



Authentication in Retail and Financial Services: Market Scan & Analysis

Presented to

Peter Ferguson
Jane Hamilton
Industry Canada

Presented by

Kristy Duncan
Duncan Consulting

June 30, 2006



duncan consulting

{ innovative banking strategies }

Table of Contents

Executive Summary	1
Introduction	3
Background & Objectives.....	3
Approach.....	4
Analysis	5
Current Use of Authentication in Industry	5
Financial Services	5
Retail E-Commerce.....	6
Trends and Future Use of Authentication in Financial Services and Retail	7
General Trends	7
Trends in Financial Services	8
Trends in Retail.....	9
Challenges Around the Use of Authentication.....	10
Views on Types of Authentication	12
Existing Industry Guidelines	13
Standard Levels of Assurance.....	14
What Authentication Levels are Needed?	15
Cross Border e-Commerce.....	16
Recommendations & Next Steps	17
Summary	20

Appendices

- Appendix A- Glossary
- Appendix B- Discussion Outline
- Appendix C- Discussion Summaries



duncan consulting

Authentication in Retail & Financial Services: Market Scan & Analysis

Executive Summary

Electronic Commerce Branch of Industry Canada commissioned this environmental scan and assessment of market trends in authentication for e-commerce applications in retail and financial services Canada, as a follow up to a more general environmental scan conducted in early 2006. As use of authentication in e-commerce tends to be more advanced in the retail and financial services sectors than in other industry verticals, the objective was to provide a high-level qualitative analysis of views and trends in authentication in these leading sectors.

We interviewed ten prominent market players in the financial services and e-retail markets. The following are highlights of the key findings and recommendations:

- While logon ID plus password remains in common use today, many organizations are layering on additional authentication methods, which are designed to strengthen the authentication, while minimizing the impact to the customer.
- Credit card issuers and acquirers/processors now offer a number of methods to authenticate cardholders, although the availability of these facilities is inconsistent from one issuer to another, and between credit card brands. This is true both within Canada, and on the global stage.
- The key trends in use of authentication in the market include strengthening the authentication via a variety of approaches, an increase in the complexity of authentication solutions (such as neural networks profiling customer behaviour), layering of multiple authentication solutions, and a trend toward more secure management of customer data.
- The challenges cited most often included:
 - overcoming the customer 'FUD' factor (fear, uncertainty, dread) around conducting commerce online;
 - balancing the strength of authentication against the ease of use and cost effectiveness of the solution;
 - lack of various industry guidelines and standards, both within Canada and globally;
 - privacy laws in some jurisdictions which impede the e-merchant's ability to authenticate a customer; and
 - 'risk creep', increasing functionality (and potentially also the risks) in e-commerce applications, without informing customers or giving them the option to decline the service enhancements.



duncan consulting

Industry Canada- Authentication in Retail & Financial Services: Market Scan & Analysis

{ page 1 }

- Most respondents agreed that multi-factor authentication can be more effective than single factor, although some respondents believed that single factor authentication remains sufficient to manage their risks. Those respondents who were moving to stronger authentication often preferred the secondary factors to be passive, meaning they would not impact or degrade the customer experience. The market is very clear that a range of authentication solutions should be available to e-commerce participants, as there is no 'one size fits all' solution for all applications.
- A number of respondents indicated they would like to see standard levels of assurance defined especially for payment solutions, and to have those standards rolled out universally both within Canada, and globally.
- The e-commerce players interviewed generally preferred an *appropriate* level of authentication, which can be selected to address the risks inherent in a particular e-commerce application. In this regard, a guideline outlining how to perform an application risk assessment would be beneficial for many market players.
- There were two main challenges noted with regard to authentication of parties to a cross-border transaction. First was the difficulty verifying customer data, (and hence authenticating a customer wishing to make a purchase), given stringent privacy laws in other jurisdictions. Second was the inconsistent availability of authentication methods across credit card brands and markets.
- The key recommendations for consideration by Industry Canada include the following:
 1. Provide education around e-commerce and authentication issues to both consumers and e-merchants in Canada;
 2. Develop or update industry best practises or guidelines, such as the *Principles for Electronic Authentication*; ID management life cycle; application risk assessment- with a range of suggested authentication solutions for each level of risk; a sample business case.
 3. Define and implement payment industry standards for instruments not covered by the CPA. The standards will promote consistency of authentication across all payment mechanisms and standardize the customer experience and expectation.
 4. Provide tools to deal with Internet Crime- including both legislation, as well as enforcement.
 5. Encourage the government to become a leader in the use of e-commerce and authentication, and define the role of each government department within that leadership.

We believe Industry Canada has an excellent opportunity to provide leadership and direction in the e-commerce and authentication market in Canada today.



duncan consulting

Industry Canada- Authentication in Retail & Financial Services: Market Scan & Analysis

{ page 2 }

Introduction

Trust and confidence form a cornerstone of secure electronic commerce, without which e-commerce cannot expand and thrive in Canada. Industry Canada (IC) has taken a leadership role to promote authentication as an essential component of e-commerce in Canada. IC convened the multi-stakeholder *Authentication Principles Working Group*, to develop and publish the Principles for Electronic Authentication¹ in 2004. The Principles provide benchmarks for the development, provision, and use of authentication services in Canada. Industry Canada also participated in developing the Security and Prosperity Partnership of North America, a framework of common principles for electronic commerce.

This document provides an environmental scan and assessment of market trends in authentication in e-commerce, focusing on retail and financial services sectors.

Background & Objectives

In early 2006, IC commissioned a high level market scan to identify the use and trends in authentication in e-commerce applications in Canada. This research revealed that retail and financial services industries and players are leaders in their use of authentication in e-commerce applications, while other industry sectors may not be as far down this new road.

Industry Canada requires a focused assessment of the retail and financial services industry verticals, to determine the extent to which authentication is being used or contemplated, and to identify potential challenges faced by market players in implementing or using authentication in their e-commerce initiatives. To this end, Industry Canada has commissioned Duncan Consulting to conduct this research, with the objectives to:

- Determine the extent to which authentication is being used or contemplated in the context of domestic and cross-border communications and transactions;
- Identify challenges faced by market players when implementing or using authentication in their domestic and cross-border e-commerce initiatives; and to
- Identify areas where Industry Canada can take an active role in promoting the use of secure electronic commerce across industries in Canada.

This research paper explores these issues, and provides recommendations for Industry Canada to promote the use of strong authentication in Canadian e-commerce going forward.

¹ These can be found at http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00240e.html



duncan consulting

Industry Canada- Authentication in Retail & Financial Services: Market Scan & Analysis

{ page 3 }

Approach

The research was conducted via one-on-one discussions with senior management from key e-commerce market participants in the retail and financial services sectors. Discussions were held between May 31 and June 27, 2006.

Duncan Consulting began the project by developing a discussion outline to address the key questions which Industry Canada wished to learn from this research. The discussion outline can be found in Appendix B of this report.

Organizations were provided with an electronic copy of the discussion outline, to allow them to familiarize themselves with the questions, and ensure the appropriate personnel were present for the discussions.

In total, ten discussions were held with the following organizations:

Organization Type	Organization Name
Financial Services	Beanstream
Financial Services	Interac/Acxsys
Financial Services	CIBC
Financial Services	MasterCard Association
Financial Services	Canadian Institute of Chartered Accountants
Retail	Retail Council of Canada
Retail	Air Canada
Retail	TicketMaster
Retail	Indigo Books & Music
Industry Expert	Paul Wing

The discussions are summarized in Appendix C.



duncan consulting

Analysis

Overall, the financial services and retail markets are tending toward stronger authentication solutions in their e-commerce applications, in order to build customer confidence and stave off ever-present fraud. However, e-merchants are reticent toward adopting authentication solutions which may be perceived by customers as onerous, as they do not wish to lose business or cause customer complaints.

The analysis will explore each of Industry Canada's key questions, which were stated at the outset of the project.

Current Use of Authentication in Industry

The research revealed that there are a variety of approaches being utilized in the retail and financial sectors to authenticate parties to an online transaction. On the whole, the market appears to be shifting from an approach of single-factor logon ID + password, to stronger authentication solutions, which provide a higher level of assurance of authentication.

The key objective expressed by most e-retailers and electronic banking service providers we interviewed was to ensure an appropriate level of security for risks inherent in an application, while not negatively impacting the customer experience.

Financial Services

In the financial services sector, we identified two key approaches to authentication for electronic banking applications. On the retail side, there is a definite trend toward stronger authentication of customers in an online environment. On the commercial banking side, we observe that many online commercial banking applications have already adopted two-factor authentication solutions, due to the potential risks involved.

Stronger authentication solutions- In the retail financial services sector, financial institutions (FIs) are moving to strengthen their traditional single-factor² (logon ID + password) authentication solutions. The FI we spoke to indicated that, in addition to the logon ID + password, it is developing behavioural profiles for its retail online banking clients. The behavioural profiles are utilized, in addition to a geographic location (geolocation²) check, to identify if a customer's behaviour or location may be outside the norm. If an irregular behaviour or location is identified, the FI can invoke additional means to authenticate the customer, such as asking additional

² See glossary in Appendix A for definitions.



duncan consulting

authenticating questions. Online retail brokerage accounts typically require a second password to be entered, when customers wish to execute a trade. We believe that other FIs in the market are considering, or have already implemented, solutions to strengthen the authentication of their online banking customers. It is interesting to note that few FIs have gone so far as to require retail customers to carry a piece of hardware (such as a token or chip card), or utilize any form of bio, to serve as a second authenticating factor.

Two factor authentication for commercial payment applications- Many commercial financial services applications, such as wire payments and other cash management services, have had two-factor authentication solutions in place already for a number of years. For example, chip cards, RACAL devices, tokens, and finger print scans have been made available to commercial clients of different FIs, offering them greater security in authorizing and authenticating payment transactions. One FI has predicted that it will be using tokens to authenticate customers at the logon level within a year.

Retail E-Commerce

Online retail purchases differ from online banking transactions, in that they generally require a third party to process the (payment) transaction. For example, an acquirer acts on behalf of a merchant to get a credit/debit card transaction approved by the card issuer (usually an FI), thus acting as the trusted third party who approves the card transaction and provides assurance of payment³ to the e-merchant.

In addition, the means available to e-merchants to authenticate customers are much different from those utilized by online banking applications, due to two key reasons: a) the e-merchant often does not have the opportunity to develop an ongoing relationship with the customer; and b) the information the e-merchant may collect is constrained by both privacy laws and merchant agreements with credit card acquirers.

Multiple means to authenticate credit card holders- One e-merchant indicated that the value and risk levels of its transactions compel it to utilize all means available to it, in order to authenticate customers in e-commerce transactions, and thereby reduce fraud. In the Canadian market, it utilizes CVV2⁴, VbV⁵, MC/SC⁶ where

³ Payment assurance does not always equate to payment guarantee. In the case of fraud or customers disputing credit card charges, it is often the merchant who takes on the risk of the transaction. For 'card not present' transactions, the merchant is at a higher risk, because there is no signature tying the customer to approval of the purchase.

⁴ CVV2- Customer validation and verification, an approach which confirms an additional number which is printed on a credit card.



duncan consulting

Industry Canada- Authentication in Retail & Financial Services: Market Scan & Analysis

{ page 6 }

available, plus manual verification with the card issuer if any of those are not available. These solutions require the participation of the (third party) acquirer and credit card issuer, to confirm the information being provided by the customer, and confirm funding of the transaction.

Authentication of Interac Online- Interac Online Payments (IOP) is a new payment solution on the market in Canada, which allows a customer to make secure payments to an e-merchant from his/her bank account. IOP utilizes an authentication approach whereby the e-merchant is authenticated electronically by the acquirer, and the customer is authenticated by the customer's FI using existing authentication methods utilized by the online banking application.

Trends and Future Use of Authentication in Financial Services and Retail

The research revealed that many players in both retail and financial services sectors are moving toward stronger authentication methods, and are layering new authentication solutions with more complex fraud detection algorithms. While the ultimate objective is to protect market players from security breaches and potential fraud, e-commerce site operators are reluctant to implement any security measures which may have a negative impact on the customer experience.

General Trends

Across the market, we identified the following trends in the use of authentication for e-commerce transactions. The reader should note that there is often overlap between authentication solutions utilized in retail and financial services sectors; a good example is the chip credit/debit card.

Trend toward stronger authentication solutions- The general trend in use of authentication in financial services and retail applications is toward stronger authentication solutions where possible. This is coupled with more robust fraud detection algorithms being developed by many market players, which attempt to confirm the profile and other information provided by the customer. It is important to note, however, that only in a few cases, are hardware-based (such as token, or chip card) and/or bio authentication approaches utilized. This confirms the need for players in these markets to authenticate customers, while minimizing disruption to customer transactions where possible.

⁵ VbV- Verified by Visa is a PIN in addition to the Visa credit card number, which is required to authenticate the customer making the purchase. Details available at <http://www.visa.ca/verified/factsheet.pdf>

⁶ MC/SC- MasterCard SecureCode enhances the security of current MasterCard accounts by using a secret code to protect against unauthorized use of the MasterCard card when shopping online at participating merchants and retailers.



duncan consulting

Industry Canada- Authentication in Retail & Financial Services: Market Scan & Analysis

{ page 7 }

Continued use of single factor solutions- A number of market players, especially e-merchants selling low dollar value items, noted that a single factor authentication solution (such as logon ID + password) is appropriate to manage the current risk levels. For this reason, they have no plans to change their customer authentication methods in the foreseeable future.

Possible trend toward two-factor authentication- With the coming adoption of chip-based credit and debit cards in Canada, online retail financial transactions may be authenticated in the future using a two-factor authentication approach. This may be accomplished via a dynamic² (or one-time) PIN, which could be generated by a generic chip card reader. This two-factor approach to authenticating both the customer (with the PIN), and the authenticity and presence of the card (by generating a valid dynamic PIN), is considered to be sufficiently strong, as to change the online purchase transaction from a 'card not present' transaction, to be a 'card present' transaction. MasterCard believes that this approach can significantly reduce the risk and associated costs incurred by all parties involved.

We note also that many online commercial banking applications in Canada already require two-factor authentication, the second factor being a chip card, token, or bio-factor.

ID Management Life Cycle- A number of e-commerce market players are starting to recognize the need for proactive management of customer IDs and passwords over the entire life of the customer relationship. This includes developing policies around issuing customer IDs and passwords, policies to address management of password re-sets in order to minimize the possibility of fraudster intervention, as well as policies around collection and use of personal information.

Trends in Financial Services

We identified two key trends in the use of authentication in financial services, which are detailed below.

Trend toward federations of authentication- The financial services industry has been a leader in developing global federations to offer new products that work in a global market. Two prime examples of this are credit cards in the retail market (via Visa and MasterCard standards), and wire payments in the commercial market (using SWIFT standards).

We expect this trend to continue with the adoption of chip-based credit and debit cards, as a global federal is established utilizing EMV (Europay, MasterCard, Visa) standards. Some markets have already adopted and implemented the EMV



duncan consulting

Industry Canada- Authentication in Retail & Financial Services: Market Scan & Analysis

{ page 8 }

standards, and Canada is already well along the path toward implementing the EMV standard.

Trend toward more sophisticated forms of authentication- During the course of the discussions, we observed that many players are trending toward more complex forms of customer authentication. For example, there appears to be an increasing use of behavioural profiling using neural networks, which, until now has generally been limited to the credit card market. Retail and/or financial services organizations may profile clients' transaction types, transaction values, and other online spending patterns, in order to develop a typical profile for each customer and identify transactions which may not fit that profile. Typically, the transactions which are identified as being outside the customer's typical behaviour, are either flagged for manual follow-up (such as phoning the customer to confirm the transaction), or they may be rejected by the service provider (similar to credit card transactions being declined).

Another example of more sophisticated authentication methods is increasing use of dynamic PINs. We expect this to evolve hand in hand with the market adoption of chip cards. Dynamic PINS could be generated either with a chip card and reader, or via a simpler solution, such as a bingo card, which has been utilized in other global markets.

A last example of a more sophisticated form of authentication is that of bio-authentication. At least one FI in Canada has launched a bio-authentication solution for commercial financial transactions. Our discussions revealed that there may be other players contemplating bio-authentication solutions in the market over the coming years.

Trends in Retail

Many players in the online retail sector are trending toward stronger authentication solutions, as well as more secure customer data management, in order to maintain customer data security and minimize fraud. Some e-merchants have decided that single factor authentication is sufficient for their needs at this time.

New Methods to Authenticate Retail Customers- Credit card issuers and acquirers are increasingly offering e-merchants new tools to authenticate cardholders for online purchases. These tools include CVV2, VbV, MC/SC (defined earlier). While these tools are very helpful for e-merchants in managing fraud, the e-merchants note that they are not universally supported by all card issuers in all markets, nor are there industry standards defined between card brands (either globally or nationally).



duncan consulting

Industry Canada- Authentication in Retail & Financial Services: Market Scan & Analysis

{ page 9 }

Payment Card Data Management- The Payment Card Industry Data Security Standard⁷ has been developed by the credit card industry as a benchmark for customer card data management, and is applicable to all players which process, transmit, or store customer card data. Many industry participants, including e-merchants in our study, have embraced these standards as industry best practises, as a means to ensure security of customer data, to the benefit of all.

Potential trend toward cell phones for payments- We observe that in other global markets such as Asia and possibly Europe, a chip capability has been applied to cell phones, enabling them to act as mobile payment devices. Wireless Payment Services⁸ is a new company in Canada, formed in 2005 with the mandate to develop payment solutions which can be facilitated by mobile phones. This solution may work in tandem with, or in competition with, the smart card initiative already underway in the market today.

Challenges Around the Use of Authentication

The interviewees identified a number of challenges they face in applying authentication solutions to their e-commerce applications.

Balancing Strength of Authentication, Ease of Use, and Cost Effectiveness- One of the primary challenges noted by e-merchants was their struggle between asking customers for more detailed information to authenticate themselves (and thereby risk incurring customer complaints, invading customer privacy, and/or losing business), versus requesting less information, but running the risk of higher fraud levels. Alternatively, e-merchants could implement highly complex neural networks to authenticate customers with very little information, although those solutions may prove costly and be difficult to justify. This appears to be a common theme across the e-commerce market- that of balancing the strength of the authentication solution against the customer convenience and the cost effectiveness of the solution.

Overcoming Customer Concerns- Hand in hand with balancing ease of use, cost effectiveness, and security, is the challenge of overcoming the 'FUD' factor (fear, uncertainty, doubt) in customers. We observe that many early adopters have already embraced e-commerce in both retail and commercial markets. However, we believe that increasing penetration of e-commerce applications will require work on the part of e-commerce service providers, in order to increase customer comfort levels and acceptance of online applications.

⁷ Can be found at: http://usa.visa.com/download/business/accepting_visas_ops_risk_management/cisp_PCI_Data_Security_Standard.pdf

⁸ More information on WPS may be found at: <http://www.wpspay.com/>



duncan consulting

Industry Canada- Authentication in Retail & Financial Services: Market Scan & Analysis

{ page 10 }

Lack of Industry-Wide Credit Card Authentication Solutions- While there is increased use of CVV2, VbV, and MC/SC in the Canadian market (and AVS in the US and other markets), not all credit card issuers or brands offer or support these or similar services. E-merchants identified a real need to make these authentication facilities universally available from all card issuers, for all card brands, and in all global markets (or at least in Canada to start). Ideally, all card brands and issuers would follow the same standards, regardless of the card brand or issuer.

Difficulty building a Business Case- Many e-commerce service providers recognize the potential risks around not implementing an appropriate level of authentication for their online applications. However, there remain some players who are unable to develop a business case to justify their own internal costs or resources required to implement appropriate authentication solutions to effectively manage the risks within their applications.

Lack of ARA Guidelines- Some market players indicated that it may be difficult for organizations to select an appropriate level of authentication for their particular e-commerce application. This may be partially attributable to the lack of industry guidelines around how to conduct an application risk assessments (ARA). ARA guidelines could assist those organizations in selecting from a range of authentication solutions which appropriately address the risks particular to their application.

Privacy Laws May Impede Ability to Authenticate- Some e-merchants are challenged by finding an authentication solution which provides an appropriate level of authentication, while not requesting too much private data from customers. One global e-merchant notes that verifying customer names and/or addresses can be particularly difficult in Europe, where privacy laws are so stringent that issuing FIs are unable to confirm (even via a simple yes or no) whether a particular credit card number matches to a card holder name and address on the issuer's file. This leaves very little for the e-merchant to authenticate against to ensure the validity of the transaction.

Rapidly Evolving Market for Authentication- Interac noted that the state of the art in approaches to authentication for online applications changes very quickly. This means that the best of breed solution does not stay that way for very long, and e-commerce players must review their authentication solutions regularly (at least annually) to ensure they remain current and appropriate given changing market conditions.

Risk Creep and Informed Choice- Another challenge identified in the discussions is that of informed choice for customers and risk creep. Risk creep can occur over



duncan consulting

Industry Canada- Authentication in Retail & Financial Services: Market Scan & Analysis

{ page 11 }

the life of an e-commerce application, such as online banking, where the product is initially launched to customers with a certain amount of functionality; then, over the life of the application, new functionality may be added, and customers may be neither informed, nor given the ability to accept or decline the new functionality and the associated risks. This can ultimately increase the risk to the customer, who signed up only for the original service, but may, unknowingly, become liable for any fraudulent activity as new functionality is offered.

We suggest that e-commerce service providers may wish to consider policies of providing customers with informed choices, which will assist customers in proactively managing risks associated with the e-commerce applications they choose to use.

Migration of Fraud to 'Card not Present'- The last challenge we identified is one which may emerge in e-commerce, upon the arrival of chip cards in Canada. Experience in other global markets indicates that the introduction of chip cards may force the migration of existing credit/debit card fraud to 'card not present' transactions, such as Internet or IVR⁹ purchases. E-merchants, acquirers, and other market players need to be aware and prepared for the possibility of this occurring in Canada.

Views on Types of Authentication

For the most part, the respondents indicated that single factor authentication solutions have been sufficient for e-commerce applications in the past. However, most research respondents recognize that single factor authentication can be compromised in a number of different ways. Having said this, some e-commerce service providers we interviewed still believe that single factor authentication continues to effectively manage the risks inherent in their online applications.

This demonstrates the wide range of views held by market players on different types of authentication. We note that many respondents felt that two-factor authentication will become the preferred approach in financial services and possibly the retail industry, within the short to medium term.

Our discussions revealed that many e-commerce players prefer a passive approach to multi-factor authentication, so as not to impact the customer experience. This means that the second factor (with the first factor being logon ID and password) is likely something the customer does not actively provide. An example of a passive factor could be an IP address. One respondent suggested that over 90% of its

⁹ IVR (intelligent voice recognition) generally refers to transactions completed by telephone.



duncan consulting

Industry Canada- Authentication in Retail & Financial Services: Market Scan & Analysis

{ page 12 }

customers access its e-commerce site from one of two computers- a home and a work computer. In this case, confirming an IP address can be a valid second factor for over 90% of customers. Another example of a passive second factor is geolocation, as fraudulent activity often originates from another country, after an account has been compromised. In both these examples, the second factor may not positively confirm that fraud is taking place (a customer may be on vacation in another country); however it does raise a flag for the e-commerce provider to seek additional means to authenticate the customer for a particular transaction.

In the migration to multi-factor authentication, the market has not yet converged on a single form factor that will dominate. We fully expect to see a number of form factors take shape for stronger authentication in Canada over the next few years. These may include any one, or combination, of the following:

- Layered forms of single-factor authentication, such as multiple levels of authenticating questions, possibly layered with IP address verification and/or geolocation
- Increased use of CVV2, VbV, MC/SC, and AVS for credit card purchases
- Chip cards with chip card readers, which can generate a dynamic PIN for use in authenticating online transactions
- Behavioural profiling, to ensure transactions are consistent with established customer behaviour
- Greater use of 'out of wallet' information to authenticate customers; examples are: Which FI holds your mortgage? How much is your monthly mortgage payment?
- Breaking the authentication into smaller chunks, and conducting different chunks via different channels, making fraud more difficult
- Cell phone payment applications, with software embedded to authenticate the user
- Bio-authentication methods for higher risk applications

From this, we conclude that the market must allow for a range of authentication solutions to be used, to enable e-commerce service providers to choose a solution which is appropriate to their particular application and risk profile.

Existing Industry Guidelines

Similar to the research conducted earlier in 2006, research participants mentioned a number of industry guidelines, legislation, or other industry policies and regulations, which have implications to their use of authentication in the Canadian market. These include:

- Privacy laws in multiple jurisdictions
- Principles for Electronic Authentication



duncan consulting

- In the financial services industry, some of the following may apply, depending on the particular business:
 - VbV, MC/SC (Association requirements)
 - Payment Card Industry (PCI)- Data Security Standard (Association requirements)
 - Canadian Code of Practice for Debit Card¹⁰ (a voluntary code of best practice, defined by industry participants)
 - Interac Online Rules (Association requirements)
 - Credit Card Association Rules (Association requirements), including EMV
 - Canadian Payments Association Rule E2¹¹ (Association requirements)

Most of these requirements are either legislative requirements or association requirements. The organizations we interviewed expressed a genuine commitment to comply with these requirements where applicable.

In the US market, the FFIEC Guidelines (Federal Financial Institutions Examination Council) were mentioned as required for operating in the US market, and evolving as a benchmark for the financial services industry in Canada.

Standard Levels of Assurance

Some organizations were reluctant to consider standards defined by any outside party. However, the Retail Council of Canada suggested that it may be appropriate to establish standards and oversight for (online) payments not currently covered under the Canadian Payments Association Rules. These standards could cover credit card payments, gift and pre-paid card purchases, payments via mobile phones, and possibly others.

The objective would be to standardize the customer experience and expectations, similar to Interac Direct Payments (IDP- payments in a bricks and mortar environment), for which standards have been defined, addressing customer authentication, customer recourse, roles and responsibilities, etc. We believe that standards can assist in reducing fraud if all customers are able to expect a standard online payment experience, regardless of payment instrument.

It was suggested that the payments industry could roll out a standard to include three or four pre-defined levels of security for card and other payments not covered by the CPA (as noted above). This standard would define:

¹⁰ Found at: http://www.fcac-acfc.gc.ca/eng/compliance/DebitCardCode/DebitCardCode_e.asp

¹¹ Can be found at: http://www.cdnpay.ca/rules/pdfs_rules/rule_e2.pdf



duncan consulting

- Authentication requirements and options, based on transaction risk levels (dollar values);
- Requirements around providing customer disclosure and recourse
- Definitions of roles and responsibilities of payment transaction participants
- Requirements to enable payment instrument issuers to ensure that their customer set-up and initialization procedures are sufficient to authenticate customers at each standard level.

Ultimately, other industry verticals may choose to follow the lead of the payments industry, and define similar standards applicable to their own requirements. There may be a role for Industry Canada to play in this process.

What Authentication Levels are Needed?

The question of what levels of authentication are needed to ensure secure electronic commerce in today's environment essentially boils down to finding the electronic equivalent to the concept of 'Know Your Customer' (KYC). KYC has always been important in the real world, but in the virtual world, it brings new significance, as well as new challenges. Authentication is the equivalent to KYC in an online environment, and the market is finding a number of approaches to address this important requirement.

Appropriate Level of Authentication- The overall feeling was that e-commerce applications require an *appropriate* level of authentication, which manages the risks inherent in the particular application. It was also suggested that the level of authentication could depend on an application risk assessment (ARA), which would be utilized to suggest an appropriate level of authentication, or a range of possible authentication approaches, for a particular application.

Some interviewees felt strongly that an overly strong authentication solution for a relatively low-risk application (such as a 16 digit password to view an invoice online) would be inappropriate. Conversely, they also felt that applications should require sufficiently strong authentication solutions in order to effectively manage the risks inherent in the particular applications. It was noted that an authentication solution can vary within an application; for example- requiring different approaches, based on the country of origin of the customer, or the dollar value of transaction.

We believe there is room to develop guidelines for e-commerce market players, in order to assist them in assessing the risks in their applications, and provide guidance on appropriate authentication approaches to manage those risks.



duncan consulting

Industry Canada- Authentication in Retail & Financial Services: Market Scan & Analysis

{ page 15 }

Cross Border e-Commerce

Of the ten organizations we interviewed, about half were doing transactions with customers outside Canada. Of these, only one had a significant presence outside Canada, and had established over a dozen websites in other countries to specifically target customers in those markets.

The challenges and differences encountered by Canadian e-commerce players when selling to customers in other countries relate mostly to the different privacy legislation, and the different mechanisms available to authenticate credit cardholders in an online purchase.

Privacy Laws in Other Jurisdictions- One large e-merchant noted that (manual) verification of customer names and/or addresses can be particularly difficult in Europe, where privacy laws are so stringent that issuing FIs are unable to confirm a credit card holder's name or address. This lack of consistency in privacy laws from one market to another causes difficulties for e-merchants operating globally to apply a standard approach to authenticate their customers.

Lack of Global Standards around Cardholder Authentication- One e-merchant noted that in the US, a number of credit card issuers offer AVS, which allows the e-merchant to validate the address provided by the customer against that which is on file with the credit card issuer. Since AVS is not yet widely available in Canada, it leaves an inconsistency across global markets for the e-merchant when applying fraud detection mechanisms and cardholder authentication routines. This has the potential to increase the opportunity for fraud in markets where these cardholder authentication facilities are not offered.

Growing Need to Cross-Certify between Schemes- As noted above, e-merchants wishing to offer online purchasing facilities to customers in different global markets, may find it difficult to operate across different payment schemes where no cross-border, or cross-scheme certification exists. This also relates to the lack of global standards, most evident in the retail card payments industry, which forces e-merchants to create separate customer authentication and payment authorization facilities for each market in which they wish to operate.



duncan consulting

Recommendations & Next Steps

The following recommendations are based on the input received during the course of this second phase of research. The reader may wish also to reference the recommendations provided in the first research phase, to gain an appreciation of the 'big picture' recommendations and next steps.

1. Education- We believe there is an excellent opportunity to provide education to the market, to both consumers and e-merchants.
 - a. Consumer Education- Consumers need a reliable source of information on e-commerce, which addresses all the benefits and risks in a simple but comprehensive manner. This could be done in the form of an FAQ list- either online at the IC web site, or via printed educational materials (or both). It could also point the consumer to other reliable resources for related issues, such as online payments, online fraud, etc. It could be produced either by IC alone, or in conjunction with other organizations such as FCAC, CBA, CPA, Retail Council of Canada, or others.
 - b. E-Merchant Education- Further to the *Principles for Electronic Authentication* which was issued in 2004, we believe there is room to publish a primer or FAQ list for potential e-merchants when considering the new channel of internet commerce. The resource could reference the *Principles*, industry best practises, application risk assessment guidelines, and point them to other helpful resources.

2. Industry Guidelines and Best Practises- The discussions with market participants identified a number of industry guidelines and best practises which either exist already and could be updated, or could be developed and published to benefit e-commerce industry players.
 - a. Update to Principles for Electronic Authentication- As the market is continuously changing, we believe it may be worthwhile to re-visit the *Principles*, to reference additional concepts such as informed consent from consumers, application risk assessments leading to options on appropriate authentication solutions, etc.
 - b. ID Management Life Cycle- Customers in e-commerce transactions need to identify themselves to the e-commerce provider in some way, and be able to provide some proof (usually something the customer *knows, has, or is*) of their identity. We believe that customer identity management must become a process in itself, and guidelines would be extremely helpful to assist organizations in understanding issues such as: what is an appropriate approach to providing a customer ID? How can an organization define its policy on customer password re-set frequencies, number of failed attempts before being locked out, etc?



duncan consulting

- c. Guidance to Assist in Authentication Solution Selection- It appears there is not any publicly available guidance for Canadian e-commerce organizations to conduct an application risk assessment (ARA) for their e-commerce applications. Ideally, this application risk assessment guideline would provide a range of appropriate authentication solutions for each of a number of standard risk levels.
 - d. Sample Business Case- In order to assist organizations to build a business case to cost justify appropriate authentication solutions in their e-commerce applications, it would be helpful to have a sample business case to follow. The sample business case could outline a number of potential scenarios for consideration, and provide a step-by-step process for e-commerce organizations to build their business case.
3. Define and Publish Payment Industry Standards- We believe there may be an opportunity in Canada to define and establish standards for payment solutions which are not covered by the CPA, in order to promote consistency of authentication across all payment mechanisms and standardize the customer experience and expectation. These instruments could include credit cards, gift and pre-paid cards, and other online payment mechanisms. The standards might include three or four pre-defined levels of security and authentication for payments not covered by the CPA (listed above). The standards would define:
 - Authentication requirements and options, based on transaction risk levels (dollar values);
 - Requirements around providing customer disclosure and recourse
 - Definitions of roles and responsibilities of payment transaction participants
 - Requirements to enable payment instrument issuers to ensure that their customer set-up and initialization procedures are sufficient authenticate customers at each standard level.
 - Requirements to cross-certify with payment schemes in other markets.With credit cards specifically, it would be helpful if credit card issuers and other payment solution providers could define basic customer authentication services available to merchants (similar to VbV and MC/SC, AVS, CVV2 and others), and make them globally available across all card issuers and acquirers, in all global markets, and across all payment solutions. This would allow e-commerce players to have a consistent approach to authenticating their online customers.
4. Provide Tools to Deal with Internet Crime- Both legislation and enforcement are required to deal effectively with Internet crime. A number of interviewees suggested that the Canadian legal framework does not provide for stiff penalties for crimes of identity theft, as a deterrent for Internet crime. As an enforcement



duncan consulting

vehicle in the US, the *Internet Crime Complaint Centre*¹² (IC3) was established jointly by the FBI and the National White Collar Crime Center. Its mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. Canada may wish to consider beefing up both the legislation (with stiffer penalties) and the enforcement as deterrents against cyber crime.

5. Become a Leader- Various departments of the Canadian federal government have taken positive steps toward establishing and promoting viable e-commerce applications. There are a number of excellent examples, including Canada Revenue Agency's e-pass initiative, the Electronic Funds Transfer Working Group's *Principles for Electronic Authentication*, the Canadian Payments Association's Rule E2, among many others. We support the concept of the government becoming a leader in the use of e-commerce as a secure and effective means to conduct business. It would be helpful to the public, if the government could define the roles that each government body is taking on, to give the public a better understanding of the big picture (roles and objectives of each initiative), and to ensure there is no overlap between initiatives.

These recommendations are designed to educate market players, define industry best practises and guidelines, define payment industry standards for online payment instruments not currently addressed by the CPA, enhance legislation and enforcement to manage Internet crime, and solidify leadership in e-commerce within the Canadian government.

¹² More information can be found at <http://www.ic3.gov/>



duncan consulting

Summary

Recognizing that single factor authentication can be compromised in many ways, Canadian e-commerce solution providers and vendors are striving to authenticate customers using appropriate solutions, which minimize the impact to the customer experience. In some organizations, authentication is evolving to become a sophisticated, multi-layered process.

Key challenges faced by e-commerce services organizations include a lack of standards for online payment solutions (at both national and international levels); difficulty navigating inconsistent privacy laws in different global markets; and a lack of guidelines for market players to develop application risk assessments and business cases.

At this juncture, we believe Industry Canada has an opportunity to take an active role in providing education to market players and consumers, and developing and promoting a number of industry best practises and guidelines.



duncan consulting

Industry Canada- Authentication in Retail & Financial Services: Market Scan & Analysis

{ page 20 }

Glossary

AUTHENTICATION- A process that attests to the attributes of participants in an electronic communication, or to the integrity of the communication.

ATTRIBUTES- Information concerning the identity, privileges, or rights of a participant or other authenticated entity.

BIO-AUTHENTICATION- A measurable physiological or behavioural trait of a living person, especially one that can be used to identify a person, or verify a claimed identity.

DUAL FACTOR AUTHENTICATION (also referred to as TWO FACTOR AUTHENTICATION)- An authentication processes which depends on two independent mechanisms for authentication; for example, an authentication which requires the participant to provide something he or she *has*, *and* something he or she *knows*. As an example, two factors could be a smart card and a password. Another factor which could be authenticated would be something the participant *is*, such as a biometric attribute (such as a voice print, retina scan, or fingerprint).

DYNAMIC PIN (also referred to as a ONE-TIME USE PIN)- a PIN generated by a token, which may be based on time, and expires after one use.

GEOLOCATION- **Geolocation** is the real-world geographic location of a internet connected computer, mobile device or website visitor based on the Internet Protocol address¹³

INTEGRITY- Assurance that the information in an electronic communication has not been modified or corrupted during the process of communication.

PARTICIPANT- An individual or organization participating in an authentication process, whether directly or through another authenticated entity, such as a data service or object, hardware device, or software program.

¹³ Definition sourced from <http://en.wikipedia.org/wiki/Geolocation>



duncan consulting

Industry Canada- Authentication in Retail & Financial Services: Market Scan & Analysis

{ glossary }

SINGLE FACTOR AUTHENTICATION- An authentication processes which depends only on a single factor being authenticated about the participant; for example, an authentication which requires the participant to provide something he or she *has* (such as a token or card), or something he or she *knows* (such as a password or shared secret).

STRONG AUTHENTICATION- An authentication process which confirms more than a static single attribute (such as a static password). It may utilize a dynamic password scheme for the participant to authenticate him/herself, or a combination of more than a single factor, such as something the participant *has, knows, or is*.



duncan consulting

Industry Canada- Authentication in Retail & Financial Services: Market Scan & Analysis

{ glossary }

Appendix B- Discussion Outline

Authentication Research for Industry Canada Environmental Scan, Market Trends, and Cross-Border Applications

Background & Objectives

Trust and confidence form a cornerstone of secure electronic commerce, without which e-commerce cannot expand and thrive in Canada. To help Canadians build this trust and confidence, Industry Canada convened the multi-stakeholder *Authentication Principles Working Group*, to develop *Principles for Electronic Authentication*¹⁴, which it published in 2004. These Principles were designed to serve as benchmarks for the development, provision, and use of authentication services in Canada.

Industry Canada has commissioned Duncan Consulting to conduct this research, in order to:

- Determine the extent to which authentication is being used or contemplated in the context of domestic and cross-border communications and transactions;
- Identify challenges faced by market players when implementing or using authentication in their domestic and cross-border e-commerce initiatives, and to
- Identify areas where the federal government (Industry Canada) can take an active role in promoting the use of secure electronic commerce across industries in Canada.

Industry Canada has taken a leadership role in other domestic and international initiatives to promote e-commerce and authentication. Of particular interest to this study is the framework of common principles for electronic commerce that has been developed with the United States and Mexico under the *Security and Prosperity Partnership of North America*¹⁵. These principles acknowledge the key role authentication has to play in strengthening the Internet as a medium for electronic commerce.

We would like to arrange an interview or conference call with a representative of your organization between May 31 and June 9, 2006. We expect this discussion to take approximately 1 ½ to 2 hours. The following page provides an outline of the information we would like to learn from this research.

Your input will be valuable in assisting the E-Commerce Branch of Industry Canada to assist Canadian business in building trust and confidence in the online environment in Canada. We appreciate your participation.

Further comments or questions may be directed to:

Kristy Duncan
Duncan Consulting
416-487-5691
kristy@duncanconsulting.com

Jane Hamilton
Manager, Strategic Security Initiatives
E-Commerce Branch, Industry Canada
613-991-0049
hamilton.jane@ic.gc.ca

¹⁴ These can be found at http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00240e.html

¹⁵ Further information can be found at <http://www.ic.gc.ca/cmb/welcomeic.nsf/ICPages/SpecialReports>

Discussion Outline

- a) Industry Role- Please describe the role and activities of your organization in the e-commerce market, and outline how authentication plays a part in that role?
- b) Authentication Use- Can you describe, and provide examples of, your organization's current or planned use of authentication, or strong authentication for:
 - domestic e-commerce applications?
 - cross-border e-commerce applications?
- c) Authentication Trends- Can you identify and describe current trends in the use of authentication in the domestic e-commerce market in your industry?
 - B2B or B2G
 - B2C
 - Do these trends apply equally to cross-border e-commerce transactions and communications in your industry?
- d) Challenges- Can you identify any challenges, faced by your organization and/or industry, to using or implementing authentication in domestic or cross-border transactions and communications?
- e) Types of Authentication- How do you view different types of authentication?
 - Single Factor
 - Two Factor
 - Other
- f) Industry Guidelines- Are there any legislative requirements, policies, regulations, standards, industry best practises, etc., issued by government or industry, that you are subject to, or have implications for:
 - Your organization's use of authentication in the domestic market?
 - Your organization's use of authentication in the cross-border market?
 - How do/will you use these policy instruments and/or practice guidelines, and in what context in your business?
- g) Standard Levels of Assurance- Do you believe that levels of assurance should be standardized in some way? If so, how would you see that happening?
- h) Authentication Levels- What levels of authentication do you believe are needed to effectively manage the risks in today's online e-commerce environment?
- i) Promotion of Authentication in the Canadian market- Can you identify any initiatives which the federal government (Industry Canada) might undertake to help promote the use of secure e-commerce in domestic and cross-border transactions?