BANK OF CANADA
BANQUE DU CANADA

Discussion Paper/Document d'analyse
2008-17

A Survey and Risk Analysis of Selected Non-Bank Retail Payments Systems

by Nikil Chande

www.bank-banque-canada.ca

Bank of Canada Discussion Paper 2008-17

November 2008

A Survey and Risk Analysis of Selected Non-Bank Retail Payments Systems

by

Nikil Chande

Financial Stability Department
Bank of Canada
Ottawa, Ontario, Canada K1A 0G9
nchande@bankofcanada.ca

ISSN 1914-0568

Acknowledgements

Considerable input was provided by Dinah Maclean, Walt Engert, Sean O’Connor, Jack Selody, Alexandra Lai, Varya Taylor, Ben Fung, and Doug Kreviazuk, but errors remain the author’s sole responsibility.

Abstract

Payment services offered by non-banks have flourished in recent years. The author provides an overview of the different kinds of non-bank retail payments schemes currently available in Canada, illustrating each by focusing on a specific example. Current players in the Canadian marketplace include electronic bill consolidators, such as epost; online payment providers, like PayPal; and pre-funded schemes, such as retailers' gift cards. The author also discusses the main risks associated with each of the schemes, such as bankruptcy, banker, security, market, and liquidity risks. While the author does not undertake a complete analysis of the market failures that may justify regulation of non-bank retail payment services, he does set out a broad framework for considering whether users and providers of these services have the incentives to manage the associated risks. Since any regulatory response, if deemed to be justifiable after a more complete analysis, must be balanced in its approach, some of the costs of regulation in this area are also considered.

JEL classification: G20, D14
Bank classification: Financial services; Payment, clearing, and settlement systems

Résumé

Les services de paiement offerts par les établissements non bancaires se sont largement développés au cours des dernières années. L'auteur brosse un tableau d'ensemble des divers types de services de paiement au détail non bancaires disponibles en ce moment au Canada et illustre chacun en mettant l'accent sur un exemple précis. À l'heure actuelle, on trouve sur le marché canadien des services de consolidation de factures électroniques, tels que postel; des services de paiement en ligne, dont PayPal; et des solutions de prépaiement, telles que les cartes-cadeaux de détaillants. L'auteur passe également en revue les principaux risques associés à chaque type de services, comme le risque du banquier, le risque lié à la sécurité ainsi que les risques de faillite, de marché et de liquidité. Même s'il n'analyse pas de façon exhaustive les défaillances du marché qui pourraient justifier la réglementation des services de paiement au détail non bancaires, l'auteur expose un cadre général qui permet d'évaluer la présence d'incitations à la gestion des risques chez les utilisateurs et les fournisseurs de ces services. Puisque l'introduction de toute contrainte réglementaire — dans l'éventualité où celle-ci serait jugée justifiable après une analyse plus complète de la question — doit répondre à un principe d'équilibre, l'auteur prend également en considération certains coûts qu'entraînerait une réglementation de ces services.

Classification JEL : G20, D14
Classification de la Banque : Services financiers; Systèmes de paiement, de compensation et de règlement

1 Introduction

In recent years, there has been considerable growth and interest in the retail payments systems offered by non-banks. Consumers have benefited from the enhanced choice and convenience associated with these systems, and the increased role played by non-banks seems to have resulted in a more competitive payments market. As a result, banks have faced pressure to develop more innovative and efficient payment services.

Although non-bank retail payments systems have imparted benefits, many of these schemes are new and are owned by entities that may not be subject to the same regulatory oversight as banks. Consequently, it is important to understand the risks associated with these services. In particular, there may be risks inherent in these schemes that private agents do not have adequate incentives to address. Moreover, because of the principal–agent relationship that characterizes these systems, it is important to pay attention to the alignment of incentives between the principal (the users of payment services) and the agent (the service provider), as well as the role of information asymmetries. Users of non-bank retail payment services need to have sufficient information concerning the associated risks, so that they can make informed decisions about their willingness to accept them.

This paper provides an overview of the different kinds of non-bank retail payments schemes currently available in Canada, illustrating each by focusing on a specific example. In addition, the paper discusses the main risks associated with each of the schemes. While the paper does not undertake a complete analysis of the market failures that may justify regulation of non-bank retail payment services, it does set out a broad framework for considering whether users and providers of these services have the incentives to manage the associated risks. Since any regulatory response, if deemed to be justifiable after a more complete analysis, must be balanced in its approach, the potential direct and indirect costs of regulation in this area are also considered.

1.1 Types of non-bank retail payments systems

Non-bank retail payments systems currently used in Canada can be broadly classified into three groups:

(i) electronic bill presentment and payment (EBPP),
(ii) person-to-person payments (P2P), and
(iii) pre-funded cards.[1]

1. This categorization is consistent with that in Bradford, Davies, and Weiner (2003). The authors organize non-bank systems into six broad groups: (i) cheque conversion, (ii) EBPP, (iii) electronic invoice presentment and payment (EIPP), (iv) P2P, (v) stored-value instruments, and (vi) contactless payments.

Cheque and payment processing services, such as those provided by Symcor, are excluded from the discussion, since these are not front-end retail services, and often they are owned by banks.[2]

Contactless technologies, such as Bluetooth, infrared, near field communication (NFC), and radio frequency identification, are increasingly associated with retail payments schemes. However, payment methods that use contactless technology will not be discussed separately, since they do not constitute a separate and distinct payments scheme, but instead represent a unique method through which payment functions can be delivered.[3]

Mobile payments (i.e., those made using a cell phone) may be considered non-bank retail payment services, depending on the manner in which the service is structured. However, these are also excluded from the analysis, since mobile payments are not yet popular in Canada.[4] Nonetheless, there is some limited use of mobile phones in Canada as an alternative method of delivering other forms of payment. For example, mobile phone subscribers can pay for parking time in Toronto and Vancouver by phoning a number on the meter and using credit or debit cards to buy the necessary time (Uribe 2007). In addition, payment instructions can be sent to PayPal via a text message. Furthermore, Visa Canada and MasterCard Canada are undergoing trials that extend their contactless credit card technologies (called payWave for Visa, and PayPass for MasterCard) to mobile devices. Mobile devices embedded with contactless chips allow customers to make Visa or MasterCard credit card purchases by waving the device past contactless readers, such as the ones used for the payWave and PayPass technologies (Payments News 2007b). Mobile payments may one day be a more prominent feature of the Canadian payments landscape.

2 Electronic Bill Presentment and Payment (EBPP)

With EBPP, a bill is presented via the Internet and it can be paid electronically.

2.1 Two main models

There are two main EBPP models:

2. Symcor, which is owned by RBC, BMO, and TD, provides payment transaction processing services, primarily to the financial services industry. Each year, Symcor processes approximately 2 billion cheques, 150 million customer payments, and 400 million customer statements (Symcor 2008).
3. The use of contactless technologies with some pre-funded cards is discussed in section 4.
4. Although interesting developments are taking place in Asia and Europe, these are beyond the scope of this paper.

1. the Biller-Direct model, where the customer sees and pays the bill directly at the biller's website (for example, where a customer views and pays their telephone bill directly at the Bell Canada website); and

2. the Consolidator model, where the customer receives and pays a bill indirectly through a third party that has established a bill presentment and bill payment agreement with the biller in question. Epost, discussed below, is an example of the Consolidator model that allows customers to view and pay any number of bills separately, such as telephone or hydro, through the epost website.

With the Biller-Direct model, a merchant sends a notice to its customers to let them know when a bill is due. Customers then visit the merchant's website to both view the bill and make payments using the payment technology available on the website. This, however, is not an example of a non-bank retail payment service, because the merchant does not have a role in the payments system itself; the merchant just receives payment through existing systems.

With the Consolidator model, bill aggregators establish agreements with a number of billers to present their bills to customers and to provide those customers with the opportunity of making payments online on one centralized site. In this way, the Consolidator acts as an intermediary by authorizing and accepting payments from customers and paying merchants on the customers' behalf.

Although a bank that offers a bill payment facility within its online banking service is acting like a Consolidator, there is a slight distinction. In addition to providing customers with an opportunity to pay the bills online, EBPP Consolidators present electronic copies of the bills to be paid, whereas banks that offer online bill payment facilities do not always present copies of the bills. However, as section 2.2 describes, some Canadian banks have integrated this Consolidator into their web-banking services, so that customers who are also users of epost can see bills they are about to pay online.

2.2 epost

In Canada, epost is the dominant provider of consolidated EBPP services. A wholly owned subsidiary of Canada Post, epost was launched in 1999 and incorporated in 2001. In 2004, epost solidified its dominant position in Canada by acquiring webdoxs, a competing Consolidator supported by numerous financial institutions (FIs).

Customers can sign up for an epost box at www.epost.ca, or through their online banking websites. Once signed up, customers select the bills they wish to receive electronically from the

list of participating billers. Currently, there are about 200 participating billers, including providers of hydro, cable, and telephone, as well as credit card companies, municipalities, and large retailers. According to an article in the *Montreal Gazette* (Kane 2005), epost is used by approximately 2 million Canadian households, and nearly 300,000 Canadians signed up for the service in the first three months of 2005.

In addition to viewing, storing, and paying bills at the epost website, customers can access their epost boxes by linking them to their FI's online banking facility. Epost is the bill presentment service available in the web banking facilities of the six biggest banks, as well as those of Laurentian, Desjardins, and about 40 credit unions. Furthermore, customers of Intuit, which makes Quicken and QuickTax, can access their epost boxes by linking them with either of these Intuit products.

Customers of epost can pay their bills by electronic funds transfer (EFT), credit card, or linking to their FI's online banking. Billers may, however, restrict payment options, and thereby influence their customers' payment methods. Epost does not charge its customers for making a payment; however, it does charge its billers for providing the service. FIs or billers may charge their own customers, depending on the chosen payment method. Customers pay their bills individually by paying epost, which in turn pays billers on the customers' behalf. When customers use EFT debits, they transfer funds electronically from their existing savings or chequing accounts with any Canadian FI. To use EFT debits, customers must first sign a pre-authorized debit agreement. When customers are linked to their FI's online banking, the FI's existing online bill payment facility is used.

2.3 Risk analysis

There are three key risks applicable to EBPP Consolidator schemes: (i) bankruptcy risk, (ii) banker risk, and (iii) security risk.

2.3.1 Consolidator bankruptcy risk

A risk inherent in the Consolidator model is that of Consolidator bankruptcy. When a customer pays a bill through a Consolidator, there is a short period of time after the Consolidator has already received the customer's funds, but before the Consolidator has paid the merchant on the customer's behalf.[5] These exposures exist for only a limited period of time; for example, with

5. For example, the pre-authorized debit agreement that epost requires from customers choosing to pay by EFT debit states that "I understand there may be a delay between the time I instruct epost to make a payment and the receipt of the payment by any epost Mailer."

epost the typical delay is one business day.[6] If the Consolidator were to declare bankruptcy during this period of time, then the merchant may not receive the customer's payment. Furthermore, a significant amount of time may pass before the release of any funds in the possession of the Consolidator at the time of bankruptcy. Depending on which creditors have priority and whether the Consolidator used a mitigating strategy such as a trust account, any funds ultimately released may be less than was originally paid by the customer. Thus, in the case of Consolidator bankruptcy, there may be some ambiguity as to which party, the customer or the merchant, would be liable for any shortfall in funds. One complicating factor is that the responsible party may depend on the type of payment made by the customer. Clarifying any ambiguity would help users make more informed decisions about the bankruptcy risk associated with using a Consolidator.

Customers and merchants face exposures they are unable to avoid in the event of EBPP Consolidator bankruptcy, because of the time lag between delivery and receipt of funds. Of course, the probability of an EBPP Consolidator going bankrupt will depend, in part, on how the float is invested. This Consolidator bankruptcy risk may be mitigated to the extent that users choose Consolidators with reputations for strong financial health. One consideration is that users may find it difficult to find information on the financial well-being of a particular Consolidator, and, where that information is available, it may be too costly for customers and merchants to digest it individually. However, other sources of information can help a potential user make a judgment about the likelihood that a Consolidator may fail. There are network externalities associated with the services of a Consolidator, since the value of the service to an individual user depends on the total number of other users: as the service gathers a critical mass of participants, it becomes more likely that the service will succeed. Therefore, a Consolidator's dominance in a given market may serve as a substitute for financial information, since a dominant Consolidator with a critical mass of participants is less likely to fail. In addition, customers can use information on an EBPP Consolidator's ownership structure to help select a Consolidator that may be less likely to fail.[7]

Even if information on an EBPP Consolidator's financial state is difficult to find or costly to process, customers can use the Consolidator's reputation for dominance in a particular market, as well as information on the strength of its ownership, to mitigate the associated bankruptcy risk. Of course, one implication of the importance of reputation is that it will be difficult for start-ups

6. Author's correspondence with Christophe Credico of epost, 20 September 2005.
7. For example, epost is owned by Canada Post, which is a Crown corporation.

with little reputational capital to make inroads into the Consolidator market. The next wave of EBPP expansion may come from the credit card industry, as players in this industry attempt to capitalize on their existing reputations by offering bill presentment and payments services on their credit card websites (Electronic Payments International 2005a).

2.3.2 Banker risk

As previously discussed, there may be a short time lag between the payment of funds to the Consolidator and the receipt of those funds by the merchant. If, during this time period, the funds are located in the Consolidator's bank account, then another risk is the potential failure of the Consolidator's banker. This banker risk is mitigated to the extent that the time lag is short and the funds may be held in trust. Moreover, risks associated with banker default are already mitigated by the regulatory regime in place that governs the financial sector.

2.3.3 Security risk

EBPP security is not flawless; for example, it is possible that a consumer's private information could be compromised through a failure in the authentication process or by a breach of the database in which the information is stored. If a customer's user ID for logging in and the associated password were discovered, then the fraudster would have access to the customer's bill(s), such as a credit card bill. This type of private information would also be at risk if the Consolidator's database was successfully hacked. A survey by CheckFree, a U.S. firm that provides EBPP technology primarily to banks, found that 18 per cent of U.S. respondents who did not pay bills online cited concern about the security of their personal information as the most significant barrier to using an EBPP service (Electronic Payments International 2005c).

In addition to breaching a customer's right to privacy, a fraudster could use information available in the compromised account to help steal the customer's identity. In these cases, which party bears the liability associated with any losses? Fraudulent credit card transactions are generally covered by the issuer, which has the financial resources to absorb the loss and pursue the responsible party. However, losses such as a fraudulent loan taken out in the name of a consumer with a compromised identity may be the initial responsibility of the consumer, which could be problematic if the consumer is financially unable to absorb the loss or pursue the responsible party.

Missing from this discussion, so far, are the Consolidators that offer the EBPP technology. For example, the EBPP Consolidator, epost, attempts to contractually limit its legal liability for losses resulting from any unauthorized access by disclaiming in its "Terms and Conditions of Use" that:

> We and the Canada Post Parties will not be responsible or liable for any delay, damage, loss or inconvenience you or any other person may incur in the event of unauthorized access to your epost box or your personal information. (epost 2008)

Notwithstanding attempts to disclaim liability from security breaches, EBPP Consolidators, and indeed all organizations doing business in Canada, are governed by the federal Personal Information Protection and Electronic Documents Act (PIPEDA) (Department of Justice Canada 2000).[8] PIPEDA sets forth ten principles that organizations must follow when collecting, using, and disclosing personal information. One of these principles is that personal information shall be safeguarded by security measures that are appropriate to the sensitivity of the information. Organizations must protect personal information from loss or theft and safeguard it from unauthorized access, disclosure, copying, use, and modification. Under PIPEDA, individuals can complain to the Privacy Commissioner about the manner in which an organization has protected the individual's personal information. The privacy dispute can also be taken to the federal court, which can order the offending organization to correct its practices and require it to pay damages to the individual.

In addition to the obligations under PIPEDA, EBPP Consolidators have strong incentives to implement secure authentication technologies, and to prevent their databases from being hacked, because of the potential for damage to their reputations and brands. The use of the new non-bank retail payments systems is contingent on customers feeling confident that their private information is not vulnerable. Even a few isolated cases of compromised accounts may be sufficient to undermine this confidence. However, this assumes that the holders of the compromised accounts are actually notified. EBPP providers that have suffered a security breach may feel discouraged from informing the public about the breach. Of Canada's data protection laws, only Ontario's Personal Health Information Protection Act currently requires the notification of a security breach (Office of the Privacy Commissioner of Canada 2006). A review of PIPEDA is under way, and one of the recommendations being considered is the addition of a duty to notify individuals when their personal information has been compromised. Nonetheless, the current version of PIPEDA does not contain such a duty.[9]

---

8. For organizations operating only in a single province or territory, where that province or territory's privacy law is substantially similar to PIPEDA, the organization will be subject to the provincial or territorial privacy law, instead of to PIPEDA (Department of Justice Canada 2000).
9. In 2007, the Office of the Privacy Commissioner of Canada developed guidelines in consultation with industry groups that organizations should follow in the event of a security breach, including notification of the people affected. However, these guidelines are only voluntary.

In the event that the public learns of a security breach, the resulting financial and reputational damage can be enormous.[10] The largest personal information breach on record occurred when hackers broke into the computer systems of TJX Companies Inc., an international retailer of apparel and home fashion.[11] Approximately 94 million debit and credit card numbers belonging to people in several countries, including Canada, were affected. IPLocks, a database security company, estimates that the TJX security breach could end up costing the company a total of US$4.5 billion (Gaudin 2007). CardSystems Inc., a U.S.-based credit card processor, also suffered major reputational and financial losses when its database was hacked and 40 million credit card accounts were exposed.[12] CardSystems was severely punished for this data compromise when both Visa and American Express reacted by terminating its status as an approved card processing agent. Faced with the prospect of endangering customers' confidence, and of suffering severe reputational and financial punishment, EBPP Consolidators have strong incentives to mitigate their security risks.

2.3.4 Summary

There are risks associated with EBPP services provided by non-FIs, such as the Consolidator bankruptcy, banker, and security risks described above.

While the risks associated with banker default are largely mitigated by the regulatory regime governing the financial sector, users may face potential exposures from the bankruptcy of a Consolidator because of the delay between the delivery of funds by customers and the receipt of funds by merchants. For example, the typical delay with epost is one business day. Some ambiguity exists as to which party, the customer or the merchant, would be liable for any shortfall in funds if a Consolidator went bankrupt before disbursing to the merchant funds it had received from the customer. One complicating factor is that the responsible party may depend on the type of payment made by the customer. However, customers may mitigate the risk that their chosen EBPP Consolidator could go bankrupt by selecting a provider that is dominant in a given market and therefore less likely to fail. The Consolidator's ownership structure can also provide useful information on the likelihood of failure.

---

10. Consequently, EBPP providers that have suffered a security breach may feel discouraged from notifying the public about the breach.
11. Winners Merchant International is a wholly owned subsidiary of TJX, which owns and operates Winners and Home Sense retail stores across Canada.
12. At the end of 2005, approximately half of the U.S. states had passed laws requiring notification of customers whose personal information had been compromised (Office of the Privacy Commissioner of Canada 2006).

With respect to security risk, EBPP Consolidators face legal requirements under PIPEDA (or substantially similar provincial/territorial privacy law) to safeguard individuals' personal information. EBPP Consolidators also have strong incentives to implement secure technologies, because of the reputational and financial damage that would result from a major security intrusion. However, in the event of an intrusion, EBPP providers may have an incentive to not disclose this information to the public, to the detriment of users.[13] This incentive to keep information about a security breach secret could be addressed by an amendment to PIPEDA that is currently under consideration. If PIPEDA were ultimately amended to include a duty to notify individuals when their personal information has been compromised, then an EBPP provider would be required by law to disclose that it had suffered a security breach.

3 Online Person-to-Person Payments (P2P)

The development of P2P (and P2B, person-to-business) payments can be attributed to online auction websites, like eBay, since buyers, as individuals, needed a safe way to transfer money to sellers.[14]

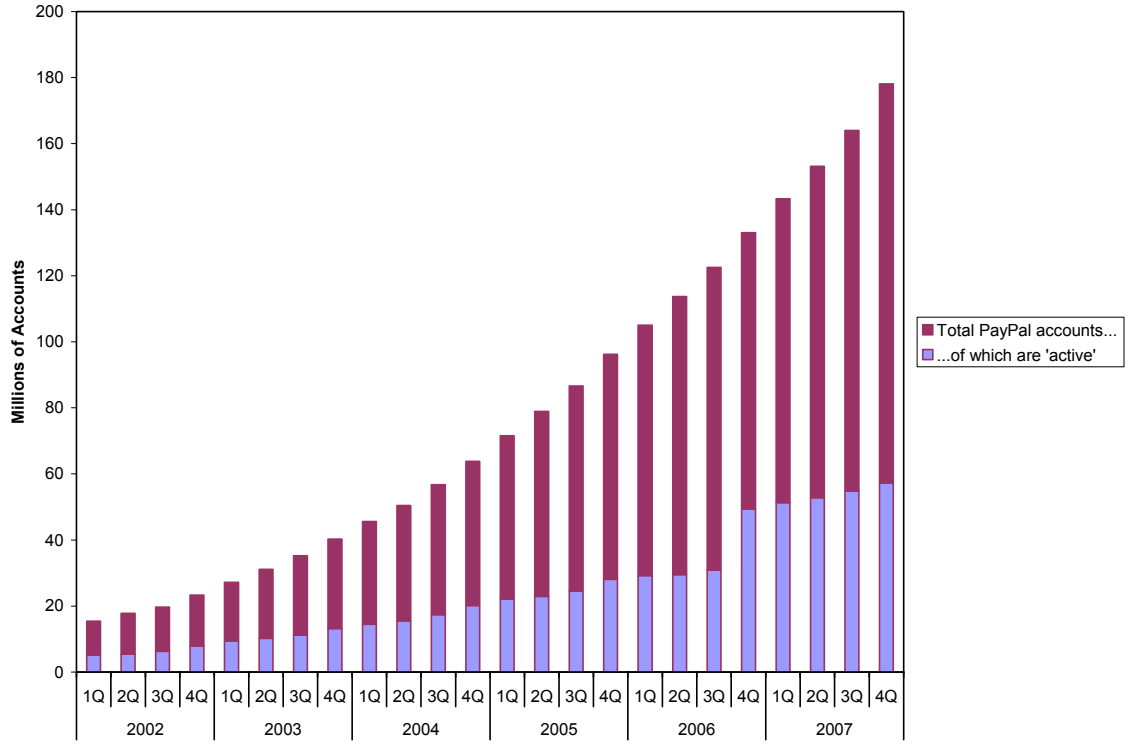
3.1 PayPal

Although there are other examples of non-bank P2P payment providers in Canada, such as TelPay and UseMyBank, the most prominent example is PayPal, which is owned by eBay. PayPal is regulated in the United States as a money transmitter and deposit broker, not as a bank.[15] In the user agreement that is applicable to an account holder in Canada, PayPal emphasizes its non-bank status by requiring account holders to acknowledge that "PayPal is not a bank and the Service is a payment processing service rather than a banking service."

The worldwide growth of PayPal accounts and PayPal quarterly value and volume has been steady, as shown in Charts 1 and 2. It is estimated that, in 2006, PayPal processed 6 per cent of online payments worldwide; credit cards are most commonly used for making payments on the Internet (Holahan 2007).

13. If the service provider felt that the public would ultimately learn about the security breach, then the service provider may have an incentive to disclose the breach.
14. For simplicity, only the acronym P2P will be used in the remainder of this section; however, comments made will also apply to P2B payments schemes.
15. However, for its European operations, PayPal received a banking licence in Luxembourg, effective 2 July 2007, so that it could market its payment services more easily (PayPal 2007).

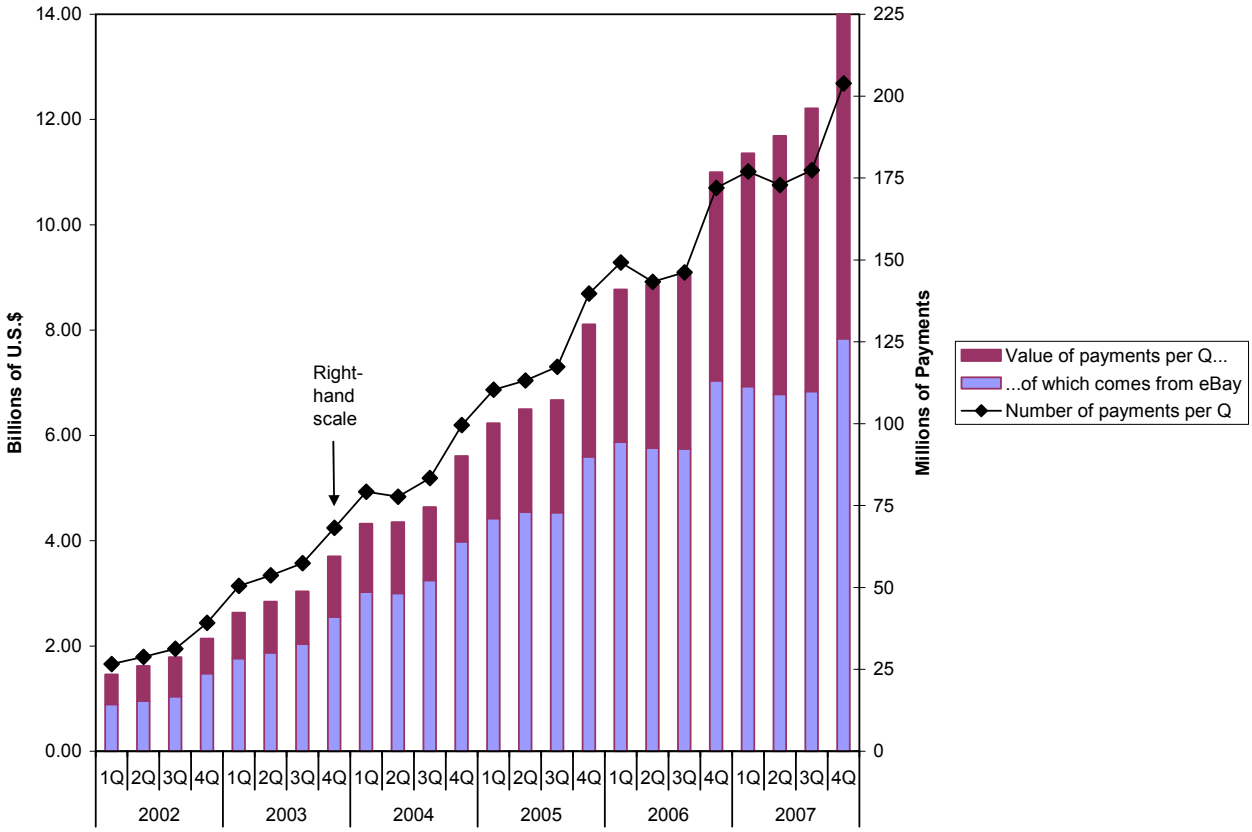
Chart 1
Growth of PayPal Accounts



Notes: The sharp increase in active accounts in 4Q of 2006 occurred because the definition changed from accounts used for at least one payment transaction during the quarter, to accounts used for at least one payment transaction during the past year. eBay stopped reporting the total number of accounts in 4Q of 2007, and thus the figure quoted above is the author's estimate (using the growth rate from 4Q of 2006).

Sources: Payments News (2007a), eBay (2007b)

Chart 2
PayPal Value and Volume per Quarter



Notes: Because of a reporting change by eBay, figures for 4Q of 2007 are net of payment reversals, whereas all other figures are reported on a gross basis. As a benchmark, in 3Q of 2007, payment reversals accounted for 2.93 per cent of gross payment volume and 5.30 per cent of gross payment value.

Sources: Payments News (2007a), eBay (2007b)

The purpose of PayPal is to allow consumers to transfer funds electronically to a merchant or an individual receiving payment without having to disclose financial information such as bank account or credit card numbers. To effect a payment, a PayPal account holder first funds its account using a linked credit card or bank account. Payments can then be sent using this value or using a value previously stored in the PayPal account. To receive a PayPal payment, the recipient must have a PayPal account.[16] The recipient can choose to leave the funds in the PayPal account

16. The receiver is charged a fee, but the sender is not.

so that they can be used for making future payments, although it is not necessary to keep funds with PayPal to use its service. Account holders that do wish to keep funds with PayPal can elect to earn a return by enrolling to invest the balance in the PayPal money market fund; however, this fund may lose value. Account holders with balances that do not enrol in this investment program will have their funds placed in a pooled account at an unaffiliated bank. As an alternative to keeping value stored in a PayPal account, the recipient can have the funds deposited in their personal bank account, which is linked to PayPal. Finally, the recipient can choose to receive the funds by cheque (in certain countries).

3.2 Risk analysis

Some of the risks applicable to EBPP Consolidators are common to P2P systems, like PayPal. Using PayPal as an illustrative example, the following risks will be discussed in turn: (i) liquidity risk, (ii) market risk, (iii) bankruptcy risk, (iv) banker risk, and (v) security risk. The first four of these risks apply only to PayPal accounts that have balances, whereas security is a risk even with empty accounts. Liquidity risk is unique in that it arises as a result of rules put in place by PayPal in order to control other risks.

3.2.1 Liquidity risk

Pursuant to section 10 of the user agreement applicable to Canadian account holders, PayPal can "place holds on funds in your account" and "limit access to an account and any or all of the account's functions," if, for example, the account holder breaches the user agreement or undertakes actions that may pose a significant credit or fraud risk to PayPal (PayPal 2008f). Furthermore, under PayPal's policy on closing accounts and limiting account access, PayPal can limit access to sending money or making withdrawals from an account (PayPal 2008f). The reasons for imposing such limits are specifically enumerated in the policy, which is incorporated by reference into the user agreement.

One way in which a PayPal dispute can arise is if a PayPal payment is associated with an eBay transaction where a buyer purports that a seller did not deliver the promised goods, or that the goods delivered were "significantly not-as-described," and decides to pursue the matter through PayPal's dispute-resolution process.[17]

In the event that a buyer's complaint is decided in the buyer's favour, the transaction is reversed and the seller is responsible for reimbursing the buyer. In some cases, the transaction may

17. If the original payment was funded by credit card, the buyer may, instead, choose to exercise chargeback rights through the credit card issuer.

qualify under PayPal's seller protection policy, in which case PayPal will reimburse the seller for the amount of the reversal or chargeback (up to a limit) (PayPal 2008f). During the period of time when PayPal evaluates a transaction to determine whether it is eligible for seller protection, PayPal will place a temporary hold on the transaction amount. In the period 2006Q4–2007Q3, on average in each of these quarters, 2.86 per cent of gross volume was reversed and 5.20 per cent of gross value was reversed.[18] Moreover, the reversal rate appears to be reasonably steady across the four quarters.

PayPal customers may also face liquidity risk, even if no dispute has been initiated, as a result of a recently announced policy on holds that can be placed on certain eBay-related payments. On 29 January 2008, PayPal announced that it may impose holds, of up to 21 days, on payments pertaining to certain eBay transactions, where it has been determined that the risk of dissatisfied buyers is high (Steiner 2008). It is estimated that the new hold policy will affect about 5 per cent of eBay transactions (note that the policy does not apply to PayPal transactions that are off-eBay) (O'Connor 2008).

If the payment is subject to a hold, then PayPal will release it when the earliest of the following occurs: the buyer leaves positive feedback; three days after confirmed item delivery; or 21 days without a dispute, claim, chargeback, or reversal filed on the transaction (Steiner 2008).

Therefore, PayPal customers are subject to the risk that PayPal may limit access to liquidity present in their accounts, or that it may remove liquidity as part of a reversal. However, PayPal is making a tradeoff in exposing customers to this liquidity risk, by attempting to mitigate risks to itself and strike a balance between the rights of senders (buyers) and receivers (sellers).

For example, PayPal can restrict access to, or withdrawals from, an account where there are reports of unusual credit card or bank account use associated with the account, or where the account has received potentially fraudulent funds. These restrictions impose liquidity risk on the account holder, but they may also help PayPal combat the risk of fraud. In addition, PayPal can reverse a transaction where a seller of goods that was paid by PayPal did not deliver the promised goods. This obviously imposes some liquidity risk on the seller, but at the same time it reduces the risk that the buyer fails to receive a good for which it has paid.[19]

---

18. Data from eBay (2007a, b) were used to calculate the reversal rates.
19. This type of reversal, and the corresponding liquidity risk, also applies to merchants that are paid by credit card. Merchants are subject to chargebacks in the event that a purchaser successfully disputes a charge, as may occur when the purchaser has not received the promised goods.

While these policies may penalize some individual sellers, overall they can have a positive effect for sellers as a group. For example, sellers may benefit if the policy enhances buyers' sense of security and thereby renders them more likely to make purchases.

Regardless of the particular balance that PayPal may choose to strike between the rights of senders (buyers) and receivers (sellers), if customers understand the conditions under which access to liquidity may be limited, then they can make informed decisions about their willingness to accept such a risk, and they can mitigate the likelihood of facing it. The conditions under which PayPal may impose account holds or transaction reversals are enunciated in the user agreement and the associated PayPal policies, which are incorporated by reference in the user agreement. All account holders are required to agree to the terms of the user agreement when they sign up for the service. By reading the user agreement and associated PayPal policies, customers learn about the nature of the liquidity risk they face and how it can be mitigated. For example, customers can mitigate liquidity risk by upholding the terms of the user agreement, by not undertaking actions that impose security and fraud risk on the system, and by delivering the promised goods (where a PayPal payment is associated with the purchase of goods). Given the importance of developing a good reputation, particularly for eBay sellers, PayPal users already have incentives to behave in ways that will mitigate liquidity risk. Although there may be instances where users are unable to avoid holds or reversals, as long as users have a clear understanding of when such holds and reversals may apply they can mitigate the associated liquidity risk by having available sufficient liquidity to meet their needs.

3.2.2 Market risk

A PayPal account holder who chooses to hold a balance can also choose to have this balance invested in the PayPal money market fund, in order to earn a return. In such a case, PayPal makes it explicit that the investments in the fund could lose value. The following is written in bold on the PayPal website:

> Investments in the PayPal Money Market Fund are not insured by the FDIC. Past performance does not guarantee future results. Although the fund strives to maintain the value of your investment at $1.00 per share, it is possible to lose money by investing in the fund. (PayPal 2008b)

The prospectus associated with the PayPal money market fund contains a more comprehensive discussion of the risks associated with the fund (PayPal 2008c).

Therefore, a customer who decides to invest its PayPal balance into the fund does so on the basis of an informed decision about the inherent risks. A customer that does not wish to face these

risks can keep value in its PayPal account without investing the balance in the fund (in which case the balance is put into a pooled account at an unaffiliated bank). Finally, a customer can also choose to keep no value in its PayPal account at all, since doing so is not a condition of using the PayPal service.

3.2.3 P2P provider bankruptcy risk

Customers that have value stored in their PayPal accounts may be at some risk of losing some or all of this amount in the event of PayPal bankruptcy. One way that customers can mitigate this risk is by choosing how long they wish to keep value stored in their PayPal accounts. Since it is not required to store value in an account to use the PayPal service, a customer of PayPal that is worried about the P2P provider's financial health can mitigate this bankruptcy risk by transferring all of the value out of the account. However, because of the potential for holds described in section 3.2.1, customers may not be able to immediately mitigate this risk.

Regardless of PayPal's financial health, customers are discouraged from simply leaving value in their accounts, because PayPal does not pay interest on these amounts. The PayPal user agreement states the following:

> You agree that you will not receive interest or other earnings on the funds that PayPal handles as your agent. PayPal may earn interest on those funds, or may receive a reduction in fees or expenses charged for banking services by the banks that hold your funds. (PayPal 2008f)

Therefore, less value is stored in PayPal accounts than if customers viewed these accounts as savings devices, thus mitigating the risk to customers from PayPal bankruptcy. Furthermore, as with EBPP Consolidators, customers have incentives to sign up with and use dominant, well-established P2P schemes, such as PayPal, which have a critical mass of participants. These dominant players are more likely to be financially sound than P2P providers with less-advantageous market positions. Finally, P2P providers, like PayPal, may institute policies and arrangements that attempt to safeguard value stored by users against creditors' claims:

> PayPal will at all times hold your funds separate from its corporate funds, will not use your funds for its operating expenses or any other corporate purposes, and will not voluntarily make funds available to its creditors in the event of bankruptcy or for any other purpose. (PayPal 2008f)

3.2.4 Banker risk

When a customer who has not enrolled in the PayPal money market investment fund chooses to keep funds with PayPal, those funds are placed by PayPal, as the customer's agent, in a pooled account with one of either Wells Fargo Bank, Comerica Bank, or Bank of America.[20] These banks are subject to the regulatory regime governing the U.S. financial sector. U.S.-dollar balances are eligible for Federal Deposit Insurance Corporation (FDIC) pass-through insurance, protecting the customer's funds against failure of the bank at which the funds are placed, up to US$250,000 (including any other deposits held by the customer at the failing bank) (PayPal 2008a).[21] Balances held in other currencies are, however, not protected by FDIC pass-through insurance, and thus all Canadian balances kept within PayPal are subject to banker risk. Customers can mitigate this risk by deciding not to leave value in their PayPal accounts, and doing so does not impair the customers' ability to use the service. However, because of the potential for holds described in section 3.2.1, certain customers may not be able to immediately mitigate this banker risk.

3.2.5 Security risks

Failure during the authentication process is another risk common to both the EBPP and P2P systems, except that with P2P schemes the ramifications are potentially more severe. For example, if a customer's PayPal account is accessed by someone else, then the fraudster may be able to transfer any value left in the compromised account to another account, perhaps with the hope of removing the funds from the system. Of course, the size of this loss is limited to the amount held in the compromised PayPal account. However, PayPal accounts can be linked with bank accounts or credit cards, and so, even if no value has been left in the compromised PayPal account by its holder, a fraudster may be able to transfer funds from that account to another PayPal account, with the ultimate goal of removing the funds from the system.

To mitigate the risk of funds being stolen from a compromised account, PayPal has instituted a number of risk mitigation measures. For example, when any PayPal payment is made from a given account, the account holder receives an email notification. Thus, an account holder who had not made the payment would know that the account had been compromised and could immediately inform PayPal. In addition, every PayPal transaction passes through fraud prevention models, similar to those used by credit card companies. In January 2008, PayPal acquired the Israeli anti-fraud company, Fraud Sciences. To help PayPal further differentiate

---

20. It does not appear that PayPal is legally obliged to do so, but nonetheless it has made this commitment to its customers.
21. On 1 January 2010, the FDIC's standard deposit insurance coverage limit will return to US$100,000.

between real and fraudulent transactions, it is integrating Fraud Sciences' risk tools with its own fraud management system. On top of these fraud detection tools, there are also spending limits associated with each PayPal account, and once these limits are reached, account holders must go through a process in which their identities are more formally verified (called "PayPal Verified"). Finally, although not a PayPal initiative, regulation already exists to deter theft of value from PayPal accounts, since theft is a criminal offence.[22]

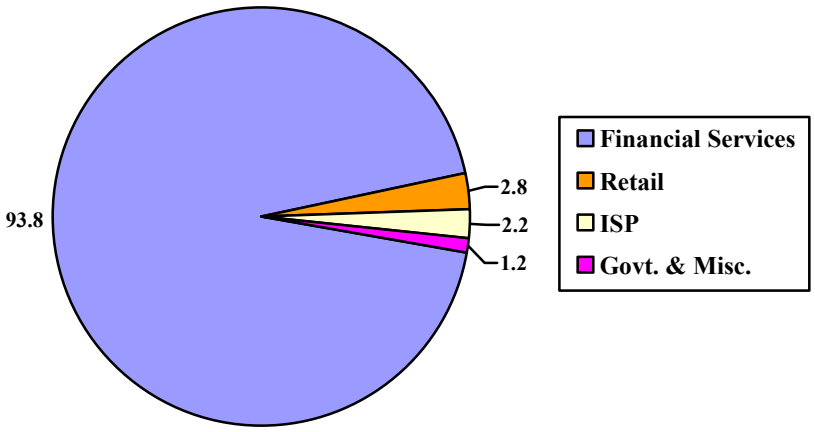
PayPal accounts can become compromised as a result of a successful phishing attack. Phishing is a major security risk to P2P payments systems like PayPal, although banks that offer online banking also face this risk. The most common form of phishing attack is a spoof email, which is an email that appears to have originated from one source when in fact it was sent from another. For example, a PayPal customer may receive an email, purportedly from PayPal, telling them that a security breach has occurred and that the customer must immediately log-in to prevent suspension of the account. A link is provided which appears to direct the customer to PayPal, but which in fact lures the customer to a fraudulent website where their log-in and password are divulged.

A recent survey by Gartner, an IT research and advisory company, found that 3.6 million Americans had lost money in phishing attacks in the 12 months ending August 2007, which was a substantial increase over the 2.3 million who had lost money in the previous year (Gartner 2007). The survey also found that, of consumers who received phishing emails in 2007, 3.3 per cent lost money because of the attack (compared with 2.3 per cent in 2006), and that those 2007 losses amounted to US$3.2 billion. PayPal and eBay continue to be the most-spoofed brands.

The U.S.-based Anti-Phishing Working Group (APWG) reported a breakdown of the industry sectors most often targeted in November 2007 (APWG 2007). As Chart 3 illustrates, the financial services sector (which, by APWG's definition, includes PayPal) was, by far, the most frequently attacked sector.

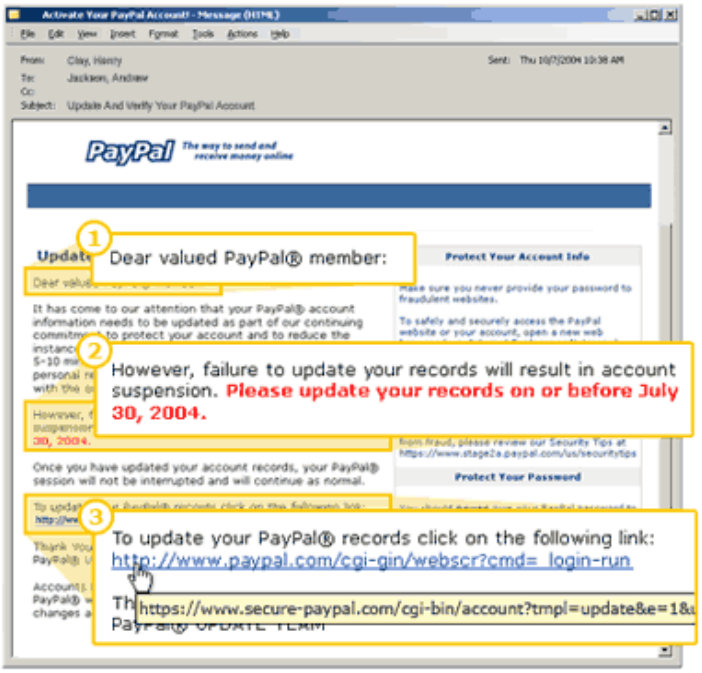
22. Under section 332 of the Canadian Criminal Code (Government of Canada 1985), everyone commits theft who fraudulently takes, or converts to their use or to the use of another person, anything with the intent to deprive the owner of it.

Chart 3
Percentage of Total Phishing Attacks by Sector



Because phishing is a significant security risk facing P2P systems, efforts to mitigate this risk have arisen freely. The development of the APWG is an example of an industry-driven initiative to report and eliminate phishing scams on the Internet. The Truemark service, offered by Iconix, helps email recipients determine whether an email they have received is genuine by placing an icon next to legitimate email messages. This service has recently become available to PayPal account holders (Iconix 2008). In addition, P2P providers and other phishing targets are using education as a tool for fighting this crime. For example, all PayPal customers are educated about how to recognize spoof emails and thereby protect themselves from email phishing attacks. PayPal's website lists "10 ways to recognize fake (spoof) emails," including the three shown in Chart 4.

Chart 4
Three Ways to Recognize Spoof Emails



1 **Generic greetings.**
Many spoof emails begin with a general greeting, such as: "Dear PayPal member."

2 **A false sense of urgency.**
Most spoof emails try to deceive you with the threat that your account is in jeopardy if you don't update it ASAP.

3 **Fake links.**
The text in a link may attempt to look valid, then send you to a spoof address. Always check the source of a link before you click. Mouse over it and look at the URL in your browser or email status bar. If the link looks suspicious, don't click on it. Be aware that a fake link may even have the word "PayPal" in it.

Source: PayPal (2008d)

PayPal also asks it customers to forward any suspected phishing emails they may receive.

So that security threats do not discourage potential customers from using its service, PayPal commits on its website that "[y]ou are not responsible for unauthorized payments sent from your PayPal account" and that "[i]f we find the transaction is unauthorized, we'll refund the entire amount" (PayPal 2008g). PayPal is not legally obliged to make such a commitment, and it cannot be said with certainty that the commitment would be honoured in the face of large losses.[23] Indeed, the Electronic Funds Transfer Rights and Resolution Policy, which is incorporated by reference into the user agreement, seems to provide PayPal with the ability to pass on some of the losses from unauthorized transactions to the affected account holder, depending on how promptly PayPal is notified about the unauthorized activity. The section in this policy on liability for unauthorized transactions states that customers should contact PayPal at once if they believe that their user ID or password has been compromised, or if someone has

23. eBay reported that PayPal fraud and protection program losses represented 0.25 per cent of the US$12.2 billion worth of payment value initiated through PayPal in 2007Q3 (eBay 2007a).

transferred money from the account without permission. In addition, the section states that prompt notification limits the customer's liability, as follows:

> If you notify us within two business days after you learn that your password or other means to access your account may have become known by an unauthorized person, you can lose no more than $50.00 if an unauthorized person uses your password or other means to access your account without your permission to initiate a transaction. If you do not notify us within two business days, and we can prove that we could have stopped someone from using your password or other means to access your account without your permission if you had told us, you could be liable for as much as $500.00.
>
> If you do not notify us within 60 days after receiving notice, you may not recover any money you lose after the 60 days if we can prove that we could have stopped someone from taking the money if you had notified us in time. If a good reason (such as a long trip or hospital stay) kept you from notifying us, we may extend the time periods. (PayPal 2008f)

Consequently, there is some ambiguity as to who is ultimately responsible for losses resulting from unauthorized activity, and this uncertainty makes it more difficult for users of the PayPal service to assess the risks they may face from security breaches.[24] Customers should be able to make informed decisions about the use of a particular non-bank retail payment service, and, in the case of PayPal, a less ambiguous policy regarding liability for unauthorized activity would help them to do so. Moreover, the incentives for mitigating security risks depend, in part, on how the liability for unauthorized activity is ultimately apportioned. If PayPal fully refunds customers in the event of unauthorized activity, this encourages the use of the service, but it creates moral hazard, shifting the incentive to avert unauthorized activity away from customers and onto PayPal. If users bear some liability, however, this strengthens the incentives that users have to protect their passwords, avoid phishing attacks, and safeguard their accounts from unauthorized access.

A customer service representative from PayPal indicated that, notwithstanding the user agreement, PayPal's practice is to fully refund customers in the event of unauthorized activity. This commitment, if credible, and a desire to avoid the reputational damage associated with a security breach, encourage PayPal to mitigate security risks by educating customers, pursuing fraudsters, and improving the security of its technology. A transaction between eBay and VeriSign, a network infrastructure and securities solutions company based in the United States,

---

24. The responsible party may also depend on how the PayPal account was funded.

demonstrates eBay's commitment to improving the security of its authentication technology, which is used by PayPal customers (Electronic Payments International 2005b). As part of the deal, VeriSign provides eBay and PayPal with security services, including the deployment of two-factor authentication. To log-in using two-factor authentication, customers use two independent means of establishing identity: typically, something they know, such as a traditional password, and something they have, such as a hardware token. Thus, even if a third party was able to acquire a customer's password, the third party would also need the customer's hardware token to access the PayPal account. In 2007, PayPal and eBay started the rollout of these authentication tokens (called PayPal Security Keys) to some of their customers as a means of strengthening their security measures (PayPal 2008c). The PayPal Security Keys are not currently available in Canada.

3.2.6 Summary

In the case of PayPal, which we use as an example to illustrate the P2P service, users face liquidity risk because of the potential for holds or reversals. In exposing its customers to this liquidity risk through its rules, PayPal is attempting to control other risks, such as fraud. Knowing the conditions under which such holds and reversals are triggered allows users to mitigate the associated liquidity risk by avoiding the triggers, and users who wish to develop good reputations (particularly, sellers on eBay) already have an incentive to do so. Where the triggers simply cannot be avoided, PayPal customers can mitigate the associated liquidity risk by having available sufficient liquidity to meet their needs.

PayPal customers who choose to keep balances in their accounts can decide to invest these balances in the PayPal money market fund, in order to earn a return. PayPal makes it very clear that there are market risks associated with this investment, and thus customers who choose to proceed are doing so on an informed basis. Customers can mitigate these risks by not leaving value in their accounts, or by leaving value in their accounts but choosing to not invest them in the fund.

Users of a P2P service, such as PayPal, also face potential exposures associated with bankruptcy of both the P2P provider and its bank. In the case of PayPal, users are able to mitigate these risks by choosing not to store value within their accounts, since it is not necessary to keep an account balance in order to use the service. However, because of the potential for holds, users may not be able to immediately mitigate these risks, if, for example, there are temporary restrictions on transferring value from the account.

The consequences of a security breach at a P2P provider, such as PayPal, are potentially quite serious, since value may be stolen from the compromised account. Choosing to store no value within an account does not completely mitigate the risk that funds may be stolen from it if compromised, because PayPal accounts can be linked to bank accounts or credit cards. In addition, there is some ambiguity as to which party, the account holder or PayPal, is ultimately liable for losses stemming from unauthorized account activity. To reduce potential losses resulting from unauthorized activity and to prevent the reputational damage that would be associated with a security breach, PayPal has incentives to mitigate security risks by educating customers, pursuing fraudsters, and improving the security of its technology.

4 Pre-Funded Cards

Pre-funded payment instruments either have value stored directly on a card or, more commonly, the value is recorded in a remote database. Pre-funded cards can be *closed, semi-closed,* or *open system*. Closed system cards, like most gift cards, can be used only with the specific merchant that issues them. Semi-closed system cards are issued by a third party and are redeemable at multiple merchants within a limited area (such as a shopping mall gift card). Open system cards, which include payroll cards issued by employers for paying salaries or benefits, are either Visa- or MasterCard-branded and may be used anywhere the brand is accepted. As a result of this network branding, open system pre-funded cards can be processed using the same point-of-sale (POS) tracks as traditional debit and credit cards.[25] Finally, all pre-funded cards can either be *single-load* or *reloadable*, with the latter being typically funded by traditional means, such as from a bank account, credit card, debit card, or cash.

Some pre-funded products rely on contactless technology, instead of swiping, to transmit the information on these cards. Payment methods that use contactless technology do not constitute a separate and distinct payments scheme, but instead represent a unique method through which payment functions can be delivered. Bluetooth, infrared, near field communication, and radio frequency identification (RFID) are all used to transmit information without contact.

One of the world's most successful pre-funded cards is the Octopus Card in Hong Kong, which is a contactless pre-funded card that relies on RFID. The Octopus Card was first introduced in 1997, to provide a means for paying public transport fares in Hong Kong, but currently it is accepted at over 3,000 retail outlets, including large chain stores, supermarkets, convenience

25. The Canadian Payments Association (CPA) has issued guidelines so that its members may better understand their rights and responsibilities with regard to pre-funded products permissible under the CPA's payable-through arrangement policy (Canadian Payments Association 2008).

stores, and fast food restaurants, as well as at 5,000 self-serve kiosks such as vending machines, photo booths, and public pay phones (Octopus Cards Limited 2008a). There are currently over 16 million Octopus Cards in circulation, and over 10.5 million transactions are processed each day, amounting to the equivalent of US$3.8 billion in payment activity each year (Octopus Cards Limited 2008b).

In Canada, Dexit Inc., established in 2001, was an early, contactless, non-bank pre-funded payments scheme that relied on RFID. Dexit customers placed Dexit tags against the merchant's tag reader to authenticate a transaction, which was usually a small-value purchase. The company is currently pursuing a modified strategy under a new corporate name, Hosted Data Transactions Solutions Inc. (HDX). It focuses its efforts on integrating the Dexit prepaid contactless technology directly with its POS system technology, allowing each client to privately brand the solution (HDX 2007). For example, one client is an Ontario high school that enables its students to pay for their cafeteria meals using contactless Dexit tags that have been branded for the school.

4.1 Gift cards

Gift cards are the most common type of pre-funded cards issued by non-banks.[26] Gift cards are typically closed system, but may be either single-load or reloadable. To purchase a retailer's gift card, customers can pay using the normal methods, after which point the merchant swipes the gift card through its POS reader to activate it for the card issuer. The issuer also inputs the sale of the card into its database. To redeem value on the card, the merchant swipes it through its POS reader, and transaction details are sent to the issuer. The issuer searches the database for the appropriate gift card number and, if there are sufficient funds, sends authorization to the merchant.

Gift cards in Canada are growing in popularity, according to a Statistics Canada survey of 80 large retailers (Bahta, Tsang, and Weise 2006).[27] Table 1 shows, for different types of large retailers, the percentage that offered gift cards in the Christmas seasons from 2003 through 2005. Only about half of large retailers offered gift cards in 2003, but, two years later, eight out of ten were doing so. Furthermore, among all retailers (i.e., not just the large ones), 55 per cent of sales in December 2005 came from stores that offered gift cards.

---

26. Pre-funded telephone cards are also commonly issued by non-banks.
27. "Large retailers" are the regular respondents to Statistics Canada's monthly survey of large retailers, which is a panel of about 80 enterprises covering Canada's largest food, clothing, home furnishings, electronics, sporting goods, and general merchandise retailers, representing approximately 35 per cent of annual retail sales (after excluding recreational and motor vehicle dealers).

Table 1
Types of Large Retailers Offering Gift Cards

Trade group	% of stores		
	2003	2004	2005
Home electronic and appliance stores	92	93	100
General merchandise stores	87	91	90
Furniture stores	84	85	85
Clothing stores, including shoes and accessories	36	54	79
Supermarkets	57	71	70
Other stores	54	81	79
Total – Large retailers	53	68	82

The reloadable Starbucks gift card, launched in 2001, is one of the most popular in North America. Almost 100 million of these cards have been activated since 2001, and they have been reloaded almost 40 million times (CBC News 2007). At the end of 2007, Tim Hortons introduced its own reloadable gift card, called the QuickPay Tim Card.

According to the J.C. Williams Group, a retail consultant firm, retailers that offer gift cards benefit from incremental sales, since 20 per cent of consumers spend almost double the initial face value of their gift card (Praw 2004). Retailers also gain from the interest earned on the outstanding balances, and, in the approximately 10 per cent of cases where outstanding balances are never redeemed, these unused amounts may be a windfall to retailers. For example, TowerGroup estimates that, of the $80 billion worth of gift cards purchased in the United States in 2006, about $8 billion is unused (TowerGroup 2006). In addition, over 2006 and 2007, the electronics retailer, Best Buy, which has a retail presence in the United States, Canada, and China, added $135 million in unused gift card income to its total operating income (Byrnes 2008).

One reason an outstanding balance might not be redeemed is if the gift card has expired, although some retailers have a policy that no expiry date shall be associated with their gift cards. This policy became the law in Ontario on 1 October 2007, when amendments to the Consumer Protection Act and Ontario Regulation 17/05 that relate to the sale of gift cards came into effect (Government of Ontario 2007). In addition to prohibiting expiry dates on cash-equivalent gift cards (i.e., gift cards for a specific dollar amount, rather than specific goods or services), the consumer protection measures eliminate fees such as those for dormancy (except for fees to

customize a card, or to replace a stolen card), and require clear and prominent disclosure of any related terms or conditions. The new rules apply to gift cards, bought on or after 1 October 2007, that are issued by single retailers (i.e., closed system). Gift cards redeemable at more than one unaffiliated retailer, such as semi-closed system cards issued by shopping malls, are temporarily exempt while the Ontario government consults with stakeholders.[28]

In Manitoba, consumer protection legislation on gift cards that is similar to that of Ontario's came into effect on 1 November 2007. In British Columbia, a consultation process is under way to help the provincial government determine whether it should regulate gift cards and certificates.

4.2 Risk analysis

Gift cards illustrate the key risks applicable to pre-funded products, since they are the most common pre-funded products issued by non-banks. The risks, discussed in turn below, are: (i) bankruptcy risk, and (ii) security risk.

4.2.1 Bankruptcy risk

Customers do face risks associated with the bankruptcy of a pre-funded card issuer, such as a retailer that issues gift cards. In Canada, there is no regulatory framework restricting the manner in which the unused gift card balances can be used, and these funds may become comingled with the firm's general operating funds. This is distinct from the United States, where most states have tried to regulate pre-funded card issuers by extending the existing "money transmitter" laws (Furletti 2004). Approximately 45 states have adopted some form of this law, which applies to non-banks performing payment services, and which limits the manner in which the float can be used (for example, unused funds must be kept in highly secure investments).

In Canada, a customer who purchases a gift card from a retailer would likely have difficulty recovering any unspent balance in the event that the retailer declared bankruptcy. Customers wishing to recoup any unspent gift card balances would have to take their place in line, as unsecured creditors, with all other creditors. The best chance a customer may have of recouping unspent balances is if the retailer, as part of a bankruptcy reorganization, is granted permission to honour outstanding gift cards in hope of maintaining good customer relations. A competing retailer may even be willing to partially honour the gift cards of a bankrupt competitor. For example, following the bankruptcy of Sharper Image Inc., Brookstone Inc. announced that it

28. Of the $1.5 billion in annual gift card sales in Ontario, approximately 85 per cent of the cards are sold by individual retailers (*Globe and Mail* 2007).

would allow holders of Sharper Image gift cards to redeem their cards for 25 per cent off any purchase, regardless of the amount of the card. But, even if customers are unable to recover unspent gift card balances, the losses suffered by individual consumers would not be large, since individual balances tend to be relatively small.[29]

Bankruptcy risk associated with store-value cards is mitigated to the extent that larger retailers are more likely to offer gift cards. Statistics Canada's gift card survey demonstrated that gift cards tended to be introduced by retailers that had higher sales (Bahta, Tsang, and Weise 2006). For example, retailers that introduced gift cards in 2003 had sales per store of $11.8 million in 2005, whereas retailers that had not yet introduced gift cards in 2005 had sales per store of $5 million. In addition, large retailers that offered gift cards during all three years of the study accounted for 71 per cent of large retailers' sales, whereas large retailers that did not offer gift cards in any of the three years accounted for only 8.5 per cent of the sales. These statistics imply that customers are more likely to purchase gift cards from large, well-established retailers. All else equal, a retailer with higher sales is less likely to go bankrupt than a retailer with lower sales. Therefore, simply by choosing retailers that are less likely to incur financial troubles associated with bankruptcy, customers mitigate the risk that the gift cards they purchase from a retailer will become useless.

Where a pre-funded card has already been purchased but the customer later becomes worried about the financial health of the issuer, the customer can immediately mitigate this bankruptcy risk by spending the card's outstanding balance.[30]

4.2.2 Security risk

An obvious security risk related to pre-funded cards is that they may be used if lost or stolen. However, the value of individual gift cards tends to be quite small, and they often contain maximum load values. Furthermore, some gift cards can be cancelled if reported lost or stolen. For example, by registering the QuickPay Tim Card online, the holder can protect the balance on the card against loss or theft. Of course, the replacement card will not include any value redeemed before the card is reported lost or stolen. Although gift cards should be treated like cash, there may be less of an overall security risk associated with the loss or theft of gift cards

29. Research by the J.C. Williams Group suggests that the average gift card value purchased is $50, while 50 per cent of purchased cards fall into the $20 to $25 range (Praw 2004).
30. This may, however, reduce the value of the product to the cardholder, if they would have preferred to spend the balance at a later date.

than with cash, because of the ability to protect unredeemed balances on some lost or stolen cards.

Another security risk is that a merchant may, accidentally or otherwise, charge the cardholder more than once for a single purchase. However, to mitigate this risk, a cardholder can get a receipt and check the account balance. In addition, a cardholder can monitor the account balance and account activity of those cards that can be registered online.

Some pre-funded cards rely on contactless technology, instead of swiping. Because of the airborne communication, pre-funded cards that transmit their information using contactless technology, such as RFID, may potentially pose a greater security risk than the traditional pre-funded cards.[31] Most RFID tags are passively powered by the electromagnetic waves emitted by the reader (Knospe and Pohl 2004). Radio communications between RFID tags and readers do raise certain security issues, such as confidentiality, availability, and authenticity.

> ***Confidentiality:*** The communication between a tag and the reader may be unencrypted. However, the communication range between the tag and the reader is generally quite small, and thus an eavesdropper must be close in order to listen in.
>
> ***Availability:*** Communications can be disturbed through the use of RFID blockers, which interrupt the communication of a reader with some or all tags (Juels, Rivest, and Szydlo 2003).[32]
>
> ***Authenticity:*** The unique identifiers belonging to each tag are not generally tamper-resistant, and thus authenticity is at risk. However, there are protocols that authenticate the tag to the reader and protect against counterfeiting.

4.2.3 Summary

The most common pre-funded cards issued by non-banks are gift cards. Some provinces in Canada are starting to regulate gift cards, focusing on specific concerns such as expiry dates and the disclosure of terms and conditions.

---

31. Of course, the additional security risks that may be associated with contactless technology exist whether the product is issued by a bank or a non-bank.
32. While Juels, Rivest, and Szydlo's (2003) stated motivation for developing the blocker is the protection of consumer privacy, they acknowledge that a blocker tag could be used to mount a denial-of-service attack against a reader.

Pre-funded cards, like gift cards, do pose bankruptcy and security risks to customers. However, if a customer is concerned about the financial viability of a particular card issuer, then they can avoid the associated bankruptcy risk by choosing not to purchase a card from them. Indeed, customers tend to purchase gift cards from large, well-established retailers that, all else equal, may be less likely to incur the financial troubles associated with bankruptcy. In terms of security risk, losing a gift card with an unredeemed balance is no worse than losing currency of value equal to the unredeemed balance. There may, in fact, be less security risk than with cash, since some card schemes protect remaining balances after the card has been reported lost or stolen.

5 Policy Implications

We have examined the three broad types of non-bank payments schemes currently available in Canada, illustrating each by focusing on specific examples, such as epost, PayPal, and gift cards. The examination has included a discussion of the main risks associated with each of the three broad categories, and of the incentives that users and providers may have to manage these risks. Again, we have relied upon the dominant forms within each category to help illustrate the associated risks and incentives. Table 2 provides a summary of the risks, and of the incentives to mitigate those risks.

Table 2
Summary of Risks and Incentives to Mitigate Risks

	EBPP Consolidator (e.g., epost)	P2P (e.g., PayPal)	Pre-funded cards (e.g., gift card)
Bankruptcy risk	The consolidator could go bankrupt during a short delay when funds are in transit	The P2P provider could go bankrupt when the customer still has value stored in its account	The card provider could go bankrupt before the customer has spent all its stored value
Incentive to mitigate bankruptcy risk	Risk mitigated by customers preferring well-established consolidator; consolidator's ownership structure may provide useful information on the likelihood of bankruptcy	Risk mitigated by customers preferring a well-established P2P provider, and by choosing to not store value in account (although, in the example of PayPal, there may be temporary restrictions on removing value)	Risk mitigated by customers preferring cards issued by large, reputable retailers
Security risk	Private information could be compromised	Stored or linked value could be transferred	Card could be lost or stolen before customer has spent all the value
Incentive to mitigate security risk	Risk mitigated by role of reputation; however, operators may have an incentive to not disclose a security breach	Risk mitigated by role of reputation; however, P2P providers may have an incentive to not disclose a security breach	Risk mitigated by incentive to treat card like cash (safeguard accordingly), and by ability to report loss or a stolen card
Market risk		In the example of PayPal, investments in PayPal money market fund could lose value	
Incentive to mitigate market risk		Clearly disclosed risks can be mitigated by not investing in the fund	
Liquidity risk		In the example of PayPal, under certain conditions, it can impose holds on, and execute transaction reversals from, users' accounts	
Incentive to mitigate liquidity risk		Knowing when holds and reversals apply allows users to mitigate risk by having sufficient liquidity; risk is also mitigated by users' incentive to establish reputation (especially eBay sellers), decreasing likelihood of holds and reversals	

This paper does not undertake a complete analysis of the market failures that may justify regulation of non-bank retail payment services. Rather, it sets out a broad framework for considering whether users and providers of non-bank retail payment services have the incentives to manage the associated risks.

A more in-depth analysis is required to confirm the existence of a market failure related to the mitigation of risks inherent in non-bank retail payment services that may justify the need for a regulatory framework governing these services. If this were to be the case, then any such regulatory framework must be balanced in its approach, weighing the benefits of regulation against the costs.

5.1 Benefits of regulation

The benefits of regulation arise from correcting a market failure, which must first be established through a more formal assessment than the analysis contained within this paper. Nonetheless, we can draw on our risk analysis to provide an illustrative example.

As highlighted in Table 2, there may exist a market failure associated with the production of information that could help consumers mitigate the security risk inherent in non-bank retail payments systems. It is important to consumers that a non-bank retail payment service provider have a reputation for operating a safe and secure system. For example, epost or PayPal customers may be willing to use these systems only if they have confidence in the safety of the personal information held by the system operators. For customers to gain this confidence, information about security breaches, and how they were handled, must be disclosed. This type of information is a public good, which has value to individual consumers, but which can be underproduced because its producers have incentives not to produce it. Non-bank retail payment service providers have an incentive to keep secret any breaches they may have suffered, given the importance of reputation to consumers. Moreover, there may exist a coordination problem, since providers of strong security may be willing to disclose breaches, but only as long as providers of weak security do the same.

These incentive problems could be addressed by an amendment to PIPEDA that is currently under consideration. If PIPEDA is amended to include a duty to notify individuals when their personal information has been compromised, then the service provider would be legally required to disclose the event if it had been successfully hacked. Thus, customers could rely on the veracity of a service provider's reputation, helping customers judge whether they are willing to accept the security risks associated with using a particular system. In addition, knowledge that a

security breach must be disclosed should increase the incentives for service providers to implement secure technologies.

5.2 Costs of regulation

As noted earlier, any benefit of regulation must be weighed against the associated costs. There are potentially both direct and indirect costs of regulation.

5.2.1 Direct costs

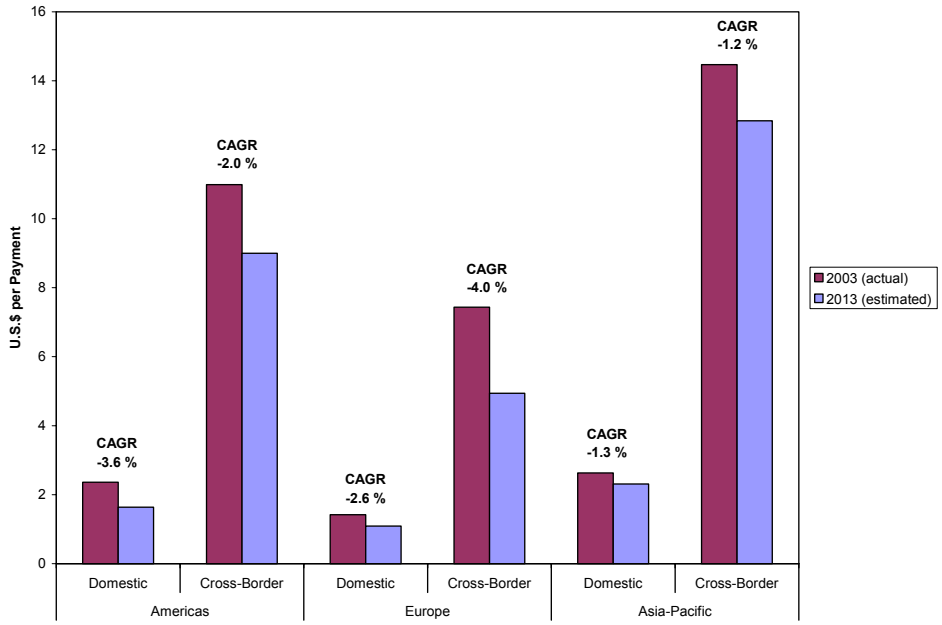
The direct costs of regulation include the costs incurred by the government to develop and administer the regulatory framework, as well as the costs incurred by the private sector to comply with it. It is estimated that, in Canada, the costs of compliance with regulation are almost twenty times the cost of administration. For example, in the fiscal year 1997/98, governments in Canada spent $5.2 billion administering their regulatory activities, whereas the private sector incurred compliance costs of approximately $103 billion (Jones and Graf 2001). A formal cost-benefit analysis of a particular regulation governing non-bank retail payment technologies must carefully consider the direct administrative costs faced by governments, as well as the direct compliance costs faced by the non-bank players.

5.2.2 Indirect costs

Since private firms have to spend scarce resources to comply with regulatory requirements, regulation can become a barrier to entry and hence also impose indirect costs by lessening competition, and thus innovation, efficiency, and choice. In addition, since there are economies of scale in the satisfaction of regulatory requirements, the regulatory burden will be felt disproportionately by small players, which are more likely to be new (PricewaterhouseCoopers 2005). In other words, the costs associated with regulatory compliance may be sufficient to keep some non-banks from entering the payments marketplace, even if their products might have otherwise become successful.

When considering the potential impact of regulation on competition, one must assess whether the increased role played by non-banks has resulted in a more competitive payments market. This does appear to be the case. In a report by Boston Consulting Group (BCG 2004), members of their global payments practice highlight the growing competitive activity of non-banks. A follow-up report by BCG (2006) argues that this is one of the forces still in play in this market. As Chart 5 illustrates, BCG expects that revenue per transaction will fall between 2003 and 2013, in part because of the increased competition from non-bank providers.

Chart 5
Revenue per Payment Transaction

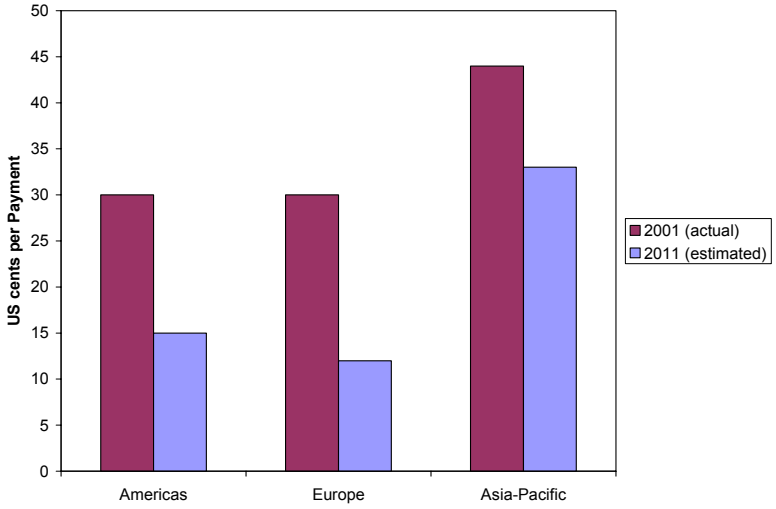


Note: CAGR is the compound annual growth rate.

Source: BCG (2006)

One of the benefits of this enhanced competition is that payment providers will face pressure to introduce significant efficiency improvements; otherwise, the fall in per transaction revenues predicted by BCG will translate into a decrease in per transaction profits, as highlighted in Chart 6.

Chart 6
Profit per Payment Transaction



Source: BCG (2004)

Consistent with the BCG study is a recent report by Hugener and Lerner (2005) on banks' franchise in electronic payments, which recognizes that banks are facing eroding payment margins. Hugener and Lerner argue that banks can no longer rely on their vast branch and ATM networks to maintain a competitive advantage in their payments business, because technology is levelling the playing field. Banks will, instead, be forced to rely on payment innovations and efficiency gains in order to drive future successes in a more competitive payments market.

Given the competitive impact of non-bank retail payments systems, the introduction of a regulatory framework governing these systems may impose indirect costs, if such regulation stifles competition, so that some of the associated benefits, such as innovation, improvements in efficiency, or enhanced consumer choice, are not realized. However, one must also recognize that the presence of regulation may not necessarily result in a less competitive marketplace, because reputation is important to users of non-bank retail payment services, and regulation may act as a substitute for reputation.

Consider, for example, the following analogy. Bank regulation and deposit insurance can act as a (partial) substitute for the development of reputational capital. Although reputation is important to depositors, such schemes allow customers to feel that their deposits are safe, even when

deposited in a relatively new bank that has not yet developed a strong reputation.[33] Similarly, regulation governing non-bank retail payment service providers may make it easier for new players to attract customers, if that regulation acts as a substitute for reputation. In such a case, the indirect costs of regulation may be less severe, since a new player may be able to compete earlier than might otherwise have been possible without a suitable reputation and associated expertise.

Therefore, when assessing whether a specific form of regulation governing a non-bank retail payment technology is justified, one must also be cognizant of any indirect costs. For example, consider the proposed PIPEDA amendment that would require companies to notify individuals if they had suffered a security breach. Such a duty, if it does not contain a minimum threshold, may result in the disclosure of a trivial security breach that nonetheless triggers the exit of some users from the service. Since these types of services often exhibit network externalities, the utility of one user is an increasing function of the number of other users. Thus, the initial exit of users in response to the disclosed security breach could prompt a flood of other users to exit, even though these customers may have felt that the security breach was trivial. In such a case, an additional cost to consider might be the loss of competition, innovation, and consumer choice in the payments market, resulting from the collapse of a non-bank retail payments system.

6 Conclusion

Payment services offered by non-banks have flourished in recent years. Current players in the Canadian marketplace include EBPP Consolidators, such as epost; P2P payment providers, like PayPal; and pre-funded schemes, such as retailers' gift cards. Not only do these non-bank retail payments systems provide customers with a wider variety of payment options, but they also place competitive pressure on banks to develop more innovative and efficient payment services.

In examining the three broad types of non-bank payments schemes currently available in Canada, this paper provides a discussion of the main risks associated with these schemes, such as bankruptcy, banker, security, market, and liquidity risks. While the paper does not undertake a complete analysis of the market failures that may justify regulation of non-bank retail payment services, it does set out a broad framework for considering whether users and providers of these services have the incentives to manage the associated risks.

33. As is well known, this same dynamic involves the generation of moral hazard.

If a more in-depth analysis was to confirm the existence of a market failure related to the mitigation of risk inherent in a non-bank retail payments scheme, then any regulatory response must be balanced in its approach, weighing the benefits against the costs. When evaluating the regulatory burden, one must be cognizant not only of the direct administrative and compliance costs, but also of the indirect impact that regulation may have on competition, innovation, efficiency, and choice.

References

Anti-Phishing Working Group (APWG). 2007. "Phishing Activity Trends - Report for the Month of November 2007." Available at <http://www.antiphishing.org>.

Bahta, D., R. Tsang, and M. Weise. 2006. "Gift Cards: The Gift of Choice." Statistics Canada, Cat. No. 11-621-MIE2006051.

Boston Consulting Group (BCG). 2004. "Preparing for the Endgame: Global Payments 2004."

———. 2006. "Navigating to Win: Global Payments 2006."

Bradford, T., M. Davies, and S. E. Weiner. 2003. "Nonbanks in the Payments System." Federal Reserve Bank of Kansas City.

Byrnes, N. 2008. "The Scramble for Gift-Card Cash." *Business Week* 4 February: 60–61.

Canadian Payments Association. 2008. "Guidelines for Pre-Funded Debit Products Permissible under the CPA's Payable-Through Policy." Available at <http://www.cdnpay.ca/publications/pdfs_publications/prefunded_debit_guidelines.pdf>.

CBC News. 2007. "Gift Cards: The Lure of Plastic." 10 December. Available at <http://www.cbc.ca>.

Department of Justice Canada. 2000. Personal Information Protection and Electronic Documents Act, 2000, c.5.

eBay. 2007a. "Financial Release, Q3:2007." Available at <http://www.ebay.com>.

———. 2007b. "Financial Release, Q4:2007." Available at <http://www.ebay.com>.

Electronic Payments International. 2005a. "Agile EBPP Rivals Keep Banks Alert." April.

———. 2005b. "eBay to Buy VeriSign Security Technology and Its Payment Gateway." November.

———. 2005c. "Banks Must Segment as EBPP Services Boom." December.

epost. 2008. "Terms and Conditions." Available at <http://www.epost.ca>.

Furletti, M. 2004. "Prepaid Card Markets & Regulation." Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper No. 04-01.

Gartner. 2007. "Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks." Press release, 17 December. Available at <http://www.gartner.com>.

Gaudin, S. 2007. "Estimates Put T.J. Maxx Security Fiasco at $4.5 Billion." *Information Week* 2 May. Available at <http://www.informationweek.com>.

Globe and Mail. 2007. "Some Ontario Gift-Card Loopholes Won't be Closed Until After Holidays." 5 December. Available at <http://www.globeandmail.com>.

Government of Canada. 1985. Criminal Code, R.S.C. 1985. c. C-46, s. 332.

Government of Ontario. 2007. "Banning Gift Card Expiry Dates." Backgrounder and press release, 6 December. Available at <http://www.gov.on.ca>.

Holahan, C. 2007. "The Bank of PayPal." *Business Week* 15 June.

Hosted Data Transactions Solutions (HDX). 2007. "HDX Launches its Dexit Prepaid Payment Service at Ontario High Schools." Press release, 18 October. Available at <http://www.dexit.com>.

Hugener, C. and L. Lerner. 2005. "Banking on Payments: Protecting and Extending Banks' Electronic Payment Franchise." Diamond Cluster. April.

Iconix. 2008. "Iconix Truemark Service Available for PayPal Customers." Press release, 28 January. Available at <http://www.iconix.com>.

Jones, L. and S. Graf. 2001. "Canada's Regulatory Burden. How Many Regulations? At What Cost?" Fraser Institute.

Juels A., R. L. Rivest, and M. Szydlo. 2003. "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy." In *8th ACM Conference on Computer and Communications Security*, edited by V. Atluri, 103–11. ACM Press.

Kane, M. 2005. "Canadians Flocking to epost." *Montreal Gazette* 13 June: D4.

Knospe, H. and H. Pohl. 2004. "RFID Security." *Information Security Technical Report* 9 (4): 39–50.

O'Connor, K. R. 2008. "eBay's PayPal Funds Freeze Plan Draws Fire." *Fortune Small Business* 11 February. Available at <http://www.money.cnn.com>.

Octopus Cards Ltd. 2008a. "Business Applications – Payments." Available at <http://www.octopuscards.com>.

———. 2008b. "Why Octopus? Statistics." Available at <http://www.octopuscards.com>.

Office of the Privacy Commissioner of Canada. 2006. "PIPEDA Review Discussion Document: Protecting Privacy in an Intrusive World." July. Available at <http://www.privcom.gc.ca>.

Payments News. 2007a. "A Look At Some PayPal Statistics." Available at <http://www.paymentsnews.com>.

Payments News. 2007b. “RBC, Visa Canada Launch NFC-Based Mobile Payments Pilot.” Available at <http://www.paymentsnews.com>.

PayPal. 2007. “PayPal Expands European Growth with Bank Charter and New European Headquarters.” Press release, 15 May. Available at <http://www.paypal.com>.

———. 2008a. “FDIC Pass-Through Insurance.” Available at <http://www.paypal.com>.

———. 2008b. “Money Market Fund.” Available at <http://www.paypal.com>.

———. 2008c. “Money Market Fund: Prospectus.” Available at <http://www.paypal.com>.

———. 2008d. “Protect Yourself from Fraudulent Emails and Websites.” Available at <http://www.paypal.com>.

———. 2008e. “PayPal Security Key.” Available at <http://www.paypal.com>.

———. 2008f. “PayPal User Agreement.” Available at <http://www.paypal.com>.

———. 2008g. “Report Unauthorized Use of Your PayPal Account.” Available at <http://www.paypal.com>.

Praw, J. 2004. “Gift Cards Are Here to Stay.” J.C. Williams Group.

PricewaterhouseCoopers. 2005. “Regulatory Burden: Reduction and Measurement Initiatives.” Report prepared for Industry Canada, 31 March.

Steiner, I. 2008. “PayPal’s 21-Day Hold Policy for eBay Sellers.” *Auction Bytes* 8 February. Available at <http://www.auctionbytes.com>.

Symcor. 2008. “Profile.” Available at <http://www.symcor.com>.

TowerGroup. 2006. “With Soaring Gift Cards Sales Poised to Exceed $80 Billion in 2006, Unused Card Values are also on the Rise.” Press release, 20 November. Available at <http://www.towergroup.com>.

Uribe, E. 2007. “Mobile Commerce: Making it Work for Canadians.” Public Interest Advocacy Centre, 3 April.