

**Comments regarding the creation of a  
new framework for electronic fund  
transfers in Canada**



**Written by  
Jacques St Amant**

**December 2007**

**Public Interest Advocacy Centre (PIAC)**

**Copyright 2007 PIAC**

Contents may not be commercially reproduced. Other reproduction, with acknowledgement, is encouraged.

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

Tel: (613) 562-4002 Fax: (613) 562-0007

Email: [piac@piac.ca](mailto:piac@piac.ca) Website: [www.piac.ca](http://www.piac.ca)

Canadian Cataloguing and Publication Data

St Amant, Jacques

Comments regarding the creation of a new  
framework for electronic fund transfers  
in Canada

ISBN 1-895060-87-7

## Summary

While there a better framework for electronic payments in Canada is urgently needed, the scope of the consultation currently held by the Department of Finance and the process it has put in place appear unlikely to lead to significant improvements.

The process must allow for real debate and must therefore provide a fairly specific basis for discussion. An effective framework must be based on a set of overarching principles. It would also preferably be established by legislation. In addition, experience shows that the current *Canadian Code of Practice for Consumer Debit Card Services* is not a sound basis for discussion, yet the process proposed by the Department curtails debate, it is based on the current code and it is so imprecise as to scope and other issues that it is difficult for stakeholders to frame comments.

We propose eight principles on which a new framework should be based: universality, neutrality, security, accountability, transparency, liberty, enforceability and legitimacy. We note the growing complexity of the electronic payments field in Canada.

We submit that a new code should have the broadest scope and, in particular, not be limited to a subset of card-based payment mechanisms. We disagree with the view that such new code should not cover payment methods which may be partly regulated otherwise, as a number of important issues remain in fact unregulated. Regulatory underlap and gaps can be more damaging than overlap.

The rationale for risk allocation between market participants must be discussed in depth before issues such as liability and redress can be addressed.

Increased disclosure is not an adequate remedy to unconscionable contractual requirements or business practices, which should be prohibited outright.

Finally, governance issues regarding the payments universe in Canada should be considered carefully, taking heed in particular of current developments in Australia and the United Kingdom.

## Table of contents

I- Beyond the nitty-gritty	1
A- A misguided approach	1
1- The context	1
2- The current approach and its faults	2
B- The intervenor and our comments	5
1- The Public Interest Advocacy Centre	5
2- Our comments	5
C- A principled approach	5
1- A set of guiding principles	5
2- Universality	6
3- Neutrality	7
4- Security	9
5- Accountability	10
6- Transparency	11
7- Liberty	12
8- Enforceability	13
9- Legitimacy	15
10 - A summary	15
II- Reviewing the Current Code	
A- Our approach	16
B- Section-by section review	16
1- The introduction	16
2- Recent Developments	19
3- Towards an EFT Code of Conduct	20
4- Issuance	24
5- Disclosure and Transaction Records	26
6- Transaction Security	30
7- Liability and Redress	33

C- Governance issues	34
1- Australia	34
2- The United Kingdom	35
3- And Canada...	37

# Comments regarding the creation of a new framework for electronic fund transfers in Canada

## I- Beyond the nitty-gritty

### A- A misguided approach

#### 1- The context

Royal Bank and Visa are currently testing a cellphone-based payment service in Ontario using contactless chips<sup>1</sup>.

Things change. Quickly.

The framework for electronic payments in Canada does not change nearly as fast, however, and the current attempt to patch it up falls far short of addressing coming challenges.

Payments stand at the centre of economic life and of consumer relationships with providers. They are increasingly processed through a growing variety of electronic channels. Clearly, the legal framework for electronic payments should be a crucial concern for all economic agents in Canada.

Yet our country's framework for electronic payments is lacking. It is fragmented. It is arcane. Parts are dated. It is largely either voluntary, rife with non-compliance, or both. It is ripe for a substantive and well-thought review.

An effective framework would stand on sound foundations both from a legal and an economic standpoint. It would mitigate operational risk and allocate it to the proper party, and it would provide a modicum of legal certainty. It would sustain a healthy competitive

---

<sup>1</sup> *Canada is not only moving to chip and PIN but also NFC.* Contactless News, November 2 2007; *Visa, Royal Bank of Canada in M-Payments Trial*, epaynews.com, November 6 2007.

market for payments by reducing informational asymmetry, apportioning costs to the least cost avoider where appropriate and promoting all-around efficiency. In short, it would be quite different from the current hodge-podge. The need for an overhaul is obvious.

## 2- The current approach and its faults

The Department of Finance<sup>2</sup> has recently initiated a review. It has opted for a short-form process selectively aimed at augmenting somewhat the *Canadian Code of Practice for Consumer Debit Card Services* (hereinafter the "Current Code"), through a mediated virtual forum and, if we understand Department indications correctly, it intends the New Code to come in force simply through industry adoption, without requiring support from other constituencies. We are respectfully of the view that all those aspects of the Department's approach are wrong.

First, we believe that the smart way to regulate electronic payments is primarily through legislation. Parliament assuredly has jurisdiction over national payment issues, whoever provides them, under *inter alia* subsections 91 (14), (18) and (20) of the *Constitutional Act, 1867*, construed as they should be through an evolutive reading<sup>3</sup>. Legislation is the only way to ensure to all stakeholders, including providers and merchants, a level playing field and the level of legal certainty and transparency that are required for the new payment environment to flourish. Our misgivings are obviously reinforced by Canada's experience with a code in the payments area over the past fifteen years, which has been mediocre at best<sup>4</sup>.

If form is important, contents is even more crucial. A new framework for electronic payments should look towards the future and tackle emerging issues. Already, trends are clear: players in the payments area are multiplying and getting more diverse, new

---

<sup>2</sup> Hereinafter also the "Department".

<sup>3</sup> The Privy Council's "living tree" metaphor still governs the construction of the *Constitutional Act*, as illustrated in *Reference re Same-Sex Marriage*, [2004] 3 S.C.R. 698, §§ 22-23, 29, and *Reference re Employment Insurance Act (Canada)*, [2005] 2 S.C.R. 669, §9. As electronic payments replace bills of exchange and raise issues such as legal tender, there can be no doubt of Parliament's jurisdiction over modern payment instruments. Even if there were, Parliament's jurisdiction over commerce could assuredly be claimed.

<sup>4</sup> Compliance failures have been documented both by Industry Canada. Office of Consumer Affairs. *Highlights from: Evaluation of Operations Related to the Canadian Code of Practice for Consumer Debit Card Services*. Ottawa, Industry Canada, October 31 2002. Available at [http://strategis.ic.gc.ca/epic/site/oqa-bc.nsf/vwapj/EKOS\\_eng.pdf/\\$file/EKOS\\_eng.pdf](http://strategis.ic.gc.ca/epic/site/oqa-bc.nsf/vwapj/EKOS_eng.pdf/$file/EKOS_eng.pdf)(and, in French, at [http://strategis.gc.ca/pics/caf/ekos\\_fre.pdf](http://strategis.gc.ca/pics/caf/ekos_fre.pdf).) and by numerous consumer organisations over the past decade.

technologies are vying for market share and new problems are catching most stakeholders' attention. Yet, the Department calls only a limited number of these stakeholders to participate in a cramped forum: most issues are likely to be left aside or will not benefit from the insight of important actors.

In addition, the format chosen by the Department will constrain discussions and will not enable stakeholders to fully debate the substantial and complex issues at stake. We believe it is more important to get the new framework right than to get it done by next spring and again, experience shows that analysis and resolution of the issues in this area simply cannot be accomplished meaningfully within six or eight months<sup>5</sup>.

We are also disconcerted by the following sentence in the Consultation Paper:

We anticipate the final electronic funds transfer code will be *ready for industry adoption* in 2008.<sup>6</sup>

Whatever flaws the current code may have (and they are numerous), organizations other than "the industry" were invited to endorse it, and some still do. When it was first drafted, it was clearly envisioned as the embodiment of a consensus between stakeholders. We can only regret that the Department has apparently abandoned all hope of reaching such a consensus and will be content with obtaining limited industry support. That orientation does not bode well either for the future code's contents or for the public support it might garner once put in place. There is therefore a serious risk that the process being proposed will in itself significantly undermine the credibility of the new code with the Canadian public.

In 2006, the Canadian Consumer Initiative<sup>7</sup> had listed six "minimal safeguards" that should be put in place to bolster the chances that a process leading to a new code be successful:

- a) the process would be chaired and steered by a person with the required expertise and moral authority;

---

<sup>5</sup> CPA's experience with rule-drafting is compelling in this respect, as is the fact that rule H-1 has needed constant fine-tuning over the past two decades. The notion that a much broader process can achieve workable results in less than a year leaves us rather skeptical.

<sup>6</sup> Our italics. Consultation Paper, section "Towards an Electronic Funds Transfers Code of Conduct", fifth paragraph.

<sup>7</sup> The Canadian Consumer Initiative, or "CCI", serves as a coalition for six of the major Canadian associations involved in consumer issues. PIAC is a CCI member.

- b) the process would not use the current Debit Code as a starting point;
- c) the process would have a specified timeline and be provided the resources required to be effective;
- d) the Code's contents would go beyond already existing legal safeguards and would provide for a level of consumer protection at least equal to best practices elsewhere in the world;
- e) any notion of consensus or majority used in decision-making would explicitly require the consent of the consumer representative category for any decision to be deemed approved;
- f) trade associations would be required to obtain a legally binding mandate from their members that the latter would comply with all provisions of any code that would be adopted and trade associations would agree to enforce such code against their non-complying members.<sup>8</sup>

Obviously, the process currently contemplated comes nowhere near fulfilling these requirements.

It would appear that there are three major paths that could be taken in order to establish a new framework for electronic payments. Government could consult stakeholders and then act, through legislation. Government could bring stakeholders to a table and foster discussions that would lead participants to agree to a number of principles and rules. Or Government could essentially let industry do as it pleases. As the process is presented in the Consultation Paper, we are of the view that debates will be too constrained to be meaningful, and there is clearly no intent to legislate: the first two paths are therefore ignored. We are highly concerned therefore that the current exercise can lead to nothing but a code drafted by the industry (and primarily by some its biggest players), with a modicum of "consultation" thrown in the process. This is in stark contrast with review processes currently implemented in the same area in the United Kingdom and Australia, to which we will return *infra*.

If such is not the Department's intent, we suggest that it is urgent that its position be clarified, and that the format be significantly improved. As things currently stand, PIAC

---

<sup>8</sup> Canadian Consumer Initiative. *Regulating electronic payments: taking the right direction, but not the best path*. Montréal/Ottawa, 2006. 27 p. The document was submitted in answer to the Department's June 2006 *Proposals for an Effective and Efficient Financial Services Framework*. The Initiative serves as a coalition of six of the major Canadian associations involved in consumer issues, including PIAC.

has nonetheless decided to submit the following preliminary comments, but reserves the right to stop participating in the process and does not consent at this point to have its input presented to other parties in any way as the expression of support for the current process or for any code or other instrument that might result therefrom.

In short, we disagree with the Department's choice of the tool to be forged in order to deal with electronic payment issues and we are rather skeptical about the process it has proposed. We retain the faint hope, however, that some input from the consumer side may still be better than none. Hence the following comments.

## **B- The intervenor and our comments**

### 1- The Public Interest Advocacy Centre

The Public Interest Advocacy Centre ("PIAC") is a non-profit organization based in Ottawa that provides legal and research services on behalf of consumer interests and, in particular, vulnerable consumer interests, concerning the provision of important public services. PIAC has been interested in payment and other financial services issues for many years. It has been involved in recent years in the review of the Current Code.

### 2- Our comments

In our view, the format proposed for the current consultation is not conducive to the in-depth debates needed on a number of crucial issues. We therefore articulate some of our views in these comments, to which we will invite stakeholders to refer. We will however post specific, short comments on the Department's forum. They should be read in conjunction with, and in the context of, the fuller examination of issues provided herein.

As already mentioned, these comments should not be read as an endorsement of the Department's process. The fact that we have not commented at this point on any issue raised in the Consultation Paper should not be construed as meaning agreement or disagreement with any position on such issue.

## **C- A principled approach**

### 1- A set of guiding principles

Before delving into the nitty-gritty of detailed rules or specific payment mechanisms, we are of the view that a clear set of overarching principles should be put in place, which

would guide the choices to be made<sup>9</sup>. We believe the following principles should stand as the foundation of any regulatory framework for electronic payments in Canada:

- **universality:** the broadest range of payment technologies should be regulated;
- **neutrality:** all technologies should be regulated by similar rules;
- **security:** payment technologies and processes should be secure and sound;
- **accountability:** risk should be supported by the party which creates it;
- **transparency:** rules, responsibilities, risk, and prices should be clear for all parties;
- **liberty:** payors should be allowed to choose the payment method they prefer;
- **enforceability:** parties should be able to ensure the framework is effectively enforced;
- **legitimacy:** the framework should be persuasive, authoritative, and it should compare favourably with best-in-class comparable instruments worldwide.

Of course, some principles might not be fully applicable in all cases. For instance, a consumer would not be able to compel a merchant to accept a credit card payment if that merchant does not participate in a credit card network. Yet these eight principles can, and should, guide the process leading to new rules for electronic payments in Canada. It may be useful at this point to summarily flesh out briefly what they entail.

## 2- Universality { TC " 2- Universality" \1 3 }

The proliferation of both diverse electronic payment mechanisms and market participants is impressive<sup>10</sup>. Both clarity and fairness to all parties require that, insofar as possible, all providers operate under similar rules as they offer similar payment mechanisms. A level playing field is important for competitors, and users of payment systems must be able to assume that their payment is entirely covered by adequate rules, whatever method they choose and notwithstanding the number of participants in the processing of the transaction.

Currently and according to the payment mechanism used, participants' rights and liabilities vary widely – often without any obvious rationale – and are set through instruments of very different legal standing. The majority of participants, including consumers and most retailers, cannot be expected to determine whether a specific payment

---

<sup>9</sup> We take due note that the Consultation Paper acknowledges that there is some room for "overarching principles" to be provided in the Code, as mentioned in the Paper's section entitled "Towards an Electronic Funds Transfer Code of Conduct".

<sup>10</sup> We shall come back to this issue in section II B 1.

mechanism is appropriately regulated or not, and if so how and by whom. The most effective way to overcome such an informational challenge is to simply establish a coherent regime where essentially all payments are covered: all interested parties therefore know that they can rely on one clear set of rules which mitigate the risks associated with transactions, and know where to find such rules.

### 3- Neutrality

However useful it may be, it is not sufficient to provide a universal regulatory framework for electronic payments. Insofar as possible, it should also be technology-neutral and therefore fairly uniform, whatever payment method may be used.

The current regime is a hodgepodge of rules with differing status, sources and contents. In case of an unauthorized transaction, for instance, the protection afforded to the consumer will vary significantly according to whether it was a credit card payment<sup>11</sup>, a pre-authorized debit<sup>12</sup>, a tele-cheque<sup>13</sup>, an Interac debit card payment<sup>14</sup>, an *Interac online* payment<sup>15</sup>, a payment through a mechanism such as PayPal<sup>16</sup> or a payment through web banking<sup>17</sup>, to give only those examples. Yet, in all cases, a consumer simply wanted to pay a merchant for a product or service and neither consumer nor merchant bargained together for the specific rules applied to the payment method that was used. Those rules are determined by third parties, are largely opaque to most payors and payees, may not serve them in a way they would deem adequate and therefore bring avoidable legal uncertainty, risk and growing inefficiency into the market.

---

<sup>11</sup> In which case legislation caps liability at \$50 and chargeback regimes voluntarily put in place by card issuers (or, in Ontario at least, legislated) may even bring the liability to zero.

<sup>12</sup> In which case a consumer has 90 days under CPA Rule H1 to have the payment unwound directly by his or her financial institution.

<sup>13</sup> In which case a consumer has 90 days to have the payment unwound directly by his or her financial institution, under CPA rule A4.

<sup>14</sup> In which case the provisions of the Debit Code should be applied, with the assorted difficulties associated with its application.

<sup>15</sup> In which case the consumer banking agreement would apply or, if it is more forgiving, the Debit Code should apply *mutatis mutandis*, assuming the consumer's financial institution has undertaken to apply the Code in such cases and effectively does.

<sup>16</sup> In which case nothing but the agreement between the consumer and PayPal and generic contract or consumer law rules will apply.

<sup>17</sup> In which case, again, the contract and contract law will provide whatever recourse the consumer (or other customer, for that matter) may have.

Where a payor is unaware of those differences, he may well opt for a payment method without appropriate knowledge of the risk he incurs.

On the other hand and insofar as payors and payees are aware of some of the legal differences between payment mechanisms, they may opt for a less than optimally efficient solution simply because it appears to lessen a specific type of risk to which they feel more vulnerable. For instance, a consumer making a payment on a website may be tempted to use a credit card to reduce her liability should the good not be delivered, but in so doing she provides to a possibly unknown retailer personal information which may be abused (*i.e.* a credit card number), she uses up credit and she imposes additional costs on the retailer. Other payment methods might be globally more efficient<sup>18</sup>, but are avoided as the consumer focuses on one specific risk and does not take into account factors which act as externalities. As a result, unnecessary discrepancies in the legal framework distort the market.

In short, there is a growing opportunity cost caused by lack of certainty, confidence or accurate information associated with payment mechanisms.

That said and if legal risk is to be properly evened out, it may be that rules governing specific payment methods will need to vary slightly. Credit and debit transactions, for instance, may require somewhat different solutions in some instances<sup>19</sup>. The end result however should be that the level of risk incumbent on the various participants would not vary significantly according to the payment method used<sup>20</sup>, with principled differentiation between specific regimes be kept to a minimum.

Underscoring the need for the implementation of the universality and neutrality principles is the immense informational asymmetry between a small number of networks or other providers, on the one hand, and most payment facility users (payors and payees) on the other. It is trite that a perfect market requires perfect information; imperfect information obviously makes for imperfect markets and the current imbalance must urgently be rectified as much as possible.

---

<sup>18</sup> and the retailer, for one, might wish the consumer to privilege a different payment method.

<sup>19</sup> Although it is noteworthy that an instrument such as the Australian *Electronic Funds Transfer Code of Conduct*, about which more *infra*, does not distinguish between debit and credit cards or other payment mechanisms (with the exception of stored value mechanisms).

<sup>20</sup> Unless, of course, the characteristics of a given method effectively compel different rules, the onus of proving such need being on the party that requires a different set of rules.

#### 4- Security

The need for a reasonably high level of security in the payment environment is so obvious we need not belabor the point. As a most fungible means of exchanging wealth, money has been surrounded since its creation by locks, guards and signatures or other modes of security and authentication. The migration to electronic payments requires however that new solutions be provided to the problem of ensuring that the right people, and only them, have access to their funds, and that they can have complete access to their funds whenever they want to.

The challenge of authentication remains whole. Current methods such as magnetic stripe cards and personal identification numbers are both vulnerable and poorly adapted to the consumer. Stored-value cards are only marginally safer. Biometric methods are not universal<sup>21</sup>, false-positive or false-negative rates are often high and social acceptability is not yet established<sup>22</sup>.

In addition and as noted by the Commission of the European Communities, security is also concerned with matters such as network availability:

[...] the New Legal Framework should address the issue of legal security of the payment environment. This includes the security evaluation of payment systems and instruments, the legal safeguards in the case of non-, defective- or unauthorised execution of payment transactions or of non-access to payment services as e.g. in a breakdown of the payment network.<sup>23</sup>

Electronic payments being dependent upon communications networks, security must also extend to those infrastructures. Both physical and logical security are imperative. The eventual expansion of payments through mobile phone and other devices will not simplify matters.

---

<sup>21</sup> That is, a proportion of the population is unable to identify itself through any given method, usually for health reasons.

<sup>22</sup> In addition, the viability of biometric solutions remains threatened by the industry's financial fragility: see e.g. Wolfe, Daniel. *Solidus' Scramble Shadows Biometric Payments*. American Banker, November 26 2007.

<sup>23</sup> Commission of the European Communities. *Communication from the Commission to the Council and the European Parliament concerning a New Legal Framework for Payments in the Internal Market (Consultative Document)*. Brussels, December 2d 2003. Document COM (2003) 718 final. P. 12.

Vast stores of sensitive information are processed or kept by payment mechanism providers, from credit card numbers to purchase histories. The multiplication of intermediaries raises grave questions in that area, where the majority of the most egregious security breaches have happened in the last few years<sup>24</sup>.

While they raise a quite different set of issues, safety and soundness must also be considered. Intermediaries in the payment chain may be in possession of funds for variable periods<sup>25</sup>, with the attendant solvency risks. Clearing arrangements are getting more complicated and may depend on unregulated participants, such as credit card networks.

In short, security in the payments area is a multi-faceted issue. It is technologically complex and the multiplication of actors does nothing to simplify matters. Yet it is imperative that it be ensured and that all participants be held to a high level of responsibility, consonant with the level of risk they generate. It is difficult to see how such a result can be achieved otherwise than through federal legislation. Codes of practice can only address some of the issues and only those providers who subscribe to such codes.

#### 5- Accountability

Electronic payment mechanisms are designed and chosen by financial institutions and specialized providers. Institutions which offer them often tout their security as one of their strengths. Yet, through contracts or codes of practice, they often seek to transfer as much of the potential liability for risk as they can on consumers, who are for the most part powerless to assess and mitigate risk, or on other parties which may not be much better equipped to manage it otherwise than by also pushing it down to the consumer.

Australian authorities remain of the view that, in many cases, an "economically efficient loss allocation rule would" assign liability on "[...] the account institution to encourage it to improve the security of the" system over time<sup>26</sup>. We agree that the least cost avoider

---

<sup>24</sup> Acquirers have fallen prey to hackers. It has also been alleged that bank employees in the United States may have leaked personal information related to up to 100 000 accounts: *Did bank employees sell account info?* CNN/Money, May 23, 2005, at [http://money.cnn.com/2005/05/23/news/fortune500/bank\\_info/index.htm?cnn=yes](http://money.cnn.com/2005/05/23/news/fortune500/bank_info/index.htm?cnn=yes).

<sup>25</sup> PayPal being a noteworthy example. Unregulated stored-value issuers raise questions such as value redemption.

<sup>26</sup> Express reliance of Australian authorities on the least cost avoider principle, elaborated first by Nobel Prize laureate Ronald Coase, goes back at least to 1999 and is reiterated in the current consultation paper: Australian Securities and Investments Commission. *Consultation Paper 78 - Reviewing the EFT Code*. ASIC, January 2007. 129 p. P. 62. The Paper can be

principle suggests in this case that payment system providers are best placed to reduce costs by improving their products at a systemic level, instead of burdening consumers with compliance with unrealistic requirements.

Liability should also be allocated taking fully into account the informational asymmetry<sup>27</sup> between providers and consumers. Financial institutions may argue that such a principle would create a moral hazard and reward negligent customers; in fact, the current legal framework effectively rewards institutions that prefer to transfer liability on consumers through contract rather than implement secure payment mechanisms. The consequences of the latter moral hazard are far more significant for the Canadian economy. Financial institutions and other major players are in a position to put in place globally safe *systems*; consumers can do nothing but to try and secure *individual transactions*. The onus on providers should therefore be obvious. They are the ones that should be held to account first.

#### 6- Transparency

While CPA rules have been in the public domain for some years, their existence and importance remain largely unknown, even within the legal community. Interac rules are not in the public domain<sup>28</sup>, nor are rules established by the Visa or MasterCard networks. That "acquirers" exist and what they do remain mysteries for most Canadians. The structure of fees associated with automatic banking machine or credit card transactions is anything but clear for consumers. In short, the vast majority of users (including retailers) do not have a clear understanding of how electronic payments work, and therefore do not know very well what they should do to make them work more effectively or how to react when problems happen. When documents are accessible, they are often very difficult to understand for the average consumer.

Payment mechanism providers are not in essence different from other utilities: they offer a service that is practically essential to all users willing to pay a (reasonable) price. There are sound reasons why utilities have been regulated for over a century; transparency

---

found at  
[www.fido.gov.au/asic/pdflib.nsf/LookupByFileName/eft\\_2007.pdf/\\$file/eft\\_review\\_2007.pdf](http://www.fido.gov.au/asic/pdflib.nsf/LookupByFileName/eft_2007.pdf/$file/eft_review_2007.pdf).

<sup>27</sup> The negative impact of informational asymmetry on markets has been theorized *inter alia* by Joseph Stiglitz through work for which he also received the Nobel Prize in economy.

<sup>28</sup> With the exception of "Interac Online Customer Service Rules", an initiative which we dare to hope is the prelude to more openness.

is one of them. The public should be able to know and debate how vital infrastructures work<sup>29</sup>.

Markets should also be reasonably transparent. Consumers should be able to understand what they pay for a service and to whom, if competition is to work and if abuse is to be avoided. Both the principles of effective regulation and proper market behavior would therefore mandate much more transparency than we can now observe in the Canadian payment environment.

The two major hurdles to overcome are secrecy and communication. We can see no reason why the rules governing payment mechanisms should be kept secret<sup>30</sup>. The notion of "proprietary information" should be assessed in the light of the impact of informational asymmetry on market behavior and competition. But the culture of secrecy is so entrenched in our banking industry that it appears likely nothing but legislative requirements will suffice to overcome obfuscation.

The communications challenge regarding the existence and contents of rules applicable to, and other aspects of, electronic payment mechanisms obviously cannot entirely be met through regulation, although a regulatory framework can set objectives to be met and mandate a minimum level of disclosure; clarity in the framework itself would help tremendously. More transparency regarding prices can also be required through legislation. Payment providers, retailers and regulators, with the support of other actors, including consumer organizations<sup>31</sup>, should do much more however to communicate better, beyond any legislative requirement.

## 7- Liberty

The rule under our law is still that the creditor is free to choose the type of payment he will accept. It is being abused by retailers who will take only one type of payment, to the

---

<sup>29</sup> The payment system is after all no less essential to our modern economy than roads, electricity or telecommunications, all of which are either provided or regulated by government.

<sup>30</sup> Even rules having to do with security processes gain by being made public: under the Kerckhoff principle, first formulated in 1883 and well known in areas such as cryptography, the security of a system must not depend upon the secrecy surrounding its structure, as it cannot be guaranteed. Transparency facilitates the discovery of flaws and therefore reinforces the system in the long run. More transparency would also go a long way to reducing the informational asymmetry between financial institutions and consumers when the former claim that their systems are overwhelmingly well-designed and tamper-proof.

<sup>31</sup> assuming of course that they can obtain the required resources.

exclusion even of money that is current and legal tender. In fact, a bookstore in downtown Montréal indicates on its front door that it only accepts debit and credit card payments, to the exclusion of any other means, including cash. Sadly, it is not an isolated case.

The result of such business practices is that consumers without a card are left on the roadside. Those with a card find themselves compelled to use a means of payment that may not suit them in the context of a specific transaction, if only because they are not keen to provide personal information to the retailer. And consumers find that notes properly issued by the Bank of Canada are useless in some stores, and perhaps eventually worthless in the market. Which they find odd, to say the least.

While it is understandable that retailers may wish to mitigate risk and control payment costs, leaving them free to choose unilaterally to disavow cash or to demand a specific type of payment is not conducive to the development of a fair, efficient and inclusive market. Consumers should have a say in how they wish to tender Canadian currency, however it is defined<sup>32</sup>, in order to discharge their obligations.

#### 8- Enforceability

When cash was still the usual tool to provide payment, it was a rare instance indeed when the payment method in itself raised any dispute. Issues such as miscounting or counterfeiting were fairly easily solved, at least in principle. Things have gotten rather more complicated.

Payment is now intangible and tendered through intermediaries. Risk has increased; some rules have been put in place to mitigate that risk but they need to be bolstered. Better rules will not do the job however if they are not effectively enforced.

At least four conditions are required to ensure enforceability. Obviously, there must be rules that apply to a given problem. The rules must be known. Those rules must be by their nature enforceable by the aggrieved party<sup>33</sup>. And there must be an adequate mechanism to provide enforceability.

---

<sup>32</sup> And the issue of defining what is legal tender in Canada in the 21st century is itself something which should be seriously considered, as section 8 of the *Currency Act*, S.R.C., c. C-52, can fairly said to have fallen behind the times.

<sup>33</sup> Under the privity of contract doctrine at common law or its civil law equivalent (codified in Québec by s. 1440 of the *Civil Code*), none but parties to a contract can sue on its terms or be subjected to liability arising from its provisions. It is therefore less than likely that consumers

First, it must be noted that the current review process appears unlikely to establish rules which would apply to a number of new payment methods emerging in the marketplace. The most basic precondition to an enforceable framework is therefore unlikely to be met.

While courts are obviously competent to enforce the legal framework around electronic payments, they are most often ill-suited to hear consumer complaints in that area. Issues may be quite technical and unfamiliar to judges and parties alike, and the amounts at stake, while significant in a consumer's monthly budget, are usually too small to warrant the expenditures associated with the judiciary process.

As for the ombudsman schemes put in place by financial institutions over the last decade, they still fall short of consumer expectations. They are not broadly known and our experience clearly indicates that consumers show them limited trust, as they remain unconvinced of their independence and impartiality. That, however, is a topic in itself.

Current regulators do not have the means to properly enforce whatever rules there might be and, in most cases, would not provide consumer redress<sup>34</sup>. In many instances, there simply aren't government regulators responsible for enforcing whatever rules may currently apply to electronic payments.

It is therefore essential that the responsibility to ensure the implementation of a new legal framework for electronic payments be allocated to a specialized body provided with the required powers and resources. Since the creation of a new regulatory body could be controversial, it may be more effective to entrust the existing Financial Consumer Agency of Canada with the responsibility of enforcing the framework to be developed. However, FCAC's mandate would need to be extended beyond federally regulated financial institutions with regard to payment issues, in order for the Agency to police other financial institutions and participants in payments mechanisms which are not financial institutions. We are not unaware of the complexities surrounding such a proposal; it does seem however to be the simplest short-term alternative to self-enforcement processes which are widely known to be ineffective in Canada.

---

could sue a financial institution under the terms of Interac or credit card network rules or the Debit Code, unless they were explicitly referenced in a contract to which the consumer is party or courts come (under stringent conditions) to the conclusion that such rules or codes embody a trade usage or custom. Enforceability of CPA rules by third parties is also somewhat problematic.

<sup>34</sup> The plight of the Financial Consumer Agency of Canada being a prime example.

## 9- Legitimacy

Beyond its ability to be enforced, a regulatory framework's success depends on the respect it earns from concerned parties. It is especially true of self-regulatory processes. The new Canadian framework must therefore be seen by all to be up to the task for which it is established.

Benchmarks exist. The United States have legislated decades ago. As we will see in further detail *infra*, the United Kingdom and Australia currently enjoy frameworks that are in many ways superior to Canada's and are striving, through broad public consultation, to improve on those schemes in order to face the new and upcoming realities of the market.

Market participants will benefit from a strong, credible framework that compares favorably with best-in-class sets of rules elsewhere in the world, especially as an increasing number of those participants have global presence. Canada cannot afford to lag behind. We cannot risk having the rules we put in place largely seen as weak or obsolete. We must put in place a framework that will inspire trust.

## 10- A summary

The proposals currently contemplated are neither universal or neutral. They leave aside many of the most crucial security issues. They do nothing to redress strategic accountability issues. Consumers' right to choose is not taken into account. Neither are most transparency and enforceability issues addressed. The end result can only be a framework that would fall far below the benchmarks set, for instance, in the United Kingdom and Australia.

A regulatory framework for electronic payments which would comply at least minimally with the basic principles which we propose would be greatly different from the one we now experience, and from the one being considered. Whether the current review process can lead Canadians closer to an adequate, modern framework for electronic payments in the foreseeable future therefore remains in our view very much in doubt.

## II- Reviewing the Current Code

### A- Our approach

This section of our comments will consider the analysis, proposals and questions found in the Consultation Document. We will generally follow the Document's plan, using its various sections' headings. We will end by raising issues surrounding governance and strategic direction for Canada's payments environment, which we believe are sorely lacking from the current process.

Specific comments to be posted on the Department's website are inserted throughout this section in bold type. As noted above, they do not detract from our fundamental position: we strongly believe it is a mistake to attempt to make improvements to Canada's framework for electronic payments simply by trying to improve incrementally on a doomed instrument such as the Current Code.

It follows that we have not to drafted specific recommendations regarding changes to the Current Code's wording. Our comments are deliberately aimed primarily at policy issues.

#### **Comment 1**

**A new, all-encompassing framework for electronic payments is urgently needed in Canada and it would preferably take a legislative form. Barring that, a new self-regulatory framework should be put in place following appropriate public consultation, with full stakeholder input and working from a base different from, and sounder than, the Current Code, as further argued in our long-form comments.**

### B- Section-by section review

#### 1- The introduction

The Consultation Document alludes in its introduction to issues surrounding the scope of the framework to be put in place. We believe it underestimates the problems that we face.

The variety of electronic payment mechanisms currently used in Canada is impressive, to say the least. It includes<sup>35</sup>:

---

<sup>35</sup> It should be noted that, from a regulatory perspective, a distinction should be made in many of those cases between transactions where payor and payee use the same financial institution

- bank machine transactions;
- point-of-sale debit transactions;
- credit card transactions with card present (*e.g.* point-of-sale)<sup>36</sup>;
- credit card transactions with card not present (*e.g.* Internet payments)<sup>37</sup>;
- Internet-based transactions on bank website, such as bill payment;
- Internet-based retailer payments through FI, such as *Interac online*;
- preauthorized debits on deposit accounts;
- preauthorized debits on credit card accounts;
- automated fund transfer credits;
- stored-value cards;
- phone account based payments (such as for "976" numbers);
- cellphone-based transactions;
- e-mail transactions (such as through PayPal).

These thirteen types of electronic payment probably do not exhaust the variety of payment methods and some should properly be broken down further into subclasses<sup>38</sup>. Still, this list indicates the array of competing methods increasingly offered to consumers (or other payors) in our marketplace.

The list of participants required to make these schemes work is no less impressive, and includes:

- deposit-taking financial institutions;
- other acquirers;
- debit card networks;
- credit card networks;
- retailers<sup>39</sup> as payees;

---

and transactions where they don't, as CPA or network rules will usually apply formally only in the latter case.

<sup>36</sup> Even where a retailer's attendant may verify the signature on the card, the transaction is essentially conducted through electronic means.

<sup>37</sup> It is increasingly difficult to characterize some transactions: for instance, there are currently MasterCard cards in the Canadian market which can be used exactly as credit cards for online transaction purposes, but without credit being issued: the customer must deposit funds first in an account, so the "credit card" acts in fact more as a debit card.

<sup>38</sup> For instance, "network" credit cards such as Visa or MasterCard are subject to their network's rules, which is not the case for retailer cards such as those issued by The Bay or Imperial Oil.

<sup>39</sup> We include here under "retailers" all business and institutional payees, such as utilities, insurance companies or other financial institutions, in addition to the more traditional extension of the word.

- retailers as credit card issuers;
- retailers as "on-us" stored-value card issuers;
- third-party stored-value card issuers;
- telecommunication services providers;
- device manufacturers<sup>40</sup>;
- aggregators;
- the Canadian Payments Association;
- other networks and providers (such as PayPal);
- customers (including consumers).

Again, we would not claim that list to be exhaustive<sup>41</sup>, and some of those categories can obviously be broken down.

Consideration of other issues can also lead to rather lengthy lists, such as "authentication"<sup>42</sup> methods, which currently include:

- knowledge of an identifier<sup>43</sup>;
- possession of a device (such as a card or RFID emitter);
- password (such as for online banking purposes);
- manual signature and card;
- possession of a device and password;
- biometrics.

The question of the scope of the New Code is therefore straightforward: either it will cover all (or at least most) of those schemes and participants, or it won't. If it does, the challenge to establish appropriate sets of rules in the Code will be significant. If it doesn't, the challenge of bringing some order and logic to the payments market will remain unmet. Following the principles we have outlined *supra*, we believe a New Code should have the

---

<sup>40</sup> While they do not participate directly in payment schemes, the specifications of their products condition how the schemes work and determine aspects such as their user-friendliness or security strengths and weaknesses.

<sup>41</sup> An interesting discussion of stakeholders in a mobile payment infrastructure can be found for instance in Jacob, Katy. *Are mobile payments the smart cards of the aughts?* in Chicago Fed Letter, Number 240, July 2007. 4 p.

<sup>42</sup> We are obviously using the term here in the broadest sense possible.

<sup>43</sup> such as a credit card number, *e.g.* for purposes of online transactions where no other authentication is required. Knowledge of a person's bank account number would also be sufficient in many cases to have preauthorized debits taken from that account.

broadest coverage possible and should not be limited to some of the card-based payment methods.

**Comment 2**

**A New Code should have the broadest scope possible and, in particular, should not be limited to some of the card-based payment methods.**

As noted above, electronic payments raise a broad array of issues, many of which are not covered in the Current Code. Using the latter as a template for a New Code is therefore a sure way to remove from the debate questions that should be discussed in depth, such as technological risk, solvency risks, consumer freedom of choice, third party liability and enforceability.

**Comment 3**

**The review process should not be based on the Current Code, as it does not provide a proper template for discussing issues such as the allocation of technology-based risk, solvency risk of non-regulated providers, payee choice of the payment method to be used, third party liability or enforceability.**

**2- Recent Developments**

The rather short section on "Recent developments in Electronic Payments" focuses mostly on cards and card-related devices, and lists as issues to be considered "disclosure, authentication, liability and dispute resolution."

Were it that simple. Online and mobile payments require no physical card for the most part, and they well might be electronic payments' real future. Preauthorized debits are just as cardless, which is not to say they are immune to problems. Payments through cards are therefore but a limited portion of electronic payments and the vision proposed at the outset in the Consultation Document is both myopic and unduly narrow.

**Comment 4**

**The Document's own analysis of current trends illustrates that the scope of the New Code should be broadened and go well beyond card-based emerging payment mechanisms.**

### 3- Towards an EFT Code of Conduct

The Consultation Document acknowledges that the current Code's scope "is not broad enough to extend to new developments in debit-based payment systems"<sup>44</sup>. While we obviously agree, we would note a few elements.

The Consultation Document advances a constitutional argument for proceeding with a voluntary code so as to "provide a common regime for federally and non-federally regulated organizations"<sup>45</sup>. As noted above, we do not believe that argument to be compelling. The *Bills of Exchange Act*<sup>46</sup> currently applies to banks, credit unions and, generally, to any drawer, drawee or holder of a bill of exchanges, notwithstanding its status as a federal undertaking or not; more importantly, it also binds third parties, whereas a code would only apply to organizations which adhere to it, and so might well not apply to a number of federally- or provincially-regulated financial institutions (or other stakeholders). We are of the view that a more significant issue is whether the current process will lead to a framework that would be applicable to all participants in the payments industry, including *inter alia* financial institutions, networks, acquirers and merchants.

It is suggested that the New Code could deal with new issues, "such as a commitment to providing consumers with information in clear and precise language". We note that the current Code's subsection 3 (1) already requires cardholder agreements to "be written in plain language" and that a perusal of actual consumer banking agreements indicates that compliance is less than perfect. As we indicated above, there is a number of other, somewhat more strategically significant, principles, which should rather be included in a New Code<sup>47</sup>.

In fact, the Consultation Document states that "there is room to provide overarching principles" in the New Code. We wholeheartedly agree and have already provided our views as to what such principles should be. The three principles proposed in the Code, however, simply will not do. Providing information is nice, but does not compensate for inherently risky systems or unfair rules. Responding to complaints "in a timely manner" is only a small part of an adequate redress and enforcement regime. As for "providing safe

---

<sup>44</sup> Consultation Document, section *Towards an Electronic Funds Transfer Code of Conduct*, first paragraph.

<sup>45</sup> Consultation Document, *ibid.*, second paragraph.

<sup>46</sup> R.S.C., c. B-4.

<sup>47</sup> Plain language being a subset of transparency issues.

and secure payment services", it is quite possibly the one aspect of the Document which will be unanimously supported (at least in principle); the devil, however, lurks in the details.

**Comment 5**

**The New Code should be based on, and provide to stakeholders, overarching principles for the regulation of electronic payments, such as universality, neutrality, security, accountability, transparency, liberty, enforceability and legitimacy, as further developed on our long-form comments.**

As to scope, the analysis appears to focus on debit-based payment systems<sup>48</sup>, yet debit-based and credit-based mechanisms currently compete in the market. The best illustration would be a retailer's website that accepts both credit cards and Interac online. Applying the principles of universality and neutrality, we recommend that the scope of the New Code include both debit- and credit-based schemes.

**Comment 6**

**Since they actually compete in the market, the New Code should cover both debit-based and credit-based payment mechanisms.**

We also underline the fact that some debit-based electronic payment mechanisms are currently governed in part by CPA rules. Debit cards, Interac online and pre-authorized debits come to mind. We are of the view that, just as the existence of CPA rules has not precluded the adoption of the current Code with regards to debit card transactions, it should not prevent the extension of the New Code's application to other payment mechanisms already covered in part by some framework. CPA's inability to enforce its rules on third parties (such as merchants or acquirers) and its less than stellar record at enforcing compliance from its own members stand among the reasons why CPA rules should be supplemented. CPA's refusal to consider a consumer concern such as the ability of a payee to require clients to waive their right to advance notification of the amount to be debited from their account in the context of pre-authorized debits<sup>49</sup> also indicates the need for other safeguards.

---

<sup>48</sup> See the second sentence of the first paragraph following the title "Towards an Electronic Funds Transfers Code of Conduct".

<sup>49</sup> Under subsection 14 b) of CPA rule H-1, a consumer who consents to a variable-amount pre-authorized debit should receive a ten-day notice of the amount to be debited. Notwithstanding constant opposition from consumer representatives since 2002, CPA has seen fit not only to

From a broader perspective, a given framework covering a payment mechanism may well not govern all aspects of how it works. It is therefore perfectly legitimate for an instrument such as the New Code to supplement such existing frameworks where they are lacking. We therefore believe it is mistaken to stake in the Document:

Building on the work undertaken to establish the Debit Card Code, a new electronic funds transfer code would cover face-to-face, on-line debit transactions and electronic banking, including those using debit cards, stored value cards, on-line and telephone banking. The new code would not govern credit card transactions as these are already covered under federal and provincial cost of credit regulations, and are augmented by voluntary codes. However, stored value products offered by credit card associations would be included in the discussion.

An electronic funds transfer code should cover electronic funds transfers, and not merely a limited selection thereof<sup>50</sup>. In terms of universality and neutrality, it is self-defeating to limit the New Code's scope at the outset. Regulatory underlaps can be more damaging than overlaps.

Tellingly, the United Kingdom's *Banking Code* applies to all types of electronic funds transfers, with specific provisions on particular mechanisms, such as banking machines, clearing cycle, direct debits, electronic purses, cards and PINs, credit cards or aggregation services as required<sup>51</sup>. Australia's *Electronic Funds Transfer Code of Conduct*<sup>52</sup> also applies to a broad range of activities, as indicated by its subsection 1.1 (a):

---

allow payees to obtain a waiver of the pre-notification notice, but to refuse to put the issue back on the agenda of the working group currently updating the rule.

<sup>50</sup> We note again that, accepting the scope as proposed in the Document, similar transactions such as preauthorized debits drawn on deposit accounts on the one hand, and preauthorized debits drawn on credit cards on the other, would remain governed by dissimilar rules, yet there is no legal or economic logic supporting such inconsistency in the market.

<sup>51</sup> *The Banking Code*. March 2005 edition, the text of which is available *inter alia* through [www.apacs.org.uk/payments\\_industry/documents/TheBankingCode2005.pdf](http://www.apacs.org.uk/payments_industry/documents/TheBankingCode2005.pdf). The Code (hereinafter also the "UK Code") is supported by the British Bankers' Association, the Building Societies Association and the Association for Payment Clearing Services. Specific references to various types of electronic payments can be found *inter alia* at sections 1.1, 5.6, 9.4, 9.5, 9.15, 10, 12.1, 12.7, 12.9 and 12.13. We realize that aggregation services are not *per se* payment services, but they do raise some of the same issues and illustrate the scope of the UK Code. The UK Code is currently under review.

<sup>52</sup> Australian Securities & Investments Commission. *Electronic Funds Transfer Code of Conduct*. The Code's text, as amended up to 18 March 2002, is available at

Part A of this Code applies to EFT transactions. EFT transactions are funds transfers initiated by giving an instruction, through electronic equipment and using an access method, to an account institution (directly or indirectly) to debit or credit an EFT account maintained by the account institution. [...]

While that scope is somewhat limited by other provisions, part B of the Australian Code applies to stored value facilities and transactions. The Australian Code thus covers *inter alia* electronic credit card transactions and payments through contactless devices, which would be excluded from the scope currently being considered for the New Code.

We also disagree with the Consultation Document's exclusion of credit card transactions. While provincial or federal legislation does cover some issues raised by those cards, numerous others are not, or are not covered consistently. Inadequate authentication requirements and risk mitigation provide an example of payment issues which are currently not covered adequately by legislation: consumer liability is usually capped to fifty dollars (\$50) in cases where the card is *lost* or *stolen*<sup>53</sup>, whereas a vast quantity of fraudulent transactions occur nowadays in circumstances where the card was neither lost or stolen, but its number was captured by fraudsters. Nor are chargeback or dispute resolution issues addressed in a coherent manner. Both the United Kingdom and Australia have made their voluntary codes applicable to credit card transactions even though their legislation includes provisions similar to Canada's, in order to supplement those provisions where required and to ensure some consistency in the rules applying to issues not covered by legislation<sup>54</sup>.

The diversification of the types of services offered by credit card networks should also be considered. While credit cards obviously allow the consumer to obtain credit, they are also often used as a substitute to cash payments as consumers pay their monthly balance on time. It has also become possible to draw the functional equivalent to pre-authorized debits on credit card accounts, although these transactions are not covered by CPA's rule H-1. Further and as noted in the Consultation Paper, networks are increasingly interested on stored value applications and are experimenting with other payment mechanisms. As the

---

[www.fido.gov.au/asic/pdflib.nsf/LookupByFileName/eft\\_code.pdf/\\$file/eft\\_code.pdf](http://www.fido.gov.au/asic/pdflib.nsf/LookupByFileName/eft_code.pdf/$file/eft_code.pdf). As noted above, the Code (hereinafter also the "Australian Code") is currently under review.

<sup>53</sup> See e.g. Québec's *Consumer Protection Act*, R.S.Q., c. P-40.1, section 123, or Ontario's *Regulation 17/05*, enacted under the *Consumer Protection Act 2002*, s. 58.

<sup>54</sup> A distinction should be made between the "credit and borrowing" aspect of credit cards, currently covered by legislation", and their "payment instrument" aspect, which for the most part is not.

same physical device – the upcoming chip card or something else – could be used to support most of these services simultaneously, it seems unwise to refrain from providing a framework for most of the "payment" aspects<sup>55</sup> of the services provided under card networks' banners. Surely consumers would have a hard time understanding why some of their transactions with their very same branded card are governed by the New Code, but not others.

In our view, the New Code's scope should at least extend to all payments performed in Canada which are initiated by an instruction given by the consumer or his agent through electronic means<sup>56</sup>. The New Code would thus cover the vast majority of payments other than through notes and coins or cheques (or other strictly paper-based items)<sup>57</sup>.

#### **Comment 7**

**The fact that payment mechanisms are partly covered by other frameworks (such as CPA rules or legislation) should not exempt them from coming within the scope of the New Code, which should cover all payments performed in Canada that are initiated by an instruction given by the consumer or his agent through electronic means.**

#### 4- Issuance

Oddly enough, the Consultation Document's section entitled "Issuance" mainly discusses authentication issues, without regard to other changes that the Current Code's section 2 might require. Clearly, coverage of new payment mechanisms and consideration of an increasingly virtual environment raise issues such as the requirement for a signed

---

<sup>55</sup> As opposed to the purely "credit" aspect of the cards, which properly comes under the remit of provincial jurisdiction, such as interest rate disclosure.

<sup>56</sup> This proposal is inspired by the Australian Code, subsection 1.1 (a). The issue of the Code's coverage of payments made abroad using a device or account associated with a Canadian provider (such as a point-of-sale debit transaction in the United States drawn on the account of a Canadian citizen at his Canadian bank) should also be considered. A recent decision of note in the United Kingdom is *Office of Fair Trading v. Lloyds TSB Bank et al.*, [2007] UKHL 48 (House of Lords, October 31 2007). New products such as Bank of Montreal's Prepaid Travel Mosaik MasterCard, especially targeted at travelers, are likely to raise interesting issues as they blur the line between debit and credit cards and between Canadian or foreign transactions.

<sup>57</sup> Cheque imagery would not make cheques come under the Code's scope, as the consumer's instruction is first given through the paper item.

request from the consumer to offer the service<sup>58</sup>. Other issues in the Current Code's section, related for instance to disclosure, should also be considered.

As to the authentication issue, it is an excellent example of why a broader debate around the Code's revision would be useful. Stakeholders need to consider in depth both the risk assessment and the technological aspects related to ascertaining a person's right to perform a given payment, as well as the various roles played by a diverse cast of participants. These are complex matters, the answer to which will likely vary according to the specific payment mechanism being considered, and which cannot be decided in a few short months through the exchange of written comments.

What is clear is that current methods are less than satisfactory, both in terms of safety and in terms of consumer convenience. Many consumers are just not comfortable with committing numerous PINs to memory and, instead of holding them liable for not fitting that mold, industry should strive to come up with alternatives that are both more user-friendly and privacy-enhancing. At the other hand of the spectrum, allowing the "authentication" of payments by simply waving an RFID device near a gas pump can be perceived as reckless disregard on industry's part – yet industry is never blamed for systemically creating conditions that are likely to "contribute to unauthorized use"<sup>59</sup> of payment devices.

Of course, an informed discussion on risk and authentication is a necessary precondition to a considered allocation of liabilities between participants to a payment operation.

#### **Comment 8**

**Before details of an extension of the Current Code's provisions related to authentication can be discussed, the rationale for risk allocation between providers, payors and payees must be reviewed in depth.**

---

<sup>58</sup> While we are of the view that payment mechanisms should not be provided without a consumer's prior request and should be documented, the sale of a stored-value card might well be acceptable without there being a signed paper request. CPA's Rule H-1 is also being adapted to transactions authorized by phone, provided that a cooling-off period is in place before the first payment is processed and that proper documentation be sent to the consumer. Subsection 2 (2) a) of the Current Code thus requires to be updated somewhat regarding its implementation, even though the principle behind the provision remains sound.

<sup>59</sup> To borrow language from the Current Code's section 5.

Other issues must also be considered. In the United States, the announcement by the Capital One family of financial institutions last summer that it would provide what has since been dubbed "decoupled debit" has raised some concern: the card issuer (in this case Capital One) does not hold the consumer's account. Instead, when the card is used at the point of sale, the request for payment is sent to Capital One (through the MasterCard network, interestingly enough) and honored, while Capital One creates an electronic fund transfer order<sup>60</sup> to debit the consumer's account held by another financial institution and bears the risk that the latter payment order will not be honored<sup>61</sup>. Could a similar product eventually be offered in Canada? Should it<sup>62</sup>?

Even within the context of debit cards therefore, the question of who issuers should be is likely to become increasingly complex. As the scope of the New Code is expanded, the issuance of stored-value cards, for instance, should be considered carefully and eventually regulated, as it currently is for instance in Australia, where the Reserve Bank has under Part 4 of the *Payment Systems (Regulation) Act 1998*<sup>63</sup> the power to regulate stored value issuers. It is in fact an offence under Australian law for a corporation to issue stored-value devices unless it is an authorised deposit-taking institution, it has been authorized to do so by the Reserve Bank or it can claim a specific exemption from the Act's application.<sup>64</sup>

#### **Comment 9**

**Beside authentication, other issuance matters should be considered, such as the possibility for decoupled debit to emerge in the Canadian market or the controls required around the offering of stored-value devices.**

#### 5- Disclosure and Transaction Records

We have two major problems with the contents of the Consultation Document's sections entitled "Disclosure" and "Transaction Records". First, it seems to assume that it is

<sup>60</sup> through the Automated Clearinghouse network.

<sup>61</sup> Bruno-Britz, Maria. *Cutting the Debit Ties*. Bank Systems and Technology, November 2007, p. 14. See also *inter alia* Breitkopf, David. *Convenience Store Operator Issuing ACH Debit Product*. American Banker online, June 25 2007.

<sup>62</sup> Under CPA rule H-1 as it might evolve, there would be an underlying agreement between the card issuer and the consumer and the consumer could waive pre-notification of payments to be processed on the consumer's account with a CPA member. While decoupled debits may remind observers of the Canadian payment scene of issues raised with payable-through arrangements some years ago, the scheme here appears to be quite different.

<sup>63</sup> Act No. 58 of 1998 as amended.

<sup>64</sup> *Payment Systems (Regulation) Act 1998*, sections 22-27.

sufficient to require disclosure of terms such as expiry date and insolvency risk for a new framework to be adequate, whereas we are of the view that substantive measures must be taken to reduce the risk thus posed to consumers or to allow for reparation. Second, the proposals rest on the notion that providers could unilaterally vary contractual terms at will, without consumer recourse other than being somehow advised of such changes.

As to the first element, some risks are unconscionable and it is not enough to disclose them to consumers: they ought to be mitigated or avoided. The problems associated with expiry date or service interruption possibly associated with stored value cards provide a good example. It is not enough to require the issuer of a \$100 card designed to be used exclusively in \$6 increments to disclose that the card is valid for only one week, that it is not redeemable, that it cannot be combined with another card to make a transaction and that stored value insufficient to make a purchase with the card is irretrievably lost<sup>65</sup>. Such egregious issuer behavior should be prohibited, purely and simply.

It is unrealistic to count on the market to clean up such issues. There may be multiple providers in a market but they may choose not to compete significantly on issues such as consumer liability for unauthorized transactions. In that case, the consumer may well be faced with "competing" offers which are all essentially tipped against her.

#### **Comment 10**

**Disclosure is not an adequate remedy to unconscionable contractual requirements or business practices, which should be prohibited by the New Code.**

Regarding a provider's ability to vary contractual terms unilaterally, the concept itself obviously raises troublesome legal questions: how can a contract be valid when one (and only one) party can rewrite it at will? If the consumer can therefore not know what her obligations will be as she binds herself, can we still talk of contract? What about the notions of consent and consideration? Common law holds that a contract can be modified only through variation, requiring mutual consent, or waiver, where the party inconvenienced by a change acquiesces after the fact<sup>66</sup>. The situation is similar at civil law:

<sup>65</sup> In this exaggerated example, assuredly at least \$4 per card sold, which would accrue to the issuer without legal cause.

<sup>66</sup> See e.g. Fridman, G.H.L. *The Law of Contract*. Fourth Edition. Student Edition. Toronto, Carswell, 1999. 895 p. P. 577.

the agreement binds the parties, who have a duty to honor their contractual undertakings, and alteration of their obligations should obey specific rules<sup>67</sup>.

Indeed, France has gone a step further in clarifying that contractual clauses allowing a merchant to vary contractual terms without a valid reason specified in the agreement, or to alter the characteristics of the service to be provided, where the consumer is thereby disadvantaged, are unconscionable and thus legally void<sup>68</sup>. France has established a *Commission des clauses abusives* to track and work on eliminating unconscionable provisions in consumer agreements<sup>69</sup>. Québec's *Civil Code* includes a provision<sup>70</sup> stating that unconscionable clauses are null and it remains to be seen whether courts will give that provision a construction similar to French law.

We therefore recommend that the New Code forbid contractual provisions allowing payment providers to alter unilaterally an agreement in a way prejudicial to the consumer.

#### **Comment 11**

**Contractual provisions allowing providers to alter unilaterally an agreement in a way prejudicial to the consumer should be prohibited by the New Code.**

As to the questions specifically asked in the Consultation Document, the code's wording will obviously need to be updated to take into account all payment methods covered by the New Code. Replacement of "cardholder" by "account holder" is probably not an avenue to be pursued, unless it is specified that the notion of "account" is not limited to accounts held at deposit-taking financial institutions; it would obviously be preferable to opt for a term that is neutral with regard both with technology and the nature of service providers. We see nothing wrong with the term "consumer".

#### **Comment 12**

**The notion of "cardholder" should not be replaced by that of "account holder"; the term "consumer" would appear to be generic enough to apply in all circumstances coming under the New Code's scope.**

---

<sup>67</sup> As an aside, Union des consommateurs and a consumer petitioned Québec courts on August 22 2007 to be authorized to launch a class action suit against an Internet service provider for having unilaterally varied contractual terms.

<sup>68</sup> *Code de la consommation*, s. L132-1 and Annex, s. 1 j), and s. R 132-2.

<sup>69</sup> The Commission's website can be found at [www.clauses-abusives.fr/index.htm](http://www.clauses-abusives.fr/index.htm).

<sup>70</sup> S. 1437.

The nature of the information that should be disclosed to consumers may vary significantly with the type of payment mechanism involved<sup>71</sup>. The Current Code provides the minimum required with regard to debit card transactions; CPA has recently sought to improve disclosure requirements and methods with regard to pre-authorized debits. By contrast, the purchaser of a stored-value card would need specific information regarding issues such as redemption and expiry date<sup>72</sup>. It is quite clear however that we can improve on the current requirements, which are insufficient in part, excessive in other cases<sup>73</sup> and generally ill-adapted to evolving market practices.

Among the issues to consider should figure the consumer's right and ability to obtain an account's or device's balance at any time and to monitor transactions. It should also always be possible to reconstitute enough of an audit trail to prove that, for instance, a consumer had effectively authorized a \$50 payment, whereas a \$500 amount was transferred, even where the transaction was handled through multiple service providers<sup>74</sup>. We note that the Australian Codes requires that institutions be able to trace and check transactions and, where necessary, correct errors<sup>75</sup>.

As to fees related to payment processes, they should be clearly and prominently disclosed, apart from the amount of the payment itself.

At this point, we are of the view that it is premature to try and define specific disclosure requirements. They can only be established once there has been agreement regarding the New Code's scope and the rights and liabilities to be ascribed to the various parties. The regime being designed, it will then be easier to determine the part information-sharing must play in an efficient and effective framework.

---

<sup>71</sup> So would formats and delivery mechanisms.

<sup>72</sup> Consideration should also be given to schemes whereby a consumer purchases e.g. prepaid cellphone time from a provider's agent and thus gets a paper "virtual voucher" which she must then use through her phone or the provider's website to convert the voucher's number into validated air time. Cash is therefore exchanged for paper-based information, which is then converted electronically to value. Such vouchers are usually unredeemable and may be usable only for a limited period. We believe such transactions should be covered by a new framework, even though they are partly paper-based.

<sup>73</sup> A \$3 transaction with a stored-value card at a parking meter probably does not require the lengthy transaction record demanded by the Current Code's section 4 (1) a.

<sup>74</sup> Such a requirement would obviously need to be tempered where a payment device allows for untraceable payments.

<sup>75</sup> Australian Code, section 9.1.

**Comment 13**

**While it is premature to attempt to specify disclosure requirements, it is clear that current requirements are inadequate, that the ability to establish some sort of audit trail should generally be preserved (except where payments are untraceable), that scheme-specific information such as expiry date of stored-value devices should be available and that fees should be disclosed clearly and distinctly from the amount of the payment itself; it is also clear that disclosure mechanisms would need to be adapted to the specific reality of diverse payment schemes.**

**6- Transaction Security**

The need for security and privacy goes to trust in payment mechanisms. Therefore, it goes beyond physical security around ATMs<sup>76</sup> and proper data security measures, however important they may be. It behooves providers to put in place a system whereby the consumer is confident that the payment she intends to make will effectively happen, and in a timely fashion.

As noted in the Consultation Paper, issues such as "authentication" and "non-repudiation" must therefore be addressed. So must finality of payment, transaction cycle length and network reliability.

A consumer cannot trust entirely a payment mechanism when she cannot be sure when her payment will be credited by a biller even if she has provided her electronic instruction to pay in a timely fashion. She cannot quite trust a mechanism where her payment might be unwound because some intermediary has suddenly stopped operating. She cannot be satisfied where her willingness to pay is compromised by the breakdown of her provider's network (or her creditor's providers' network, for that matter) – especially when breakdowns appear to recur<sup>77</sup>.

---

<sup>76</sup> While the Current Code requires that ATM and POS terminals' immediate surroundings afford some privacy, daily experience shows how compliance with this provision remains dismally lacking.

<sup>77</sup> The major breakdowns experienced by Royal Bank and CIBC obviously come to mind, but they are not isolated cases: Desjardins, for instance, suffered network breakdowns in July 2006, March 2007 and September 2007, not to mention a partial breakdown in September 2004. We are aware that major stakeholders, such as the Government of Canada, have raised the issue with the industry; it is also a significant consumer concern.

The New Code should therefore clarify that a consumer is deemed to have paid his creditor at the moment the payment service provider accepts the consumer's instruction to "push" funds to the creditor or the latter's instruction to "pull" them<sup>78</sup>.

It is unlikely that a code of practice can effectively and fully address issues related to a provider's insolvency or unexpected shutdown: a code can hardly impose effective prudential regulation or prevail over bankruptcy legislation. It might however require providers which are effectively in control of funds<sup>79</sup> to obtain some security on behalf of their customers when those funds are not otherwise guaranteed by deposit insurance.

The New Code should also impose on providers reliability standards and liability for delayed or non-processed payments when those standards are not met and consumers have suffered damages. It is incidentally interesting to contrast the rule on liability in case of network breakdown in the Australian Code<sup>80</sup>, which explicitly prohibits a financial institution from denying "implicitly or explicitly, a right to the user to make claims for consequential damage which may arise as a result of a malfunction of an institution system", on the one hand, and a provision such as the following, currently found in the Bank of Montreal's account agreement:

We will not be responsible or liable for any delay, damage, loss or inconvenience you [...] may incur if you are unable to access FirstBanking Automated Services in the event or any malfunction for any reason whatsoever [...]<sup>81</sup>

The Australian rule clearly makes sense: operational risk should not be supported by users who have no power whatsoever on system configuration or operation, and it should not be

---

<sup>78</sup> Float and ensuing interest income issues between intermediaries should be settled between them.

<sup>79</sup> Stored-value issuers clearly come to mind, but *inter alia* schemes designed on the PayPal model may also hold funds belonging to customers at some point in the process, perhaps without being a regulated financial institution themselves.

<sup>80</sup> See subsection III-B 2), *infra*.

<sup>81</sup> Bank of Montreal. *Agreements for Everyday Banking Effective date June 1, 2007*. Section V, subsection 10. Other institutions have similar language in other agreements, such as TD Visa, which states that the institution will not be liable for any damage resulting from equipment failure "even if we knew that damage was likely or the damage was a result of our negligence [...]": Toronto-Dominion Bank. *The TD Green Visa Cardholder Agreement and Benefit Coverages Document*, p. 9, subsection "Liability for damages limited". Document # 586302(1206), available at [www.tdcanadatrust.com/tdvisa/pdf/green.pdf](http://www.tdcanadatrust.com/tdvisa/pdf/green.pdf)

transferred on them by increasing their legal risk. Security includes system integrity, which is the provider's responsibility.

Providers' technological choices condition the level of security of their services and they are best placed to implement secure mechanisms. Their record, however, is lackluster. Magnetic stripe card and PIN schemes are neither particularly safe or consumer-friendly. Whether smart cards will effectively be safer once fraudsters have sufficient market incentive to attack them on a broad scale remains to be seen. RFID technologies are prone to interception. Most biometric identification devices either have fairly high false-positive or false-negative rates, raise daunting privacy issues or remain poorly accepted by users.

Debit card issuers are currently not shouldering the full cost of their technology's weaknesses: they push as much of the liability as they can on customers by denying their liability for unauthorized transactions, even when it means breaching the Current Code's provisions. Quite simply, they morph their self-inflicted operational risk into customers' legal risk. They therefore lack incentives to make needed improvements. It is unclear to us whether, in the current setting, a voluntary code can change this situation and improve market conduct and market efficiency<sup>82</sup>. What is clear is that security should be designed into systems. Such design should not result in the consumer being almost unavoidably the weakest link in the system, burdening him with undue liability.

In the current setting, consumers will remain dependent on providers' choices. Higher security standards should be put in place and the onus of liability should in the future rest explicitly on the shoulders of those who choose the technologies that are deployed, as they usually are the least cost avoider.

Current security challenges with debit cards have nothing to do with the Code's provisions: they are inherent to the technologies that have been deployed. If the New Code is to have any impact, it must impose more stringent standards than the industry is currently willing to tolerate, or put more clearly the onus of offering weak products on the providers.

---

<sup>82</sup> Obviously, we assume that deploying a less than optimal technology and having the cost of this inefficiency borne by parties that are powerless over that decision (i.e. consumers) is not an efficient allocation of resources.

**Comment 14**

**In the broadest sense, issues to be considered under the heading of "security" are not limited to immediate transaction security but include topics such as system conception, network reliability, solvency and payment finality for all payment mechanisms covered by the New Code.**

7- Liability and Redress

Consumers' experience with the Current Code in terms of liability and redress is less than stellar. While it is true that "clear attribution of responsibilities" and "transparent processes" are "strong factors to promote confidence" in a payment system (or Code), the Document fails to mention the strongest factor of all: the rules must not only clearly set liability, they must do so fairly. Processes must not only be transparent, but they must be fair. Experience indicates that the fairness test is failed more often than not.

Section 5 of the Code is ambiguous and, in particular, its reliance on an ill-defined notion of "unintentional contribution" to unauthorized use would gain by significant clarification. Financial institutions' agreements and practices further narrow the Code's benefit to consumers, for instance by demanding that a consumer notify the card issuer of the loss of the card "immediately"<sup>83</sup> or within twenty-four hours of discovering the event<sup>84</sup>. The effectiveness of redress mechanisms, and in particular of financial institutions' internal dispute resolution schemes, is less than obvious to consumers who frequently dread, and sometimes experience, less than perfectly impartial processes.

As currently drafted, the Code does not provide an effective framework for establishing liability or obtaining redress regarding problems experienced with debit cards. The question therefore should not be which of its provisions should be extended to other payment mechanisms, but how a better framework can be put in place.

---

<sup>83</sup> TD Canada Trust. *Cardholder and Electronic Banking Services Terms and Conditions*. Section 11. Consulted December 12, 2007 at [www.tdcanadatrust.com/accounts/cardholder.jsp](http://www.tdcanadatrust.com/accounts/cardholder.jsp).

<sup>84</sup> whereas the Code requires notification "within a reasonable time", a phrase already constrained by the Guide to the interpretation of section 5 to mean "as soon as possible"; in both cases, however, it may well be more than 24 hours before the consumer notices the loss or can effectively act on the discovery (especially when abroad). The 24-hour notification requirement is found *inter alia* in Bank of Montreal's account agreement.

**Comment 15**

**Provisions in the Current Code regarding liability and redress are already inadequate and therefore do not provide a sound foundation for regulating a broader array of electronic payments. A principled analysis of the characteristics of the mechanisms to be covered is required before liability allocation rules can be set.**

**C- Governance issues**

The current consultation ignores governance issues related both to the Code's implementation and to the payments sector in general. Canadian practices thus stand in marked contrast to those prevailing in Australia or the United Kingdom, yet this is a vital issue.

**1- Australia**

In Australia, the Code's monitoring comes under the aegis of the Australian Securities and Investments Commission ("ASIC"). ASIC publishes a yearly report on compliance, itemizing breaches by the Code section involved, providing information on non-compliant institutions and recommending best practices<sup>85</sup>. As noted *supra*, ASIC is currently leading a consultation on the code's update; the consultation document thoroughly discusses issues in order to help stakeholders participate fully in the process; it weighs in at 129 pages (in remarkable contrast to the Consultation Document). As for the *Code of Banking Practice*, which deals with broader issues, compliance is ensured by the independent *Code Compliance Monitoring Committee*<sup>86</sup> and the Code's review is entrusted to another independent body.

The Australian payments industry currently advocates "well-designed co-regulation" as the way forward so as to enhance the efficiency and competitiveness of the payment system<sup>87</sup>. The Reserve Bank of Australia is proud however to claim that it "has one of the clearest and strongest mandates in the world to oversee the operation of the payment

<sup>85</sup> The most recent such report we found on the Commission's website at the time of writing dates from December 2005: ASIC. *Report 63 – Compliance with the EFT Code of Conduct (April 2003 to March 2004)*. 43 p.

<sup>86</sup> Whose website is at [www.bankcodecompliance.org](http://www.bankcodecompliance.org).

<sup>87</sup> Australian Payments Clearing Association. *Submission to Reserve Bank of Australia on "Reform of Australia's Payment System: Issues for the 2007/08 Review"*. Sydney, August 2007. 21 p. P. 2, § 5. The Association's website is at [www.apca.com.au](http://www.apca.com.au). Consumer issues do not appear to directly play a significant part in the Association's approach to efficiency and are not considered in that submission, the market being characterized as "unusual" and in need of understanding (see §73).

system."<sup>88</sup> In particular, the Reserve Bank has under the *Payment Systems (Regulation) Act 1998*<sup>89</sup> the power to designate and regulate payment systems<sup>90</sup> and, as noted above, the power to regulate stored value issuers.

## 2- The United Kingdom

Payment system governance issues have attracted considerable attention in the United Kingdom. Some were raised in 2000 in the Cruickshank Report<sup>91</sup>, then in responses thereto. In March 2004, the Office of Fair Trading established a Payment Systems Task Force whose remit was to consider and resolve competition, efficiency and incentive issues relating to payment systems<sup>92</sup>. The Task Force was also charged with considering consumer issues "where appropriate". Two representatives of the consumer community were among the Task Force's fifteen members.

The Task Force did consider a number of consumer issues, including maximum clearing times for value and fund availability to be implemented by November 2007<sup>93</sup>. The industry has agreed to ensure that payments made by phone or Internet would be transferred within approximately two hours, seven days a week, rather than within three days as is currently the case, also starting in November 2007<sup>94</sup>.

The Task Force's most lasting legacy, however, is likely to be its work regarding governance issues, which the Chancellor of the Exchequer endorsed in November 2006. The Task Force recommended that a new body be created and that it center its work around "three key objectives: promoting strategic vision across the payments industry, promoting

---

<sup>88</sup> Reserve Bank of Australia. *Australian Payments System*. The document is available at [www.rba.gov.au/PaymentsSystem/australian\\_payments\\_system.html](http://www.rba.gov.au/PaymentsSystem/australian_payments_system.html).

<sup>89</sup> Act No. 58 of 1998 as amended.

<sup>90</sup> A power akin to that granted to the Minister of Finance under the *Canadian Payments Act*, R.S.C., c. C-21, Part 2.

<sup>91</sup> Cruickshank, Don. *Competition in UK Banking – A Report to the Chancellor of the Exchequer*. London, HMSO, March 2000. 338 p.

<sup>92</sup> Office of Fair Trading. *Press releases 2004 – Payment systems task force members and terms of reference announced*.

<sup>93</sup> Payment Systems Task Force. *Final Report of the Payment Systems Task Force*. OFT 901. London, February 2007. 55 p. Pp. 18-19. It is worthy of note that all cheques deposited in current or basic accounts should be cleared for withdrawal (that is, funds should be fully available) at most four (4) days after the item has been deposited. The Task Force's final report is available at [www.of.gov.uk/shared\\_of/reports/financial\\_products/of901.pdf](http://www.of.gov.uk/shared_of/reports/financial_products/of901.pdf).

<sup>94</sup> *Ibid.*, p. 22. Introduction of these faster services has since been rescheduled to May 2008: APACS. *UK banking industry announces revised timescale for faster payments service*. Press release, August 14 2007, at [www.apacs.org.uk/media\\_centre/press/08\\_14\\_07.html](http://www.apacs.org.uk/media_centre/press/08_14_07.html).

increased transparency and innovation and ensuring the integrity of all member schemes."<sup>95</sup> The Payments Council started its activities in March 2007.

The Payments Council defines itself as "the organisation which sets strategy for UK payments" and strives to ensure that the "UK payments and services meet the needs of users, payment service providers and the whole economy."<sup>96</sup> It has given itself as one of its first tasks

[...] to manage a full public consultation process, leading to the creation and adoption of a National Payments Plan. This plan will look at things such as opportunities rising from new technologies, the improvement of supply chain efficiency and e-invoicing, the future of the cheque guarantee scheme and the impact of SEPA on UK payments.<sup>97</sup>

In addition to planning a strategy for the payment system, the Council has the power to "give directions to, and set standards for, payment schemes" and schemes agree to comply with the Council Board's decisions<sup>98</sup>. The Board may sanction non-compliant schemes<sup>99</sup>.

The Council's board has fifteen (15) members, eleven of which come from the industry and the four (4) others being independent. Interestingly, the four independent directors, voting together, hold veto power over board decisions. While a minority, they may therefore be able to make themselves heard, a situation stakeholders not from the industry sitting on various entities within the Canadian payments governance structure can only envy<sup>100</sup>. Board minutes are published on the Council's website as they are approved by the Board.

This new Council therefore has authority over the British equivalents to the CPA acting as the operator of the Automated Clearing and Settlement System and Large Value Transfer System, to Interac and to The Exchange network. Its mandate is imbued with

---

<sup>95</sup> *Ibid.*, p. 1, § 1.2.

<sup>96</sup> Payments Council homepage, at [www.paymentscouncil.org.uk](http://www.paymentscouncil.org.uk).

<sup>97</sup> Payments Council website, "About us" page, at [www.paymentscouncil.org.uk/about\\_us](http://www.paymentscouncil.org.uk/about_us).

<sup>98</sup> Payment Systems Task Force, *op. cit.*, p. 14, §§4.11 and 4.12.

<sup>99</sup> Payments Council. *Rules*. Subsection 27.3. The Council's Memorandum and Articles of Association and its Rules can be found on its website, the rules being published at [www.paymentscouncil.org.uk/files/Rules.pdf](http://www.paymentscouncil.org.uk/files/Rules.pdf).

<sup>100</sup> In addition, any vote by the board needs eleven (11) "ayes" for a motion to carry. See [www.paymentscouncil.org.uk/about\\_us/structure](http://www.paymentscouncil.org.uk/about_us/structure).

public interest concerns and it remains to be seen whether it will escape capture by its members, which are financial institutions and other payment service providers<sup>101</sup>.

The United Kingdom has recently embarked on a broad public consultation on a "National Payments Plan". The 52-page long consultation document<sup>102</sup> raises issues such as consumer education, financial inclusion and costs in addition to looking at specific trends such as the growth of mobile payments. This approach stands in stark contrast with the current "consultation" in Canada.

As to the British Banking Code, compliance has been monitored since 1999 by the Banking Code Standards Board, whose role it is to enforce the code. The Board is an independent body and six of its ten directors (including the chair) are independent from the industry, five being "public interest directors". In order to assess compliance, the Board conducts reviews of subscribers' practices, surveys and mystery shopping. When significant breaches of the Code are detected, it does not hesitate to name names and to shame. The Board has non-negligible resources to perform its tasks, with an annual turnover in 2006/7 of £ 1 343 418<sup>103</sup>. It is therefore able, for instance, to hold annual mystery shopping surveys covering hundreds of branches.

### 3- And Canada...

Needless to say, Canada does not compare. There is no strong body able to provide some strategic direction, nurture debate and enforce compliance. The result is a muddle that serves no one and not even, in our view, the long-term interests of the current major providers themselves.

The field is ripe for change. A number of concerns should be addressed.

For instance, is it part of CPA's remit to establish consumer protection measures in its rules? If so, is its mandate clear enough?<sup>104</sup> Can it succeed in doing so when such measures are likely to be seen by CPA members as conflicting with their own commercial interests?

---

<sup>101</sup> Including, interestingly, PayPal.

<sup>102</sup> Payments Council. *National Payments Plan – Consulting on change in UK payments*. London, Payments Council, 2007. 52 p. The document is available at [www.paymentscouncil.org.uk/files/NPP%20Consultation%20Final.pdf](http://www.paymentscouncil.org.uk/files/NPP%20Consultation%20Final.pdf).

<sup>103</sup> Banking Code Standards Board. *Annual Report 2006/07*. London, 2007. The document can be consulted at [www.bankingcode.org.uk/pdfdocs/Annual\\_Report\\_final.pdf](http://www.bankingcode.org.uk/pdfdocs/Annual_Report_final.pdf).

<sup>104</sup> CPA's view, based on a legal opinion obtained in 2002, apparently is that consumer protection is outside its remit. We respectfully find that conclusion hard to reconcile with subsection 5 (2)

More broadly, should an operator of clearing and settlement systems find itself in a situation where its rules may hinder other clearing systems' operators or the activities of its members' competitors? Should the rule-making activities, therefore, be wholly separate from system operation? Is that realistic, considering that operators do have the needed expertise? How can impartiality be ensured?

How are providers other than financial institutions to be heard and regulated, in a context where their importance in the payments market is likely to grow significantly over the next decade?

Where can other stakeholders have a significant input in the governance of the payments system? Notwithstanding efforts made by CPA over the last few years, it is crystal clear to participants in those processes that, at the end of the day, direct clearers still rule without compunction. What a few of them deem inappropriate, from a financial or technological standpoint, is very unlikely to happen indeed<sup>105</sup>. Yet there is no other forum where payment issues of interest to the various stakeholders can be discussed.

There should be. The balance between proprietary rules and some level of standardization must be reviewed<sup>106</sup>. The balance between large financial institutions on the one hand, and other providers and users on the other, must be altered. Relevant data must be disclosed, so that issues are well understood. Real debate must be allowed. A new model must be implemented.

In the last few years, major issues regarding the payment system in the United States have been taken to court, interchange fees being the prime example. Others, while debated publicly, have remained mired in congressional disputes. We are therefore certainly not inclined to provide the United States as a model.

Inspiration can be taken however from the United Kingdom and Australia and, to a lesser extent perhaps, from the European Union as a whole. Faced with challenges similar to those coming to Canadian stakeholders, they have chosen to consult widely, to bring

---

of the *Canadian Payments Act*, which directs CPA "in pursuing its objects" to "take into account the interests of users."

<sup>105</sup> The fact that the same institutions also have significant weight in networks such as Interac, Visa and MasterCard increases their power over the evolution of the payment system and, incidentally, sometimes make it difficult to understand their strategies.

<sup>106</sup> The issue is currently raised in the United Kingdom in the context of the consultation on the National Payments Plan, *op. cit.*, p. 38.

forth the necessary debates and to lay the groundwork for a framework that will fit evolving realities and, hopefully, endure.

Canada cannot afford a limited, muted effort at revamping an obsolete tool if it is to establish the modern, strong framework for electronic payments that all stakeholders need.

**Comment 16**

**Broad governance issues regarding the Canadian payments environment must urgently be considered, possibly along the lines currently established or explored in Australia and the United Kingdom.**

## Appendix

### List of specific comments

#### Comment 1

**A new, all-encompassing framework for electronic payments is urgently needed in Canada and it would preferably take a legislative form. Barring that, a new self-regulatory framework should be put in place following appropriate public consultation, with full stakeholder input and working from a base different from, and sounder than, the Current Code, as further argued in our long-form comments.**

#### Comment 2

**A New Code should have the broadest scope possible and, in particular, should not be limited to some of the card-based payment methods.**

#### Comment 3

**The review process should not be based on the Current Code, as it does not provide a proper template for discussing issues such as the allocation of technology-based risk, solvency risk of non-regulated providers, payee choice of the payment method to be used, third party liability or enforceability.**

#### Comment 4

**The Document's own analysis of current trends illustrates that the scope of the New Code should be broadened and go well beyond card-based emerging payment mechanisms.**

#### Comment 5

**The New Code should be based on, and provide to stakeholders, overarching principles for the regulation of electronic payments, such as universality, neutrality, security, accountability, transparency, liberty, enforceability and legitimacy, as further developed on our long-form comments.**

#### Comment 6

**Since they actually compete in the market, the New Code should cover both debit-based and credit-based payment mechanisms.**

#### Comment 7

**The fact that payment mechanisms are partly covered by other frameworks (such as CPA rules or legislation) should not exempt them from coming within the scope of the New Code, which should cover all payments performed in Canada that**

are initiated by an instruction given by the consumer or his agent through electronic means.

#### **Comment 8**

Before details of an extension of the Current Code's provisions related to authentication can be discussed, the rationale for risk allocation between providers, payors and payees must be reviewed in depth.

#### **Comment 9**

Beside authentication, other issuance matters should be considered, such as the possibility for decoupled debit to emerge in the Canadian market or the controls required around the offering of stored-value devices.

#### **Comment 10**

Disclosure is not an adequate remedy to unconscionable contractual requirements or business practices, which should be prohibited by the New Code.

#### **Comment 11**

Contractual provisions allowing providers to alter unilaterally an agreement in a way prejudicial to the consumer should be prohibited by the New Code.

#### **Comment 12**

The notion of "cardholder" should not be replaced by that of "account holder"; the term "consumer" would appear to be generic enough to apply in all circumstances coming under the New Code's scope.

#### **Comment 13**

While it is premature to attempt to specify disclosure requirements, it is clear that current requirements are inadequate, that the ability to establish some sort of audit trail should generally be preserved (except where payments are untraceable), that scheme-specific information such as expiry date of stored-value devices should be available and that fees should be disclosed clearly and distinctly from the amount of the payment itself; it is also clear that disclosure mechanisms would need to be adapted to the specific reality of diverse payment schemes.

#### **Comment 14**

In the broadest sense, issues to be considered under the heading of "security" are not limited to immediate transaction security but include topics such as system conception, network reliability, solvency and payment finality for all payment mechanisms covered by the New Code.

**Comment 15**

**Provisions in the Current Code regarding liability and redress are already inadequate and therefore do not provide a sound foundation for regulating a broader array of electronic payments. A principled analysis of the characteristics of the mechanisms to be covered is required before liability allocation rules can be set.**

**Comment 16**

**Broad governance issues regarding the Canadian payments environment must urgently be considered, possibly along the lines currently established or explored in Australia and the United Kingdom.**