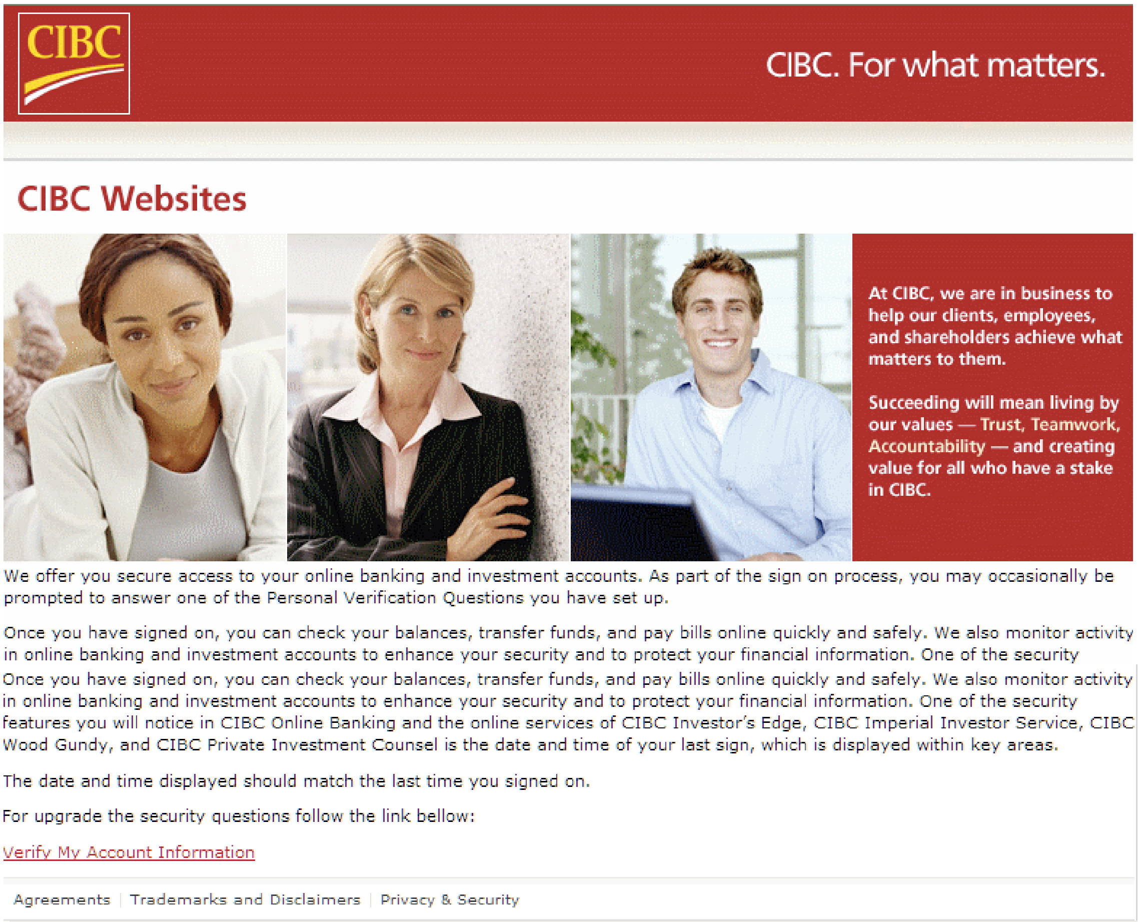
Phishing threats to authentication systems

Phishing is a new and growing online threat to e-commerce that directly targets authentication systems. Attackers attempt to fraudulently acquire a user’s personal information, such as username, password and credit card details by masquerading as a trustworthy entity in electronic communication. Often, this is accomplished by a “hook” and a “lure”. An e-mail “hook” is normally sent to the potential victim, and contains a warning intended to cause immediate concerns – such as a security upgrade, incomplete or out of date account information or recent account activity. The “hook” of phishing e-mails is increasingly convincing, such as requests for the user to update their security questions and verify account information. (Figure 1) The e-mail often appears to be from their financial institution and phishers take great care to replicate brands and security images so the e-mail seems authentic. The e-mail will also contain a link to the “lure,” a website that spoofs the real authentication system so that the user will input their account information, which is then routed from the fraudulent website to the fraudster without any indication of this diversion to the victim.

card theft or fraud, 26% stated identity theft and loss of personal information, and 9% stated lack of security, breaches or spyware. Other risks were also noted: 8% of respondents stated fraud and scams, 8% stated hackers. See Q13N.

[43] Canadian Alliance Against Software Theft (CAAST), November 2005 cited in Electronic Commerce Branch presentation, *supra* note 10.

[44] *Supra* note 1.



CIBC

CIBC. For what matters.

CIBC Websites

At CIBC, we are in business to help our clients, employees, and shareholders achieve what matters to them.

Succeeding will mean living by our values — Trust, Teamwork, Accountability — and creating value for all who have a stake in CIBC.

We offer you secure access to your online banking and investment accounts. As part of the sign on process, you may occasionally be prompted to answer one of the Personal Verification Questions you have set up.

Once you have signed on, you can check your balances, transfer funds, and pay bills online quickly and safely. We also monitor activity in online banking and investment accounts to enhance your security and to protect your financial information. One of the security

Once you have signed on, you can check your balances, transfer funds, and pay bills online quickly and safely. We also monitor activity in online banking and investment accounts to enhance your security and to protect your financial information. One of the security features you will notice in CIBC Online Banking and the online services of CIBC Investor's Edge, CIBC Imperial Investor Service, CIBC Wood Gundy, and CIBC Private Investment Counsel is the date and time of your last sign, which is displayed within key areas.

The date and time displayed should match the last time you signed on.

For upgrade the security questions follow the link bellow:

Verify My Account Information

Agreements | Trademarks and Disclaimers | Privacy & Security

Figure 1. An example of a phishing e-mail that appears to come from CIBC and requests the user to verify their account information and "upgrade" their security questions. Note the use of CIBC branding and images in order to bolster its authenticity.

Phishing is one of the fastest growing online threats, as Symantec reports that they observed 87,963 phishing hosts, which was a dramatic 559% increase in phishing web site hosts in 2007.[45] Financial services are the most targeted industry sector, accounting for the majority of attacks, followed by government e-services, retail websites and internet service providers.[46] An AOL Canada study

[45] Symantec, *Symantec Global Internet Security Threat Report: Trends for July-December 07*, Volume XIII, April 2008, online: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf at p. 70. In the second half of 2006, Symantec detected 13,353 phishing web site hosts, compared to 32,939 in the first half of 2007 and 87,963 between July 1, 2007 and December 31, 2007.

[46] There are conflicting statistics on the targets of phishing attacks. The Anti-Phishing Working Group reported that in December 2007, 91.7% of attacks targeted financial services, followed by 5.5% of attacks directed at government and 1.4% of attacks targeting retail. See Anti-Phishing Working Group, "Phishing Activity Trends: Report for the Month of December, 2007" online: http://www.antiphishing.org/reports/apwg_report_dec_2007.pdf. Symantec publishes different statistics, breaking down phished sectors by volume of phishing websites. According to Symantec, 66% of phishing websites were financial services, 18% internet service providers, 11% retail, 3% internet community, and 1% government. Despite the difference in statistics, it is clear that financial

found that nearly 1 in 3 Canadians received e-mail from a company purporting to seek confirmation of their account information.[47] The trend of increased phishing can be attributed to efficiencies gained by the availability and adaptability of phishing toolkits and the use of botnets.[48]

Phishing schemes are increasingly elaborate, as traditional indicators of forged websites are no longer easily detectable by regular web surfers – flaws in the trusted website's own scripts can be used against victims and fake security certificates are created. Phishing attacks continue to evolve. One phenomenon is the "contextual" phishing attempt, where the phisher takes advantage of publicly available information to profile and select potential victims. This technique increases the success ratio of phishing attempts and demonstrates the dangers of data warehouses and consumer profiling.[49]

Phishers also use "man in the middle" (MITM) attacks by infiltrating network lines to strategically position themselves between two communicating parties to glean information. Information intended for the legitimate site is passed to the attacker, who saves the valuable information, passes on the information to the legitimate site and forwards the response back to the user. The legitimate site appears to be working properly and the attacker now has the user's authentication information. MITM attacks have been used to defeat true two-factor authentication.[50]

Two recent examples demonstrate the need to re-examine the security and privacy of electronic authentication processes and consumer authenticators. A July 2008 University of Michigan study found that more than 75% of banks are vulnerable to cybercriminals because of website design flaws. The flaws could not simply be fixed by a patch, as they included placing authentication processes and contact information on insecure web pages and failing to keep visitors on the

services are the most popular target for phishing attacks. See also Symantec *Internet Security Threat Report*, *ibid.* at p. 66.

[47] "Identity Theft Rated Primary Online Security Concern Among Canadians" (29 March 2005) AOL, online: http://canada.aol.com/press/press_03_29_05.adp.

[48] Symantec *Internet Security Threat Report*, *supra* note 46 at pp. 71-73.

[49] For more information on spear phishing, see: "Spear phishing: Highly targeted phishing scams" (14 July 2008) Microsoft, online: http://www.microsoft.com/protect/yourself/phishing/spear.mspx.

[50] For example, Nordea Bank in Sweden encountered a MITM attack in October 2005 that defeated its Entrust OTP scratch card. Bank customers had been given a scratch sheet containing a number of hidden passwords so that as the customer used the service, it would uncover the next password in the list to grant access to the account. During the attack, the fake website complained about the user's entry and asked for the next password, in reality attempting to collect several scratch codes for its own use. In July 2006, Citibank encountered a MITM attack that defeated its Vasco OTP token. The token generated an additional password that changed every minute. The phishing site submitted the data provided by the user to the actual Citibusiness login site, using botnets to mask the IP address of the attackers. MITM attacks are increasingly easy to deploy, as universal MITM kits are made available on hacker sites for a sale price of $1000. For more information about MITM attacks, see TriCipher Solutions, "The Perfect Storm: Man in the Middle Phishing Kits, Weak Authentication and Organized Online Criminals" (18 February 2007), online: http://www.antiphishing.org/sponsors_technical_papers/TriCipherMITMWhitepaper.pdf.

site they initially visited.[51] Second, in July 2008, WestJet stopped using credit cards as an authenticator at their automated kiosks in Toronto Pearson Airport when credit card companies linked fraudulent activity to the use of credit cards to authenticate at self-serve kiosk machines at airports.[52] The WestJet incident demonstrates the importance of authentication design and the dangers of using sensitive personal information as authenticators. As phishing schemes continue to target authentication systems of financial services, increased caution and vigilance need to be exercised in the design and implementation of consumer authentication.

Widespread consumer adoption of authentication technology will only occur if individuals trust the strong privacy and security protections built into authentication systems.[53] Consumers need to be assured that authentication systems will continue to be effective in the face of new technology and evolving online threats such as phishing. At the same time, authentication systems should be consistent and user-friendly so they do not overly confuse or deter consumers from using their systems. These needs call for standards in electronic authentication that bolster consumer confidence in electronic authentication so that electronic commerce can achieve its full potential.

[51] Jennifer LeClaire, "More than 75 percent of bank sites at risk, study says" (24 July 2008) Newsfactor.com, online: http://www.newsfactor.com/news/Most-Bank-Sites-at-Risk--Study-Says/story.xhtml?story_id=1200044YQ0IO.

[52] Peter Kovessy, "WestJet shuts down credit card check-ins" (23 July 2008) Ottawa Business Journal, online: http://www.ottawabusinessjournal.com/292222276877641.php.

[53] *Supra* note 2.

PRINCIPLES OF ELECTRONIC AUTHENTICATION

History and context of the Authentication Principles

Industry Canada convened the Authentication Principles Working Group to study the issue of authentication in Canada, with broad representation from industry and professional associations, government departments and consumer groups.[54] The Working Group published *Principles for Electronic Authentication – A Canadian Framework* in May 2004 (Authentication Principles), which were designed to function as benchmarks for the development, provision and use of authentication services in Canada.[55] The Authentication Principles aim to foster a well-functioning, fair and competitive marketplace for authentication products and services. Applying broadly to all types of electronic communication between organizations and individuals, the Authentication Principles extend to the relationship between businesses and consumers.

The Authentication Principles form the basis of codes of conduct for businesses using authentication systems and are meant to be a self-regulatory and voluntary framework. The Authentication Principles do not address issues of consumer protection or liability. In 2004, it was assumed that legislative or policy measures would evolve to address the needs of end users, in particular the risk and liability assumed by consumers participating in authentication services.[56] Such measures have not been implemented.

The Authentication Principles are required to be reviewed every five years. In 2006, the Working Group reconvened to assess the need to update the Authentication Principles to address technological advances, marketplace development and new public policy pressures. In particular, the Working Group was to ensure the Authentication Principles applied to new authentication environments, to assess the need for additional policy instruments to underpin the Authentication Principles, and to explore their relationship to online identity management.[57] The Working Group last met in February 2007 and has not met since.

The Principles of Electronic Authentication

The Authentication Principles define authentication as “a process that attests to the attributes of participants in an electronic communication or to the integrity of

[54] See Authentication Principles document, *supra* note 3 at p.3 for a full list of participants on the Authentication Principles Working Group. A wide range of government, businesses, and industry sector associations participated in the discussions, including technology companies, financial institutions and banking associations, legal firms, accountants, VISA, consulting, telecommunications providers, and insurance companies. As well, PIAC participated in the Working Group.

[55] *Supra* note 3.

[56] *Ibid.* at p. 4 “How and Why to Use the Principles.”

[57] Industry Canada, “The Digital Economy in Canada: Electronic Authentication” online: http://www.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00090e.html.

the communication."[58] Participants include individuals and organizations who participate in the authentication process, whether directly or through another authenticated entity, such as a data service or object, hardware device, or software program. There are six general principles for electronic authentication.

Principle 1: Responsibilities of Participants

Participants in an authentication process should be aware of the functions they are performing and of the responsibilities associated with those functions. Participants' responsibilities are proportional to the degree of knowledge and control they can reasonably be expected to have and to exercise. This Authentication Principle requires participants to act prudently and take reasonable steps to inform themselves of the nature of the authentication process, including its requirements and limitations.

Principle 2: Risk Management

The risks associated with authentication processes for electronic communications should be identified, assessed and managed in a reasonable, fair and efficient manner. The Authentication Principles recognize that consumers cannot reasonably be expected to identify, assess and manage risk to the same extent as more experienced participants with more significant resources. A number of categories for risk are identified: immediate, direct and consequential financial risk and damage, loss of confidentiality or privacy, damages to reputation, and identity theft. Contracts can provide a framework for allocating risk. Principle 2 recognizes that some contracts are not freely negotiated among equal parties and thus efforts may be needed to protect the interests of weaker parties.

Principle 3: Security

All participants in an authentication process should be responsible and accountable for security, in proportion to their roles in that process. All participants have a responsibility to contribute to the mitigation of risk through sound security practices. However, infrastructure providers and those involved in authentication administration bear much of the burden to design and maintain systems based on policies and procedures that take into consideration legislation, regulation, policy, industry standards and the socio-cultural environment.

This Authentication Principle also emphasizes continual review and assessment of security programs to ensure the ongoing efficacy of a security program. As well, a periodic review of the security practices surrounding an authentication process should be conducted by an independent person.

Principle 4: Privacy

Organizations engaged in the design or operation of authentication processes should comply with the data protection standards set out in relevant codes of

[58] *Supra* note 3 at p. 7, "About the Principles: Concepts and Terminology."

practice (privacy codes) in addition to complying with applicable legislation and jurisprudence (privacy laws). In particular, the collection, use and disclosure of personal information in the context of authentication should be minimized. As well, personal information should be retained only for the purpose of authentication.

Principle 5: Disclosure Requirements

Participants that offer authentication services should disclose information to other participants to ensure that all participants are aware of the risks and the responsibilities associated with participation. The information disclosed should include policies, practices and procedures of authentication services, including information about whether the services are periodically reviewed or audited. Appropriate disclosure requires information to be provided in sufficient detail in plain language and conspicuously. The amount and nature of information disclosed should be sufficient such that participants can understand their responsibilities and make informed risk-management decisions concerning their reliance on the authentication. Where changes are made, participants should be notified.

Principle 6: Complaints Handling

Organizations implementing authentication processes should make available a complaints-handling process that enables participants to resolve complaints efficiently and effectively and to respond appropriately to non-compliance issues. Complaints-handing processes should be visible, accessible to all participants, responsive, fair and objective, free-of-charge to the complainant, confidential and private, accountable, and seek continual improvement.

Initiatives related to electronic authentication since 2004

Governments and consumer groups have undertaken several initiatives, both domestic and international, that are relevant to electronic authentication since the Authentication Principles were published.

International cooperative efforts to address authentication

There are a few international cooperative efforts for electronic authentication. The Article 29 Data Protection Working Party adopted a working document on online authentication services in January 2003.[59] The Working Party addressed the expansion of online authentication services, examining the case studies of the Microsoft .NET passport and the Liberty Alliance Project to highlight privacy concerns. As described above, if a user has a Microsoft .NET passport, they can use their e-mail address and password to authenticate for a variety of online services and retailer websites. The passport reduces the number of accounts a user needs to create by making more services accessible to a single authentication process. The Liberty Alliance Project is a global identity

[59] Article 29 Data Protection Working Party, *Working Document on on-line authentication services*, adopted on 29 January 2003, 10054/03/EN, online: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp68_en.pdf.

consortium of approximately 30 organizations with the goal of developing open technical, business and privacy standards for federated identity management. Their vision is to link devices and identities of all kinds by open federation and protected by universal strong authentication.[60] In examining the Microsoft .NET passport and the Liberty Alliance Project, the Working Party emphasized the need to respect the data protection principles of the European Data Protection Directive.[61]

In 2003, the Organisation for Economic Co-operation and Development (OECD) Working Party on Information Security and Privacy (WPISP) surveyed the legal and policy frameworks for electronic authentication services and e-signatures in OECD member countries. The survey found that virtually all OECD member countries have some form of legislative or regulatory framework in place to provide for the legal effect of electronic signatures. It was determined that WPISP should work to bridge legislative, legal and policy frameworks for cross-jurisdictional acceptance of authentication services and for the legal effect of electronic signatures.[62]

In June 2007, the OECD released their Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication.[63] The document was developed by the OECD Committee for Information, Computer and Communications Policy (ICCP) through WPISP. The OECD Guidance document lists a number of foundational principles for authentication:

(1) a systems approach focusing on overall system security;
(2) proportionality between responsibility and risk;
(3) all participants have roles and responsibilities;
(4) all participants are responsible for security and trust;
(5) compliance with OECD privacy guidelines; and
(6) risk management.

The OECD Guidance Document also lists a number of additional operational principles to guide the implementation of authentication systems:

(1) usability for individuals and organizations;
(2) security fits the purpose;
(3) business continuity to develop user confidence;

[60] For more information about the Liberty Alliance Project, see online: http://www.projectliberty.org/liberty/about/general_faq.

[61] European Union data protection website, online: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.

[62] Working Party on Information Security and Privacy, Organisation for Economic Cooperation and Development, "Summary of Responses to the Survey of Legal and Policy Frameworks for Electronic Authentication Services and E-Signatures in OECD Member Countries" (3 August 2004) DSTI/ICCP/REG(2003)9/FINAL, online: http://www.olis.oecd.org/olis/2003doc.nsf/LinkTo/NT0000730E/$FILE/JT00167912.PDF.

[63] Organisation for Economic Cooperation and Development, "OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication" (June 2007), online: http://www.oecd.org/dataoecd/32/45/38921342.pdf.

(4) education and awareness of the benefits and proper uses of authentication;
(5) appropriate disclosure of information to participants;
(6) efficient and effective complaints handling;
(7) independent audits and assessments;
(8) consistent standards and agreement to facilitate cross-jurisdictional approaches; and
(9) standards for coordinated implementation of authentication systems.

On the basis of the guidance document, the OECD Council made a Recommendation to foster the development, provision and use of electronic authentication products and services that meet participants' needs, in particular with respect to security and privacy of their information and identity.[64]

Canadian government initiatives regarding authentication

The United Nations General Assembly adopted the *Model Law on Electronic Commerce* in 1996.[65] This was the basis for the Canadian *Uniform Electronic Commerce Act* (UECA) in 1999, which is a model for provincial electronic commerce laws.[66] The UECA contains a series of rules based on the principle that electronic records are functionally equivalent to paper-based records and should have the same legal effect. Electronic contracts are considered legally valid and enforceable. As well, the UECA allows electronic signatures to fulfill the legal requirement for a signature. By its nature, an electronic signature could be used for authentication, but very few systems use them. The UECA has been implemented, in some instances with minor modifications, in all provinces and territories except for the Northwest Territories.[67]

As stated above, when the Authentication Principles were published in 2004, it was assumed that legislative or policy measures would evolve to address the needs of end users, in particular the risks and liabilities assumed by consumers who participate in authentication services. Few government departments have reviewed their relevant legislation and proposed frameworks for authentication to govern the delivery of online services in their area.

[64] *Ibid.* at pp. 11-12.

[65] *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment*, adopted in 1996, online: http://www.jus.uio.no/lm/un.electronic.commerce.model.law.1996/doc.html.

[66] *Uniform Electronic Commerce Act*, adopted by the Uniform Law Conference of Canada in September 1999, online: http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u1.

[67] Alberta: *Electronic Transactions Act*, S.A. 2001, c. E-5.5; British Columbia: *Electronic Transactions Act*, S.B.C. 2001, c. 10; Manitoba: *The Electronic Commerce and Information Act*, S.M. 2000, c. 32; New Brunswick: *Electronic Transactions Act*, S.N.B. 2001, c. E-5.5; Newfoundland and Labrador: *An Act to Facilitate Electronic Commerce by Removing Barriers to the Use of Electronic Communication*, S.N. 2001, c. E-5.2; Nova Scotia: *An Act to Facilitate Electronic Commerce*, S.N.S. 2000, c. 26; Nunavut: *Electronic Commerce Act*, S.Nu. 2004, c. 7; Ontario: *Electronic Commerce Act, 2000*, S.O. 2000, c. 17; Prince Edward Island: *Electronic Commerce Act*, S.P.E.I. 2001, c. 31; Quebec: *An Act to Establish a Legal Framework for Information Technology*, R.S.Q., c. C-1.1; Saskatchewan: *The Electronic Information and Documents Act, 2000*, S.S. 2000, c. E-7.22; Yukon: *Electronic Commerce Act*, R.S.Y. 2002, c. 66.

In September 2007, a Department of Finance facilitated working group discussions to expand the Debit Card Code to cover a broader array of electronic payments.[68] The Department of Finance developed a new code of conduct for electronic funds transfers (EFT). The new code is intended to be a voluntary code of practice for federally and non-federally regulated organizations involved in electronic funds transfers, covering face-to-face transactions, online debit transactions (not credit based, only asset based) and electronic banking. Electronic banking includes the use of debit cards, store valued cards, online and telephone banking. The code aims to set out the rights and responsibilities of all parties involved in EFT transactions in Canada, as well as standards to measure good practices to protect consumers and increase public confidence in EFT transaction methods. The Department of Finance anticipates that a final EFT code will be ready for adoption by December 2008.

Other government departments have published discussion papers on electronic authentication. The Office of the Privacy Commissioner of Canada released “Policy Scan: Survey of Identification and Authentication Issues in Canada” in February 2005 and “Guidelines for Identification and Authentication” in October 2006.[69] The Guidelines focus on authentication techniques between organizations and individuals, examining how organizations can authenticate customers in a way that respects the fair information practices in the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*).[70] Authentication systems must comply with the fair information practices in Schedule 1 of *PIPEDA* or the equivalent provincial private sector privacy legislation.[71]

Industry Canada has also produced documents on electronic authentication. In March 2006, they hired a consulting firm to assess market trends in authentication in e-commerce.[72] Their findings are referenced throughout this report. As well, the E-Commerce Branch of Industry Canada has prepared a paper to better understand digital identity management issues.[73] As mentioned above, identity management is beyond the scope of this report, though authentication issues lend themselves to a broader discussion about digital identity management. In particular, the E-Commerce Branch paper focused on the usability, privacy and security of digital identity management and what kind of

[68] Department of Finance, “Developing a Code of Conduct for Electronic Funds Transfers” (Discussion Paper, September 2007).

[69] *Supra* note 1 and *supra* note 7.

[70] 2000, c.5, online: http://laws.justice.gc.ca/en/frame/cs/P-8.6///en.

[71] Alberta: *Personal Information Protection Act*, S.A. 2003, c. P-6.5; British Columbia: *Personal Information Protection Act*, S.B.C. 2003, c. 63; Quebec: *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q. c. P-39.1.

[72] *Supra* note 25.

[73] Electronic Commerce Branch, Industry Canada, “Understanding and Addressing the Challenges of Online Assurances: Protecting and Managing Digital Identities in Canada” (Working Draft, November 2007).

governance structure could be implemented as digital identity solutions in Canada.

Consumer group comments about authentication

Consumer groups have participated by contributing to government consultations for their legislative reviews. PIAC participated in the Department of Finance consultation on the Code of Conduct for Electronic Funds Transfers, advocating for a broader consultation process and a new approach that did not rely solely on changes to the Debit Card Code. In addition, PIAC suggested legislation and regulation to support a voluntary code and recommended a number of foundational principles for an EFT framework.[74]

Civil society groups joined together as the Public Voice Coalition to contribute to the OECD Ministerial Meeting on the Future of the Internet Economy in June 2008. The Coalition published a background paper with recommendations and policy principles spanning a range of topics from fueling creativity in access to knowledge, the public domain, copyright and freedom of speech and convergence by interoperability, open standards and net neutrality. As well, the Coalition canvassed the topic of consumer and privacy protection and building confidence in the internet economy, specifically discussing identity management and authentication issues. According to the Coalition, "the failure of large-scale single sign-on services in the nineties has shown that citizens and customers are only accepting identification technologies and services if they are sure their privacy is respected at the same time."[75]

The Coalition suggests important elements for new authentication technology to ensure user privacy and security:

(1) Minimal disclosure: Identity and authentication systems must only provide the information that is needed for the actual transaction. For this, full anonymity must be the default option, and single information bits are then added consciously and sparingly. Regulation must ensure that data is not collected if it is not needed for the service in case.

(2) Non-Linkability: Digital identifiers have to be constructed in a way that they can not be linked across contexts and transactions, and allow context-sensitive pseudonyms. This will protect users from profiling and at the same time significantly shield against identity theft.

[74] PIAC, "Comments regarding the creation of a new framework for electronic fund transfers in Canada" (15 January 2008), online: http://www.piac.ca/financial/comments_regarding_the_creation_of_a_new_framework_for_electronic_fund_transfers_in_canada/.

[75] The Public Voice Coalition, "Civil Society Background Paper: Fueling Creativity, Ensuring Consumer and Privacy Protection, Building Confidence and Benefiting from Convergence" submitted to the OECD Ministerial Meeting on the Future of the Internet Economy, Seoul, Korea, 17-18 June 2008, online: http://thepublicvoice.org/events/seoul08/cs-paper.pdf at p. 29.

(3) Non-Traceability: Increasingly, online authentication towards third parties (like business and government agencies) is done by identity providers. Identification systems that are based on this model must ensure that the identity provider can not trace and track the services the user has used.

(4) User Control: All identifying information about an individual must flow through the individual's hands, and it must be readable by the individual. This concept of "user-centric identity" must become the basis for general identification and authentication systems in the public and private sector.

(5) Application to Government-issued Identity Tokens: The above-mentioned principles are especially relevant when moving towards government-issued identity tokens. Additionally, legislation must ensure that citizens can still use paper-based documents.

(6) Relationship Information Belongs to Both Parties: Social networking platforms have to take into account that information about a relationship belongs to both parties. Therefore, services allowing users to publish information about others as well as about relationships have to ensure this can only be done when both parties have agreed to it under the same conditions.[76]

Among other things, the Coalition recommended that OECD member countries implement the OECD Recommendations on Electronic Authentication and promote user-control and user-centricity in the development and deployment of identity management systems.

The Center for Democracy and Technology established an Authentication Privacy Principles Working Group to draft basic privacy principles that should be considered in the design and implementation of authentication systems in the United States.[77] The privacy principles are intended for companies to use as a guide in building privacy and security protections into authentication technologies for consumer-initiated transactions. There are six privacy principles:

(1) provide user control by obtaining informed consent before information is used for enrollment, authentication and any subsequent uses;

(2) support a diversity of services so that individuals have a choice of authentication tools and providers in the marketplace;

(3) use individual authentication only when appropriate, using identity information only when the information is needed to complete the transaction, that is, individual identity need not and should not be a part of all forms of authentication;

(4) provide notice through a clear statement about the collection and use of information so that individuals can make informed decisions;

[76] *Ibid.* at p. 30.

[77] *Supra* note 2.

(5) <u>minimize collection and storage</u> to only the information necessary to complete the intended authentication function; and

(6) <u>provide accountability</u> such that authentication providers are able to verify that they are complying with applicable privacy practices.

CRITICISMS OF THE AUTHENTICATION PRINCIPLES AND PROPOSED SOLUTIONS TO STRENGTHEN THE PRINCIPLES

The Authentication Principles fail to provide adequate protection for consumers. They are too broad to provide helpful guidance on authentication systems that respect consumer privacy and guarantee adequate security. The Authentication Principles lack sufficient specificity to increase consumer confidence in electronic authentication. In relation to present authentication systems, consumers have indicated that they feel vulnerable to the risks of identity theft, monetary fraud and loss of their privacy.[78]

There are three main gaps in the Authentication Principles: the failure to guarantee meaningful consumer security in authentication processes, vague privacy protection for consumers who use authentication processes, and the failure to provide consumers with certainty regarding who is liable in the event of loss from improper authentication. At the same time, authentication systems must be user-friendly so that online transactions are not overly cumbersome and allow the digital economy to strive for its full potential.

The Authentication Principles provide insufficient assurance of consumer security

Authentication Principle 3 addresses security. However, the security principle is drafted in a manner that is too vague to be meaningful. For example, the security principle does not provide organizations with specific guidance about how to provide secure authentication systems. The security of authentication systems must be proportional to their use – that is, the level of security must reflect the sensitivity or the nature of risk of the transactions that are available to the end-user following proper authentication. The Authentication Principles fail to provide guidance indicating how an organization might achieve appropriate proportionality to optimize security.

Multi-layer single-factor authentication is not always secure enough

On the internet economy, single-factor authentication is prevalent for business to consumer transactions. Millions of people manage their bank, PayPal and retail accounts online, which are almost all protected only by passwords.[79] Passwords are no longer safe authenticators, as it is easy to lose control of them. People choose passwords that are easy to guess, people write them down and passwords are easily intercepted. As people create more accounts with various online retailers and financial institutions, they are likely to use the same passwords so that they do not forget.[80] Fraudsters have begun stealing passwords through complex phishing attacks. If a fraudster captures a

[78] PIAC survey at Q22N.

[79] Bruce Schneier, “Customers, Passwords and Web Sites” (July 2004) IEEE Security & Privacy, online: http://www.schneier.com/essay-048.html.

[80] Shirley Gaw & Edward W. Felten, “Password Management Strategies for Online Accounts,” Symposium on Usable Privacy and Security (SOUPS) (Pittsburgh, PA: July 12-14, 2006), online: http://cups.cs.cmu.edu/soups/2006/proceedings/p44_gaw.pdf.

password, they may gain the capability to take over the victim's full online identity. Single-factor authentication is not sufficiently secure for all consumer financial transactions. Security expert Bruce Schneier suggests that passwords have reached the end of their useful life and only work for low-security applications.[81]

Multi-layer single-factor authentication systems are not much of an improvement to single-factor authentication, as they merely ask for more personal information. Financial institutions have started asking "security questions" such as "what is your mother's maiden name" and "what is your favourite colour" as an additional authenticator after the correct password is entered. The use of security questions is based on the assumption that privacy comes from the obscurity of our personal information and the difficulty others have in accessing in.[82] But the advances of internet communications and our networked society means that additional "security questions" do not strengthen authentication systems when much of the personal information required to answer security questions is more public than a password. Even worse, financial institutions seem to use the same series of secret questions.

Multi-layer single-factor authentication may be secure enough for low risk consumer transactions, but where authentication provides access to a range of financial transactions and highly sensitive financial information, multi-layer single-factor authentication is not sufficiently secure.

Out-of-band or two-factor authentication should be implemented to provide minimal security for highly sensitive B2C transactions, but still might not be strong enough

True two-factor authentication is currently used for some business-to-business transactions and real world consumer point-of-sale and ABM transactions in Canada. Two-factor authentication requires that the knowledge-based authenticator is supplemented or replaced by the other two categories. Most two-factor authentication systems currently rely on "what I have" factors, such as a debit card or a credit card. Until recently, few authentication systems have utilized the "what I am factor" which generally leads to biometrics.

As discussed above, financial services have introduced and are looking toward implementing authentication systems that rely on biometrics. There are numerous controversies concerning biometrics, and PIAC has discussed these concerns in detail elsewhere.[83] Besides the common concerns of the biometric being highly invasive and the questionable reliability of biometrics, it is far from clear that consumers are ready to accept widespread deployment of biometrics

[81] Bruce Schneier, "The curse of the secret question" (9 February 2005) Computerworld, online: http://www.schneier.com/essay-081.html.

[82] Bruce Schneier, "Does Secrecy Help Protect Personal Information?" (January 2007) Information Security, online: http://www.schneier.com/essay-168.html.

[83] *Supra* note 5.

for authentication by submitting voiceprints and iris scans as authenticators. Consumers should never be required to use a biometric to authenticate. Where biometric authentication systems are rolled out, there must be a non-biometric manner to authenticate the consumer that is at least equally and reasonably secure as the biometric authentication system.

While true two-factor authentication is used for payments in the real world, true two-factor authentication has not been widely implemented in online business-to-consumer transactions. Supplementing "what I know" factors with an additional category for internet-based transactions is not trivial. In particular, it may require consumers to procure and install readers as a peripheral to their computer. Despite these difficulties, the evidence increasingly suggests that two-factor authentication should be the minimum standard, especially for online transactions that involve highly sensitive personal and financial information such as banking and financial service transactions. Two-factor authentication can help mitigate the problem of static passwords.

One possible solution is the one-time-password (OTP), which can be provided to the consumer through a token or scratch card issued by the financial institution or retailer. The token would generate an OTP that would expire after the user has completed their transaction. PayPal has recently begun issuing security keys to their users for a $5 fee. Financial institutions around the world have been using OTP authentication but this has yet to be implemented in Canada.

Implementing two-factor authentication for online transactions will increase the security of consumer transactions that involve sensitive financial and personal information, but it is not a complete solution. While more secure than single-factor authentication, Schneier warns that two-factor authentication will not stop phishing and identity theft, as it merely "solves the security problems we had 10 years ago, not the security problems we have today."[84] Fraudsters will continue to modify their methods to overcome two-factor authentication. For example, OTP tokens or scratch cards do not protect against man-in-the-middle attacks, as the user will input the OTP into the attacker's fake website and the attacker will use it to access the bank's real website and display the results back to the user. The user may never realize that they were at a fake website, and the attacker will disconnect the user and make any fraudulent transaction that they want or pass along the user's banking transactions while making their own transactions at the same time.[85]

Another possible solution is providing OTPs or confirming authentication through a secure SMS text message or mobile phone.[86] This is an example of multi-

[84] Bruce Schneier, "Two Factor Authentication: Too Little, Too Late" (April 2005) Communications of the ACM, vol. 48, no. 4, online: http://www.schneier.com/essay-083.html.

[85] *Ibid.*

[86] Justin Stanford, "Gone phishing: protecting yourself and your business" (August 4, 2008) Bizcommunity.com, online: http://www.bizcommunity.com/Article/196/16/26979.html. See also discussions about out-of-band or multi-channel authentication, discussed by the Federal financial Institutions Examination Council, *supra* note 8.

channel or out-of-band authentication and is more secure than typical username and password authentication systems, even though out-of-band authentication may use a single factor. Out-of-band authentication may be a practical solution for consumers who have mobile phones. This solution offers increased security as it is unlikely that a phisher would have stolen or duplicated his or her phone. Out-of-band authentication need not always use mobile phones to confirm authentication. Other channels can be used, such as via e-mail or landline phones.[87] One advantage of out-of-band authentication is that it can result in stronger security without extra hardware. As well, because it confirms authentication via a different communication channel than the first step of authentication, it is much harder to eavesdrop through man-in-the-middle attacks.[88]

However, it is not clear whether out-of-band authentication would be widely accepted by consumers for online banking transactions. Additional research should be undertaken to assess the effectiveness and acceptability of these authentication technologies before they are implemented. Where offered, out-of-band authentication should not be imposed and must be offered as a choice to consumers, particularly for consumers who do not have mobile phones and customers who are not comfortable using their mobile phone for authentication purposes.

Deployment of two-factor or out-of-band authentication for online business-to-consumer transactions will require an investment into additional technology. As well, consumers may require OTP tokens or access to a mobile phone. OTPs can be cumbersome and expensive to implement, which is likely the reason they have not gained widespread use in business-to-consumer transactions in Canada.[89] If implemented, the costs associated with additional factors should be absorbed by the business or bank, as they should strive to guarantee their customers services that are as secure as possible.

The need for specific technical authentication standards

Authentication processes that are considered to be weak and provide little security to end-users should be deemed obsolete and should no longer be allowed for financial online transactions. Documented standards and protocols for the authentication industry would serve to indicate which authentication processes are too weak and therefore obsolete, identify authentication processes that are appropriate for low-risk transactions and suggest authentication processes that are secure enough for consumers' online financial transactions. These standards must be continually reviewed to respond to the changing online

[87] The American financial sector has been discussing the use of out-of-band authentication systems. See "Industry Round Table: Experts Discuss Improving Online Security" Scientific American (August 2008), online: http://www.sciam.com/article.cfm?id=industry-roundtable&page=4. In particular, see Sherstobitoff's first comment on that page.

[88] *Supra* note 84.

[89] *Ibid.*

threat landscape, as no authentication process is ever completely foolproof against hackers and phishing.

Authentication standards should promote strong authenticators that are non-linkable and non-traceable.[90] These authenticators should only be relevant in the specific context that they are generated for and should not be linkable across contexts and transactions. By ensuring that businesses cannot track or trace other services the consumer uses, the authenticator is stronger and the authentication system is more secure. Standards should promote the diversity of good authentication practices and diverse authenticators, such that consumers can choose what types of personal information they are comfortable with using as an authenticator. Consumers should always be able to manage their personal information in the manner they choose.

Avoid risk creep by constantly re-assessing authentication systems to reflect the level of risk

Finally, organizations must guard against adding extra layers of risk behind established layers of low-security authentication. This is often referred to as "risk creep." For example, many financial institutions provide an online portal so that consumers can access a range of services. Portal access relies on a multi-layered single factor authentication system, which asks for the account number and user password and may prompt for answers to "security questions." Initially, the online portal allowed users to check their account balance and pay bills. However, financial institutions have added more transactional capabilities to these online portals. Recently, RBC and TD Canada Trust added a feature through which a customer could use the online portal to transfer funds from their account to another person with a bank account at a participating financial institution via e-mail. However, the single-factor authentication process did not change to reflect the added risk that these transfers could pose. Thus, if an attacker were able to gain access to a user's financial service portal, they could transfer the balance of the user's account by e-mailing funds to their own e-mail address. The security of authentication systems must be strengthened as more financial transactions are offered by single sign-on online portals, thereby increasing the value of risk.

Need to clarify who is liable for losses – and it should not be consumers

With constantly evolving online phishing and hacking threats, there is no perfect protection against security breaches. When an organization experiences a security breach – be it an imposter successfully gaining access into a customer's account or a hacker accessing a personal information database – consumers may experience a range of losses. In particular, a customer may experience identity theft, monetary loss or fraud, or loss of privacy.

[90] *Supra* note 75 at p. 30.

Historically, the fundamental principle of loss allocation for payment systems was that the burden of unpreventable losses should rest with the provider of the payment system rather than with the users of the payment system. This principle was established in the old English case of *Price v. Neal*, which precluded a payor bank from any recovery when it paid a check bearing the forgery of the drawer signature.[91] Thus, where a customer's signature is forged, the loss rests with the payor bank rather than with the bank's customer. Loss apportionment has also been discussed in the development of the new Code of Conduct for Electronic Fund Transfers that changes the 1992 Debit Card Code.

Use of standard form contracts to make liability of organizations unclear

One trend of concern is the use of standard form contracts by businesses and financial institutions to confuse the issue of who bears the liability for losses when they occur. As these organizations institute new security and authentication measures, they use contracts to force consumers to agree to vaguely worded clauses that might limit the organization's liability to nominal dollar amounts.

Businesses and financial institutions require the consumer to agree to their terms and conditions in order to complete their transaction. These contracts are often long and contain clauses in legal language printed in fine print such that most customers will not bother to read in its entirety. Even if a customer did read the contract, most clauses are worded vaguely and they may not fully understand the extent to which the organization has contracted out of liability in the event of loss.

For example, Visa card issuers send all of cardholders a cardholder agreement. For example, buried in a lengthy Canadian Visa card issuer cardholder agreement under "Personal Identification Number and Other Security Features" is a "Zero Liability Policy" which promises that:

> … you will not be responsible for charges to your Visa Account as a result of the fraudulent and unauthorized use of your Visa Card, Visa cheques or Visa Account number, provided that you take reasonable steps to protect your Visa Card and Visa cheques against loss or theft and safeguard your PIN and other security codes in the manner set out in this Agreement or as we may otherwise advise you from time to time.

The agreement goes on:

> You will however remain fully liable for all charges if you voluntarily disclose your PIN or other security code or otherwise contribute to the unauthorized use of your Visa Card or access to your Visa Account, or fail to tell us in a reasonable time that your Visa Card or Visa cheques have been lost or stolen or that someone else may know your PIN or other security code.[92]

[91] 3 Burr. 1354, 97 Eng. Rep. 872 (K.B. 1763). See also James S. Rogers, "The Basic Principle of Loss Allocation for Unauthorized Checks" (2004) Boston College Law School Faculty Papers, Paper 10, online: http://lsr.nellco.org/bc/bclsfp/papers/10.

[92] RBC Royal Bank, "RBC Royal Bank Visa Agreement," received July 2008.

Earlier in the agreement, a clause stipulates that “no one but you is permitted to know or use your PIN or any other security codes such as passwords, access codes and account numbers that may be used or required for Internet or other transactions. You must keep these security codes confidential and separate as well.” Furthermore, “you” is defined to exclude Authorized Users unless otherwise indicated, who are not indicated in the section of the agreement discussing liability.

It is not clear what are “reasonable steps” expected of the cardholder to protect their Visa Card and associated PINs and passwords, particularly given the increasingly sophisticated phishing and fraud threats that exist on the internet. If a cardholder unknowingly discloses their PIN or password to a phisher who then incurs unauthorized Visa charges, it is not clear how her actions will be judged as reasonable. It must be clear what “reasonable” steps Visa expects their customers to take when participating in e-commerce: whether customers are expected to encrypt their traffic, check for security features and the domain name on a website before inputting their passwords. In the current threat context, phishing occurs when a customer is tricked into giving their password to a spoof of a retailer or bank’s authentication system. Given that phishing replicates weak authentication systems and attempts to deceive customers, consumers should not be responsible for losses that occur when they are victims of phishing.

Additionally, consumers are unable to negotiate the terms of many online financial transactions, as they are forced to agree to standard form terms and conditions in order to complete their transaction. Businesses and financial institutions who limit their liability to zero in the event of fraud and phishing by attaching these terms as a condition of transactions are unfairly taking advantage of consumers who want to participate in the electronic commerce marketplace. If consumers were to take on liability for losses occurring from fraudulent transactions and weak authentication systems, then this should be based on consumer choice and informed consent. However, the allocation of liability to consumers has not been fully or adequately communicated to consumers, especially when liability clauses are printed in a lengthy and legally-worded contract. The allocation of liability in the event of loss must be clear to consumers by providing clear and unmistakable notice, at minimum highlighting these clauses within the contracts to bring attention to them.

Externalizing costs

Simply because electronic commerce has led to increased fraud is not enough reason to justify a shift in the burden of loss from banks and businesses to consumers, who are often at the mercy of whichever authentication system a business chooses to implement and in a vulnerable position as they are unable to negotiate standard form contracts and terms of service. Modern consumer protection laws must respect the historical check rule, meaning that banks and retailers must bear the burden of responsibility for unpreventable losses in relation to modern authentication systems, and not pass this burden on to the users of their services. Banks and retailers should not be able to shift the liability of losses from businesses to consumers by instituting an authentication process that consumers do not want or agree to. Banks and retailers must be liable whenever they collect and use personal information for authentication and when providing their goods and services to consumers.

Information technology security experts have lashed out at the idea that end-users should bear some liability for losses that occur as a result of online banking fraud.[93] Schneier suggests that vendors must be liable for the security flaws of their system. According to Schneier, authentication security is an economic problem as the organizations we trust to protect our personal information do not suffer when information gets exposed, whereas individuals who suffer when their personal information is exposed do not have the capability to protect that information.[94] Instead of spending the money to improve and implement secure software, money is spent to deal with the effects of insecure software. In economic terms, this is an externality: a cost of a decision that is borne by people other than those making the decision. Schneier advocates for software vendors to be liable for security vulnerabilities in their products and financial institutions that are liable for fraudulent transactions.[95] Not only are these parties in the best organization to mitigate the risks, but once banks, retailers and software vendors are liable for security vulnerabilities in their authentication systems and online services, CEOs will have an incentive to fix the problem and protect consumers against fraudulent transactions.

A legislated requirement on banks and retailers to cover losses arising from weak authentication systems will be an added incentive to ensure that their authentication systems protect the privacy of their customers. This would align with the 2001 Principles of Consumer Protection for E-Commerce to protect consumers from unfair liability by providing equivalent protection.[96]

Furthermore, legislation concerning liability for losses would provide certainty for consumers who wish to make online financial transactions, which would help combat what Industry Canada calls the consumer "FUD" factor – fear, uncertainty

[93] Karen Dearne, "Banks liable for net fraud – experts" (May 8, 2007) Australian IT, online: http://www.australianit.news.com.au/story/0,24897,21688968-15317,00.html. The idea that consumers should bear some liability for losses caused by security breaches to home PCs was raised by the Australian Securities and Investments Commission review, despite bank awareness that the home PC was not designed to perform secure transactions. IT experts remarked that there was a substantial increase of malware exploits designed to steal online banking credentials, meaning that "a user's computer may be compromised despite their best endeavours to keep their software and security up to date."

[94] *Supra* note 82.

[95] Bruce Schneier, "Information security: How liable should vendors be?" (28 October 2004) Computerworld, online: http://www.schneier.com/essay-073.html. See also Bruce Schneier, "Make Businesses Pay in Credit Card Scam" (23 June 2005) New York Daily News, online: http://www.schneier.com/essay-086.html.

[96] Consumer Protection in E-Commerce Working Group, *Principles of Consumer Protection for Electronic Commerce: A Canadian Framework* (August 1999), online: http://cmcweb.ca/epic/site/cmc-cmc.nsf/en/fe00113e.html at Principle 6.

and dread – in response to e-commerce.[97] Additionally, such legislation would align with consumer expectations. In PIAC's survey, an overwhelming majority of consumers responded that banks and retailers should bear responsibility for losses that arise from unauthorized transactions.[98] Consumers still thought that even if banks and retailers implemented true two-factor authentication, these organizations should continue to bear responsibility for losses arising from unauthorized transactions.[99]

The Authentication Principles fail to adequately protect consumer privacy

Security breaches threaten users' financial and personal information. No matter how secure an authentication system, fraudsters will continue to adapt their methods to gain access to valuable financial and personal information. Security breaches will continue to occur and accordingly, the damage flowing from these breaches must be mitigated. By prioritizing consumer privacy, less harm would result from security breaches related to the authentication process.

Review Authentication Principles to integrate fair information practices in *PIPEDA*

Authentication Principle 4 addresses privacy in general, stating that organizations who design and implement authentication processes should comply with data protection standards and *PIPEDA*. However, the Authentication Principle fails to tie in corresponding sections of the *PIPEDA* fair information practices. While the Office of the Privacy Commissioner of Canada's (OPCC) "Guidelines for Identification and Authentication" are useful to businesses that are implementing authentication systems for their customers, they fail to bridge the gap between the Authentication Principles and *PIPEDA*. Besides espousing general privacy practices, the only instance in which the OPCC Guidelines cites *PIPEDA* is when the Guidelines state that authentication should be consistent with Principle 4.4 in *PIPEDA* that the "collection of personal information shall be limited to that which is necessary for the purposes identified by the organization."[100]

The Authentication Principles fail to provide specific links to privacy law and privacy safeguards for consumers who use authentication. Though Authentication Principle 4 proposes the development of authentication standards in accordance with privacy laws and codes, these standards have not yet been discussed. Beyond reviewing the Authentication Principles to integrate specific

[97] *Supra* note 25.

[98] In PIAC's survey at Q14, 87% of respondents believed that the bank or retailer should bear the loss if their user account was accessed without permission. 12% of respondents stated that responsibility for the loss should be shared between the account holder and the bank or retailer.

[99] In PIAC's survey at Q15, 75% of respondents believed that the bank or retailer should bear the loss if their user account was accessed without permission where two factor authentication was used. 20% of respondents stated that responsibility for the loss should be shared between the account holder and the bank or retailer.

[100] *Supra* note 7.

PIPEDA fair information practices, standards that address consumer privacy concerns must be created.

<u>Minimize the collection of personal information and monitor compliance with the prohibition of its secondary use</u>

The Authentication Principles suggest that the collection of personal information should be minimized. Specifically, institutions that use authentication systems should only collect the information necessary to complete the intended authentication function.[101] Consumers have stated that they sometimes cancel purchases when too much personal information is collected, as they have identity theft and fraud concerns.[102] *PIPEDA* requires organizations to minimize the collection of personal information to what is necessary for purposes identified by the organization. However, the minimization of personal information collection for authentication is narrower than *PIPEDA*'s requirements.

Under *PIPEDA* Principles 4.5 and 4.3.1, the secondary use of personal information that has been collected is prohibited unless the individual's consent is obtained or the use is encapsulated under subs. 7(2). Thus, the secondary use of personal information collected for authentication is prohibited. The prohibition on secondary use can protect consumers in three important ways. First, organizations will not be able to profile or track their users through their authenticators, thereby enhancing consumer privacy. Second, user security is also enhanced when authenticators are non-linkable and non-traceable.[103] Restrictions on secondary use of authentication information will not stop phishing, but could make aggregated databases of authentication information less valuable to hackers. Finally, consumers gain confidence in authentication systems when they know that organizations are not using the personal information collected for authentication for other purposes. Consumers should not be forced to accept the sharing of personal information for secondary uses as a condition of utilizing the authentication system.

Given that secondary use of personal information is currently prohibited under Canadian law, the issue then is that there is a lack of compliance with the prohibition. Personal information is often used by organizations to profile their customers, which can result in more spam, direct mail and telemarketing for individuals, often with the claim that this personal information enables

[101] *Supra* note 2 at Principle 5.

[102] In PIAC's survey at Q21, 29% of respondents stated that they had cancelled a purchase attempt or online banking session. When asked why they were uncomfortable at Q22N, 29% stated that they were uncomfortable because of identity theft or too much information being collected, 20% stated they were uncomfortable due to an unsecured site or hackers and 11% stated that they did not trust the seller, retailer or vendor.

[103] *Supra* note 75 at p. 29.

commercial organizations to "leverage their relationships" to realize new revenue and cost saving opportunities.[104]

Finally, certain sensitive personal information should only be used as authenticators in very limited situations. For example, some financial institutions have discussed the use of customer IP addresses as an authenticator, though this will be more difficult with the use of dynamic IP addresses. IP addresses should rarely be used for authentication purposes, as IP addresses may lend themselves to user tracking and profiling in the future.

Increased consumer choices in the authentication process to reflect the user's privacy preferences

Where possible, consumer choice should be strongly promoted in the authentication process. There are three important areas of consumer choice. First, for essential and widely performed commercial transactions, consumers should be able to choose to authenticate for the transaction in-person. Second, for single sign-on service portals, particularly for those that deliver financial services, consumers should be able to choose which services they want active or de-activated after assessing their level of comfort with the service portal's authentication system. Finally, consumers should be able to choose which pieces of personal information they wish to use as authenticators, if any.

While authentication may be a condition of completing certain transactions, authentication through an online system should never be required as a condition of service, particularly for essential services such as those provided by financial institutions. The option to use paper-based documents must be retained as a valid and significant option as more financial services move online.[105]

As mentioned above, risk creep is of particular concern, as more financial services are added to online portals, such as e-mail funds transfers, which can increase the value of risk for a consumer.[106] When transaction options are added to online service portals, the consumer's continued use of their online account is deemed to be consent to the terms of the added services. Consumers

[104] Electronic Privacy Information Center, "Comments on the FTC Consent Order on Microsoft Passport", FTC File No. 0123240, M03 (9 September 2002), online: http://epic.org/privacy/consumer/microsoft/ordercomments.html.

[105] *Supra* note 75 at p. 29.

[106] For example, online banking previously only allowed customers to check their account balance and pay bills online. If an attacker were to gain unauthorized access to the customer account, they would not have any options to move money around, other than making bill payments for the customer or collecting financial information about that person for use elsewhere. Then account transfers were introduced, where the customer could use their online account to transfer funds to the account of another customer with the same financial institution. With the introduction of e-mail fund transfers, a customer can use their online account to e-mail funds to any valid e-mail address, whereupon the recipient can deposit the funds into their own account with a participating financial institution. Arguably, someone with unauthorized access into a customer's online banking account can now e-mail funds to an e-mail account, which are easy to set up. When banks add new features to their online portals, there may be an increase in the value of risk for online banking customers.

must be able to choose – by opt-out or preferably by opt-in – which financial services they want enabled in their individual online bank account portal. This way, they are able to assess their level of comfort with their bank's online authentication system and activate the services that reflect their perceptions of risk and security. By giving consumers meaningful consent and control over their personal information and online accounts, increased trust will be built in authentication and online banking.[107]

Finally, consumers should have the choice of what personal information to provide as authenticators. The informed consent of the consumer must be obtained before their personal information is collected for authentication and other subsequent uses. For example, if biometric authentication systems are implemented as discussed earlier in this paper, consumers must be able to choose not to provide their biometrics as authenticators without losing access to these services. When consumers can exercise choice over what personal information to provide as authenticators, they retain control over their personal information and can act in ways to best protect their own privacy against the threats they perceive to be most risky.

Databases should be purged regularly such that personal information is not retained longer than necessary

The Authentication Principles state that personal information provided solely for authentication purposes should be retained only for such purposes. A retention policy should be mandated that specifies that organizations shall not retain personal information that is collected for authentication purposes longer than necessary and shall destroy and purge their databases regularly, including user data stored on back-up systems.[108] By limiting the storage of personal information used for authentication to what is absolutely necessary to perform the authentication, consumer privacy is further safeguarded.

Furthermore, consumers should be provided with the option to delete their accounts if they do not plan to have an ongoing relationship with an online retailer. Schneier supports this, suggesting that customers should be able to terminate their accounts and delete their usernames, passwords and whatever personal information was collected and stored in the account such that their financial information is no longer retained by the company.[109] These online retailers should also regularly destroy and purge their databases of terminated account information.

Privacy-enhancing technologies in a more secure networking environment

Ontario Information and Privacy Commissioner Ann Cavoukian is a strong proponent of privacy-enhancing technologies (PETs). She states that reduced

[107] *Supra* note 2 at Principle 1.

[108] *Supra* note 104.

[109] Bruce Schneier, "Authentication and Expiration" (January 2005) IEEE Security & Privacy, online: http://schneier.com/essay-079.html.

privacy should not be the trade-off to increased security. The new digital ecosystem relies heavily on "cloud computing," internet-based computer technology that allows users to access technology-enabled services without knowledge or expertise in how to control the technological infrastructure that supports these services. "Cloud computing" is a concept that incorporates technological trends such as software as a service and "Web 2.0." With the advance of "cloud computing," privacy and security concerns that accompany practices such as storing sensitive personal information in databases and scattering software around the internet must be addressed while providing flexible, user-friendly ways to authenticate users.[110]

One way to promote consumer privacy in the cloud is to encourage the use of anonymity and pseudonyms when actual names or links to a physical identity are not necessary. For example, for online retail transactions where low-cost goods are exchanged for payment, consumers should be able to complete the transaction anonymously, like a cash purchase transaction in the offline world. This would require the verification of the customer's ability to pay, as opposed to requiring the customer to authenticate and choose a payment method that also requires further confirmation of the customer's identity. For more complex transactions, PETs such as an authentication token present an encrypted form of a user ID to the service provider, allowing the consumer to appear anonymous. However, it would be possible to reveal the true identity of the user if there was a need for investigation by a designated authority upon which there would be strong restrictions and conditions.[111] Allowing the use of pseudonyms and multiple discrete but valid identities protects consumer privacy.

The Authentication Principles must mandate full public disclosure and consumer education

Consumers should be able to decide for themselves whether they are comfortable and confident in the security of authentication processes. They will only be able to evaluate authentication processes if the implementation of these processes is transparent. There are five components: 1) notify consumers when a service is added to the portal offerings behind the initial authentication process or when stronger authentication process is implemented; 2) indicate what personal information is collected in order to authenticate customers before requiring consumers to sign up for an account; 3) full disclosure of authentication audits performed by independent auditors and the organization's compliance with authentication standards; 4) a positive obligation on organizations to notify their customers when their authentication system is affected by a security breach; and 5) visible consumer education explaining how users can effectively protect their privacy when using the institution or service's specific electronic authentication processes.

[110] Ann Cavoukian, "Privacy in the Clouds: A White Paper on Privacy and Digital Identity: Implications for the Internet" (28 May 2008) Information and Privacy Commissioner of Ontario, online: http://www.ipc.on.ca/images/Resources%5Cprivacyintheclouds.pdf at p. 6-7.

[111] *Ibid.*

Notify consumers when the authentication system is changed, services are added to the portal or the terms and conditions change

When a bank or retailer makes changes to their authentication system, clear and visible notification should be provided to their current and new users detailing the changes and how they affect user security and privacy. As well, users should have the ability to opt out of the changes or discontinue their account if they do not feel comfortable with the changes to the authentication system.

As discussed earlier in this report, there is the potential for "risk creep" when banks add on financial services to the online portal that their consumers use for online banking. When services are added to a portal of financial services, banks must notify consumers about these services. Additionally, consumers should have the option to deactivate or opt out of these added financial services. Ideally, customers would be able to opt-in to added financial services. This is especially important for consumers to have a meaningful opportunity to gauge whether they feel the added services increase their risk and whether they are comfortable that the level of security of the authentication process will protect them against their perceived risk. These are valid concerns, especially given that banks often do not adjust the security of their authentication systems to reflect the risk level of added financial services.

Make information available before requiring user to create an account

The informed consent of the consumer should be obtained before information is collected for authentication purposes.[112] Often, consumers are asked to create an account and authenticate in order to complete their orders, without information on what information will be required for payment and future authentication. Online banks and retailers should explain the authentication process before asking consumers to create accounts. A web page about the authentication process used to verify accountholders and further authentication that may be required for certain methods of payment should be displayed to the consumer before the consumer is required to sign up for an account. This way, the consumer can make an informed decision about whether this retailer has sufficient security and privacy practices before creating an account to complete a purchase.

Full public disclosure of audits and compliance reviews

Authentication Principle 3 (security) suggests continual review and assessment by persons independent to the authentication process. As well, Authentication Principle 4 (privacy) suggests the performance of privacy compliance. There should be a positive requirement on banks and retailers to fully disclose the results of the audits and assessments performed on their authentication systems to consumers. Public scrutiny improves security and allows consumers to accurately assess their own risk. Secrecy precludes public debate about security

[112] *Supra* note 2 at Principle 1.

and inhibits security education that leads to improvements.[113] Audits and assessments should be made by a "qualified, objective, independent third-party professional."[114] By providing audit information to the public and ensuring its visibility and accessibility on their webpage, organizations can promote public confidence in their authentication system.

For privacy requirements, the Office of the Privacy Commissioner of Canada already has adequate audit powers under *PIPEDA*. Legislation would be required to allow a federal regulatory body such as the Office of the Superintendent of Financial Institutions Canada (OSFI) to audit financial institutions on this basis. Provincial audit requirements likely would be required for audits of major retailers. Further consultation with stakeholders in the financial and retail environments (including retailers, the Retail Council of Canada, the Canadian Marketing Agency (CMA), provincial consumer protection authorities and consumer groups) should be undertaken in pursuit of this goal (likely in combination with discussions on consumer education – see below).

Security breach notification

There is currently no law in Canada that requires organizations to notify affected customers when their authentication systems or personal information databases are compromised. Security breach notification legislation should be implemented and should specifically address security breaches in authentication systems. When an authentication system is compromised or an organization's database containing consumer personal information is stolen, consumers should be informed of the extent of the security breach and the nature of the compromised information so that they can monitor their accounts for suspicious activity and make appropriate changes to their online habits. If organizations are required to report the nature and extent of security breaches to their customers, they will have an incentive to ensure their systems are secure and avoid the public relations mess. The merits of security breach notification have been addressed in great detail by PIAC and others elsewhere.[115]

Consumer education

Consumers must be educated about how to properly use authentication systems in order to maximize their security and protect their privacy. A fact sheet for consumers on authenticating for financial services should be produced by a

[113] Bruce Schneier, "Full Disclosure of Security Vulnerabilities a 'Damned Good Idea'" (January 2007) CSO Online, online: http://schneier.com/essay-146.html.

[114] *Supra* note 104.

[115] See PIAC Media release, "Data Breach Notification Proposal is Carte Blanche for Business Data Spills" (25 April 2008), online: http://www.piac.ca/privacy/data_breach_notification_proposal_is_carte_blanche_for_business_data_spills. See related paper: PIAC, "Submission to Industry Canada Following the Stakeholder Consultation on the Proposed Model for Data Breach Notification" (25 April 2008), online: http://www.piac.ca/files/piac_submission_to_ic_re_pipeda_2008_apr_25_08.pdf. See also the Canadian Consumer Initiative Identity Theft Policy Position (1 February 2005), online: http://www.piac.ca/financial/canadian_consumer_initiative_identity_theft_policy_position.

central agency, such as the Financial Consumer Agency of Canada (FCAC), and promoted by banks and financial services that require their consumers to authenticate. Such a fact sheet would explain good authentication practices in clear non-technical terms, detailing important practices that individual users can easily adopt, such as how to select strong authenticators and how to protect account information and user privacy. In addition, a fact sheet explaining online threats such as phishing to internet consumers would be extremely useful. The fact sheet should show consumers what security features to look for during an authentication process and demonstrate typical methods that phishers use to trick consumers into giving away sensitive passwords and personal information. These fact sheets should be made available in bank branches and websites and on the FCAC website.

Regarding retailers, the Retail Council of Canada, the Canadian Marketing Association (CMA), provincial consumer protection authorities and consumer groups could attempt to draft similar consumer information, in consultation with the FCAC and Industry Canada.

Beyond a general information fact sheet about authentication, financial institutions and online retailers should also provide their customers with specific information regarding the security features of their authentication system in understandable terms. For example, a positive requirement could be placed on banks to inform their customers about authentication security and privacy practices through a regulation in the *Bank Act* and amendments to provincial consumer protection or electronic commerce acts could make similar requirements for online retailers.

As well, financial institutions should make special educational efforts to counter phishing strategies. Financial institutions could make their policies on how they contact their customers very clear so that phishing threats can be correctly identified and avoided by consumers. For example, financial institutions should clarify the circumstances in which they might contact a customer by e-mail and what a customer can do to verify that the e-mail did originate from the bank. A list of situations that the financial institution will never e-mail to their customer should be made equally clear: i.e. the bank will never request that the user update their account information, provide their password or PIN, or update their security questions (such as in Figure 1) by clicking on a link provided in the e-mail.

Consumers are not guaranteed protection in a voluntary framework: the need for a better regulatory framework to address electronic authentication

Though the Authentication Principles represent a collaborative effort of industry associations, government departments and consumer groups, a voluntary electronic authentication framework fails to adequately protect consumers. In particular, there are no incentives to encourage businesses to implement more secure or better privacy-respecting authentication systems. As the implementation of better authentication systems is generally more expensive, it remains more cost effective for businesses and banks to implement weaker authentication systems and deal with losses that might arise later. As well, the principles are voluntary and thus there is no mechanism through which consumers can seek compliance or redress.

Regulating banks and financial services

One of the ways to regulate authentication is through sectoral regulation. Banks are regulated federally under the *Bank Act*.[116] Because banks host a vast collection of individuals' sensitive financial information, they should be subject to stricter authentication regulations. Consumer security when authenticating fo transactions with financial institutions would be enhanced by inserting authentication standards into the *Bank Act*. For example, single-factor authentication should never be enough for banking transactions in the real world. Moving online authentication beyond single-factor authentication is a challenge, but potential solutions to strengthen online authentication include out-of-band authentication using multiple channels or two-factor authentication using OTP tokens. Two-factor authentication generally provides increased security, but discussions that lean toward biometric authenticators must consider the broader implications of biometrics. Because of the controversies surrounding the reliance and invasiveness of biometric authenticators, biometrics should be avoided and if used, consumers should be able to choose whether they wish to provide biometric information for authentication.

In addition, the *Bank Act* should be modified to clarify the extent to which consumers bear liability for losses that may result from unauthorized authentication. As discussed above, it is unclear what "reasonable steps" consumers are expected to take to protect their accounts from unauthorized authentication. Further clarity could be provided in *Bank Act* regulations and should also require financial institutions to draw consumer attention to the clauses in lengthy standard for contracts that explaining liability.

Clear mechanisms must be implemented for consumer recourse when they encounter weak security or privacy breaches related to authentication systems. The FCAC should issue guidelines for the handling of consumer complaints about authentication systems of federal financial institutions. Authentication problems must be addressed in a fair, timely, effective and affordable manner. Currently, when consumers have complaints with their banking institution, they can complain directly to their bank and the Ombudsman for Banking Services and Investments and follow up with the FCAC if their issue remains unresolved. Thus, authentication issues with online banking services should be pursued through the Ombudsman for Banking Services and Investments and if necessary,

[116] 1991, c. 46, online: http://laws.justice.gc.ca/en/ShowFullDoc/cs/B-1.01///en.

FCAC. However, FCAC does not currently have any legal power to settle consumer complaints.[117]

A drawback on the reliance on amendments to the *Bank Act* and FCAC is that customers of credit unions and *caisses populaires* will be without protection and recourse. This may be especially problematic in Quebec, British Columbia and the Prairie provinces, where credit unions and *caisses* have significant market share.

Regulating retailers and payment systems

Regulating authentication in the retail sector is much more challenging, given that the retail industry is under provincial jurisdiction and it is unlikely that provinces would implement laws to regulate authentication for the retail industry within the province. The challenge is compounded by the fact that there is a range of different retail scenarios, such as small retailers to large corporate entities. As well, there are a variety of retail transactions that may require authentication, such as a purchase of goods or payment for services, a return or a refund. Because consumer retail transactions are generally less sensitive than banking transactions, regulation of authentication in the retail industry need not be as strict as regulation of authentication in the financial services sector.

Given the challenges associated with regulating authentication in the retail sphere, the impetus to improve authentication in retail may have to rely on inspiration drawn from strong regulation for authentication in the financial services industry. If financial institutions institute more secure authentication systems for online transactions such as OTP tokens and out-of-band authentication, payment systems such as Visa and MasterCard may be inclined to follow and thus these authentication standards would move into e-commerce.

While FCAC may be in a position to deal with consumer complaints about authentication, no similar body exists for retail companies. The CMA might be the best enabled agency to deal with consumer complaints regarding the retail authentication systems of its members. As well, provinces may have better suited entities to respond to consumer complaints regarding online authentication systems, as many e-commerce laws are within the provincial jurisdiction.

Finally, the FCAC should compile statistics on the number of complaints that are made about authentication systems. The Ombudsman for Banking Services and Investments should also inform the FCAC of its complaints numbers in relation to authentication systems at federal financial institutions. This could simply be an additional ledger in their present complaints tracking system. By tracking the number of complaints that are specific to authentication, consumers, academics and policymakers can get a better grasp on the scope of consumer authentication experiences and analyze authentication trends.

[117] *Financial Consumer Agency of Canada Act*, 2001, c. 9, online: http://laws.justice.gc.ca/en/ShowFullDoc/cs/F-11.1///en.

Overarching privacy legislation for authentication issues

The Office of the Privacy Commissioner of Canada (OPCC) and the provincial information and privacy commissioners could be mandated to oversee authentication practices. The privacy commissioners are best suited to adapt their requirements to regulate authentication practices. In particular, the OPCC would oversee all financial institutions and the retail organizations operating within a province that does not have provincial private sector privacy legislation. In Alberta, British Columbia and Quebec, retail organizations within the province would be overseen by their respective information and privacy commissioner.

While the OPCC has already issued "Guidelines for Identification and Authentication," they are very general and fail to demonstrate how authentication practices should be modified to comply with *PIPEDA*. The OPCC has a general audit power which can be used to ensure that financial institutions and retail organizations comply with the fair information principles stipulated in Schedule 1 of *PIPEDA*. As well, consumers can use the *PIPEDA* complaint mechanism where the have concerns with consent or the collection, use, disclosure or retention of their personal information in the authentication process. The Privacy Commissioner has the power to investigate consumer complaints and issue a decision. If an organization is found in breach of *PIPEDA*, the OPCC often works with the organization to bring their practices into compliance.

As well, the OPCC and the thirteen provincial and territorial information and privacy commissioners are well-placed to educate consumers on authentication systems and practices consumers can adopt to best protect their personal information and privacy.

CONCLUSION

As electronic authentication becomes widespread in retail and banking transactions, consumers need to be assured that these systems are secure and protect their privacy. As our survey demonstrates, there is still a lack of consumer trust in electronic authentication systems. Increasingly complex phishing threats directly target weak authentication systems and also undermine consumer confidence in authentication. The Authentication Principles drafted by Industry Canada’s Working Group do not adequately protect consumers who use electronic authentication systems, as they are too broad to provide helpful guidance in the design and implementation of electronic authentication systems that respect consumer privacy and guarantee security. Until changes are made in Canada’s electronic authentication framework, consumers will continue to be skeptical of electronic authentication systems and the full potential of electronic commerce cannot be realized.

Our report suggested some recommendations to strengthen the electronic authentication framework in Canada. These recommendations are summarized below.

Assure consumers of their security when using authentication systems

Multi-layer single-factor authentication is insufficient to protect consumers for online financial and retail transactions. At minimum, true two-factor authentication should be implemented for in-person banking transactions as banking information is very valuable and involves highly sensitive personal information. For online banking, multi-layer single-factor authentication is inadequate and more secure authentication solutions such as out-of-band or multi-channel authentication or two-factor authentication with OTP tokens should be considered. More secure authentication systems will not wholly protect consumers against increasingly complex threats of phishing, but will at least provide better protection than is currently in place. Additional research should be conducted to assess the effectiveness and acceptability of these authentication technologies.

As authentication for banking transactions consider multi-factor authenticators, the use of biometric authenticators are currently under consideration and in some cases already implemented. Because of the controversies surrounding the reliability and invasiveness of biometric authenticators, consumers should never be required to use a biometric to authenticate. Consumers must be able to choose an authentication process that does not require a biometric authenticator.

The industry should document standards and protocols for consumer authentication systems, documenting which authentication systems are now considered obsolete and weak and which authentication systems are appropriate for more risky financial transactions. These standards must be continuously reviewed to respond to changing threats. As well, these authentication standards should promote strong authenticators that are non-linkable and non-traceable.

Finally, organizations who provide a portal of services to their customers must avoid “risk creep” by ensuring that as additional services are provided to consumers, the authentication system is strengthened to match the risk level of these services.

Clarify who bears the liability for losses related to authentication

The historical check principle of *Price v. Neal* should continue to apply in modern electronic payment systems. This means that the provider of the payment system should bear the burden of unpreventable losses, not consumers. Consumers should have protection against unpreventable losses and payment system providers should not be able to contract out of their liability through a fine print standard form contract. Banks and businesses should not be able to shift liability for losses onto the consumer by instituting an authentication system and they must remain liable whenever they collect and use their customers’ personal information.

A legislative requirement on banks and businesses to cover losses arising from weak authentication systems will protect consumers by giving organizations an incentive to ensure that their authentication systems protect consumer privacy and guarantee security. Such a law would also align with consumer expectations. Furthermore, organizations should be required to highlight clauses in their standard form contracts that discuss the apportionment of liability in the event of loss. Consumers must be aware of the circumstances in which they may be responsible for losses arising from unauthorized transactions.

Protect consumer privacy in authentication systems

Consumer privacy must be prioritized so that if security breaches related to authentication occur, the harm to consumers is minimized. The Authentication Principles must be reviewed to integrate the fair information practices of *PIPEDA*, as they are currently vague and do not suggest specific standards to protect consumer privacy. As required under *PIPEDA*, the amount of personal information collected should be limited to what is necessary in order to authenticate the customer and secondary uses of personal information collected for authentication is prohibited so that consumers cannot be profiled or tracked. Organizations must be monitored for compliance with these requirements. Furthermore, consumer accounts should expire if they are not used regularly and businesses should purge expired account personal information from their databases. These privacy practices will boost consumer confidence in authentication systems.

Consumers should be able to choose to authenticate for a transaction in person, particularly where the transaction is an essential and widely performed commercial transaction. As well, consumers should be able to choose which services to activate and de-activate when using a single sign-on portal that offers access to a multitude of services. Consumers should be able to choose which personal information authenticators they wish to provide for authentication. When consumers retain control over their personal information, they can act in ways to best protect their own privacy against the perceived risks. Finally, when possible, authentication systems should allow consumers to complete transactions under pseudonyms or with the protection of anonymity if the circumstances allow.

Mandate full public disclosure and consumer education about authentication systems

Consumers should be fully informed about the risks and benefits of electronic authentication systems before initiating a financial transaction or registering for an account. Only when they are fully informed are consumers able to make decisions that protect their personal privacy and boost their confidence in electronic authentication systems. Consumers must be notified when a service is added to the numerous services offered by a portal behind the initial single sign-on authentication process and when a stronger authentication system is implemented.

While the Privacy Commissioner has the power to audit organizations under *PIPEDA*, a legislative requirement should allow a federal regulatory body such as the Office of the Superintendent of Financial Institutions Canada to audit financial institutions' authentication systems. A similar audit requirement should be implemented at the provincial level to address authentication in the retail environment. Organizations must provide full public disclosure of the authentication audits performed by independent auditors.

A positive obligation should be placed on organizations to notify their customers when their authentication system is affected by a security breach. As well, comprehensive and visible information should be provided to educate consumers about how to effectively protect their privacy when using specific electronic authentication systems. This consumer education should be provided by a central agency such as the Financial Consumer Agency of Canada and promoted by organizations to their customers. Specific consumer education initiatives should be coordinated by financial institutions and retailers to complement FCAC's efforts by educating their customers about security features of their authentication systems and phishing threats.

Guarantee consumer protection by improving the regulatory framework for electronic authentication

A voluntary set of principles for electronic authentication do not provide adequate consumer protection. By strengthening legislation that applies to financial institutions and retail organizations, authentication will be better regulated. Financial institutions should be subject to stricter authentication regulations as they deal with a multitude of highly sensitive financial and personal information details for a number of people. Authentication by financial institutions can be best regulated under the *Bank Act*, though credit unions and *caisses populaires* are not within the scope of the *Bank Act*. Nonetheless, the *Bank Act* should be amended to set minimum authentication standards for in-person and online banking and to clarify the extent to which consumers bear liability for losses related to authentication.

Regulation of authentication for retail transactions is much more difficult, as the retail industry is within provincial jurisdiction. The challenge is compounded by the range of different businesses and the myriad of potential retail transactions that may require authentication. Thus, regulation for authentication in the retail sphere may rely on authentication standards set for payment services which will likely arise if strict authentication requirements are placed on financial institutions.

Consumers need a mechanism through which they can seek organizational compliance and redress if their privacy or security is breached. The Financial Consumer Agency of Canada should issue guidelines for handling consumer complaints about authentication systems. Authentication issues with banking services should be pursued through the Ombudsman for Banking Services and Investments. A similar complaint mechanism should exist for online retail companies. Finally, FCAC should compile statistics on the number of complaints made about authentication systems.

In conjunction with better regulation of banks and retailers through sectoral regulation, the federal and provincial privacy commissioners should be mandated to oversee authentication practices. Privacy commissioners can adapt their audit and complaint investigation requirements to oversee authentication while protecting consumer privacy.

APPENDIX A – POLLARA SURVEY RESULTS

Q1: Do you bank online?

Yes	86%
No	14%
N Size	2414

Q1AN: Which services do you use with online banking (check all that apply)?

Check Balances	95%
Pay Bills	93%
Email Money Transfers	33%
Purchase Investments Or Stocks	17%
Account Transfers	6%
Purchases	1%
Monitor Investments	<1%
Loans	<1%
Purchase Check	<1%
Foreign Exchange/Currency	<1%
Mortgage Rates (NONSPECIFIC)	<1%
Credit Cards	<1%
Deposits	<1%
Set Up New Accounts	<1%
Withdrawals	<1%
Direct Deposits	<1%
Other	1%
Don't Know/Refused	<1%
N Size	2022

Q2: How often do you bank online?

Daily	22%
Weekly	62%
Monthly	14%
Less Frequently Than Once A Month	2%
N Size	2022

Q3: Have you made an on-line purchase in the last 12 months?

Yes	81%
No	19%
N Size	2414

Q4: How many times have you made an on-line purchase in the last 12 months?

Once	8%
2-5 Times	54%
6-10	20%
More Than 10	17%
Not Sure	1%
N Size	2001

Q5: Please estimate the overall dollar value of all purchases made on-line in the last year including taxes, is it ...?

Under $500	54%
$500 - $1500	28%
Over $1500	17%
Not Sure	1%
N Size	2001

Q6: Has your on-line purchasing increased, decreased or remained the same in the last year?

Increased	43%
Decreased	6%
Remained The Same	51%
N Size	2001

Q7N: Why has your on-line purchasing decreased?

Financial Reasons	47%
Don't Need/Not Interested	21%
Security Concerns	18%
Usability	4%
Privacy Concerns	3%
Product Issues (E.G. Product Didn't Work)	3%
Other	3%
Don't Know/Refused	2%
An Actual Fraud	1%
N Size	116

Q8: Have you noticed any banks (or retailers) asking for more than a login and password?

Yes	58%
No	31%
Not Sure / Don't Know	12%
N Size	2414

Q9: Does this extra step increase your confidence in security?

Yes	67%
No	24%
Don't Know	9%
N Size	1325

Q10: Do you feel there is a risk involved in online banking?

Yes	62%
No	30%
Don't Know	7%
N Size	2414

Q10A: On a scale of 1-10 where 1 is not at all risky and 10 is extremely risky how risky would you say on-line banking is?

Not At All Risky	<1%
2	7%
3	19%
4	15%
5	15%
6	13%
7	15%
8	9%
9	4%
Extremely Risky	3%
Don't Know	1%
N Size	1503

Q11: Do you feel there is a risk involved in purchasing goods on-line?

Yes	77%
No	16%

Don't Know	7%
N Size	2414

Q11A: On a scale of 1-10 where 1 is not very risky and 10 is very risky how risky would you say purchasing goods on-line is?

Not At All Risky	<1%
2	4%
3	11%
4	12%
5	16%
6	13%
7	16%
8	17%
9	7%
Extremely Risky	4%
Don't Know	<1%
N Size	1880

Q12N: What do you think is the risk inherent in your online banking?

Hackers (GENERAL)	70%
Identity Theft/Loss Of Personal Info	16%
Credit Card Theft/Fraud	11%
Human Error/Employee Error/Bank Error	3%
Risk/Trust	3%
Quality of Goods/Not Received	2%
Don't Use Public/Wireless Computers	1%
Server Failure/Crashes	<1%
Other	1%
None/Don't Bank Online	2%
Don't Know/Refused	8%
N Size	1503

Q13N: What do you think is the risk inherent in your online retail transactions?

Loss Product/Money	31%
Credit Card Theft/Fraud	28%
Identity Theft/Loss Of Personal Information	26%
Lack Of Security/Breach/Spyware	9%
Fraud/Scams	8%
Hackers (GENERAL)	8%
Overcharging/Additional Charges/Cost	3%
Other	2%
Don't Know/Refused	10%
N Size	1880

Q14: If your account is accessed without your permission, who should bear the loss?

The Account Holder	2%
The Bank Or Retailer	87%
Shared Between Account Holder Bank/Retailer	12%
N Size	2414

Q15: If the bank/retailer has added the: "two factor" security discussed earlier who should bear the loss?

The Account Holder	5%
The Bank Or Retailer	75%
Shared Between Account Holder Bank/Retailer	20%
N Size	2414

Q15A: Please enter four on the scale below to mark your place in the survey?

1	<1%
2	<1%
3	<1%
4	93%
5	2%
6	2%
7	1%
8	1%
9	<1%
10	1%
N Size	2414

Mean	4.18

Q16: Have you ever had a problem using authentication systems (that is, you could not complete your transaction or it went: wrong)?

Yes	38%
No	55%
Not Sure	8%
N Size	2414

Q17: Were you able to contact the bank/company about it?

Yes	72%
No	21%
Don't Know	7%
N Size	969

Q18: Was the problem resolved to your satisfaction?

Yes	90%
No	8%
Don't Know	2%
N Size	689

Q19: Have you ever cancelled a purchase attempt or online banking session because you were confused by it?

Yes	46%
No	54%
N Size	2414

Q20N: What were the sources of confusion? [Check all that apply

Unfamiliar Questions Or Steps	60%
Asked Too Much Personal Information	57%
Links To 3Rd Party Payment Providers	36%
Possible Incompatibility With Browser/Oprtng Sstm	34%
Not Compatible In Canada	1%
Poorly Designed Website	1%
Shipping Charges/Cost	1%
Link Not Secure/Faulty	1%
Incomplete Transactions	<1%
Lack Of Information	<1%
Incorrect Passwords	<1%

Additional Purchases	<1%
Confirmation/Transactions	<1%
Other	4%
N Size	1207

Q21: Have you ever cancelled an purchase attempt or online banking session because you felt uncomfortable?

Yes	44%
No	52%
Not Sure	4%
N Size	2414

Q22N: Why were you uncomfortable?

Identity Theft/Too Much Information	29%
Unsecured Site/Hackers	20%
Did Not Trust Seller/Retailer/Vendor	11%
Confusing/Complicated	9%
Did Not Feel Right/Intuition	7%
Browser Problems/System Too Slow	5%
Cost	3%
Not Comfortable With Payment Options	3%
Transactn Took Too Long/Wld Nt Complete	2%
Don't Remember/Recall	1%
Forced Into Further Purchase	1%
Fraud	<1%
Other	7%
Don't Know/Refused	8%
N Size	1129

Q23: Some websites use seals of approval (For example Thawte). Do: seals of approval (Thawte, etc) make you feel more secure about the authentication process?

Yes	20%
No	34%
Not Sure	46%
N Size	2414

Q24: Different authentication providers have different methods of conducting authentication and therefore different styles, would a common look and feel for authentication products make you feel ...?

More Comfortable About The Transaction	38%
Less Comfortable About The Transaction	5%
Would Not Affect Level Of Comfort	35%
Not Sure	22%
N Size	2414

Q25AN: Why do you say that - More Comfortable About The Transaction?

Common Standard Procedures	39%
Better Security/Protection	13%
Ease Of Use/Not Confusing	9%
Familiarity/Comfort	8%
Trustworthy/Confidence	6%
Risk/Fraud (NONSPECIFIC)	2%
Confirmation/Transaction	2%
Web Site Lay Out/Safety	2%
Online Retailers	2%

Third Party	<1%
Dishonesty	<1%
Other	6%
Don't Know/Refused	11%
N Size	901

Q25BN: Why do you say that - Less Comfortable About The Transaction?

Easy To Hack/Poor Security	40%
Easy To Duplicate/Falsify	34%
Should All Be Different/Own Authentication	5%
Fraud/Scams	4%
Don't Trust	2%
Dislike Giving Credit Card Number Online	2%
Other	5%
Don't Know/Refused	11%
N Size	129

Q25CN: Why do you say that - Would Not Affect Level Of Comfort?

Hackers/Phishers/Crooks	12%
Comfortable/Secure	11%
Easy To Duplicate	10%
Confident/No Difference/Safe	8%
Level Of Risks	7%
Use Sites I'm Familiar With	6%
Don't Trust/Scam/Theft	6%
Not Comfortable/False Level	6%
Unfamiliar/Unsure	5%
Depending On The Company/Reputation	3%
Appearance Can Be Deceiving	2%
Don't Purchase Online	2%
Uniformity	1%
No Specific Reason	1%
Not Important To Me	<1%
Other	7%
Don't Know/Refused	16%
N Size	853

Q26: Gender

Male	48%
Female	52%
N Size	2414

Q27: Which age group are you in

Under 21	5%
21-24	6%
25-29	9%
30-34	8%
35-39	9%
40-44	11%
45-49	11%
50-54	10%
55-59	8%
60-64	6%
Over 64	18%
N Size	2414

Q27A: Genderation

Male - 18 To 34	10%
Male - 35 To 54	18%
Male - 55+	20%
Female - 18 To 34	18%
Female - 35 To 54	22%
Female - 55+	12%
N Size	2414

Q28: Please indicate your approximate household income (before taxes) for statistical classification only,

Less Than $20,000	8%
$20,000 To $39,999	12%
$40,000 To $59,999	17%
$60,000 To $79,999	15%
$80,000 To$99,999	11%
$100,000 To $149,999	13%
$150,000 And Over	8%
Rather Not Say	15%
N Size	2414

Q29: Please indicate your highest level of education completed

High School	14%
Some College	8%
College	20%
Some University	13%
Undergraduate Degree	23%
Some Post Graduate	7%
Graduate Degree (Including Law Degree)	13%
Rather Not Say	3%
N Size	2414

Q30: Are you currently

Married Or Living Common Law	60%
Divorced	9%
Single: Never Married	25%
Widowed	3%
Rather Not Say	3%
N Size	2414

Q31A: What is your Postal Code?

Rural	15%
Urban	85%
Don't Know/Refused	<1%
N Size	2414

Q33: Language

English	79%
French	21%
N Size	2414

Q34: Province

Newfoundland	2%
Nova Scotia	3%
New Brunswick	2%
Prince Edward Island	<1%
Quebec	24%
Ontario	38%
Manitoba	4%
Saskatchewan	3%
Alberta	10%
British Columbia	13%
Territories	<1%
N Size	2414

Q35: Region

Atlantic	7%
Quebec	24%
Ontario	38%
Prairies	6%
Alberta	10%
BC/Territories	14%
N Size	2414