2003

Consumer Liability in Unauthorized Electronic Funds Transfers

Benjamin Geva

Osgoode Hall Law School of York University, bgeva@osgoode.yorku.ca

Follow this and additional works at: http://digitalcommons.osgoode.yorku.ca/scholarly_works

This work is licensed under a Creative Commons Attribution-Noncommercial-No Derivative Works 4.0 License.

Recommended Citation


This Article is brought to you for free and open access by the Faculty Scholarship at Osgoode Digital Commons. It has been accepted for inclusion in Articles & Book Chapters by an authorized administrator of Osgoode Digital Commons.
CONSUMER LIABILITY IN UNAUTHORIZED ELECTRONIC FUNDS TRANSFERS

Benjamin Geva*

CONTENTS

I. Introduction ................................................................. 208
II. Consumer Retail Electronic Payments .................................. 212
III. General Law ................................................................. 224
   1. Issues under General Law ............................................ 224
      (a) What is an Unauthorized Transfer? ...................... 224
      (b) Between the Financial Institution and the Customer, Who Bears Unauthorized Transfer Losses, and to What Extent? ...... 228
      (c) Between the Financial Institution and the Customer, Who Has To Prove What, and What is the Standard of Proof? .......... 232
   2. Inadequacy of General Law ........................................ 236
IV. Specific Consumer Protection Schemes ............................. 241
   1. Consumer Legislation in the United States ................ 241
   2. Consumer Legislation in the United Kindom .................. 248
   3. Federal Regulations and Provincial Legislation in Canada .... 250
   4. Consumer Legislation in Denmark ............................... 252
   5. Voluntary Codes — The United Kingdom and Australia ........ 257
   6. Voluntary Code in Canada ........................................... 267
   7. EU Pronouncem ents ................................................... 272
V. Concluding Remarks and Proposed Principles ..................... 275

* Professor, Osgoode Hall Law School, Toronto. This paper was presented at the 32nd Annual Workshop on Commercial and Consumer Law at the Faculty of Law of the University of Toronto on October 19, 2002. It draws on, and its conclusions slightly clarify and improve on, a research paper “Consumer Protection in Electronic Funds Transfers” prepared by the author for Industry Canada/Office of Consumer Affairs and submitted on Research Paper for Industry Canada/Office of Consumer Affairs March 21, 2002 and presented in a draft form at the EFT Working Group’s discussion on February 5, 2002. Ongoing support from the Office of Consumer Affairs, Industry Canada and constructive feedback by the EFT Working Group as well as participants in the Annual Workshop are acknowledged with gratitude. For research assistance I am grateful to Osgoode Hall Law School students Lin Yu, Muharem Kianieff and Jules Grunwald. Funding for the preparation of this paper was provided by the Innovation Centre Law and Policy at the University of Toronto Faculty of Law.
I. INTRODUCTION

This article focuses on loss allocation caused by unauthorized funds transfers in low-value electronic retail or consumer payment systems in Canada. Funds transfers or payments are broadly defined to include non-cash payments to third parties, cash withdrawals, and transfers from one account to another belonging to the same person. Value to be accessed for the execution of such transactions may be either in the form of credit to an account with, or loaded on a product issued by, a financial institution. An account with a financial institution may be either an asset account, reflecting deposits of actual funds, or an account set up according to a credit plan.

Value can be electronically accessed by consumers either with or without a payment card. A payment card may be a credit, debit or stored-value card. Electronic authentication of payment instructions may utilize personal identification number (PIN) or password identification, a digital signature, or (in the future) a biometrics authorization, and for cards, may be carried out in connection with either magnetic stripe or chips technology. The communication of the payment instructions could be over dedicated lines, the telephone system, or the Internet.

The article's focus is on unauthorized electronic authorizations. At the same time, limiting the discussion to electronic access to such payment systems is impractical. Electronic payment systems are the outgrowth of the traditional paper-based system, with each evolutionary stage building and improving on its predecessor. To that end, lines cannot always be clearly drawn and hybrid systems do exist. Moreover, in practice the same physical device can be used by a consumer to initiate either an electronic or non-electronic payment. Last but not least, information contained on the device can be used to initiate payment over the system without the physical use of the device itself.

1. Typically, payment is by the consumer to a third-party merchant. Yet, retail funds transfer networks may also be used in the reverse direction, namely, in conjunction with a refund made to a consumer from a third-party merchant.
The credit card is the best example. In principle (though not historically), the credit card can be conceptualized as an improvement on the cheque-guarantee card. It is the basis from which the debit card sprang. While the authorization for a credit card payment is typically supported by the consumer’s written signature, card authentication is performed electronically. Regardless, the same physical card can be used as either a credit or debit card. Finally, a credit card payment can be made in telephone or mail orders, and even in payments over the Internet, without the physical use of the card itself.

Against this background, it is only consumer payments whose authorization is strictly on the basis of handwritten signature that can safely be excluded. While the focus of the article is on retail payments instructed by the consumer electronically, it is recognized that precise and definite borders are not easily drawn. With this in mind, coverage is extended to all payments authorized other than by merely written signature, which are processed in retail payment systems.

The central issue in consumer protection in electronic funds transfers is that of liability and allocation of risk in connection with an unauthorized payment. This article exclusively explores this topic. Other consumer protection issues in electronic funds transfers involve risks of merchant default, paymaster default and system malfunction. Related topics include transparency and disclosure requirements, error and dispute resolution, and privacy. All such risks and topics are outside the scope of this article.

In Canada, cheques, including those issued by consumers, are governed by the Bills of Exchange Act, though in the context of the general law governing the relationship between bank and customer. There is no statute that governs electronic funds transfers, including those involving consumers. Rather, the central document governing consumer electronic funds transfers is the Canadian Code of Practice for Consumer Debit Card Services (the Code). To that end, this article recommends upgrading of the Code or, more specifically, replacing it by a more comprehensive and up-to-date electronic funds transfer code of practice for Canada. In some countries, consumer electronic funds transfers are governed by statute and regulations. It appears, however, that the overall experience with the Code in Canada has been positive. Accordingly, this article does not
question the viability of a code to govern the matter in Canada and thus does not consider the replacement of this regulatory approach.

The Canadian Code has been in effect since May 1992, and was revised in 1996. A subsequent revision in 2002 added an Interpretation Guide to the provision governing liability for loss but changed nothing in the language of the Code itself. The Code is a voluntary code of practice that “has been developed through consultation among representatives of consumer organizations, financial institutions, retailers, and federal and provincial governments”. It covers only debit cards used with personal identification numbers. It provides for the issue of debit cards and PINs, debit cardholder agreements, debit card transactions, liability for loss, and principles for dispute resolution. In general, “[t]he code outlines industry practices and consumer and industry responsibilities, which will help to protect consumers in their use of debit card services in Canada”. Organizations endorsing the Code undertake to “maintain or exceed the level of consumer protection it establishes”; also protection given by other laws and standards is not precluded by the Code.4

It is further recognized that principles and rules prescribed by the Code are not engraved in stone. To that end, it is specifically provided that “[t]he code will be reviewed regularly to ensure relevance to current technology and business practices, and its effectiveness in promoting consumer protections in electronic funds transfers”.5 Indeed, with the expansion of electronic payment services, the scope of the present Code appears to be inadequate.

The principal objective of any proposed set of principles and rules to be prescribed is to implement and enhance fairness to consumers. The desired fairness is, however, to be attained in the context of an overall scheme that is designed to maximize benefits to society as a whole and strike a sound balance among the interests of all participants. These participants fall into three major categories: consumer customers, merchants and financial institutions. The position of merchants is outside the scope of the article, which focuses on the relationship between consumers and financial institutions offering consumer electronic funds transfers and holding or maintaining consumer accounts used for such transfers.

4. Canadian Code, Section 1(3).
5. Canadian Code, Section 1(5).
Policy considerations must also be taken into account in assessing the desirability of any specific rule applicable to consumer transactions that varies from the general law. Policies are also relevant in determining whether varied rules ought to exist for different retail payment systems. It should in any event be stressed that the overall framework for the search to implement or achieve consumer fairness is market-oriented. Stated otherwise, solutions put forward are not designed to adversely affect the benefits to consumers and will not in fact deprive society as a whole of free competition.

Nevertheless, a few premises ought to be stated at the outset. First, benefits of competition are unlikely to outweigh costs of or losses stemming from unfairness to consumers. In this context, long-term gains to some consumers later are not a good answer to short-term losses to others now. Secondly, the focus of competition is on the lowest price for the best quality product; risks associated with unfair terms may be underestimated by consumers, and competition with respect to contract terms is unlikely to generate optimal risk allocation. Finally, the most effective means to achieve loss avoidance or minimization may be the initial allocation of losses to the party best able to avoid or minimize such losses. Contract is unlikely to be the most effective tool to achieve this result. Accordingly, the general framework includes some form of regulation, though in the overall context of a market-oriented approach, as the best means to achieve fairness to consumers in the marketplace under the conditions of free competition.

Another policy consideration is the degree of technological neutrality. In this sense, the goal to be attained is that of achieving a balance between general principles that transcend technological innovations while reducing such principles to specific rules applying to existing and anticipated technologies. In this context, a review of existing technologies is followed by a discussion of anticipated new technologies. Attention is given to the impact of technology on liability rules.

In considering options for reform, attention is also given to the need to harmonize the legal position in Canada with prevailing standards in other developed countries. In this context, attention is given also to the possibility and need for North American harmonization, though only with the United States, with which, to a large extent, retail payment systems are harmonized, and substantial cross-border retail trade exists.
II. CONSUMER RETAIL ELECTRONIC PAYMENTS

Generally speaking, electronic retail payment systems link terminals to a financial institution computer system(s). A transaction through such a system may involve, other than the consumer and possibly the payee, one or more financial institutions, as well as a third-party processor or system network operator. Terminals may be located in a publicly accessed place or at the consumer’s home. A terminal accessed by the public may be located on the premises of a financial institution or in a public place such as a shopping centre, in which case it is an Automated Banking Machine (ABM) or an Automated Teller Machine (ATM). Alternatively, it may be located on the premises of a merchant, at a point of sale (POS). ABMs (or ATMs) are used for cash withdrawals and funds transfers from one account to another. POS terminals are used in payment for goods or services. Typically, particularly from a terminal located other than on the premises of the consumer, a transaction is initiated by means of a card allocated to the consumer by his or her financial institution. Such cards may be used, primarily for cash withdrawals, in terminals located on the premises of, and operated by, financial institutions. Finally, card information may be used for making oral telephone, written mail, and Internet orders.

From a Canadian perspective the evolution of non-cash consumer payments can be set out as follows:

1. The cheque is the oldest device. It constitutes a written unconditional order to the deposit-taking institution to pay and is authenticated by the consumer’s manual signature on the cheque. The cheque is not debited to the consumer’s account upon its issue, but rather, in the course of its processing in the payment and clearing system. A payee to

---

6. The process described below is of the conceptual evolutionary development of the various devices, each as an improvement and enhancement of its predecessor. Strictly from an historical point of view, the account may not be fully accurate. Yet, it is the conceptual evolutionary development set out below which explains the survival of some devices and the demise of others.

7. A cheque is “a bill drawn on a bank payable on demand”. A “bill” “is an unconditional order in writing, addressed by one person to another, signed by the person giving it, requiring the person to whom it is addressed to pay, on demand or at a fixed or determinable future time, a sum certain in money to or to the order of a specified person or to bearer”. “Bank” is broadly defined to include every member of the Canadian Payments Association and credit union member of a central co-operative credit society that is a Canadian Payments Association member. See Bills of Exchange Act, supra, footnote 3, ss. 165(1), 16(1), and 164. See further in text and footnote 22, infra.
whom a cheque is issued is not guaranteed payment and is faced with the risk of dishonour for lack of cover or any other reason.\(^8\)

2. The cheque guarantee card was developed to protect the payee from the risk of dishonour. However, the facility did not involve any communication to the deposit-taking institution at the time the cheque was issued. Therefore, it worked only for small amounts, without affording the deposit institution any meaningful protection from fraudulent use.

3. The credit card facilitated instant communication from the point of payment to the financial institution to for authorization. This afforded an immediate guarantee of payment to the payee by the financial institution, which could verify both cover and whether the card had been reported lost or stolen. But without being able to receive online instant authentication from the cardholder, the financial institution debits a credit rather than an asset account of the consumer.

4. The authentication of payment instructions by means of a secret code, such as a PIN, enabled the financial institution to promptly upon authorization debit the consumer’s asset account. This is how the credit card evolved to a debit card.\(^9\)

5. The stored-value card was developed to eliminate the need to communicate the payment instructions from the point of payment to the financial institution for authorization. Unlike credit and debit cards, which are access products facilitating access to value “stored” in an account held with and operated by the institution, value in the stored-value card is stored and processed on the card itself. Authorization and transfer of value are thus performed on and from the card.

6. Public key cryptography, and in the future, biometrics, are security enhancement features, designed to improve on the reliability of the PIN for electronic authentication of payment

---

\(8\) By itself, the issue of the cheque does not constitute a transfer of the cover to the payee, even when such a cover is available in the drawer’s account. See Bills of Exchange Act, ibid., s. 126.

instructions, given on either a debit card or stored-value card.

7. Parallel to the development of payment cards, personal computer (PC) banking has developed, allowing for access to accounts with financial institutions and storage of value from and on personal computers.

8. Finally, payments can be carried out on the basis of providing card information over the telephone, in the mail and over the Internet.

In the final analysis, a consumer’s payment authorization can be given in instructions authenticated in a variety of ways:

1. **By manual signature**
2. **At a terminal**
   (a) by inserting and running a card
      (i) and a manual signature
      (ii) alone
      (iii) and entering a PIN or another type of secret code
      (iv) and making an electronic signature
   (b) without a card
      (i) by entering a PIN or another type of secret code
      (ii) by making an electronic signature
3. **By providing card information**
   (a) on a (signed) mail order
   (b) on an (oral) phone order
   (c) over the Internet by e-mail
   (d) over the Internet by (secured) e-mail

Manual signature is the typical method of authorizing a cheque payment. In principle, to avoid the risk of dishonour on the basis of lack of cover for the cheque, a cheque payment may be guaranteed, in which case its issue is accompanied by a cheque guarantee card. This method has not been widely used in Canada and may not even exist anymore. Historically, charge and credit cards may have been seen as merely guaranteeing the cardholder’s manually signed undertaking on a sales draft; with technological developments, the

---

10. Manual signature will also be required to initiate a consumer credit transfer.
11. For a description of an old credit card system, under which the sales draft is “forwarded to the member bank which originally issued the card”, very much like a cheque, see e.g. *Harris Trust and Savings Bank v. McCray*, 316 NE 2d 209 at p. 211 (III. App. Ct. 1974).
card payment has been transformed to a payment category on its own.

At-the-terminal authorization can be made with or without a card, depending on the particular application. Terminals may fall into several categories:

1. an unattended public-access terminal, usually either an automated teller machine or an automated banking machine for cash withdrawals, inter-account transfers, and payments to pre-designated parties;
2. an in-the-bank attended terminal, particularly for cash withdrawals;
3. a POS public-access terminal at a retail establishment for payment for goods and services;
4. an exclusive-access (home-banking) terminal used solely by one consumer (possibly also by other household members) and located at the consumer's home (or at no fixed place when it is a laptop computer under the control of the consumer), which could be the consumer's own computer or, at the other extreme, a simple telephone or television set, and which could be used for all consumer payments, other than cash withdrawals; or
5. a (typically unattended) vending machine at a retail establishment, such as a gas station, movie theatre, or a parking lot (usually for small amounts).

Originally, a POS terminal was a mechanical device, known as a zip/zap manual terminal, on which the retailer ran a sales draft, filled in with the amount of payment, under an embossed credit card so as to stamp the draft with the card information. The customer then authenticated payment by signing the stamped draft. Approval was given by the financial institution in response to a telephone call by the merchant at the time of the transaction. The merchant deposited sales drafts with its bank that forwarded either them or relevant information to the issuer who charged the cardholder's account with each such a sales draft. Manual POS terminals are on their way out; unless indicated otherwise, a reference to a terminal in this article is to an electronic terminal. However, this procedure is still used

---

12. So far as payment cards are concerned, this article focuses on their use to authorize payment rather than as a means of identification, which is quite common in inter-branch banking in Canada.
whenever the electronic POS authentication procedure is not available, even temporarily. In effect, this procedure relies on the manual signature for proving the consumer’s liability; nevertheless, even where the charge to the consumer’s account is posted on the basis of the signed sales draft, the financial institution’s undertaking to the merchant is given on the basis of the card authentication. It is in this sense that one can speak of terminal authorization even in the manual terminal card payment.

Terminal authentication becomes more visible in conjunction with the electronic POS terminal, where the manually signed draft plays no role, even in the procedure leading to posting the charge in the consumer’s account. The electronic POS terminal improved on the manual terminal card payment by facilitating electronic authorization by the financial institution, the electronic deposit by the merchant and, ultimately, the automated debit to the consumer’s account. At an electronic POS terminal, authorization may be given by the insertion of the card by the merchant, accompanied by the consumer’s manual signature on a sales draft. This is the typical credit (or charge) card payment. In practice, the terminal reads the card information from a magnetic stripe and transmits the information to the issuer for approval. Effectively, this transmission authorizes both the deposit to the merchant’s account and the debit of the cardholder’s credit (or charge) card account. In fact, both the deposit (to the merchant’s account) and corresponding debit (to the consumer/cardholder’s account) are triggered by the card issuer’s authorization approval. The cardholder settles his or her cumulative indebtedness to the issuer periodically, upon the receipt of a periodic statement, though payment to the issuer can be made at any time, and any number of times during a billing cycle. Payment for the credit (or charge) transactions can be made to the issuer by cheque, from an ATM/ABM or home computer or telephone. Regardless, the signed sales draft plays no role in the payment process; it is kept, usually by the merchant, as a proof of the consumer’s authentication, to be made available to the consumer through his or her financial institution (upon request, usually) where the consumer denies the transaction.

A cash advance on a credit card may be given in the same manner in an in-the-bank attended terminal where the card is run by the bank and a cash advance draft is signed by the consumer. At a vending machine, authorization is given by the mere insertion of the card by the consumer into the terminal. This is typically
done for low-amount credit (or charge) card payments in gas stations, movie theatres or parking lots. Typically, such a terminal is unattended. In fact it is a specie of a POS terminal into which an authorization is made by merely inserting the card. To keep distinctions clear it is treated here separately and not included in the POS terminal category.

Magnetic stripe technology can be utilized beyond the electronic deposit to the merchant's account and the debit to the cardholder's credit account. It can also accommodate a full electronic authorization, leading to a debit to the cardholder's asset account, provided a short (usually four-digit) secret PIN is entered by the cardholder into the terminal. In attended POS terminals the card is inserted into the terminal by the merchant and the PIN is entered by the consumer. In an unattended ATM/ABM the card is also inserted and the PIN is entered by the consumer. Either way, this could be a debit card payment, which might be debited directly to the asset account of the consumer.

The fundamental distinction between credit and debit cards is the type of account to be accessed for an immediate debit. In Canada, underlying the distinction has been what is accompanying, or added to, at-the-terminal authorization so as to attribute it safely to the consumer. At-the-terminal authorization, unaccompanied by a secret code entered by the consumer, is not sufficiently reliable for the account-holding institution to debit the consumer's asset account. Hence, a separate credit account is debited, with the consumer not being required to settle before he or she is presented with a statement containing all debits similarly incurred during a billing cycle. This is the credit card facility.

Otherwise, when the at-the-terminal card authorization is accompanied by entering a personal code, the issuer is presented with a stronger and more reliable means of attributing authorization to the cardholder so as to justify debiting immediately the consumer/cardholder's asset account. This is the debit card facility. In practice, the same card may be used in connection with both a PIN as well as a manual signature or no-signature authorization, so as to fulfil both functions, that of a credit and debit card. Moreover, a PIN or any other applicable secret code may be entered by a consumer instructing that payment be made out of the credit card account. In any event, outside Canada financial institutions have not been particularly scrupulous in not debiting an asset account until they receive direct authentication from the consumer. For example, up to
present days, though subject to a forthcoming change, national debit card systems have operated in the United Kingdom on the basis of card authorization supported by a manual signature; no operational distinction thus exists in the United Kingdom between the authentication of credit and debit card payments, and the only distinction between the two types of cards is in the type of the account to be debited.\textsuperscript{13}

The charge card is a card linked to a credit (rather than an asset) account, which differs from the credit card in not permitting a deferred payment option, typically subject to incurring appropriate finance charges, beyond the end of the billing cycle. Charge card and credit card facilities are thus related. In fact, as a payment mechanism, the charge card is indistinguishable from the credit card, with no distinct function or feature of its own. The deferred payment option is irrelevant for the present discussion and the charge card will thus not be treated separately from the credit card.

Other than in a POS or in-the-bank (attended) terminal, as well as in an (unattended) vending machine, some form of electronic authorization is required; a card used in such transactions will universally perform a debit card function. In connection with an (attended) POS terminal, both credit and debit card functions are associated. In an in-the-bank (attended) terminal only the credit card function is performed. Consumer home-banking payments can be authorized either with or without a card, but in each case at least a PIN or other short secret code may be required to be entered by the consumer.

At-the-terminal authorization, whether from home or from a public-access terminal, and whether or not accompanied by the use of a card, may be given by means of an electronic signature. The latter can broadly be defined to be data in electronic form that are attached to or logically associated with other electronic data and that serve as a method of authentication. In practice, an electronic signature could be digital. Public key cryptography, underlying the digital signature, enables customers to control unique, secret information (a private key) for which they can provide related non-secret information (a public key) that can be used by

\textsuperscript{13} Similarly, the forthcoming transformation in the United Kingdom to POS PIN authentication will apply to both credit and debit cards. It will be carried out in connection with chip/smart card technology and not that of the magnetic stripe. In contrast to POS card payments, ATM card transactions have been authenticated in the United Kingdom on the basis of card and PIN, as in Canada and the United States.
the financial institution to verify that instructions issued by them have been signed using these keys. Provided that this scheme is soundly implemented, and that customers keep their signature keys secret and under their own exclusive control, transactions signed with them can be attributed to the customers with a high degree of confidence. Implementations of public key cryptography depend on calculations with very large numbers, and are in principle dependent on the use of quite powerful computers. But they have been comfortably within the capabilities of ordinary desktop computers for some years.\(^4\)

In principle, an electronic signature may be based on the electronic capture and transmission of biometric information, premised on unique physiological properties of the customer such as iris, handwriting or voice recognition, fingerprints and retinal scans. These may safely be used to authenticate instructions. However, at this point, such methods are not commercially available.

Alternatively, a card may be a smart-card, containing a micro processor, participating in, or even taking over, the authentication process, whether with regard to a secret code such as a PIN or an electronic signature. Where smart-card authorization is employed, either during in-home banking or from a public-accessed terminal, no confidential information need be communicated between the terminal and the issuer.

Other than in connection with smart cards, authorization in home banking, POS and ATM/ABM transactions requires interactive communication between the terminal and the authorizing financial institution or its agent. Smart-card authorization may be given on the card itself; other than in connection with e-money discussed below, resulting information must nevertheless travel from the terminal to the institution. Communication between the terminal and the financial institution is either in a closed system, over dedicated or phone lines, or in an open system, that is, over the Internet. In practice, communication over the Internet is available only in home banking and not in connection with public-access terminals. Home banking not relying on the Internet for communication is sometimes referred to as personal-computer (PC) banking.

---

14. For public key cryptography and the digital signature see e.g. J. Kaufman Winn, "Couriers Without Luggage: Negotiable Instruments and Digital Signatures" (1998), 49 S. Car. L. Rev. 739.
Other than in a bank account, "value" out of which payments are to be made may be loaded either on a card or computer software. These are known as stored-value products (SVP), as distinguished from access products, in connection with which value is "stored" in the bank account. Value stored on an SVP is known as "e-money". An SVP is either "electronic purse" or "digital cash". In the former, value is stored on the card itself, which is an integrated-circuit (IC) card containing a microprocessor chip — namely, a "smart card". In the latter, value is stored in computer software. Both types require at-the-terminal authorization. Digital cash constitutes a home-banking product. At-the-terminal authorization of an SVP may require the additional authentication by means of either a secret code such as a PIN or an electronic signature. For small amounts at vending machines it may not require any such additional authentication procedure.

Finally, the authorization of a card payment may be made without the physical presentation or processing of the card itself, that is, without its insertion at a terminal. Rather, authorization may be given by means of the communication of the card information from the consumer to the merchant. Typically, relevant information is card type or issuer, account number, name of cardholder, and card expiry date. The merchant will seek approval from the issuer, and thereby confirm the accuracy of the card information, through normal request-for-approval channels. In the course of the authorization-approval process, the consumer's account will be debited. This method is used in connection with credit (or charge) card payments between distant parties not present in the same premises. Card information may be communicated to the merchant by mail ("mail order"), over the phone ("phone order") or over the Internet. A mail


16. Possibly together with the Network name (for example, Visa or Mastercard) and a sponsor (such as an airline).
order is manually signed. A phone order is oral and is unauthenti-cated. An Internet order is in an e-mail message that may or may not be over a secured link.

Phone banking, in the sense outlined below, is not widespread in Canada. This is a service permitting customers to access their accounts and instruct payments by calling their banks and inter-actively speaking with bank staff members. In such a service the telephone is used as a telephone; it is to be distinguished from home-banking facility, substantially more available in Canada, where a touch-tone telephone is used as a PC. In the former type of phone banking the customer is requested to authenticate oral instructions by means of a password and/or confirming secondary security information such as mother's maiden name or wedding anniversary. The confirmation of such secondary security information may be sought by a financial institution wishing to verify “online”, in the process of a transaction authorization, the identity of a cardholder attempting to make payment. Obviously, this practice is awkward, may be embarrassing to the cardholder, and cannot be routinely relied upon.

In connection with the manual signature, the authorization pro cess does not involve any electronic element; no electronic funds transfer thus occurs. Manual signature authorization is thus outside the scope of this article. Conversely, the POS (as well as the in-the-bank) terminal credit card payment is initiated on the basis of electronic authorization; the sales draft containing the manual signature serves only as a back-up evidence, to be sought and re-trieved for presentment to the consumer/cardholder only where the latter denies, or seeks proof of, authorization. Accordingly, the credit card payment involves, to some extent, an electronic funds transfer, so as to be looked at in the present article.

All other types of card authorization, and all home banking at-the-terminal authorization, fall squarely into the subject-matter and are fully covered in this article. At the same time, strictly speaking, card-information authorizations, other than those communicated over the Internet, do not generate an electronic funds transfer. Nevertheless, the subject is considered in this article for two reasons. First, the authorization-approval sought from the issuer is through the same authorization-approval request channels as in the card-authorization payments. Second, this method of payment is intimately linked to card-authorized payments, which do fall within the scope of this article.
Telephone banking, operating through the interactive voice communication between the financial institution and the customer, also does not involve, in any way, electronic authorization. At the same time, similarly to electronic funds transfers, the service involves communication over telephone lines and requires authentication other than in writing. Taking into account that the service is not widespread in Canada, it will nevertheless be touched upon only in passing, either by way of comparison, or as part of a broader discussion.

It should be noted that in third-party payments, all forms of authorization, other than the mere manual-signature one, involve a guarantee of payment by a financial institution. This underlies the attraction of these payment methods to third-party merchants at the expense of the cheque payment. Indeed, this increased acceptability of the non-cheque payments enhances the popularity of all such payment methods in consumers’ eyes. Nevertheless, in providing this guarantee, the financial institution counts on reimbursement from the consumer, exactly like a financial institution that purports to debit the customer’s account for the customer’s cheques. Unauthorized payment is thus a risk that the institution would have liked to shift away to the customer.

The institution providing the guarantee is called the issuer, by reference to the issue of the payment card, where applicable. In theory, “issuing” and “account holding” are two separate functions which may or may not be carried out by the same financial institution. In Canada, however, it is quite common for the account-holding institution to be the issuer as well; particularly where the consumer’s account is an asset (as opposed to credit) account, this is quite natural. Regardless, the present article does not deal with the allocation of risks among business participants. No distinction between the account holding and issuing institutions is thus pursued, and the discussion proceeds on the assumption that one financial institution fulfils both functions.

In Canada, such an institution is not required to be a “bank” regulated under the Bank Act. In theory, it is not even required to be a member of the Canadian Payments Association (CPA) by the Canadian Payments Act. Yet, terminology here may be confusing.
Other than in the Canadian strict legal context, "banking" denotes financial intermediation between deposit taking and credit extension, and any institution fulfilling this function in the ordinary course of its business is a "bank". This is so notwithstanding regulatory treatment to the contrary in Canada, under which such an institution could be a trust company or credit union. Payment services are regarded as incidental to the deposit-taking function, and hence to "banking" in the above-mentioned general sense. But even in Canada, terminology is not entirely consistent; under the Bills of Exchange Act, a "bank" on which a cheque is to be drawn need be neither a "bank" under the Bank Act nor necessarily a regulated and insured deposit-taking institution. Rather, every qualified CPA member, including a life insurance company or an investment dealer, is a "bank". To avoid controversy, and respecting the separate institutional identity of the various players, particularly other than in connection with cheques, I endeavour to employ neutral terminology, such as "financial institution" or "account holding institution". Nevertheless, historically, in so far as a deposit-taking institution has universally been a "bank", the relationship between a deposit-taking institution and its customer has been labelled as "banking". It is thus impractical to abandon completely this terminology, particularly in light of both the dominant role of banks (namely, those institutions regulated as such under the Bank Act) as well the existing general meaning of "banks" other than under Canadian regulatory legislation.

19. See United Dominion Trust, Ltd. v. Kirkwood, [1966] 1 All E.R. 968 (C.A.) and the EU Banking Directive, under which "credit institution" is defined to mean "an undertaking whose business is to receive deposits or other repayable funds from the public and to grant credit for its own account". See Art. 1 of EC, Council Directive 77/780 of December 12, 1977 on coordination of laws and regulations administrative provisions relating to the taking up of the business of credit institutions, [1977] O.J. L. 322/31 (hereafter the First Banking Directive).

20. A trust company is permitted to accept deposits from any person under s. 423(1) of the Canada Trust and Loan Companies Act, S.C. 1991, c. 45; A credit union may accept deposits from designated depositors under s. 180 of Ontario's Credit Unions and Caisses Populaires Act, S.O. 1994, c. 11.


22. For CPA expanded membership see Canadian Payments Act, supra, footnote 18, at s. 4(2). Under s. 164 of the Bills of Exchange Act, supra, footnote 3, each such member is a bank for the purpose of the cheque provisions.

23. In addition to cases cited, supra, in footnotes 19 and 21, see also Joachimson v. Swiss Bank, [1921] 3 K.B. 110 (C.A.).
III. GENERAL LAW

1. Issues under General Law

In dealing with the allocation of unauthorized transfers losses under general law, three distinct issues are to be explored:

1. What is an unauthorized transfer?
2. Between the financial institution and the customer, who bears unauthorized transfer losses, and to what extent?
3. Between the financial institution and the customer, who has to prove what, and what is the standard of proof? For example, is it the financial institution, wishing to debit the customer’s account, that has to prove that the transfer was authorized, or is it the customer, wishing to avoid liability, who has to prove that the transfer was unauthorized? As well, to the extent that loss is shared, who has to prove the various elements underlying the division of losses, as for example, the existence or absence of fault?

(a) What is an Unauthorized Transfer?

It is useful to analyse this question by recognizing that in purporting to carry out a funds transfer for its customer, a financial institution will act on instructions given:

1. by the customer himself/herself;
2. under the customer’s actual authority;
3. under the customer’s apparent authority;
4. in compliance with an agreed upon security procedure such as the entering of a PIN or a digital signature; or
5. neither by the customer or under the customer’s authority, nor in compliance with an agreed upon security procedure.

Obviously, transfers carried out on the basis of instructions falling into the first two categories are of authorized transfers, for which the customer is fully responsible. In fact, this is so even when such instructions have not been properly authenticated. At the same time, it is obvious that transfers carried out on the basis of instructions falling into the fifth category are unauthorized.

Actual authority, under the second category, may be express or implied and is a matter between the principal giving the authority and the agent on whom the authority is conferred. Conversely, so far as the third category is concerned, apparent authority exists in
the absence of actual authority, on the basis of a representation made by the customer/principal to a third party relying on this representation.\(^2\) Strictly speaking, in the absence of communication between the principal-customer-representator to the financial institution, no representation is involved, and hence, no apparent authority is created by enabling somebody to comply with an agreed upon security procedure. This may be viewed as unfair to the financial institution, so that, arguably, intentionally and wilfully enabling somebody to comply with the agreed upon security procedure is to be treated as tantamount to representing him or her, to the entire world, including the financial institution, as authorized to bind the customer. Whether that somebody misused the trust and exceeded the authority given to him or her, or, arguably, even whether no actual authority was given to begin with, is entirely off the point.\(^2\) Arguably, the voluntary delivery of an access device to another ought not to be treated differently from either the consensual delivery of goods by an owner to a mercantile agent, or the voluntary act of a buyer leaving with the seller goods bought. In both such cases ownership is forfeited in favour of an innocent third party who acquired them from the mercantile agent or seller in possession;\(^2\) the third party’s views of the lawful possessor as having acted with the authority of the owner is regarded as justified. Otherwise, at least where actual authority was exceeded, the customer is to be held bound.\(^2\) It may even be argued that the mere delivery of a credit card will suffice to clothe its bearer with apparent authority, even when a written signature is required, since a proper identification of a cardholder is rarely practised.

25. For cheques, a contrary rule exists in English law under *Smith v. Prosser*, [1907] 2 K.B. 735 (C.A.). Thereunder, a distinction is drawn between the consequences of an unauthorized completion and issue of a blank signed cheque delivered by the signer (i) with authority to issue it, and (ii) for a mere safekeeping. This, however, is an aberration (see e.g. I. Ackermann, “Signature and Liability in the Law of Bills and Notes” (1993), 8 B.F.L.R. 295) derived from a particular strict interpretation of a provision in the Bills of Exchange Act, *supra*, footnote 3, which needs not to be extended to the area of electronic funds transfer.
26. Sections 2(1) of the Factors Act, R.S.O. 1990, c. F.1, and 25(1) of the Sale of Goods Act, R.S.O 1990, c. S.1, as am. At the same time, the need to provide for these two cases by statute may support the view that they are not cases of apparent authority and hence, the mere delivery of an access device to another, without more, is not to be viewed as clothing the latter with apparent authority.
27. This would be a case of apparent authority, on the basis of the principal’s representation of authority not subject to limitations. See Reynolds, *supra*, footnote 24, at p. 91.
Neither actual nor apparent authority is involved in cases covered by the fourth category, and hence they result in unauthorized transfers. Whether the financial institution is nevertheless justified in such cases to rely on the compliance with the agreed-upon security procedure is a different issue, to be discussed in connection with the second issue, that of who bears unauthorized transfer losses.

The following occurrences may lead to unauthorized transfers:  

1. Cards may be stolen or otherwise reach unauthorized hands.  
2. Card information may be obtained by the physical examination of the card or a record of a legitimate card transaction.  
3. Card information may be intercepted in transit, particularly over phone lines or the Internet. Risk can be avoided in transactions carried out by the cardholder using a web browser to connect a supplier's web page, where a secure connection is established.  
4. A PIN, any other secret code or password, as well as a private key needed for a digital signature, may be improperly recorded or kept by a customer so as to facilitate breach of confidentiality and availability to unauthorized persons.  
5. Short PINs and other codes may be correctly guessed. Similarly, secondary security information, facilitating access to phone banking, such as mother's maiden name or wedding anniversary, may be known to a relative or unfaithful friend who may become an unauthorized user.  
6. The confidentiality of a PIN or any other secret code or password shared between the customer and the financial institution may be breached by insiders with the financial institution.  
7. Security information may be intercepted in telephone banking (where available) and to a lesser degree in PC as well as Internet banking.  

29. In general, intercepting the content of traffic between modems is much more difficult than with voice calls. At the same time, if the consumer gains access through a local network such as that of his or her employer, additional interception risks may be involved, where the employer’s local network operates a firewall to protect its internal
8. Unless a customer and a financial institution exchange messages signing respective private keys and verified by means of their public keys, that is, unless they exchange messages digitally signed, the customer’s communication over the Internet may be diverted to a fraudulent imitation system so as to reveal to the owner of the fraudulent site transaction and security information.

9. To some extent, the security of banking computer systems has not been fully established. Regardless, serious concerns exist with respect to customer PC software security. Security may be breached in the course of software installation by a dishonest “expert” neighbour or friend. PCs used on the Internet are vulnerable to attacks in which software is remotely installed to capture and transmit the user’s keyboard data to a remote location. An even more potent attack would be based on a computer virus. Such attacks may capture security and account information. Even a private key may be compromised.

10. Secret data held in hardware — for example, in smart cards — are much less vulnerable to being discovered by an attacker. However, hardware solutions are not infallible; many smart cards are vulnerable to a fake machine extracting their secrets by observing the power they consume while calculating a digital signature. As well, solutions bypassing PCs require the card to have a powerful processing capability of its own which raises considerable cost implications. A required PIN may be entered into a small keypad and a digital signature may be processed in the card. Nevertheless, it is only the use of biometric data that could secure safe communication of security information.

The first three risks may lead to unauthorized credit card transactions, even where a supporting signature is required, since even
then merchants typically tend to rely on the possession of the card rather than on the verification of the identity of its holder. The other risks lead to unauthorized transfers authenticated in compliance with the agreed upon security procedure.

(b) Between the Financial Institution and the Customer, Who Bears Unauthorized Transfer Losses, and to What Extent?

Naturally, as a matter of both fairness and common sense, the starting point is that the customer is not responsible for unauthorized transfers. For manually signed cheques, this rule is explicitly codified in Canada, and it is reasonable to treat it as applicable, by analogy, to electronic funds transfers as well. In effect, the real issue is the existence and scope of exceptions to the rule exonerating the consumer from responsibility for unauthorized transfers. One question arises as to whether the financial institution may lawfully debit the customer's account for transfers merely on the basis of authentication in compliance with an agreed-upon security procedure, irrespective of the absence of either actual or apparent authority. Namely, the question is whether the customer is liable for transfers falling into the fourth category set out in Part III.1(a) above. Similarly, there may be a question when neither compliance with a security procedure beyond card insertion nor a manual signature is required. Such is the case in a telephone or Internet order, as well as a vending-machine purchase. Another question relates to both the fourth and fifth categories, and has to do with the role of fault in the allocation of unauthorized transfer losses.

The first question, raised with respect to the fourth category, is whether the mere compliance with the agreed-upon security procedure is adequate by itself to allow the financial institution to charge the customer. A handwritten or manual signature is individual to the signer; as such, it identifies the signer. Any signature, other than that of the authorized signer, is by definition unauthorized, and may not serve as a valid authentication on the purported signer's behalf. Prima facie, the financial institution thus would not be justified in debiting the purported signer's account. Conversely, electronic authentication is carried out by means of compliance with an agreed-upon security procedure, which can be entered into a terminal by anyone to whom it becomes available.

Electronic authentication is a means of **legitimizing** the action of that person, or of attributing it to him or her, but not of identifying him or her. It is very much like a door key facilitating entry to the system, or better, a seal affixed to an instrument, authenticating it, but not identifying the one who actually placed it. Consequently, any technologically effective entry of an access code, even when it is carried out by an unauthorized person to whom it may have become available unlawfully, appears to the financial institution as a valid authentication. **Prima facie**, the electronic authentication would thus justify the account institution in debiting the customer's account. In this sense, the authentication by means of compliance with a security procedure is not an electronic equivalent to a manual signature; rather, it is more analogous to the placement of an "electronic seal". The financial institution is unable to distinguish between an authorized and unauthorized authentication and is likely to be inclined to pass the risk of an unauthorized but properly authenticated transfers onto the customer. This may however allocate to the customer enormous losses, against which he or she may not be always able to protect himself or herself. Conversely, the allocation of such losses to the financial institution will enhance effective loss distribution and will encourage financial institutions to invest in the development of technologies designed to introduce authentication premised on biometric information, which will facilitate the identification of the person giving payment instructions. It is noteworthy in this context that the EU Directive on Electronic Signatures confers the status of a manual signature only to an "advanced electronic signature", the latter being required to be "uniquely linked to the signatory", "capable of identifying the signatory", and "created using means that the signatory can maintain under his sole control"; effectively, only

---


34. EC, *Council Directive 99/93 of 19 January on electronic signatures*, [2000] O.J. L 13/12 at arts. 2(1), 2(2) and 5. The fourth requirement under art. 2(2) is for the electronic signature to be "linked to the data to which it relates in such a manner that any subsequent change in the data is detectable". Linkage "to the signatory and to no other person" and exclusive control over the signature creation data are required to make an electronic signature that of a given person also under art. 6 of Draft UNCITRAL Model Law on Electronic Signatures, UNCITRAL, 37th Sess., UNDoc. A/CN.9/483 (2000).
the (still commercially unavailable) biometric (and not the currently commercially available digital) signature will meet this standard.

Mere card authentication, unsupported by either compliance with a security procedure or a manual signature, is equally incapable of creating a linkage to the customer to be made liable. Such is the case in a vending-machine payment. It may be argued that facilitating payments without providing adequate security is a risk to be assumed by the financial institution. In effect, this means that where the customer denies responsibility, the risk ought to be allocated primarily to the financial institution that chose to facilitate a transfer not reliably authenticated. At the same time, where an issuer is technologically precluded from preventing unauthorized use of stored-value cards, or "electronic purse", loaded value may be treated as the equivalent of cash; loss of such devices may be tantamount to the loss of cash, to be borne by the consumer. Yet, in fairness to consumers, such a rule is to be implemented only in a framework where value loaded on such devices is strictly limited, and the inability of the issuer to prevent future unauthorized use is inherent in the nature of the product, rather than a matter of a business decision, designed to bypass communication from the terminal, as could be the case in connection with the vending machine authentication of a credit card.

The next question relates to the role of negligence or fault in generating and assuming responsibility for unauthorized transfer losses, whether of the fourth or the fifth category. Indeed, the customer's fault or negligence may have contributed to an unauthorized funds transfer. That is, due to the customer's fault, a person may unlawfully assume control of the card and code, or bypass their use altogether, and initiate an unauthorized transfer. For example, the customer may have been negligent in the choice of the secret access code, where such choice was available. For instance, the customer could have selected obvious numbers or letters, such as those of the customer's car licence plate, birthday or name. As well, the customer might have failed to advise the financial institution properly and promptly of the loss or theft of either the card or code, or of any other security breach. Or else, upon receiving notification from the institution of a transfer, the customer may have failed to act diligently and promptly in discovering the lack of authority.

The customer may have thereby precluded prompt recourse by the financial institution against the wrongdoer, prior to the latter's
disappearance or insolvency, and further enabled that wrongdoer to continue drawing on the account without the customer's authority. Obviously, allocating to the customer losses caused by his or her fault will enhance diligence and minimize losses. However, loss distribution will not be enhanced. Moreover, litigation regarding the existence of fault and the degree of causation may be wasteful, and worse, may put the consumer, who has fewer resources, in a disadvantageous position. The alternative is loss sharing between the customer and the institution—that is, to allocate to the consumer losses only up to a low threshold, irrespective of fault, thereby enhancing diligence without causing the consumer undue hardship. This can be done by either statute or agreement.

Fault leading to unauthorized losses may also be attributed to the financial institution. Indeed, in the case of a manual signature, the institution's obligation is in detecting the forgery on each instrument, individually. At the same time, in the case of the electronic authentication, the institution is bound to implement a safe system for the distribution of access devices, a safe security procedure for the authentication of payment instructions, as well as an effective system of blocking access upon being advised of loss or theft of the access device. At least historically in English law, banks' liability for payment of forged cheques has been premised on banks being "bound to know the hand-writing of their customers", rather than on a duty of care to detect forgeries. In contrast, in an electronic environment, the institution's duty ought to be premised on negligence. Typically, such negligence is not individual to an institution's employee, as where the latter failed to detect the forgery of a manual signature; rather, in the electronic context, we are concerned with "systemic negligence" by the institution organization as a whole and on the level of implementing satisfactory computer as well as office procedures. Breach of required standards by the institution, while not necessarily attributable to any individual employee, is nonetheless negligence.

In principle, the financial institution's fault may be relevant in two major ways. First, it may be raised as an answer to the alleged

35. The financial institution may also be charged with a duty to ensure the safety and security of public-access terminals.
fault of the consumer, where the latter is relevant. Second, it is reasonable to expect that where the institution seeks to be justified in acting on the basis of an agreed-upon security procedure, namely, in carrying out transfers of the fourth category, the security procedure set up by the financial institution must be safe, sound, and reliable, and that no negligence occurred in its conducting of the verification procedures.

(c) Between the Financial Institution and the Customer, Who Has To Prove What, and What is the Standard of Proof?

This issue relates to questions of evidence, or more particularly, to both onus and subject-matter of proof. For example, is it the financial institution, wishing to debit the customer's account, that has to prove that the transfer was authorized? Or is it the customer, wishing to avoid liability, who has to prove that the transfer was unauthorized? As well, to the extent that loss is shared, who has to prove the various elements underlying the division of losses, as for example the existence or absence of fault?

In principle, it is for the financial institution to provide justification for debiting the customer's account; it may debit the customer's account only where it has a mandate to do so. An institution has thus to prove that in debiting the customer's instructions it acted on the basis of the actual or apparent authority of the customer. It may nevertheless be debatable how far the financial institution ought to go in making its case.

In connection with a manual signature, the institution must prove that the signature actually emanated from the customer. Indeed, a forgery may be either crude or skilful. However, physiological properties are strictly individual. Accordingly, in principle, even skilful forgeries can be spotted by means of forensic examinations, which are not limited to naked-eye examination of the image of the signature. The other side of the coin is that the attribution of an individual signature to the actual signer is provable. Obviously, relevant examinations may be costly and they do not guarantee full accuracy. Nevertheless, on the whole such risks have not

proven to be burdensome. Similarly, in principle, unique physiological properties or biometric information, other than handwriting, such as iris or voice recognition, fingerprints and retinal scans, may safely be used to link instructions to their actual giver. However, at this point, such methods are not commercially available.

Regarding an allegation as to the loss of a card, it may appear reasonable, at least at first blush, to allocate the onus of proof on the consumer. Conversely, with regard to security procedures, such as PIN or digital signature, the issue is more complex. It is the financial institution that ought to be required to prove proper verification. In this context, the financial institution ought to be required to prove three things. First, the institution ought to be required to prove actual verification, including, where applicable, that it was the actual card issued by it, rather than an unauthorized copy of it, or even no card at all, that was used in the relevant transaction. Second, the financial institution ought to be required to prove the soundness of the security procedure used for verification. Third, the institution should be required to prove its own lack of negligence in the verification process. At the same time, the institution is unlikely to be able to prove actual or even apparent authority, namely, that compliance with the security procedure was not made by one who unlawfully became able to comply. On the other hand, the consumer may be ill-equipped to challenge the institution’s technical evidence as to proper verification; taking into account the circumstances under which an intruder may unlawfully acquire required security information, the onus of proving intrusion cannot usually be sustained by a consumer.

Accordingly, while typically the financial institution cannot be expected to put forward evidence more than in relation to compliance with a sound security procedure, this ought not to suffice to justify the debit to the consumer’s account on the basis of the consumer’s authority. A rule not permitting a debit under such circumstances may encourage the institution to invest in technological enhancements facilitating electronic identification, to increase surveillance in public-access terminals, or to do both. Otherwise, a court is left with the need to choose between the financial institution’s proof of compliance with the security procedure and the consumer’s denial of authority. In such a case, the court will be bound to assess the evidence of the consumer denying

39. See above, text around footnote 28.
the instructions and ought to determine the case accordingly. Stated otherwise, it is for the institution to prove actual or apparent authority. Typically, it will produce evidence supporting compliance with an agreed-upon sound security procedure, and will be entitled to judgment, unless its evidence is met by the consumer's denial, which ought to be assessed on its merit. On his or her part, the consumer ought not to be required to prove that the instructions were given by an unauthorized person or that no breach of security occurred; rather, the consumer ought to put forward evidence that will convince the court that the financial institution's evidence as to compliance with the security procedure is insufficient to prove authority. Stated otherwise, it is not that the consumer ought to prove loss of the card, or otherwise lack of authority. Rather, the consumer's task is to show that the institution has not proven authority. This indeed may include proof of loss of the card as well as of no breach of security at the consumer's own household, but not over the entire system.

Some assistance may be provided to the consumer by fastening on the financial institution, as a condition precedent to any recovery, a duty to fully investigate any allegation of unauthorized use and make the result of such investigation fully known. On his or her part, the consumer ought to be required to fully co-operate in such investigation. Not infrequently, such investigation will confirm the unauthorized use, and even that the genuine card was not used in the transaction. Yet, there will remain cases in which the evidence will consist of that of the institution as to verification and that of the consumer as to denial of authority.

Indeed, in a civil case, the standard of proof is that of a balance of probabilities, often referred to as "proof on a preponderance of probabilities" or "proof on a preponderance of evidence". There is no requirement to meet the higher standard, required for a conviction in criminal cases, of proving the occurrence of facts beyond a reasonable doubt. In normal circumstances it may thus be easy for a financial institution to meet the standard in relation to compliance with security procedure. Even in connection with a security procedure not exclusively used for communication from public-access terminals over a dedicated financial system, the balance of probability may support the lack of intrusion. In the absence of denial by the

consumer this may suffice to meet the burden of proof with respect to authority. At the same time, it is the credibility of the denying consumer’s evidence that ought to be crucial in convincing the court that even if the security procedure has been complied with, on the balance of probabilities, the institution has failed to prove authority. Unfortunately however, the task of the court in assessing such evidence may not be easy.

In a credit card or mail order payment alleged to be unauthorized, the financial institution is to be required to prove the genuineness of the required signature. This may not apply to a card transaction where the financial institution proves the cardholder voluntarily and willingly relinquished possession to the one who became the wrongdoer, which may be treated as a case of apparent authority.\textsuperscript{41} Where no signature is required, as in telephone orders, Internet transactions, or vending machine credit card payments, it is still for the financial institution to prove either actual or apparent authority;\textsuperscript{42} the institution may discharge the onus by proving a valid card authentication, subject to the consumer’s ability to convince the court with the genuineness of his or her denial. With regard to a mere card authorization at a vending machine, a question may arise as to the reasonableness of the security procedure, particularly if such payments are allowed to occur for high sums, which may not be the case at present. As a rule, in a telephone order, unless the consumer’s voice call was recorded, the consumer’s task in convincing the court with the genuineness of his or her denial seems to be easier.\textsuperscript{43} In a vending-machine transaction, the financial institution will fail in proving authority where loss of the card prior to the alleged transaction is proved by the consumer. However, this is not to say that the consumer ought to prove lack of authority; rather, it is up to the consumer to upset what otherwise would have been an appropriate inference from the proof of card authentication.

Where loss allocation is determined according to fault, the onus of proof lies on the party alleging it. However, the soundness of the security procedure and lack of negligence in performing the

\textsuperscript{41} See discussion on apparent and actual authority in the paragraph containing notes 24-28, supra.

\textsuperscript{42} See supra, text around footnote 38.

\textsuperscript{43} Where time permits, the merchant may seek the cardholder’s confirmation for a telephone or Internet order before releasing the goods. But this is not always feasible; depending on the circumstances, a mere callback may not be adequate. Also, origination at the consumer’s e-mail address or phone number, where provable, has evidentiary value.
verification ought to be proved by the financial institution. This is so since such matters form the foundation of its case as to the financial institution’s right to debit the consumer's account on the basis of the “legitimation” of the instructions according to the contract with the consumer.

2. Inadequacy of General Law

A detailed analysis of applicable general law is outside the scope of this article. Yet, a few observations may be made. First, a fundamental issue with which legal systems struggle with varied degrees of success is that of the scope of unauthorized transfers, particularly those carried out by someone who unlawfully obtained control of the means of access and thus complied with the security procedure agreed upon between the financial institution and the customer.

Second, regarding the allocation of loss, only the American Uniform Commercial Code provides a comprehensive and coherent scheme, specifically tailored to fit the issue of unauthorized electronic funds transfers. Briefly summarized, under UCC Article 4A, a business customer may be found liable for an unauthorized transfer where the financial institution proves verification of authority in compliance with an agreed-upon commercially reasonable security procedure. The customer may nevertheless avoid liability by proving that transfer has not emanated from customer’s organization or somebody within customer’s sphere of influence.

In the absence of specific legislation anywhere else, both common law and civil law jurisdictions determine the question under broad principles of general contract law or of more specific mandate doctrines. Solutions are thus neither comprehensive nor coherent. Between the two systems, it seems that the civil law is clearer and more decisive in taking into account customer’s fault, irrespective of any agreement on the point. Both systems take into account the financial institution’s fault. In any event, there is nothing to preclude, in both common and civil law, the attainment of the same result as under the UCC, by means of contract.

Whether and how far financial institutions may disclaim liability for breach of the duty of care is not entirely clear. Overall such

44. See discussion, on which observations below draw, in B. Geva, Bank Collections and Payment Transactions (Oxford, Oxford University Press, 2001), pp. 392-421.
disclaimers are more specifically enforceable in civil than in common law. Presumably, in civil law, by means of a properly drafted disclaimer, a slightly negligent financial institution may shift liability away onto a non-negligent customer not in breach of any duty. This seems to be less conceivable in common law.

In the final analysis, so far as loss allocation of unauthorized consumer electronic funds transfers is concerned, and other than in connection with the onus of proof, general law provides a focal point for an antithesis or departure point rather than a model to be followed. Automatic liability on the basis of compliance with security procedures seems to be unfair, since a consumer may not be in position to provide a positive proof that he or she has not given the instructions. As well, questions may arise regarding the role of consumer's negligence as grounds for asserting full liability. Finally, in consumer transactions, broadly drafted disclaimer clauses are inappropriate.

Fairness to consumers will be enhanced by balancing between loss distribution and loss prevention or minimization. Loss distribution points to the financial institution as the best risk bearer. However, such a scheme will not encourage diligence and loss prevention by consumers, and will result in diligent consumers subsidizing careless ones. At the same time, a scheme based on consumers' fault may be unfair in a case of a momentary negligence, will prolong litigation, and may give the institution unfair advantage in settlement negotiations; after all, compared with the average individual consumer, the financial institution is likely to have more resources and greater long-run interest in the evolution of rules restrictive to consumers, much beyond the amount at stake at any given litigation. In any event, loss prevention or minimization does not universally point to the consumer as the appropriate risk bearer. Rather, the imposition of loss on financial institutions will enhance the development of improved technologies for precluding unauthorized transfers as well as for identifying the wrongdoer and his or her apprehension. It is against this background that some balance ought to be struck between loss distribution and loss prevention or minimization.

One option is that of loss allocation to the financial institution, subject to a fixed deductible, in a relatively low amount, to be fastened on the consumer, once the institution proves proper verification of applicable security procedure. The theory of the deductible is the prevention of financial catastrophe to the consumer,
while still encouraging him or her to act diligently. Consumer liability for the full amount is, however, not to be precluded once the consumer becomes aware of unauthorized transfers but does not advise the financial institution that would have been in a position to deny access to the wrongdoer. If consumer fault is to be nevertheless taken into account, one question that arises is that of the interplay between a broad principle of negligent consumers' responsibility, to be applied in each given case, and that of enumerating specific acts or omissions which constitute required negligence. Another question which arises under a consumer fault regime is that of the automatic deductible; if the financial institution is entitled to full recovery from a negligent consumer, there may be no justification to fastening any liability on a non-negligent one.

Finally, regarding the third question, that of the onus and standard of proof, there is no real legitimate controversy as to the obligation of the financial institution to prove authorized use on the balance of probabilities. What may be debatable is how much ought to be inferred from proof by the financial institution of compliance with a commercial reasonable security procedure.

Accordingly, in reviewing the ensuing specific consumer schemes and purporting to establish the optimal solutions, attention is to be given to the following points:

1. The scope of authority. Is the voluntary surrender of the means of access tantamount to conferring apparent authority so as to become liable for all subsequent transfers?

2. The impact of the proof put forward by the financial institution as to the verification of authority in compliance with the agreed-upon commercially reasonable security procedure. Does it fasten full liability on the consumer? What more, if anything, ought to be proven by the institution to become entitled to full recovery? Alternatively, what kind of evidence is to be brought by the consumer wishing to avoid liability? In fact, this issue is concerned with the scope of authority as well as the onus of proof.

3. What is the role and scope of consumer's fault? Ought it to fasten or increase liability, to what extent, and ought careless acts or omissions specifically be defined and/or advised to consumers?
4. Particularly in light of some of the foregoing difficulties, is it advisable to provide for a minimum no fault liability on the part of the consumer, in effect a deductible to be applied for unauthorized transfers, and if so, in what circumstances?

Statutory as well as code schemes often impose minimum liability on consumers for unauthorized funds transfers, irrespective of fault. At first blush, such a rule is unjustifiable. The rationale for such a rule, and possible exceptions to it, may however be analysed as follows:

1. As already indicated, in effect, card transactions authenticated by both card reading and manual signature are carried out on the basis of the card authentication alone, with the manual signature serving as a mere backup evidence. In this context, the minimum liability serves as an incentive to consumers to safeguard their cards and advise promptly the issuer of any loss or theft.

2. This rationale equally applies to authentication by mere card reading (without a manual signature) but not to authentication on the basis of card information, whether transmitted by mail, through the phone, or over the Internet. Accordingly, minimum liability could be imposed in connection with authentication by mere card reading, but ought not to be imposed with respect to authentication on the basis of card information.

3. This rationale does not stand on its own where authentication is by means of verifying compliance with a security procedure. True, minimum liability will serve as an incentive to guard the card and secret code. However, in my view, in such a case, minimum liability can also be, and in fact is better, rationalized on the inability of the financial institution to usually prove, on the balance of probabilities, more than compliance with the security procedure, which leaves open the possibility of security breach outside the consumer's sphere of control and ability to prove. Minimum liability purports to balance between the inadequacy of available proof and the encouragement of consumers to safeguard their means of access.

4. In this light, there is no justification whatsoever even for limited liability when the institution is unable to prove
security verification, including, when and where required, card authentication.

5. Where it exists, minimum liability is premised on the failure to prove authority. An exception releasing the consumer from liability may thus be rationalized on the existence of proof as to lack of authority. One reason against such an exception is that the value of resources to be invested in litigation is likely to be disproportionate in relation to the low amount in dispute (that is, the minimum liability) to be settled.

6. An exception raising the consumer’s liability to the entire loss may be justified only where the consumer’s fault has substantially contributed to such loss. An issue then arises as to the degree of fault to be required — that is, whether it is simple negligence or only gross negligence which will fasten extended liability on the consumer. Yet any such rule may lead to wasteful litigation and may be unfair to a consumer who may have underestimated the risk. Nevertheless, the existence or absence of a fault-based exception is a matter of valid choice. Possibly, a broad principle linking expanded liability to negligence could be replaced by rules linking liability to enumerated prescribed and precise acts or omissions constituting gross negligence, such as writing the PIN on the card.

7. It becomes clear in this context that a requirement fastening on the consumer a duty to carefully examine periodical statements, and advise the financial institution of any unauthorized transfer recorded in them, so as to preclude further such transfers to be carried out by the same wrongdoer, will reduce losses. Such a requirement is reasonable and is thus a legitimate policy choice, even in the absence of a broader duty to act diligently with the view of preventing losses.

8. Daily withdrawal and transaction limits ought to provide ceilings for consumer exposure in the case of unauthorized transfer losses.

Overall, both the liability for unauthorized losses and its limits and exceptions are designed to balance between providing incentives to consumers to minimize unauthorized transfer losses and the practical difficulties in providing adequate evidence. It remains
to be seen how this balance is struck. This point is discussed below, first in connection with the various existing schemes, and subsequently in the context of a proposal for reform.

IV. SPECIFIC CONSUMER PROTECTION SCHEMES

1. Consumer Legislation in the United States

In the United States, the liability of a credit card holder for the unauthorized use of the card is governed by §133 of the federal Consumer Credit Protection Act — Chapter 2: Credit Transactions and §226.12 of Regulation Z Truth in Lending implementing it. Consumer liability for unauthorized transfers initiated from either public access (that is, ATM as well as POS) terminals or exclusive access terminals (namely in connection with home banking) is governed by §909 of the federal Electronic Fund Transfer Act and Regulation E implementing it. Both Regulations Z and E were issued and are implemented by the Board of Governors of the Federal Reserve System. In both cases, that of the unauthorized credit card payment and the unauthorized electronic fund transfer, there is a ceiling for the consumer's exposure for unauthorized payments, and the consumer's fault is irrelevant, other than in connection with the failure to promptly advise. The two schemes are however not identical.

In terms of scope, Reg. E applies to "any electronic fund transfer that authorizes a financial institution to debit or credit a consumer's account". The consumer's account must be an asset account; a credit account or plan is thus excluded. "Electronic fund transfer" is broadly defined to cover "any transfer of funds that is initiated through an electronic terminal, telephone, computer or magnetic tape for the purpose of... instructing... a financial institution to

49. Reg. E §205.3(a).
50. Reg. E §205(2)(b)(1), which further provides that "an occasional or incidental credit balance in a credit plan" will not qualify an otherwise credit account.
51. "Electronic terminal" is defined, somewhat tautologically, in §205.2(h), to mean "an electronic device, other than a telephone operated by a consumer, through which a consumer may initiate an electronic funds transfer. The term includes, but is not limited to, point-of-sale terminals, automated teller machines, and cash dispensing machines."
debit or credit an account", including "transfers resulting from debit card transactions, whether or not not initiated through an electronic terminal". Stated otherwise, a debit card transaction covered by Reg. E could be authenticated either electronically or otherwise, including by means of a manual signature. Interestingly, neither "debit card" nor "debit card transaction" is defined; terminology must be in reference to a payment card facilitating the transfer of funds from or into a consumer asset account. Electronic home banking is covered as well, regardless whether access is made by means of a debit card. In any event, the dividing line between the credit card covered by Reg. Z and the debit card covered by Reg. E is not the method of authentication, but rather the type of account to be accessed with the card; the former accesses a credit plan while the other accesses an asset account.

Under Reg. Z §226.12(b)(1), unless greater protection to the cardholder is afforded either by other applicable law or an agreement, "[t]he liability of a cardholder for unauthorized use of a credit card shall not exceed the lesser of $50 or the amount of money, property, labor, or services obtained by the unauthorized use of a point-of-sale transfer, automated teller machine transfers, direct deposits or withdrawals, and transfers initiated by telephone. Preauthorized transfers are included; see Official Staff Commentary on Regulation E Electronic Fund Transfers 205(3)(b)(1)(iii) as am. effective May 30, 2000. Presumably, they are "direct deposits or withdrawals of funds" under Reg. E §205.3(b)(3).

In the terminology used in this article, a debit card transaction "not initiated through an electronic terminal" (as envisaged by Reg. E §205.3(b)(5)) so as nevertheless to be an "electronic fund transfer", will include a debit card transaction initiated through a terminal whose authentication is supported by means of a manual signature rather than by means of an electronic code. In any event, no meaningful distinction is to be made between "terminal" and "electronic terminal".

See Official Staff Commentary on Regulation E Electronic Fund Transfers, as am. Effective on May 30, 2000, to §205.3(b), point #(iv) (hereafter Official Commentary on Reg. E), under which Reg. E covers "A transfer from the consumer's account resulting from a debit card transaction at a merchant location, even if electronic terminal is involved at the time of the transaction, if the consumer's account is subsequently debited for the amount of the transfer."

Obviously, delineation is not always straightforward. A card accessing an asset account tied to an overdraft line as well as a card that accesses both an asset and credit account could be a credit card governed by Reg. Z. Official Staff Commentary on Regulation Z Truth in Lending as am. effective March 31, 1999, to §226.2(a)(15), point 2(i)(A) and (B) (hereafter Official Staff Commentary on Reg. Z). Presumably, Reg. Z will apply to activities in the credit line and Reg. E to the asset account activity. Details are outside the scope of this article. See Reg. E §205.12(a) and Official Staff Commentary on Reg. E 205.12(a). See also Reg. Z §226.12(g).

52. Reg. E §205.3(b).
53. Reg. E §205.3(b)(5). Other transfers included in the non-exhaustive list of paragraph (b)(1) to (4) are point-of-sale transfers, automated teller machine transfers, direct deposits or withdrawals, and transfers initiated by telephone. Preauthorized transfers are included; see Official Staff Commentary on Regulation E Electronic Fund Transfers 205(3)(b)(1)(iii) as am. effective May 30, 2000. Presumably, they are "direct deposits or withdrawals of funds" under Reg. E §205.3(b)(3).
54. In the terminology used in this article, a debit card transaction "not initiated through an electronic terminal" (as envisaged by Reg. E §205.3(b)(5)) so as nevertheless to be an "electronic fund transfer", will include a debit card transaction initiated through a terminal whose authentication is supported by means of a manual signature rather than by means of an electronic code. In any event, no meaningful distinction is to be made between "terminal" and "electronic terminal".
55. See Official Staff Commentary on Regulation E Electronic Fund Transfers, as am. Effective on May 30, 2000, to §205.3(b), point #(iv) (hereafter Official Commentary on Reg. E), under which Reg. E covers "A transfer from the consumer's account resulting from a debit card transaction at a merchant location, even if electronic terminal is involved at the time of the transaction, if the consumer's asset account is subsequently debited for the amount of the transfer."
56. Obviously, delineation is not always straightforward. A card accessing an asset account tied to an overdraft line as well as a card that accesses both an asset and credit account could be a credit card governed by Reg. Z. Official Staff Commentary on Regulation Z Truth in Lending as am. effective March 31, 1999, to §226.2(a)(15), point 2(i)(A) and (B) (hereafter Official Staff Commentary on Reg. Z). Presumably, Reg. Z will apply to activities in the credit line and Reg. E to the asset account activity. Details are outside the scope of this article. See Reg. E §205.12(a) and Official Staff Commentary on Reg. E 205.12(a). See also Reg. Z §226.12(g).
before notification to the card issuer". This limit was interpreted to be set in conjunction with a "series of unauthorized uses"; such uses are not stated to be necessarily related. No increased liability is provided for the failure to promptly advise the financial institution so that, in fact, the incentive for prompt notification is lost once $50 unauthorized use loss has been incurred. Notification to the card issuer of the loss or theft may be given, at the option of the person giving it, in person, by telephone, or in writing. For the purpose of this provision, "cardholder" means any person, not necessarily natural, to whom a credit card is issued, for any purpose, including business, commercial, or agricultural use, "or a person who has agreed with the card issuer to pay obligations arising from the issuance of such a credit card to another person". "Unauthorized use" is defined as "the use of a credit card by a person, other than the cardholder, who does not have actual, implied, or apparent authority for such use, and from which the cardholder receives no benefit".

Three conditions are stated to apply in order to fasten any liability on a cardholder for the unauthorized use of the credit card. First, the card must be an accepted credit card, that is, either a "credit card that the cardholder has requested or applied for and received, or has signed, used, or authorized another person to use or obtain credit", or a credit card "issued as a renewal or substitute in accordance with this paragraph". Second, "the card issuer has provided adequate notice of the cardholder’s maximum potential

---

58. Official Staff Commentary on Reg. Z, supra, footnote 56, to 226.12(b)(1), point #2.
59. Compare with the requirements of Reg. E, discussed below, under which the limit applies to a series of related unauthorized transfers.
60. Except that settling a balance on a periodic statement containing unauthorized transfers can be viewed as the adoption of the unauthorized transfers, for which the customer becomes liable under agency law, specifically when payment is made with knowledge of such unauthorized transfers.
62. Reg. Z §226.2(a)(8). See also §226.12(a) as well as (b)(5). The latter allows an issuer to contract out of the limited liability rule only where at least 10 cards are issued for the use of employees of an organization, provided liability of the employees remains governed by the provision.
63. Reg. Z §226.12(b)(1), note 22, effectively reproducing §103(o) of the CCPA, supra, footnote 45.
66. "Adequate notice" is defined as "a printed notice to a cardholder that sets forth clearly the pertinent facts so that the cardholder may reasonably be expected to have noticed it and understood its meaning. The notice may be given by any means reasonably assuring receipt by the cardholder." Reg. Z §226.12(b)(2)(ii), note 23.
liability and of means by which the card issuer may be notified of loss or theft of the card". Third, the card issuer must have provided "a means to identify the cardholder on the account or the authorized user of the card". Where any of these conditions is not satisfied, the cardholder is not responsible for any unauthorized use of the card.

"Credit card" is defined as "any card, plate, coupon book, or other single credit device that may be used from time to time to obtain credit". This definition focuses on the credit facility provided by the card, and does not address the means of authenticating the payment by it. Nevertheless, the need for authorized users' identification under the third condition for liability for unauthorized use, set out above, was interpreted to cover manual signature, photograph or fingerprint on the card, as well as magnetic stripe used in conjunction with a code. There is some ambiguity as to whether the cardholder may be held liable for payment made upon mere card presentation, but it is understood that phone orders, and presumably Internet as well as mail orders, in which the card is not physically used, are not covered. With respect to such orders, there is thus no cardholder's liability whatsoever for unauthorized use.

At the same time, nothing is stated as to the proof of the unauthorized use. This, however, is not an issue where the card transaction is authenticated by an added manual signature, which is anyway quite normal for a credit card transaction. But there is no guidance for either PIN authentication or disputed phone or Internet orders.

67. Reg. Z §226.2(a)(15), which goes on to define "charge card" to mean "a credit card on an account for which no periodic rate is used to compute a finance charge".
68. Official Staff Commentary on Reg. Z, supra, footnote 56, to §226.12, at paragraph 12(b)(2)(iii), points #1 and 2.
69. Ibid., point #3. The ambiguity stems from the statement under which "[t]he cardholder may not be held liable ... when the card itself (or some other sufficient means of identification of the cardholder) is not presented". I would take this to mean that authentication by mere card presentation is adequate. However, in the absence of this statement, I would have supposed, particularly in light of the text at the immediately previous footnote, that mere card presentation, unaccompanied by either manual signature or PIN (or any other electronic) authentication, will not suffice to identify the actual authorized user. Mail (as well as Internet) orders are not specifically mentioned, but must be taken to be excluded, by parity of reasoning with the exclusion of phone orders, since in all such cases the card itself (as opposed to the information it contains) is not used.
70. At the same time, to impose liability, "the card issuer must conduct a reasonable investigation", in which "the card issuer may reasonably request the cardholder's cooperation". Official Staff Commentary on Reg. Z, supra, footnote 56, to §226.12, paragraph 12(b), point #3.
The approach for regulating unauthorized consumer electronic fund transfers under Reg. E is entirely different from that of UCC Article 4A for unauthorized business funds transfers. As well, the approach taken is not identical to that under Reg. Z for the unauthorized use of a credit card. The point of departure for both Regulations is quite similar; yet the scheme of Reg. E appears to be an improvement on that of Reg. Z. No effort has been made, however, to harmonize between the two Regulations; particularly in connection with electronic authentication, the distinction does not appear to be justified.

The underlying principle of Reg. E is that a consumer is liable for authorized transfers, as well as, upon the failure to promptly advise the bank, for a limited amount of unauthorized transfers, up to the time of notification to the bank. Where such a notification is not given by a designated deadline, the customer is liable for the entire amount after the expiry of the notification period. The consumer's negligence contributing to an unauthorized transaction, other than in failing to give a timely notification, is not a factor in determining the consumer's exposure.

Reg. E §205.2(m) defines "[u]nauthorized electronic fund transfer" to mean:

an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit. The term does not include an electronic fund transfer initiated:

(1) by a person who was furnished the access device to the consumer's account by the consumer, unless the consumer has notified the financial institution that transfers by that person are no longer authorized;

---

71. Touched upon in Part III.2, above. So far as terminology is concerned, no distinction is to be made between a "funds transfer" per UCC Article 4A and "fund transfer" per EFTA, supra, footnote 47, and Reg. E, supra, footnote 48.

72. This includes an erroneous or fraudulent transfer initiated by an employee of the financial institution as well as by the consumer himself or herself where "the consumer has been induced by force to initiate the transfer". See Official Staff Commentary on Reg. E, footnote 55 above, to §205.2(m), points #1 and 4.

73. Defined in Reg. E §205.2(a)(1) to mean "a card, code, or other means of access to a consumer's account, or any combination thereof, that may be used by the consumer to initiate electronic fund transfer".

74. In furnishing the access device, the consumer must have acted voluntarily. Accordingly, where control of the access device is surrendered by the consumer as a result of robbery or fraud, the fund transfer initiated by the robber or the defrauding person is "unauthorized". In contrast, the exception applies so that the transfer is not "unauthorized" where "a consumer furnishes an access device and grants authority to make transfers to a person (such as a family member or co-worker) who exceeds the authority given". See Official Staff Commentary on Reg. E, supra, footnote 55, to §205.2(m). Prior to this interpretation by the Federal Reserve Board, there was some judicial
(2) with fraudulent intent by the consumer or any person acting in concert with the consumer; or
(3) by the financial institution or its employee.

Transfers thus excluded are evidently deemed authorized to which the consumer is fully responsible.

In connection with debit card electronic authentication, it was held that “[i]n an action involving a consumer’s liability for an electronic fund transfer . . . the burden of going forward to show an ‘unauthorized’ transfer . . . is on the consumer”. However, “[t]o establish full liability on the part of the consumer, the bank must prove that the transfer was authorized”. One can attempt to reconcile these two statements as follows: to succeed in its action, the bank must initially make a *prima facie* case that the transfer was authorized. To that end, it is adequate for the bank to prove that the transfer was initiated by means of the access device it had issued to the consumer. At that point, the burden of proof shifts to the consumer alleging an unauthorized transfer. Proof of loss or theft of the access device, put forward by the consumer, is adequate to meet this burden. Obviously, notice of loss or theft given by the consumer to the bank is no more than *prima facie* evidence of loss or theft.

Ultimately, however, where loss or theft of the access device is not claimed, in determining the question of authorized or unauthorized transfer, the court may be forced to choose between the consumer’s testimony and the bank’s computer printout, often backed by some evidence as to the reliability of its security procedure. A review of case law reveals that a credible witness, usually where his or her testimony is corroborated, typically by some system malfunction, has consistently overcome the machine. Nevertheless, witness credibility may differ from one case to another. Furthermore, relevant case law is from the first half of the

---

75. *Ogibene*, ibid., at p. 847.
eighties; it is quite possible that with time, confidence in the reliability of computer systems increases, so that greater weight may be given to evidence generated by them.

In the final analysis, as indicated, an unauthorized transfer may be caused by computer fraud or even an internal fraud at the financial institution. Both causes do not necessarily manifest machine malfunction and are outside the ability of the consumer to prove. To that end, existing case law, as described above, is inadequate.

The extent of consumer liability for "an unauthorized electronic fund transfer or a series of related unauthorized transfers" is governed by Reg. E §205.6. Thereunder, and subject to specified ceilings, liability is limited to unauthorized transfers occurring before the consumer advises the bank either of the loss or theft of the access device or of an unauthorized transfer that appears on a periodic statement. Where the consumer is not aware of the loss or theft of the access device, for unauthorized transactions occurring up to 60 days after the transmittal of a periodic statement containing an unauthorized transfer, the consumer is not liable. However, for such transfers, the consumer is liable up to a $50 ceiling where he or she learns of the loss or theft of the access device and advises the bank of it within two business days. The $50 ceiling does not apply where the consumer learns before the expiration of that 60-day period of the loss or theft of the access device but fails to advise the bank of the loss or theft within two business days. In such a case, the $50 ceiling applies only until the close of two business days.

77. See discussion on occurrences that may lead to unauthorized transfers in Part III.1, text, supra, around footnote 28.

78. To be entitled to the amounts specified in the provision, the bank must have provided the consumer with certain disclosures as to the extent of the liability, the telephone number and address for providing notices to the bank, and the bank's business days. As well, "[i]f the unauthorized transfer involved an access device, it must be an accepted access device and the financial institution must have provided a means to identify the consumer to whom it was issued". See Reg. E § 205.6(a). An "accepted access device" is generally defined (in § 205.2(a)(2)) as an access device requested and received or used by the consumer. In order to be entitled to any amount of unauthorized transfers, the bank must establish the existence of these conditions. See Ogibene, supra, footnote 74, at p. 847.

79. For an account to or from which electronic fund transfers can be made, a financial institution is required, under Reg. E§205.9(b), to send a periodic statement for each monthly cycle in which an electronic fund transfer has occurred. Such requirement is not dispensed with for passbook accounts updated upon presentation, except where the accounts may be accessed "only by preauthorized transfers to the account". See Reg. E§205.9(c)(1)(i).
after learning of the loss or theft, and the overall liability for the period ending at the close of the 60-day period will not exceed $500. Liability beyond the 60-day period is unlimited, until notice is given to the bank. To be entitled to the $500 as well as the unlimited ceilings, the bank must establish that the consumer’s timely notification would have prevented the loss.

Under Reg. E §205.6(4), time periods for notification may be extended “to a reasonable period” where the consumer delayed notifying the bank “due to extenuating circumstances”. However, in *Kruser v. Bank of America NT&SA*,[80] this provision did not assist a consumer who admitted that “she received . . . bank statements during her recuperation”.[81] In one such a statement, she failed to notice and advise the bank of a $20 unauthorized ATM withdrawal. Almost a year later, the consumer received statements containing close to $10,000 unauthorized ATM withdrawals. The consumer then promptly advised the bank of all unauthorized withdrawals, including the one that was almost a year old. In the court’s view, the consumer failed to show the required “extenuating circumstances”. Having delayed the notice for the first $20 unauthorized transaction, the consumer was thus held liable for the entire amount of the unauthorized transfers.

2. Consumer Legislation in the United Kingdom

In the United Kingdom, in relation to credit accounts, a cardholder’s liability for unauthorized use is governed by s. 84 of the Consumer Credit Act.[82] Its scheme is fundamentally the same as in the United States.[83] At the same time, there is no legislation in the United Kingdom in relation to unauthorized funds transfers from asset accounts and the issue is regulated there by a voluntary code of conduct discussed further below in Part IV.5.

[83] At first blush, one difference is that in the United States the limited liability applies even if not specified in the contract. Yet, this is a theoretical difference of no practical significance. First, United States card issuers will be anyway inclined to include a term regarding the liability. Second, in any event, to enforce the liability, issuers in the U.S. are required to meet three conditions, one of which is disclosure of the cardholder’s maximum potential liability and of means by which the card issuer may be notified of loss or theft of the card.
Section 84 deals with the misuse of credit tokens, which are defined in art. 14(1) as:

- a card, voucher, coupon, stamp, form, booklet, or other document or thing given to an individual by a person carrying out a consumer credit business, who undertakes
  - (a) that on the production of it (whether or not some other action is also required), he will supply cash, goods and services (or any of them) on credit, or
  - (b) that where, on production of it to a third party (whether or not any other action is also required), the third party supplies cash, goods and services (or any of them), he will pay the third party for them (whether or not deducting any discount or commission), in return for payment to him by the individual.

As in the United States, this covers a card associated with a credit facility, authenticated by the production of the card, either alone, or supported by manual signature or some form of electronic authentication, but not mail, phone or Internet orders authorized without the physical production of the card. Arguably, the language of s. 14(1)(b) is broad enough to cover also the debit card used in connection with transfers from an asset account. However, s. 84 is stated to be an exception to the broad principle provided for in s. 83, under which a debtor under a regulated consumer credit agreement shall not be liable to the creditor "for any loss arising from the use of the credit facility by another person ....". As a result, s. 84 applies only to "loss arising from use of the credit facility" which excludes a transfer from an asset account.

Notwithstanding the no-liability rule under s. 83 for credit facilities, s. 84(1) validates a term in a credit-token agreement, relating to a credit facility, under which the debtor is to become "liable to the extent of £50" (or the credit limit if lower) for loss to the creditor arising from use of the credit token by other persons during a period beginning when the credit token ceases to be in the possession of any authorized person and ending when the credit token is once more in the possession of an authorized person". Nonetheless,

85. Under s. 8, a regulated consumer agreement is an agreement between an individual (the debtor) and any other person (the creditor) by which the creditor provides the debtor with credit not exceeding £15,000 (that is, around $37,700 CAD), unless it is exempted under s. 16.
86. Hapgood, supra, footnote 84, at p. 318 and note 12.
87. Around $125 CAD.
under s. 84(2), by agreement, the debtor may be made liable "to any extent for loss to the creditor from use of the credit token by a person who acquired possession with the debtor’s consent". Both terms are effective only for the use of the credit token until the creditor is advised of the dispossession or misuse, and where the credit-token agreement contains adequate disclosure as to the destination of the notice of dispossession or misuse.  

It is noteworthy that the U.K. Consumer Credit Act contains a provision dealing with the onus of proof in an action by the creditor to enforce liability under a credit-token agreement. Accordingly, under s. 171(4)(a), "it is for the creditor to prove that the credit-token was lawfully supplied to the debtor, and was accepted by him". As well, under s. 171(4)(b), in such an action, if the debtor defends the action denying an authorized use, it is incumbent on the creditor to prove either (i) "that the use was authorized" or (ii) "that the use occurred before the creditor had been given notice" of the loss or theft of the credit token. If successful, in the former case, the creditor will be entitled to recover the entire disputed amount. In the latter case, the creditor will be able to recover up to the £50 (or lower credit limit) ceiling. Unfortunately, no guidance is provided as to what facts have to be proved for succeeding in satisfying s. 171(4)(b)(i).

3. Federal Regulations and Provincial Legislation in Canada

In Canadian federal law, liability of cardholders for the unauthorized use of their credit cards are dealt with in separate sets of regulations, each applicable to one type of institutions falling under federal jurisdiction. For example, in connection with credit cards issued by chartered banks, the scope of liability is set out in s. 12(1)(c), (d), and (e) of the federal Cost of Borrowing (Banks) Regulations.  

For transactions authenticated other than by PIN at an ATM, the scheme adopts a pre-advice $50 limit, in connection with lost or stolen cards; that is, Internet, phone and mail orders are not covered.

The scheme under the regulations can be outlined as follows. Other than for a transaction entered into an automated teller machine by using the borrower's PIN, if a lost or stolen credit card is

88. Section 84(3) and (4).
used in an unauthorized manner, the maximum liability of the borrower is the lesser of $50 and the maximum set by the credit agreement. For a credit card transaction entered into an ATM by PIN, the ceiling is as set by the credit agreement. In either case, liability is only for unauthorized transactions occurring before an oral or written report of a lost or stolen credit card received by the bank from the borrower.

A few points are noteworthy. First, the exclusion of the $50 limit applies to card and PIN authentication in ATMs, but not POS terminals. However, credit card PIN authorization in a POS terminal may be quite unusual in Canada. Second, these particular regulations bind only chartered banks, regulated under the Bank Act, and not any other type of a credit card issuer, including all other deposit-taking institutions and CPA members. This seems to raise issues as to consistency as well as harmonization. Third, in the absence of specific provisions in a statute, disclosure regulations cannot be seen as the ideal manner to deal with the matter.

There is also some provincial legislation in Canada on this point. For example, under s. 123 of the Quebec Consumer Protection Act, upon the loss or theft of a credit card, “the consumer incurs no liability for a debt resulting from the use of such card by a third person”, which arises “after the issuer is notified of the loss or theft by telephone, telegraph, written notice or any other means”. At the same time, as long as such notice has not been given, under s. 124, “the liability of the consumer . . . is limited to the sum of $50”. There is jurisprudence in Quebec defining “loss or theft” in these provisions by reference to criminal law and particularly distinguishing unauthorized use following “theft” from the mere “abusive use” by one in lawful possession.

Federal jurisdiction over credit cards issued by banks is in relation to “banking”. Provincial jurisdiction over credit cards in general is a matter of power in relation to “property and civil rights”. In case of inconsistency, it is federal law which is paramount. While all such provisions are not fundamentally different,

92. Constitution Act, 1867, s. 91(15).
93. Constitution Act, 1867, s. 92(13).
94. For “federal paramountcy”, under which “where there are inconsistent (or conflicting) federal and provincial laws” it is the federal law which prevails see P.W. Hogg, Constitutional Law in Canada, student ed. (Toronto, Carswell, 2001), p. 402
the fragmented approach to the treatment of the subject is not commendable. At least provincial uniformity and federal-provincial harmonization are called for. However, neither a survey of all existing legislation and regulation in Canada, nor a search for a strategy to achieve uniformity and harmonization falls into the scope of this article.

4. Consumer Legislation in Denmark

In Denmark, liability for losses caused by the unauthorized use of a "payment instrument" is governed by s. 11 of the Act on Certain Payment Instruments.\textsuperscript{95} “Payment instruments” are broadly defined in s. 1 to cover cash cards, codes and biometric values, and “claims registered electronically . . .”, to the extent that they are offered or available for use in Denmark and “can be used to acquire goods or services, arrange for the transfer of funds, withdraw cash or make other payment transactions”. The involvement of a manual signature in the authentication of a payment transaction is not stated to exclude the “payment instrument” from the coverage of the statute. At the same time, the Minister for Trade and Industry is authorized to “lay down provisions according to which a payment instrument is fully or partially exempted from the provisions of [the] Act” as well as to “lay down more specific rules to the effect that certain types of payment instruments shall be fully or partially exempt from the provisions of [the] Act”.\textsuperscript{96}

With respect to consumer payment instruments,\textsuperscript{97} the salient features of s. 11 can be summarized as follows:

1. The holder\textsuperscript{98} is not liable for unauthorized use:
   (a) that takes place “after the issuer\textsuperscript{99} has been informed that the payment instrument has been lost, that an unauthorized person has obtained knowledge of the code, or

\textsuperscript{95} Act No. 414 of May 31, 2000 (hereafter Act on Certain Payment Instruments), which includes provisions implementing Article 8 of Directive 97/7, note 101 below, on the protection of consumers in respect of distant contracts.
\textsuperscript{96} Section 1(6) and (8).
\textsuperscript{97} The Act covers also payment instruments which are offered for the purpose of both business and non-business but the liability provisions do not apply “if the issuer is able to prove that . . . the holder has undertaken to use the payment instrument solely for business purposes”. See s. 1(5).
\textsuperscript{98} Defined in s. 3(1) to mean “anyone who makes an agreement with an issuer for the use of a payment instrument or anyone who is the lawful holder of a prepaid payment instrument in relation to the issuer”.
\textsuperscript{99} Defined in s. 3(2) to mean “the entity with which the holder makes an agreement on the issue or use of a payment instrument”.

that for other reasons the holder requests a stop on the payment instrument”. The issuer is required to facilitate receipt of such information from the holder as well as to confirm it;

(b) where the payee\textsuperscript{100} knew or should have known that the payment instrument had been subject to unauthorized use; or

(c) where a payment card has been used fraudulently in connection with “a distance contract.” \textsuperscript{101}

Lack of liability for any unauthorized use occurring prior to the acceptance of the payment instrument and the code by the holder is not specifically mentioned.

2. In circumstances other than specified in no. 1 above, the holder is liable for all losses “without any limitation of the amount”, where:

(a) the personal secret code associated with the payment instrument has been used, and

(b) the issuer is able to prove that:

(i) the holder has disclosed the code to the person who has made unauthorized use of the instrument, and

(ii) the instrument has been used in circumstances in which the holder realized or should have realized the existence of a risk of abuse.

Presumably, the onus of proof regarding the use of the personal secret code is on the issuer. Regardless, strictly speaking, unlimited liability does not require the voluntary surrender of the payment instrument by the holder to the unauthorized user. Nor does it apply in circumstances of

\textsuperscript{100} Defined in s. 3(4) to mean “any entity at which the holder may use the payment instrument to acquire goods or services, arrange for the transfer of funds, or make other payment transactions”.

\textsuperscript{101} As per art. 2(1) of EC Council Directive 97/7 of June 4, 1997 on consumer protection in respective of distance contracts, [1997] O.J. L. 144/19 (hereafter Directive 97/7), “distance contract” means any contract concerning goods or services concluded between a supplier and a consumer under an organized distance sales or service-provision scheme run by the supplier, who, for the purpose of the contract, makes exclusive use of one or more means of distance communication up to and including the moment at which the contract is concluded. Article 2(4) states that “means of distance communication” are any means which, without the simultaneous physical presence of the supplier and the consumer, may be used for the conclusion of a contract between those parties.
such a voluntary surrender unaccompanied by the disclosure of the secret code, as, for example, delivery for safekeeping. Rather, it is the disclosure of the code, followed by the unauthorized use, whether anticipated or that should have been anticipated, that triggers the unlimited liability. However, practically speaking, where the code has been disclosed, it is the possession of the payment instrument by the person to whom the code has been disclosed which is likely to give rise to the realization by the holder of the risk of abuse. In any event, it should be pointed out that not every case of code disclosure accompanied by the delivery of possession of the payment instrument to somebody ought necessarily to give rise to the holder’s realization of the existence of the risk of abuse. Stated otherwise, by itself, voluntary surrender is not to be treated as conferring apparent authority. For example, no realization of risk of abuse, and hence no apparent authority and ensuing unlimited liability, may occur in connection with the delivery of the instrument or code to a trusted family member who nevertheless misused the trust. Finally, unlimited liability is not stated to be subject to restrictions set by available withdrawal or transaction limits.

3. Other than in circumstances enumerated in no. 2, unless circumstances enumerated in no. 1 apply, the holder is liable for losses caused by unauthorized use of the payment instrument by another person only up to a specified ceiling.

4. The ceiling for the holder’s liability under no. 3 above is DKK 8,000\(^{102}\) where:
   (a) the issuer is able to prove that the personal secret code associated with the payment instrument has been used and
   (i) the holder has failed to advise the issuer promptly that the code has become known to an unauthorized person;
   (ii) the holder has disclosed the code to the person who has made unauthorized use of the instrument, without the matter being covered by no. 2 above.

---

102. Around CAD $1765. Amount is subject to change by the Minister for Trade and Industry, as may be required “by the development of prices”.
Particularly, this will be the case where it cannot be said that the instrument has been used in circumstances in which the holder realized or should have realized the existence of a risk of abuse; or (iii) the holder, by grossly irresponsible conduct, has made unauthorized use possible; or

(b) the payment instrument has been read physically or electronically, and in association with this, the unauthorized person has used a forged signature, provided the issuer is able to prove that:

(i) the issuer was not promptly advised of the loss of the instrument; or

(ii) the holder (or another person to whom the holder has entrusted the payment instrument) has made unauthorized use possible “by grossly irresponsible conduct”.

“Grossly irresponsible conduct”, for which the ceiling is DKK 8,000 under no. 4(a)(iii) and (b)(ii), is undefined. Yet it is obvious that slight negligence will not suffice. Quaere whether as to 4(b)(ii), voluntary surrender to a trusted family member or friend that should not have been trusted is tantamount to “gross negligence”.

5. The default ceiling under no. 3 “for losses caused by unauthorized use of the payment instrument by another person in case of the personal, secret code associated with the payment instrument has been used” is DKK 1,200. This ceiling applies in circumstances not exempted under no. 1, and falling neither under no. 2 (unlimited liability) nor no. 4 (the DKK 8,000 ceiling). Such will be the case where the personal secret code associated with the payment instrument was used, but the holder had neither disclosed the secret code to an unauthorized user nor by grossly irresponsible

103. Holder’s liability is limited to DKK 8,000 also where he or she is liable under both (a) and (b).

104. The question does not arise in connection with 4(a)(iii), since the case falls anyway under 4(a)(ii), namely surrender by a holder that should have realized the existence of a risk of abuse.

105. Around CAD $265. The amount is subject to change by the Minister for Trade and Industry, as may be required “by the development of prices”.

2003]
conduct made unauthorized use possible, and where applicable, advised the issuer promptly that the code had become known to an unauthorized person.

So far as the holder is concerned, the scheme can thus be summarized as (1) no liability (i) after notification, (ii) where the payee knew or should have known unauthorized use, or (iii) in an unauthorized use in connection with "a distance contract"; (2) full liability in case of voluntary surrender, compliance with the security procedure, and realization of the existence of a risk of abuse (as proven by the issuer); (3) limited, though quite extensive, liability when either (a) the issuer proves compliance with security procedure, together with one of the following three: failure to advise, voluntary surrender without realization of risk of abuse, or holder's gross negligence, or (b) instructions were authenticated by both card reading and manual signature, and the issuer proves either lack of prompt notification or gross negligence; and (4) limited and substantially lower liability (up to notice or unless payee's fault is present) where the issuer is able to prove mere compliance with security procedure.

The Danish statute is remarkable for several reasons:

1. It is quite comprehensive in its application to electronic authentication, card authentication accompanied by manual signature, and distant contracts. In effect, the Act applies to payment carried out from public-access (ATM as well as POS), home, and at-the-bank terminals. Section 11 thus applies to both credit and debit cards, as well as use of codes other than with a card.

2. Liability is fastened on the consumer when the issuer merely proves compliance with security procedure, but only in the absence of prompt notification or payee's fault. Exposure is anyway quite limited (around CAD $265). There is no indication as to the required level of proof in connection with an allegation of a "phantom" transfer, namely, when the consumer alleges either computer crime by an intruder or fraud within the bank. Arguably, however, the low amount at stake may make it inefficient to litigate such questions.

3. To benefit from a substantially higher ceiling (around CAD $1,765), the issuer must meet a quite onerous onus of proof.
In addition to proper authentication, the issuer must prove known breach of security or gross negligence. This ceiling also applies for card authentication and forged signature where issuer was not notified of loss or theft and holder was grossly negligent. To claim all losses the issuer must prove proper authentication and the voluntary surrender of the code accompanied with realization as to the existence of a risk of abuse.

4. On the other hand, while the consumer is not responsible for fraudulent use of the card information in a distance contract, there is guidance as to neither the onus of proof regarding the existence of a genuine transaction nor as to the allocation of losses in case of a dispute between the consumer and the merchant as to the amount of payment in a genuine transaction.

5. The Act provides for holder's limited liability for a transfer authenticated by card and a forged signature, but only where the holder was grossly negligent.

5. **Voluntary Codes — the United Kingdom and Australia**

The discussion on voluntary codes is divided between selected overseas codes, in the United Kingdom and Australia, and the one adopted in Canada.\(^{106}\) This presentation is simply designed to highlight the features of the Canadian Code and is not an indication that it is inherently different from other codes. Among the codes discussed in this article, so far as coverage is concerned, the U.K. Code is the most comprehensive, as its scope extends also to matters such as lending, foreign exchange services, and financial difficulties. At the same time, with respect to electronic funds transfers, it is the Australian Code which is the most comprehensive in both transaction coverage and treatment of issues. This is not surprising; being the most recent and focusing on the entire range of consumer electronic payments, this code purports to respond to inadequacies that have surfaced under previous codes.

\(^{106}\) The current U.K. Banking Code, that of January 2001, can be found in <www.bba.uk>. The current Australian Electronic Funds Transfer Code of April 1, 2001 can be found in <www.asic.gov.au>. It was subsequently amended on March 18, 2002, though for matters that do not pertain to the present article. It became effective on April 1, 2002. The current Canadian Code of Practice for Consumer Debit Card Services, Revised 2002, can be found at <http://strategis.ic.gc.ca/ssg/ca01581e.html#Terms>.
In the glossary of the U.K. Banking Code, "card" is defined to cover "any plastic card which may be used to pay for goods and services or to withdraw cash" other than an electronic purse. That is, a card must be an access and not a stored-value product. As well, electronic access by PIN alone\textsuperscript{107} or any other security procedure not involving cards is not covered. The card definition is however broad enough to cover both credit and debit card transactions, in which authentication involves a manual signature, an electronic code, or the communication of card information. In addition to the Banking Code, as discussed in Part IV.2 above, payment cards are governed by the Consumer Credit Act.

Part A of the Australian Electronic Funds Transfer Code of Conduct applies to "funds transfers initiated by giving an instruction, through electronic equipment and using an access method, to an account institution . . . to debit or credit an . . . account\textsuperscript{108} maintained by the account institution".\textsuperscript{109} "Electronic equipment" is defined to include "electronic terminal, computer, television and telephone".\textsuperscript{110} An "access method" is stated to consist "of one or more components including (but not limited to) devices, identifiers,\textsuperscript{111} codes or a combination of these". It does not include manual signature comparison serving as "the principal intended means of authenticating user's authority . . . ." Quaere as to authentication by card and manual signature. In such a case, at the point of service, authentication is by card only. Nevertheless, in the case of dispute, it is ultimately the signature which will determine the cardholder's liability. In any event, "[t]he access method or some of its components need not have been issued by the financial institution, e.g. a PKI private key on a smart card issued by a third party".\textsuperscript{113} Part B of

\textsuperscript{107} Cf. \textsuperscript{110}, providing for the issue of a PIN separately from a card, though arguably to be subsequently used with the card. That is, the separate issue of PIN and card mandated by the provision is for security reasons.

\textsuperscript{108} Business as well as biller accounts are specifically excluded in clauses 1.3 and 1.4. "Biller account" is an account maintained by a supplier of services (and not a financial institution) as for example an electricity company's and department store's customer account. See Clause 1.5.

\textsuperscript{109} Clause 1.5.

\textsuperscript{110} Clause 1.5.

\textsuperscript{111} "Identifier" is defined in Clause 1.5 to be non-confidential information known to the user that must be provided to or through a device or electronic equipment to access the account. "An identifier may be, for example, an account number, card number, card expiry date". See supra, footnote 9.

\textsuperscript{112} Clause 1.5.

\textsuperscript{113} Clause 1.5, footnote 4.
the Australian Code covers consumer stored value facilities and stored value transactions.

Voluntary codes of practice in Australia and the United Kingdom (as well as in Canada) are unanimous in fastening the entire amount of unauthorized use losses on a negligent consumer debit card holder. These codes provide so, regardless of the fault of the financial institution, except for the fact that arguably, in some circumstances, the adequacy of its security procedure may be an important element for the bank's case that the payment order was indeed initiated pursuant to that procedure. However, the codes exempt the customer from any substantial responsibility in the absence of fault on his or her part.

Thus, under ¶14.8 of the January 2001 U.K. Banking Code, irrespective of fault, customers' liability for transactions not authorized by them, and carried out before the card issuer has been notified of the loss or theft of the card, will be limited to a maximum of £50.114 Evidently, this no-fault limited exposure is designed to encourage customers to be diligent in safekeeping the card and access code. No liability is stated to exist when "someone else uses [the] card without [the customer's] permission, and the card has not been lost or stolen". In any event, the £50 ceiling does not apply where the financial institution "can show" that the customer acted fraudulently or without reasonable care,115 in which case the consumer will be liable for all losses. Taking care of a card and code may consist of the following safeguards, set out in ¶14.1:

(a) not to keep the cheque book together with cards, (b) not to permit anyone else to use card and code, (c) to learn the code and destroy the notification promptly upon receipt,116 (d) never to write down

---

114. Around CAD $125. This £50 no-fault liability is consistent with s. 84 of the Consumer Credit Act, supra, footnote 82, dealing with the misuse of credit tokens, and discussed in Part IV.2, text, supra, around footnote 82.

115. "Without reasonable care" replaces "with gross negligence" of the previous ¶4.16 of the 1998 Revised Edition, so as in theory to expand the consumer's sphere of responsibility, and apply the unlimited liability to the case of an ordinary negligence (that is, the failure to exercise reasonable care) and not only gross negligence. Yet, the implication of this change in language need not be overstated. As indicated below, acts or omissions constituting the fulfillment of the duty to take care of the card and the code under the 2001 text are not fundamentally different than (though indeed somewhat broader than) examples for avoiding "gross negligence" listed in the 1998 Revised Edition.

116. This corresponds to two separate requirements in the previous ¶4.16 of the 1998 Revised Edition: (c) to take reasonable steps to keep the card safe and the code secret, and (f) to destroy any code advise promptly on receipt.
the code,\textsuperscript{117} and (e) to take reasonable steps to keep the card safe and the code secret.

It is noteworthy that §§14.1 and 14.5 in the United Kingdom are quite broad in requiring the customer to take care of cheques, passbooks, cards, electronic purse, PINS, and other security information, and advise the financial institution of any loss or security breach. Upon such advice the financial institution "will take immediate steps to try and prevent" misuse. Nevertheless, as discussed,\textsuperscript{118} §§14.8, the liability provision, applies only to card transactions. "Card" is defined in the glossary to cover "any plastic card which may be used to pay for goods and services or to withdraw cash" other than an electronic purse. That is, a card must be an access and not stored-value product. As well, electronic access by PIN alone or any other security procedure not involving cards, is not covered. The card definition is however broad enough to cover both credit and debit card transactions, in which authentication involves a manual signature, an electronic code, or the communication of card information. In any event, notwithstanding the Banking Code, loss arising from the misuse of a card which is a credit-token used in connection with a "credit facility" is limited, under s. 84 of the Consumer Credit Act, to loss incurred prior to notice of loss or theft, up to a ceiling of £50, irrespective of customer's fault, and not subject to fault-based increased liability. Moreover, where the Consumer Credit Act applies, the customer will further benefit from its s. 171(4)(b), under which it is for the financial institution to prove either that use was authorized (in which case the customer is responsible for all transactions) or that loss occurred prior to notice (in which case the customer is responsible to up to £50).\textsuperscript{119}

Arguably, however, it is up to the financial institution to prove authorized use even in the absence of s. 171(4)(b) of the Consumer Credit Act. It appears that once PIN authentication is proved by the financial institution, "the Banking Ombudsman's practice has been to place the burden of proving that the machine was not at fault on the [financial institution], and if the [financial institution] can prove

\textsuperscript{117} This is (unreasonably) broader than the corresponding duty under the previous §4.16 of the 1998 Revised Edition, under which the requirements were not to write down or record the code on the card "or on anything kept with or near it" as well as not to write the code down "without disguising it".

\textsuperscript{118} See supra, text and footnote 107.

\textsuperscript{119} For the Banking Code and the misuse of credit tokens under the Consumer Credit Act, supra, footnote 82, see discussion by R. Hooley in Hapgood, supra, footnote 84, at pp. 315-19, and further in text around footnote 114.
that there was no technical breakdown, then shift the burden to the customer to prove that he definitely did not use his card and PIN and that a third party as not gained access to the card or the PIN”. It was however observed in this context, that “[i]n the overwhelming majority of cases the customer is unable to discharge this heavy burden”.\textsuperscript{120} At present, PIN authentication is practiced in the U.K. in connection with ATM and not POS terminals. It is however anticipated that POS PIN authentication will shortly be introduced.

It is noteworthy that the £50 limit applies in the U.K. even when it is evidently clear that the customer has not contributed to the loss. By way of comparison, s. 5.6 of the former Australian Electronic Funds Transfer (EFT) Code of Conduct of 1989 provided for situations in which “[w]here the cardholder has contributed to losses resulting from unauthorized transactions by voluntarily disclosing the [code], indicating the [code] on the card, or keeping a record of the [code] (without making any reasonable attempt to disguise the [code]) with any article carried with the card or liable to loss or theft simultaneously with the card”. In such cases, similarly to the United Kingdom, the customer’s liability was for the entire actual losses, up to the time of notification to the issuer. However, unlike under its U.K. counterpart, a $50 no-fault liability was imposed on the customer under s. 5.5 only where it was unclear whether the customer had contributed to losses resulting from unauthorized transactions. No such liability was fastened on a customer where it was evidently clear that he had not contributed to the loss.

Separate provisions, ¶14.9-12, apply to the electronic purse. The customer is instructed to treat the electronic purse “like cash in a wallet”, so that if it is lost or stolen, the customer “will lose any money in it, in just the same way as” the wallet is lost. However, the customer’s exposure is usually limited to amounts credited to and loaded on the electronic purse by unauthorized withdrawals. Unless the financial institution can show that the customer has acted “fraudulently or without care”, exposure is then limited to £50, out of unauthorized withdrawals occurring before the financial institution is advised. Exposure is stated to be unlimited where the customer acts fraudulently. Exposure may be unlimited when the customer acts “without reasonable care”, as for example where safeguards set out in ¶14.1 are not followed. In effect, the loading of the electronic purse is treated under this scheme like a cash

\textsuperscript{120} Hapgood, \textit{ibid.}, at pp. 316-17.
withdrawal with a card and PIN, while the electronic purse itself is treated like cash.

In connection with voluntary codes, difficulties arise in the interpretation of some of the specific requirements giving rise to unlimited customers' liability. In general, the U.K. Code is intentionally drafted in non-technical, or non-legalistic language. Presumably, this is designed to enhance the accessibility of the Code to consumers. Yet, this may be at the expense of legal clarity and certainty; for example, no consequences are spelled out for the breach of the duty to take care of cheques. Unfortunately, however, a more legalistic language does not universally guarantee certainty and clarity. For example, under the previous Australian provision, the circumstances under which a customer will "keep . . . a record of the [code] (without making any reasonable attempt to disguise [it]) with any article carried with the card or liable to a loss or theft simultaneously with the card", are not all that self-evident.

As well, difficulties may arise in gathering the evidence establishing the specific requirements, and it is not specifically stated who proves what and to what extent. Presumably, the onus was on the bank that purported to prove the customer's fault; yet, greater clarity would have been welcome. However, this is a matter of improving the language of a Code and not of the fundamental stylistic choice. In the final analysis, it seems to me that a clear and precise legal language need not be extremely technical and is preferable to the U.K. colloquial style. Stated otherwise, Code accessibility to consumers should not compromise legal certainty and clarity. Both objectives are to be accommodated, though priority has to be given to certainty and precision.

A revised text of the Australian Electronic Funds Transfer Code of Conduct came out on April 1, 2001. Its Part A applies to "funds transfers initiated by giving an instruction, through electronic equipment and using an access method, to an account institution

---

121. *Quaere* whether this duty is to be taken as fastening on consumers a duty of care in derogation from general law on the point per *London Joint Stock Bank Ltd. v. Macmillan*, [1918] A.C. 777 (H.L.) at p. 789 (customer's duty of care is limited to the manner in which a cheque is drawn), in which case it is further unclear whether the duty is adequately spelled out. This is apart from the broader question as to whether a voluntary banking code is the right framework for reducing consumer rights.


Consumer Liability in Unauthorized EFTs

... to debit or credit an ... account124 maintained by the account institution".125 Clause 5 of the Australian Code extensively deals with liability for unauthorized transactions. Its salient features can be summarized as follows:

1. "Unauthorized transaction" is defined as one "not authorized by the user".126 Transactions "carried out by the user or by anyone performing a transaction with the user's knowledge and consent" are specifically excluded, so as to be considered authorized. Presumably, a transaction carried out by an agent exceeding his or her authority or a custodian with lawful possession but only for safekeeping will then be an "unauthorized transaction". Specifically, a third-party's possession of a device, plus knowledge of the code, giving the third party full control of the access method, with the knowledge and consent of the user, will not suffice to make a transaction by the third party, made with the access method, into an authorized one. A third party's transaction shall be authorized only when the transaction itself, and not merely the full control of the access method, is with the user's knowledge and consent.

2. The account holder is not liable for
   (a) losses caused by the fraudulent or negligent conduct of employees or agents of the account institution, merchants, and other network participants;
   (b) losses relating to a component of access method that are forged, faulty, expired or cancelled;
   (c) losses arising from transactions that occurred before the user has received any device or code required for the transaction, as must be proven by the account institution;127

124. Business as well as biller accounts are specifically excluded in clauses 1.3 and 1.4. "Biller account" is an account maintained by a supplier of services (and not a financial institution) as for example an electricity company's or department store's customer account. See Clause 1.5.
125. Clause 1.5.
126. "User" is broadly defined in Clause 1.5 to be the person authorized by the account institution to use the access methods. It may or may not be the account holder and is not necessarily the actual user of the access device in a given case.
127. The presumption is that the user did not receive the item, "unless the account holder can prove otherwise", as for example, by putting forward an acknowledgment of receipt obtained from the user. Notwithstanding any contract stipulation to the contrary, proof of mail delivery to the address of the user will not suffice.
(d) losses caused by the same transaction being incorrectly debited more than once to the same account;

(e) losses resulting from unauthorized transactions occurring after notification by the account holder to the account institution “that any device forming part of the access method has been misused, lost or stolen or that the security of codes forming part of the access method has been breached”; and

(f) losses resulting from unauthorized transactions “where it is clear that the user has not contributed to such losses”.

3. The account holder is liable when “the account institution can prove on the balance of probability” that user contributed to losses (i) through user’s fraud, (ii) breach of specified duties as to the confidentiality of the code,128 or (iii) unreasonable delay in notification after becoming aware of the misuse of the devise or breach of confidentiality as to the code. In each such a case, liability is limited by available withdrawal or transaction limits,129 provided they are reasonable,130 and to losses from accounts with respect to which an access method was agreed upon. In connection with losses contributed to by user’s fraud or breach of code confidentiality “all reasonable evidence must be considered, including all reasonable explanations for the transaction occurring”. Moreover, the fact that the account was accessed with the

128. When the access method includes more than one code and the account institution proves breach of the confidentiality requirements with respect to one or more but not all codes, it must further prove “on the balance of probability” that the user’s breach was “the dominant contributing cause of the losses”.

129. Stated limits are daily, periodic, and by reference to available balances. In this context, three points ought to be made. First, other than in connection with losses created by delaying notification, available account balance is stated to include prearranged credit. The rationale for omitting this component from loss created by a delayed notification is not all that clear. Second, an account institution that allows customers to exceed limits, and even to incur overdrafts above pre-agreed limits, is not protected for any unauthorized amount above the contract limits. Third, ceilings to the account holder’s liability apply also in connection with losses generated by user’s fraud and not only negligence.

130. Reasonableness may depend on the adequacy of protection accorded to the account holder through “the security and reliability of the means used by the account institution to verify” authorization as well as in connection with an unauthorized funds transfer involving the drawing on a line of credit accessible by the access method, adequate disclosure regarding “the risk of the access device being used to make unauthorized transactions on that line of credit”.
correct access method, "while significant", is not by itself "proof on the balance of probability that the user contributed to losses" through fraud or breach of code confidentiality.

4. Otherwise, liability is limited to the least of $150^{131} (or any lower figure as may be determined by the account institution), available balance limits, or actual loss upon notification to the account institution. Presumably, this will apply when the account institution fails to prove "on the balance of probability" that user contributed to losses through fraud or negligence (so as to be entitled to the recovery of a larger amount as in no. 3 above), but nevertheless, the user may have contributed to the loss, that is, "it is [not] clear that the user has not contributed to such losses", so as to altogether be exonerated from liability under no. 2(f) above.

5. The following specified acts or omissions by the user are listed as contravention of the code confidentiality:
   (a) a voluntary disclosure of one or more of the codes, "including [to] a family member or friend";
   (b) for an access method requiring both a device and a code, an indication of one or more of the codes on the outside of the device, as well as keeping a record of one or more of the codes, "without making any reasonable attempt to protect the security of the code records", "on one article, or several articles, carried with the device or liable to loss or theft simultaneously with the device";
   (c) for an access method requiring a code without a device, keeping a record of one or more of the codes, "without making any reasonable attempt to protect the security of the code records", "on one article, or several articles so that they are liable to loss or theft simultaneously with the device";
   (d) a selection, contrary to the account institution's specific instruction and warning, as proven by it, of "a numeric code which represents the user's birth date or an alphabetical code which is recognisable part of the user's name"; or

131. Around CAD $134.
(e) an action "with extreme carelessness in failing to pro-
tect the security of all the codes".

"Extreme carelessness" is defined as "a degree of care-
lessness with the security of the codes which greatly ex-
ceeds what would normally be considered careless
behaviour. For example, storing the user's username and
password for Internet banking in a diary or personal or-
ganiser or computer (not locked with a PIN) under the
heading 'Internet banking codes'."

6. The user's engagement in a conduct expressly authorized
or expressly or impliedly promoted or endorsed (quaere as
to whether this covers also "recommended or advised") by
the account institution will not constitute a contravention
of the above mentioned requirements. This may include
the promotion or endorsement of an account aggregator
service that entails the surrender by consumers of their
codes to the service provider. At the same time, the account
institution may provide for its users guidelines on ensuring
the security of an access method. Regardless, a reasonable
attempt to protect the security of a code record includes
the making of any reasonable attempt to disguise it and/or
the taking of reasonable attempt to protect the security of
the code record, which may involve "hiding or disguising
the code record among other records or in places where a
code record would not be expected to be found, by keeping
a record of the code in a securely locked container or
preventing unauthorized access to an electronically stored
record of the code".

7. Account institutions are required to provide an effective
and convenient means by which users can notify a lost or
stolen device, unauthorized use of a device, or breach of a
security of a code. "Where such facilities are not available
during particular periods, any losses occurring during these
periods that were due to non-notification are deemed to
be the liability of the account institution . . .", provided
adequate notification was given "within a reasonable time
after the facility again becoming available". Account insti-
tutions are required to implement procedures for acknowled-
ging receipt of notifications.
8. In connection with a credit card or charge card account, recovery from the account holder is to be reduced by an amount the account institution could charge back to the merchant, where such a charge-back right could have been exercised under the merchant agreement.

Consumer stored-value products are governed by Part B of the Australian Code. Under Clause 16, refund for lost or stolen stored-value is available only upon the fulfilment of two conditions. The first condition is that “a stored value operator, together with relevant system participants, has or can create a reliable record of the amount of stored value controlled by a stored value facility from time to time”. The second condition is that “the stored value operator and any relevant system participants can prevent any further transfers of stored value from the facility”. The stored value operator is required to provide the user with a means to advise promptly of loss or safe. Refund is to be made when advice is properly given. There is however no ceiling or exception for liability for unauthorized use prior to the giving of notice of loss or theft.

6. Voluntary Code in Canada

The Canadian Code of Practice for Consumer Debit Card Services of 1992 (revised February 1996) “applies only to services that use debit cards and personal identification numbers (PIN) to access point-of-service terminals, such as automated banking machines (ABM), point-of-sale (POS) terminals and debit card terminals in the home”. It “does not cover transactions that take place outside Canada, or that transfer funds into or out of Canada”. 132

Unfortunately, “debit card”, “debit card service” and “debit card transactions” are defined in s. 8 so as to refer to each other, without completely highlighting all the distinctive features of the debit card, that distinguish it from any other access device. True, “debit card” is defined in s. 8(5) to mean “a card with electronically readable data that is used, in conjunction with a PIN to confirm the identity of the cardholder and authorize debit card transactions”. In departure from the position in both the United Kingdom and the United States, the definition is in terms of the specific electronic authentication without any reference to the type of account accessed.

132. Section 1(4).
Whether the limitation to an asset account is still intended is unclear. Literally read, the Code does not apply to a debit card accessing an asset account when authentication is supported by a manual signature (or any other means of authentication except PIN), but will apply to a credit card, accessing a credit plan, used with a PIN. While the former card may not exist in Canada and with respect to the latter card the Code may be superseded by legislation or regulation, the ambiguity is unhelpful; if desired, departure from the position elsewhere ought to be spelled out more unequivocally. Be it as it may, it is clear that only card plus PIN authentication is covered by the Code in Canada.

The Code covers funds transfers from both public-access (POS and ABM) and exclusive-access (home) terminals, provided they are initiated by card together with PIN (and no other) method of authentication. Whether access is to asset or credit accounts makes no difference; hence, the Code applies to credit cards authenticated with PIN. At the same time, stored-value products are not intended to be covered; nevertheless, when authentication of a stored-value card transaction requires a PIN to be entered, the picture is not all that clear. Thus, the loading and unloading of a stored-valued card from and into an account, can be viewed as “withdrawal” and “deposit”, so as to be a “debit card transaction”, to which the Code will apply. Moreover, “payment” to a third party by means of such a card may be viewed as covered as well. While the first conclusion is defensible, that is less so for the latter. Nevertheless, nowhere does the Code specifically state that the “debit card” is strictly an access and not stored-value product, facilitating access to accounts operated by a financial institution.

With regard to cardholders’ responsibility for debit card transactions, the basic principle, set out in s. 5(1), is that “[c]ardholders are responsible for all authorized use of valid cards”. A Guide to the Interpretation of Section 5 “agreed to by the Electronic Funds Transfer Group” in January 2002 was added as Appendix A to the Code. Thereunder, “[a]n authorized transaction is one in which

133. See Part IV.3, above.
134. This is consistent with their exclusion from the Bank Act Regulations, discussed above in Part III.8, text around footnote 168, dealing with the unauthorized use of credit cards.
135. “Debit card transactions” are defined in s. 8 to mean “deposits, withdrawals, payments, or other funds transfers made at point-of-service terminals using a debit card”.
136. Canadian Code, s. 1(2).
the card and PIN are used to carry out the transaction and the cardholder has not been the victim of trickery, force, intimidation or theft". Presumably, an unauthorized use by a person to whom the cardholder voluntarily delivered the card and advised of the PIN, is "authorized", so that the cardholder is liable for it; arguably this cannot be viewed as a case of "trickery". Stated otherwise, while this is not certain, the better view appears to be that "trickery" is limited to the circumstances under which the card or PIN has been obtained by the user, and does not cover the fraudulent use of the card by an authorized person in lawful possession of both the card and PIN. Yet, the approach undertaken in the definition is questionable; that is, whether a transaction is authorized or not is a matter of actual or apparent authority, and not actual use of card and PIN. In effect, the Interpretation expands "apparent authority" to include all cases of use following the voluntary surrender of the card and code. Indeed, by itself, a rule fastening full liability for the use by a person in lawful possession is defensible. Nevertheless, it would have been more appropriate to provide for such a rule more directly.

The status of the Guide to the Interpretation of Section 5 is not entirely clear. Stated otherwise, there is a question as to whether it is binding on subscribing Institutions exactly as the Code. As well, there is no guidance as to determining a conflict between the Code and the Interpretation Guide. For example, point 4 to Interpretation to Clause 5 provides that the use of "a PIN combination selected from the cardholder's name, telephone number, date of birth or social insurance number" is tantamount to a voluntary PIN disclosure. This may be seen as expanding cardholder's exposure. It is arguable that this went beyond mere interpretation and provided for substantive rules, some of which may be seen as going too far. Thus, it is difficult to see how the use of a PIN selected from the date of birth is equivalent to voluntary disclosure; at the most, it is contribution to loss by negligence. However, the existence of negligence and its causation to loss is a matter of assessment in any given case. For example, if a thief stole the card without any document revealing the cardholder's date of birth, and having acted without knowledge of the date, nevertheless managed to use the card, it is hard to see how the choice of the birth date as PIN amounted to a voluntary PIN disclosure which makes the cardholder fully responsible. Furthermore, a voluntary disclosure is deemed to exist under the quoted language of point 4 even when the PIN is a combination of date of birth, name, telephone number, or social security number.
Note that in Australia, under Clause 5.6(d) of the EFT Code, for the selection of “a numeric code which represents the user’s birth date or an alphabetical code which is a recognizable part of the user’s name” to be a violation by user, the financial institution must “immediately before the user’s selection”, “specifically instruct . . . the user not to make such a selection and warn . . . the user of the consequences of such a selection . . .”. Only Australia (and not the EU, U.K. or Denmark) enumerates the choice of code as possibly involving fault leading to full exposure. Arguably, point 4 ought to be eliminated, so that only poorly disguising the code as possibly involving negligence. Only Australia (and not the EU, U.K. or Denmark) enumerates the choice of code as possibly involving fault leading to full exposure. Arguably, point 4 ought to be eliminated, so that only poorly disguising the code as possibly involving negligence.

Under s. 5(3)(b) of the Canadian Code, cardholders are not liable for losses resulting from the unauthorized use of the card and PIN in circumstances under which the issuer is responsible for preventing such use, as for example after the card has been reported lost or stolen, the card is canceled or expired, or where “the cardholder has reported that the PIN may be known to someone other than the cardholder”. However, there is no requirement for an issuer to make available and to advise consumers of a 24-hour phone line to which a notice could be given free of charge from anywhere where the card could be used.

Under s. 5(3)(c), cardholders are not liable for losses resulting from the unauthorized use, “where the cardholder has unintentionally contributed to such use, provided the cardholder co-operates in any subsequent investigation”. The provision raises a fundamental policy question: indeed, co-operation may be a factor in assessing the cardholder’s credibility — but could it be a factor in the loss allocation? Where it is found that loss resulted from circumstances beyond cardholder’s control, no liability ought to be fastened on cardholder, regardless of co-operation.

In contrast to the exoneration from liability provided by s. 5(3)(c), under s. 5(4), a cardholder who contributes to an unauthorized use “will be liable for the resulting loss”, though up to “established debit card transaction withdrawal limits”. So far as

137. The Interpretation provides the example of a cardholder who has been the victim of fraud, theft, or has been coerced by trickery, force or intimidation, as long as the cardholder reports the incident promptly and co-operates fully in any subsequent investigation. In conformity with the Interpretation to s. 5(1), ibid., under which a transaction by a victim of trickery, force, intimidation or theft is unauthorized, such a victim will nevertheless be liable if not promptly advising and fully co-operating.
the account balance serves as such limit, s. 5(4) points out that loss “may exceed the actual balance in an account” in two situations: that of a line of credit or overdraft protection linked to the account, and “a fraudulent deposit at an ABM”. It is not clear whether such a fraudulent ABM deposit is that of the customer or the wrongdoer; while s. 5(2) specifically holds cardholders responsible “if they make entry errors at point-of-service terminals, or if they make fraudulent or worthless deposits”, s. 5(4) is silent as to who has made the “fraudulent deposit at an ABM” so as to inflate the available balance for withdrawal.

Section 5(5) elaborates on the circumstances under which a “cardholder contributes to unauthorized use”, so as to be liable for the resulting loss under s. 5(4). Such would be the case where the cardholder voluntarily discloses the code, writes it on the card, or keeps a poorly disguised record of it in proximity with the card, as well as upon the cardholder’s failure, “within reasonable time” after the event,¹³⁸ to advise the issuer of the loss, theft, or misuse of the card, or the loss of confidentiality as to the code. The Interpretation clarifies that a cardholder whose PIN is obtained by coercion, trickery, force or intimidation, or whose PIN is observed at a point-of-sale terminal, does not disclose it voluntarily. Similarly, the fact that a customer uses the same PIN for more than one card does not constitute contribution to unauthorized use. Conversely, a cardholder contributes to unauthorized use when he or she selects his or her birth date as their PIN and keep the debit card in proximity with his or her driver’s licence which has a record of the birth date. However, a PIN is reasonably disguised, upon its concealment within the record, namely, by rearranging the numerals, substituting other numerals or symbols, or surrounding it by other numbers or symbols. In the final analysis, “[t]he reasonableness of an attempt to disguise a PIN should be assessed from the point of view of the reasonable cardholder, not from the point of view of the thief or the card issuer’s official who through experience have become familiar with many types of disguises and their strengths and weaknesses”.

It should be pointed out that the relationship among subs. 3(c), 4, and 5 of s. 5 of the Canadian Code is not all that clear. Under subs. 3(c), a cardholder is not liable for losses resulting from

¹³⁸. According to the Interpretation, “within reasonable time” means promptly, or more specifically, “as soon as the cardholder becomes aware of the loss or disclosure”.

circumstances beyond the cardholder’s control, such as “unauthorized use where the cardholder has unintentionally contributed to such loss, provided the cardholder co-operates in any subsequent investigation”. At the same time under subs. 4, “[i]n all other cases, when a cardholder contributes to unauthorized loss, the cardholder will be liable for the resulting loss . . .”. A list of events when “cardholder contributes to unauthorized loss” is set out in subs. 5. But even if in such events (voluntary disclosure of PIN etc. or failure to report loss) the cardholder can be said to be negligent, does it necessarily follow that cardholder has not “unintentionally contributed to . . . loss” so as to be excluded from subs. 4? That is, negligence and lack of intention are not mutually exclusive.

Regardless, most other sources require more than negligence; rather, what is required is “extreme carelessness” in Australia, “extreme negligence” in the EU, or “gross irresponsible conduct” in Denmark. Only the United Kingdom is satisfied with lack of “reasonable care”. Be it as it may, the Canadian Code is not explicit in allocating responsibility on the basis of fault. Rather, situations involving fault are deemed to constitute voluntary disclosure. However, as indicated, the better view is that voluntary disclosure and fault contributing to loss are in fact distinguishable and ought not to be confused. Specifically, voluntary disclosure and surrender may be viewed as a matter of apparent authority, which may automatically justify full liability. In contrast, fault and the loss caused by it, for which the cardholder is to become liable, are matters to be assessed in each given case.

7. EU Pronouncements

EU Directive 97/7/EC on the protection of consumers in respect of distance contracts deals with non-face-to-face consumer transactions. It addresses some issues relating to payment by cards in such contracts, namely, in situations where payment is carried out on the basis of card information communicated to the supplier.

Article 8 of the Directive requires Member States to ensure that appropriate measures exist to allow a consumer “to request cancellation of a payment where fraudulent use has been made on his payment card in connections with distance contracts . . .”, as

---

well as, "in the event of fraudulent use, to be re-credited with the sums paid or have them returned". "Fraudulent use" is not defined; presumably it includes unauthorized use. Quaere as to whether it includes fraud by the seller as to the existence of a transaction or the price agreed, where there was a genuine communication between the seller and consumer. Regardless, no provision is made as to the onus of proof.

EU Recommendation 97/489/EC\(^{140}\) covers transactions by electronic payment instruments, broadly defined, in arts. 1 and 2, to encompass both access and stored-value products. Regarding the unauthorized use of an electronic payment instrument, the recommendation provides in arts. 5-8 as follows:

1. The holder\(^{141}\) is not liable, "if the payment instrument has been used without physical presentation (of the instrument itself)". To that end, "[t]he use of a confidential code or any other similar proof of identity is not, by itself, sufficient to entail the holder's liability".

2. Other than as provided below, up to notification the holder bears "the loss sustained in consequence of the loss or theft of the electronic payment instrument up to a limit, which may not exceed ECU 150".\(^{142}\)

3. However, the limit does not apply in the following situations:
   (a) Where the holder acted "with extreme" negligence.
   (b) Where the holder acted in contravention of specified duties. These duties can be set out as follows: (i) to use the electronic payment instrument according to the terms governing its issuing and use, and in particular, to take all reasonable steps to keep safe the electronic payment instrument and the means (such as a personal identification number or other code) which enables it to be used; (ii) to advise the issuer without delay after

---


\(^{141}\) "Holder" is defined in art. 2(f) as "a person who, pursuant to a contract concluded between him/her and an issuer, holds a payment instrument". The context requires that he/she remains "holder" even when he/she does not "hold", as a result of having been dispossessed of the payment instrument. "Payment instrument" in the definition of "holder" must be taken to mean "electronic payment instrument".

\(^{142}\) Around CAD $245.
becoming aware of the loss or theft of the electronic payment instrument or the secret code, the recording on the holder's account of any unauthorized transaction, or any error or other irregularity in the maintenance of the account by the issuer; or (iii) not to record secret code in any recognizable form, in particular on the electronic payment instrument or any item which the holder keeps or carries with it.

(c) Where the holder acted fraudulently.

For the limit under no. 2 to be inapplicable, no causal link is required between any such a breach and the actual loss.

4. Other than when the holder acted fraudulently, there is no holder's liability for loss arising in consequences of the loss or theft of the electronic payment instrument, "[a]s soon as the holder has notified the issuer" of the loss or theft of the electronic payment instrument or the secret code.

5. The issuer is required not to disclose the holder's secret code "except to the holder", as well as to provide an effective means of notification in case of loss or theft. The issuer is further required, in the case of a dispute with the holder concerning a transaction effected by means of an electronic payment instrument, "and without prejudice to any proof to the contrary that may be produced by the holder", to prove that the transaction "was accurately recorded and entered into accounts", and that it "was not affected by technical breakdown or other deficiency".

The EU Recommendation is stated in art. 1(1) to apply to (a) "transfers of funds, other than those ordered and executed by financial institutions, effected by means of an electronic payment instrument", as well as to (b) "cash withdrawals by means of an electronic payment instrument and the loading (and unloading) of an electronic money instrument, at devices such as cash dispensing machines and automated teller machines and at the premises of the issuer or an institution who is under contract to accept the payment instrument". 143 "Electronic payment instrument" is defined to be "an instrument enabling its holder to effect transactions of the kind specified in art. 1(1)". This is stated to cover "both remote access

143. Emphasis added.
payment instruments and electronic money instruments”. “Remote access payment instrument” is in effect an access product. It is defined to mean “an instrument enabling the holder to access funds held on his/her account at an institution, whereby payment is allowed to be made to a payee and usually requiring a personal identification code and/or any other similar proof of identity. This includes in particular payment cards (whether credit, debit, deferred debit or charge cards) and phone- and phone banking applications”. “Electronic money instrument” is effectively a stored-value product; it is defined to mean “a reloadable payment instrument other than a remote access payment instrument, whether a stored-value card or a computer memory, on which value units are stored electronically, enabling the holder to effect transactions of the kind specified in Article 1(1)”.

Accordingly, all consumer-initiated electronic funds transfers, whether by means of access or stored-value products, are covered by the EU Recommendation. While art. 1(1)(a) appears to cover payment into accounts, including from home or a POS terminal, art. 1(1)(b) covers all cash withdrawal and the loading and unloading of stored-value product. Yet, a few doubts remain. First, per the definition of “remote access payment instrument” reproduced above, electronic authentication must be one “usually requiring a personal identification code and/or any other similar proof of identity. This includes in particular payment cards (whether credit, debit, deferred debit or charge cards) and phone- and phone banking applications”. Other than for the reference to “usually”, which may suggest that the definition is not exhaustive, this would have excluded the involvement of a manual signature in conjunction with the card authentication. Second, it is uncertain whether “instrument” requires a physical device so as to exclude, other than in connection with “phone- and phone banking applications” which are specifically mentioned, a mere PIN or digital signature authentication, unaccompanied by the use of card. In the alternative, the reference to “phone- and phone banking applications” may be designed to indicate that an “instrument” need not be a physical device.

V. CONCLUDING REMARKS AND PROPOSED PRINCIPLES

The Canadian Code of Practice for Debit Card Services currently in effect is fundamentally sound. Prima facie, it needs more

---

144. Terms are defined in art. 2.
of an update than of an upgrade; this is in response to fast-moving technological developments and not basic flaws. Still, the experience with the Code, side by side with experience elsewhere, permits the introduction of changes with the view of enhancing protections to consumers and the presentation of improvements to the scheme.

Undoubtedly, the most comprehensive model is that of the new Australian EFT Code. Nevertheless, the view presented in this article is that the positions adopted by that code ought not to be slavishly followed. A few points should be highlighted.

First, there is some ambiguity as to whether authentication by card and signature is covered. As indicated, it is recommended that the proposed Code will cover all methods of authentication other than by mere manual signature. Historically in the United States, the different treatment given to credit and debit card payments is a reflection of the different era and context in which each of the two modes of non-cash payment devices was introduced. Specifically, credit card legislation was passed in the context of consumer protection in credit rather than payment transactions, and in an era that preceded the invention of magnetic stripe technology facilitating PIN authentication. Arguably, this facilitated the emergence of a model premised on two unrelated liability regimes which has gained worldwide popularity. It is specifically proposed here to break away from this model. On this point, the Danish statute is much more satisfactory.

Second, regarding unauthorized transfers, the position adopted by the drafters of the Australian Code in relation of the role of the consumer's fault is not self-evident and its rationale ought to be reconsidered. As indicated, a rule based on fault may increase litigation costs and is likely to give financial institutions more than what is needed to promote due diligence by consumers. While recognizing that most sources do take into account fault in the allocation of unauthorized consumer electronic funds transfer losses, the position recommended here is inspired by the legal position in the United States. Thereunder, what counts for expanding consumer liability above a low ceiling is only negligence in the failure to read bank statements or advise the financial institution of a known unauthorized transfer or breach of security.

Third, the Australian Code may not provide an optimal definition for an "unauthorized transfer". Particularly, more thought has
to be given to transfer made without actual authority (whether express or implied) by a person who is nevertheless in lawful possession of the access device and Code. Arguably, the Australian Code treats this as an unauthorized transfer. The American position seems to be the opposite, while the Danish position purports to strike a middle ground, under which transfer is to be deemed authorized only if the holder realized or should have realized the existence of the risk of abuse.

Fourth, while the Australian Code is unique in addressing specifically and in detail the onus of proof question it may not go far enough in that regard. True, the Australian Code recognizes that the onus of proving balance of probability for an unauthorized transfer is on the financial institution and it goes on and provides that the mere fact that the account was accessed with the correct access method, that is, in compliance with the agreed upon security procedure, “while significant”, is not by itself “proof on the balance of probability that the user contributed to losses”. But at the same time, it does not specifically say whether the mere proof as to the use of the correct access method is “proof on the balance of probability” as to whether the transfer was authorized.

Presumably, the implication is that it is not adequate; otherwise, if the transfer is to be regarded as authorized, there would not have been any question as to loss or contribution to the loss. Arguably, three situations are covered: (a) where unauthorized use is proven and no contribution to losses by user is proven, user is exonerated from any liability whatsoever; (b) where both loss caused by unauthorized use and user’s contribution to loss are proven, user bears extensive liability; and (c) when unauthorized use, but not user’s contribution to loss, is proven, that is, in a case where user’s lack of contribution to loss is not affirmatively proven, user bears limited liability only. Nevertheless, detailed as it is, the scheme gives no guidance as to what constitutes proof on the balance of probability that the transfer was unauthorized. Presumably, the position in Denmark is clearer, as limited liability may be fastened on the basis of proof of mere compliance with security procedures.

In conclusion, the various substantive provisions of a new code may build on past experience as well as on statutes, regulations and voluntary codes from various sources. However, in the final analysis, for each issue, the merit of each position ought to be

145. Emphasis added.
considered on its own so as to provide the optimal scheme for consumer electronic funds transfer in Canada.

On the basis of the preceding discussion, a statement of principles to guide in the drafting of a revised comprehensive Consumer EFT Code for Canada is put forward. Such principles aim at the enhancement of fairness to consumers in the context of an overall scheme designed, in a market-oriented framework, to maximize benefits to society as well as to strike a sound balance between consumers and financial institutions.

The scope of the provisions ought to be comprehensive in terms of both transactions and participants. To that end, it ought to become a Consumer EFT Code of Conduct, covering all payments authenticated by consumers other than by means of a mere signature, and binding on all institutions providing either such payment services or accounts into which such payments are posted.

Proposed principles are set out as follows:

1. An all-inclusive definition is to be given to an "authorized transfer", as covering actual as well as apparent authority or authority by estoppel, and excluding cases of trickery or physical coercion. More generally, the principle is that an "authorized transfer" is one for which a customer is bound under the law of agency. In connection with apparent authority or estoppel, specific rules ought to be stated as to whether the mere voluntary surrender of means of access is tantamount to conferring such authority, or whether as in Denmark, for full liability, there has to be an added requirement of realization of the existence of a risk of abuse.146

2. A consumer is liable for the amount of all authorized transfers as well as of fraudulent transfers where he or she knew of or took part in the fraud.

3. To charge the consumer with liability so as to be entitled to debit his or her account with the amount of an electronic funds transfer the financial institution must prove either an authorized transfer or a fraudulent transfer with either the

146. In this context, a question may also arise as to the voluntary breach of confidentiality, as for example, by writing a secret code on a card. While in principle this raises the issue of liability on the basis of negligence, this type of conduct is quite close to actual disclosure.
knowledge or participation of the consumer. The onus of proof is that of balance of probabilities or on a preponderance of evidence or probabilities. This onus of proof applies to all material details of transfer and not only its existence.

4. To rely on verification according to a security procedure agreed upon between the financial institution and the consumer, the institution must prove that:
   (1) the financial institution accepted the payment order in compliance with the security procedure, including, where required, that a genuine card issued by the institution was used in the transaction;
   (2) the security procedure is a commercially reasonable method for the verification of authority and attribution; and
   (3) at all material times the computer system that verified authentication to the satisfaction of the financial institution was operating properly, or if it was not, the fact of its not operating properly did not affect the integrity of the system.

"Security procedure" includes the use of card, PIN, digital signature, password, and card with manual signature, PIN or digital signature.

5. By itself, and against the denial by the consumer of an authorized transfer, such evidence is not sufficient proof of an authorized transfer. In response to the consumer’s denial, the financial institution ought to conduct full investigation and make its results available to the consumer. The findings of this investigation will be taken into account in assessing whether the financial institution has proven authority.

6. A consumer who denies a transfer was authorized notwithstanding proper proof as to verification, is required to fully co-operate with the financial institution, to act in good faith, disclose all relevant information, and assist in the investigation. The consumer’s compliance with this obligation will be taken into account in determining whether the financial institution has complied with the onus of proof as to an authorized transfer.
7. With respect to unauthorized transfers, occurring before the consumer advises the financial institution of the loss or theft of his or her card (or any other access device) or of material breach of security, proof of verification, as required under principle no. 4 above, entitles the financial institution to claim from the consumer the smaller of the amount of the unauthorized transfers and a prescribed (small) sum and charge it to the consumer’s account. (This is on the basis of the statute in Denmark.) (Alternatively, as under Reg. E in the United States, minimum sum liability is only as of two days after actual knowledge of unauthorized loss, with the amount increasing thereafter up to another low sum.) An annual ceiling may be set for liability under such a principle. There is thus a limited liability for properly verified transfers not proven to be authorized.

8. A consumer is under an obligation to examine carefully all periodic statements sent to him or her by the financial institution. In connection with passbook accounts, the consumer is under an obligation to update it regularly, at least every 30 days, and carefully examine all entries so updated. A consumer who learns of an unauthorized transfer or should have learned of such a transfer had he or she complied with this obligation, and does not report it to the financial institution, becomes liable to all unauthorized transfers occurring as of 30 days after he or she learned or should have learned of the unauthorized transfers, whichever is earlier. (The period may be shortened in cases of actual knowledge by the consumer.) Liability under this principle is not limited to transfers properly verified by the financial institution.

9. Under any of the above, consumer is liable for unauthorized transfers only:
   (1) where timely advice by him or her would have prevented the loss;
   (2) where a proper mechanism for notifying the financial institution is available and properly advised to the consumer; and
   (3) within applicable withdrawal and transaction limits.

10. A special rule ought to apply to lost SVPs in circumstances where the issuer cannot prevent future unauthorized use.
Yet, loaded value is to be treated as lost cash only in a framework that puts strict limits on the amount of value that may be loaded on an SVP, particularly in connection with mere card authentication.