1989

The E.F.T. Debit Card

Benjamin Geva

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

Source Publication:

Canadian Business Law Journal. Volume 15, Issue 4 (1989), p. 406-440.

THE E.F.T. DEBIT CARD

Benjamin Geva *

CONTENTS

1. Introduction

The debit card is a new payment device providing access to funds deposited in a bank account. Having grown out of the paper based credit card, it developed primarily in the course of evolution of electronic funds transfer ("EFT") systems. This article purports to examine the elements of the EFT debit card transaction and explore the legal regime governing it.

Part 2 sets out the fundamentals of the EFT debit card as a device facilitating electronic access to funds so as to initiate payment from terminals at points of sale ("POS") and automated banking machines ("ABMs"). Part 3 delineates the setting within

* Professor of Law, Osgoode Hall Law School, Toronto. This article is part of a study on the allocation of risks in payment mechanisms supported by a grant from the Foundation of Legal Research of the Canadian Bar Association. Much of the information draws on interviews and written materials provided by bankers, lawyers and regulators in Canada, Australia, the United Kingdom, and the United States. I am particularly grateful for the assistance of John S. Roberts, Penny-Lynn McPherson and their colleagues at the Canadian Payments Association; Catherine Irwin and M.B. Anderson of the Bank of Montreal; Norman Cromie of the C.I.B.C.; S.R. Morran of the TD Bank; Richard Crooker of Amex Canada; D.A. Fry of Interac Association; Marie T. Ibell of Hudson's Bay; David Bruce and his colleagues at the National Australia Bank; staff of the Australian Trade Practices Commission; D. McCallum of EFT-POS Development in the United Kingdom; Richard Field, Leslie Wollin and James Bauer of Manufacturers Hanover Trust Company; Susan Levine and Linda L. Walker of Chase Manhattan Bank; and Brian Frumkin, Charles Jeffrey, Brian O'Hare, Doug Newman, Lorna Sieper and Steve Yotter of the Bank of America. However, the analysis, conclusions and possible errors are mine alone.

which the EFT debit card transaction takes place. It thus outlines the various system components, such as terminals, computers, telecommunication links, and clearing and settlement. Part 4 investigates the legal issues arising in the course of transactions whose elements have been explored in the previous parts. It thus considers the relative position of retailers, consumers, and depositary financial institutions in EFT debit card transactions. The article concludes with some observations as to the proper avenue for the future development of debit card law and the role of the Canadian Payments Association in that process.

In Canada, as elsewhere, the law governing the EFT debit card is in its early evolutionary stage. This article is designed to assist in setting a direction and providing a framework for its development. It is written primarily, though not exclusively, from a Canadian perspective.

2. Cards, PINs and Access to Funds

Plastic cards bearing information as to cardholder, card number, and card issuer, issued to customers by depositary financial institutions such as banks[1] ("payment cards") are not a novelty in consumer payment systems. For several decades now, payment cards have been used in various ways. First, a card may be used solely as a means of verifying the identity of the payer to the payee's satisfaction, so as to assist the latter in assessing the authenticity of the former's payment instructions. Secondly, a payment card may be used to give the payee the issuer's authorization to accept the card. Such an authorization may provide the payee with the issuer's assurance either of payment, or at least, as to the payer's identity, that is, as to the authenticity of his payment instructions. Finally, a card can access funds and initiate payment itself.

In the course of their development, payment cards have fallen into several categories. A card providing an assurance of payment of a cheque is a cheque guaranty card. A card providing an assurance of payment to a merchant accepting the card under an

[1] Two caveats ought to be noted. First, payment cards may also be issued by nondepositary financial institutions such as retailers. Second, depositary financial institutions include chartered banks, trust companies, and co-operative credit societies. In this article they are all treated as "banks". This is modelled on the statutory definition of bank in s. 164 of the Bills of Exchange Act, R.S.C. 1985, c. B-4.

agreement with the issuer or with the merchant's bank is a credit card. A card facilitating access to funds in the cardholder's deposit account is a debit card. Finally, a card initiating payment, that is, facilitating access to funds in the cardholder's account solely on the basis of information communicated electronically, is an EFT debit card. The list may not be exhaustive. Nevertheless, it covers the main stages of the development of the payment card.

Depending on available technology and pertinent use, payment cards have emerged in different forms. In general, three generations of cards have surfaced: the "mere plastic" or embossed card, the magnetic-stripe card, and the "smart" or memory card.[2]

The information contained in the first generation cards can be obtained solely by a physical examination of the card. This information can be copied by the payee on the piece of paper containing the paying cardholder's payment instructions, usually a cheque. The task of manual copying can be avoided where the "mere plastic" card is embossed. The embossed card has raised characters on its surface. These characters can be reproduced on paper when the card is run through an imprinter which is used to manually print the information appearing on the face of the card. Embossed cards have primarily been used as credit cards where the information contained on the card is imprinted on the sales draft embodying the cardholder's payment instructions.

First generation cards contain the cardholder's signature for cross-verification with the signature on the cheque or sales draft. These cards have been used either solely as identification cards, to verify the identity of the paying cardholder or, more often, as a means of giving the payee an assurance of payment. The cheque guaranty card as well as the credit card are cards giving such assurance of payment. As explained below, the outgrowth of the first generation credit card and its development to meet current functional needs by taking advantage of new technologies, underlies the evolution of the second and third generation cards within which the EFT debit card has evolved.

To benefit from the assurance of payment in credit card transactions, the payee-merchant is typically required by contract[3] to

[2] See, in general, D. Martres, "Le Smart Card" (1989), 96 Canadian Banker 1:26 (in English). For a more comprehensive treatment, see D. Chorafas, *Electronic Funds Transfer* (London, Butterworth & Co. Ltd., 1988), primarily Chapter 22.

[3] The contractual setting, in the context of the legal framework for bank credit cards in Canada, is described in S. Goldstein, *Changing Times: Banking in the Electronic Age* (Ottawa, Government of Canada, 1979), Chapter VI.

verify whether or not the particular card is in the current list of misused cards. Such lists are distributed periodically to retailers. Futhermore, for a large payment, the merchant is required to obtain the issuer's prior authorization to accept the card. The issuer's authorization will be given where payment is within the cardholder's existing credit limits and the card is not among the misused cards.

The request for authorization is made by the payee communicating the card information to the issuer. Authorization can be requested and obtained by phone. Originally, the merchant seeking to accept a credit card payment was required to call the card issuer directly. The system was improved when communication between the merchant and each issuer could be intermediated through the authorization centre of the merchant's own bank. This design saves time by enabling the merchant to call his own bank regardless of who the issuer of the card is.

Requiring authorization for each credit card payment, and not only for high value transactions, would eliminate the need to distribute lists of misused cards. It would also eliminate situations where credit limits of a cardholder are exceeded due to a series of low value transactions. Expediting the authorization process has thus become important, and not only in connection with large payments.

The need for a faster authorization process was met by the magnetic-stripe card. This is the second stage in the evolution of payment cards. The magnetic stripe is a technological device by which pre-recorded information is stored on a card. Magnetic stripes containing card information are inexpensive and have been placed on first generation cards. When a magnetic-stripe card is passed ("swiped") by the payee-merchant through a terminal at the point of sale, the information stored in the magnetic stripe is "read" and communicated directly to the merchant's bank authorization centre without the need of further human intervention such as a phone call. Where the issuer and the merchant's bank are different institutions, the request for authorization is directed by the latter to the former. Authorization is communicated back from the issuer, via the merchant's bank where it is a separate institution, to the point-of-sale terminal. This allows the merchant to proceed and to accept the card payment. In this process, the magnetic-stripe card initiates the online electronic authorization.

Electronic authorization is the forerunner of the electronic

deposit of funds. The deposit occurs when the data from the card transaction, which has been communicated from the terminal at the point of sale, can be captured at the receiving end. Online data capture facilitates the giving of credit to the payee-merchant account.[4]

Also, in theory, the cardholder's account could have been debited at this stage. Nevertheless, the move to direct debit has been fraught with difficulties. Sound banking practices require that no account be debited unless the authenticity of the paying customer's instructions can be established to the satisfaction of the bank maintaining the account ("account holder"). This is because a successful challenge by the customer to a debit in his account requires the account holder to reverse the debit.[5] A successful challenge can further expose the account holder to liability for consequential loss, which can be substantial, where the wrongful debit left the account with insufficient funds to meet valid payment instructions that consequently were dishonoured.[6]

Because of these difficulties, the account holder is well justified in requiring unambiguous proof supporting payment instructions. An internal system verifying the authenticity of each payment request may prevent a wrongful debit and the resulting wrongful dishonour. As well, the retention of evidence authenticating payment instructions enables the account holder to meet a customer's challenge as to that authenticity. This is also true where, for business reasons, individual verification prior to payment of each request is unworkable. Under such circumstances, the account holder assumes the risk of subsequent wrongful dishonour, but is able to protect itself against unfounded allegations by the customer of lack of authenticity of payment instructions.

Data captured in the course of the electronic authorization of a credit card transaction falls short of allowing an account holder to

---

[4] The evolution from electronic authorization to electronic deposit, and the subsequent move to direct debit, are set out in *POS in Canada*, a report prepared by American Express Canada, Inc. (April, 1985).

[5] In principle (though subject to available defences) a paying bank cannot debit its customer's account where payment was made without mandate from the customer and was not ratified. For this principle, see, *e.g.*, *Barclays Bank Ltd. v. W.J. Simms Son & Cooke (Southern) Ltd.*, [1980] Q.B. 677 at p. 699, *per* Goff J.

[6] Liability for wrongful dishonour is discussed in B. Crawford, *Crawford and Falconbridge Banking and Bills of Exchange*, 8th ed. (Toronto, Canada Law Book Inc., 1986), Vol. 1, §3901.4.

access the cardholder's account. Such a process fails to produce evidence which is capable of convincing the account holder of the authenticity of the payment instructions. Only the use of the card, but not its user's identity, is verified. True, a successful challenge by the customer as to the authenticity of the payment instructions undermines the validity of the electronic deposit of funds to the payee-merchant's account. However, the contractual arrangement between the merchant and his bank is likely to allow the latter to reverse credits made against uncollected funds. In general, a bank is likely to assume risks generated by such provisional credits.[7] It does not follow that it is willing and ready to assume the risk of unauthorized debits.

In a credit card system, funds are credited to the merchant's account on the basis of a deposit of sales drafts, by the delivery of tapes (on which payments are recorded), or by electronic deposit. Funds are paid to the bank for deposit by the card issuer. In the course of this process, the cardholder's credit card account is debited by the card issuer without the issuer being satisfied with the authenticity of the payment instructions. However, no cardholder's funds at his current account are accessed throughout this process. Access is made subsequently and solely on the basis of the cardholder's own confirmation made by the act of payment for items charged to his credit account and billed to him periodically. Where a dispute arises as to an item charged, the existence of a validly signed sales draft will determine its resolution. It is the signed piece of paper[8] which entitles the account holder to proceed against the cardholder.

In fact, there are card systems where the cardholder's funds are accessed on the basis of the electronic deposit generated in the

---

[7] Indeed, the cheque collection system is premised on a provisional credit being given to the depositor which may be revoked upon the subsequent dishonour and return of the cheque. See, *e.g.*, *Bank of Nova Scotia v. Sharp* (1975), 57 D.L.R. (3d) 260, [1975] 6 W.W.R. 97 (B.C.C.A.).

[8] Two qualifications ought to be noted. First, in a telephone credit card payment the sales draft is generated by the merchant according to the authority given by the buyer. Needless to say, this may produce additional evidentiary problems as to authority and content of payment instructions. Second, in practice, a card issuer may devise a scheme where no signed piece of paper is required and charges to the cardholder's charge account are made on the basis of running the card at the point of sale alone. It must be recognized however that under such a scheme an issuer faced with an unauthorized use plea runs an evidentiary risk. By contractual means these risks may be shifted to the merchant or his bank. No bank runs such a scheme. One such scheme is operated in Canada by an oil company where the value of each sale is relatively low.

course of the online authorization. The sales draft is kept ("truncated")[9] by the merchant at the point of sale. It will be retrieved only upon a challenge by the cardholder as to the pertinent charge in his account. In this environment, the payment card has facilitated access to funds and turned the credit card into a debit card. None the less, the authentication of the payment instructions remains dependent on the signature verification. As a result, this is a paper-based and not an EFT debit card.

The operation of such a paper-based debit card system is not free of controversy. First, the practice of accessing the cardholder's funds prior to the issuer having an opportunity to satisfy itself as to the authenticity of the payment instructions exposes the account holder to the risk of an unauthorized debit leading to a wrongful dishonour.[10] As for proving the authenticity of the payment instructions on the basis of the signed sales draft, there may also be the practical difficulty of retrieving the sales draft from a remote merchant dealing with a remote foreign bank. Second, where a blank authorization is sought in advance for an open-ended obligation, such as a car rental or hotel bill, funds may be frozen in the cardholder's account on the basis of the online authorization. It is not entirely clear whether the online authorization may then be treated as the equivalent of cheque certification[11] so that the frozen funds may be withdrawn from the cardholder's account prior to the crystallization of the payment obligation. This would permit the account holder to dishonour cheques and other payment items competing for the same funds and striking the account prior to the completion of the transaction. These uncertainties have led to the demise of the paper-based debit card in Canada.[12]

---

[9] For "truncation" in the cheque collection system see B. Geva, "Off-Premises Presentment and Cheque Truncation Under the Bills of Exchange Act" (1986-87), 1 B.F.L.R. 295, particularly at pp. 296-302.

[10] See the discussion around footnote 6, *supra*. In theory, the solution to this particular problem lies in the replication of the cheque collection system, under which no account is debited until there is an opportunity to verify the signature on the pertaining cheque. For cheque clearing see, *e.g.*, Geva, *supra*, footnote 9, at pp. 303-5 and 317. This may however defeat the objectives of curtailing paper movement and eliminating the float.

[11] For cheque certification and the withdrawal funds payable under a certified cheque see B. Geva, "Irrevocability of Bank Drafts, Certified Cheques and Money Orders" (1986), 65 Can. Bar Rev. 107, at pp. 123-30.

[12] This is in contrast to the United States where Master Debit and Visa Debit have been set as such paper-based debit card systems. In Canada, Master Card II, the predecessor of Master Debit, has not gained momentum.

Direct debit to the cardholder's account on the basis of data captured in the course of electronic authorization is feasible where such data serves also to verify the cardholder's identity so as to authenticate his payment instructions. Stated otherwise, an "electronic signature" must be communicated to the account holder from the terminal at the point of sale.

The Personal Identification Number ("PIN") was devised to serve as such an electronic signature. This is a relatively low cost electronic means of customer identification in the form of a secret code, intended for the sole use of each cardholder, and designed to authenticate his instructions given at a terminal.[13] Since the stripe can be easily read with a very cheap device, no PIN information is stored in it. Rather, information used to derive the PIN is stored in the magnetic stripe and "read" when the card is inserted at the terminal. This information and the secret number entered by the cardholder at the terminal are used by the card issuer, using an algorithm, to verify the PIN. This verifies the identity of the cardholder[14] and authenticates his instructions. The audit trail provides proof of the exercise. This allows the account holder to access the cardholder's account and debit it in the course of the electronic authorization process.[15] Thus, the addition of the information, from which the PIN can be derived, to the data stored on the magnetic stripe, underlies the transformation of the paper-based payment card to the EFT debit card.[16]

EFT debit cards originated in cash disbursement transactions at cash dispensers.[17] A terminal, usually unattended, that issues cash to a cardholder is a cash dispenser.[18] On the basis of PIN verification followed by an authorization, and in response to a

---

[13] For a definition of PIN and a brief explanation see, *e.g.*, two recent reports (collectively referred to below as "POS documents") of the Canadian Payments Association: (1) *The Fundamental Elements of EFT/POS — Revised and Recommended Version* (September 23, 1988), p. 7; and (2) *The EFT/POS Consultative Process: A Status Report* (October 12, 1988), p. 6. Respectively these reports are to be referred to below as "EFTPOS Fundamentals" and "EFTPOS Consultative Process".

[14] Strictly speaking this is card authentication more than cardholder identification except that both are performed on the basis of the card.

[15] See, *e.g.*, Chorafas, *supra*, footnote 2, at pp. 181, 186, 195 and 203.

[16] For other uses of PIN technology in cheque authorization and guarantee systems, see N. Penney and D.I. Baker, *The Law of Electronic Fund Transfer Systems* (Boston, New York, Warren, Gorham & Lamont, 1980, with a 1987 Cum. Sup. by D.I. Baker and R.E. Brandel), Chapter 8. No such systems are in place in Canada.

[17] See, *e.g.*, Chorafas, *supra*, footnote 2, at pp. 339-41.

[18] Goldstein, *supra*, footnote 3, at p. 167.

cardholder's request made at the terminal and communicated to the issuer's host computer, cash stored at the dispenser is released to the cardholder and his account is debited. Under such circumstances, the PIN controlled verification process is the only proof of the authenticity of the cardholder's disbursement request. As corresponding needs arose in retail transactions, and large numbers of retailers and banks joined a programme, the same machinery was put to work at point-of-sale terminals.

Whether in cash disbursement or point-of-sale transactions, an EFT debit card environment is characterized by the account holder's reliance on information communicated by electronic means as establishing the cardholder's payment instructions. This information is communicated in the course of the verification/authorization process. However, it does not follow that such information must be acted upon promptly. That is, the ability to access funds need not translate itself into immediate debit or even credit. Accounts may be updated daily, whether with respect to that day or a previous day,[19] at set times during the day, or instantaneously. As well, the respective debit and credit stemming from each payment need not be triggered simultaneously. A debit card payment is thus characterized by the initiation of payment by means of the electronic communication of card information. Indeed, online communication of card information may facilitate realtime payment from end to end so as to assimilate the card payment to cash payment. However, slower payment scenarios are also consistent with the notion of a debit card payment.

Nor is online verification/authorization an indispensable component of an EFT debit card transaction. Regardless of the timing of the account adjustment, the online authorization communicated by the card issuer to the terminal constitutes its assurance of payment, as in a credit card transaction. However, there may be incentives to bypass the online verification/authorization process. This may be done either to reduce costs or to control retail data and maintain cardholder base where a nonbank card issuer is prepared to assume risks eliminated by the bank's online verification/authorization.[20] In principle, there is no such

[19] In the United Kingdom "[a]t present there is a delay, of up to four days, which is the notional equivalent of the time it takes to clear a cheque". See D. Barchard, "The debit card becomes a success story", *The Financial Times*, December 31, 1988. Obviously this is done for marketing purposes.

[20] *Cf.* models reviewed in EFTPOS Consultative Process, *supra*, footnote 13, at pp. 9-14 as

third party at a cash disbursement transaction at a cash dispenser. Hence, the elimination or replacement of the verification/authorization process will be considered only in connection with terminals at points of sale. It will be demonstrated that alternative procedures are available, although at a cost and risk which make them unappealing.

Thus, the online verification/authorization process consists of two distinct components: card authentication ("verification") and payment assurance ("authorization"). The process involves an interactive communication between the terminal and the bank's host computer. Where this interactive communication process is bypassed, messages entered at the terminal may be batched and forwarded for deposit offline and periodically, usually at the end of the day, by means of delivery of tapes or by batch transmission. Collection from the account holder may be made through the bank of deposit.

Sound banking practices preclude the possibility of bypassing the verification component. Nor can interactive verification be replaced by a delayed verification process. Under the latter procedure, the cardholder's request for verification is communicated to the host computer, not necessarily in realtime, but in any event, is not acknowledged. The merchant may proceed with the transaction at his risk. The authenticity of the payment instructions can only be confirmed subsequently. Such a procedure is open to abuse; a dishonest cardholder may be tempted to enter a false PIN and then deny liability.

As well, the account holder does not expect to gain from a system premised on online verification unaccompanied by funds release authorization. Such a system treats the verification and access to the account as two distinct stages and requires the management of two separate databases. Consequently it is bound to produce inefficiencies.

An offline environment can exist where verification is performed at the terminal, with no online communication to the bank's host computer. It can also exist where verification is performed by a nonbank card issuer, such as the retailer himself, or by a third party.

At-the-terminal verification is facilitated by the use of the third generation of payment cards,[21] the smart card, known also as the

---

well as Appendix B (the latter being a position paper of the Retail Council of Canada, dated July 30, 1986) and Appendix D.

[21] For the three generations of payment cards see text at footnote 2, *supra*.

memory card.[22] This is a card with a built-in microchip which carries a wider range of information than a conventional second generation card with a magnetic stripe. The chip measuring only a few cubic millimetres stores and processes within the card itself the data required for many types of transaction. This includes functions and information that in the case of a magnetic-stripe card require communication from terminals to a host computer.

The utilization of smart-card technology in points of sale is premised on local in-the-terminal approval in a semi-online terminal. That is, PIN verification is performed at the terminal solely on the basis of information stored in the card and without further communication to a host computer.

The verification by a nonbank card issuer (such as the retailer or other third party) can be performed in the context of existing magnetic-stripe technology by means of interactive communications between the terminal and a host computer of the nonbank card issuer. In such an environment, the PIN is provided to the cardholder and is controlled by the nonbank card issuer which performs the verification. In practice, a nonbank card issuer may be less scrupulous than a bank and may forgo PIN verification altogether. A nonbank verification can thus be performed by means of ID identification, signature on a sales draft kept at the point of sale, or by the mere possession of the card. But even when interactive online verification is performed by the nonbank party, so far as the account holder is concerned this is an offline environment since collection is made on the basis of batch processing via the bank of deposit.

Neither smart-card technology nor nonbank's verification provides access to the cardholder's account. In an offline environment, in the absence of the account holder's authorization, the risk of insufficient funds ("NSF")[23] is borne by the merchant. This is unless the smart card has been prepaid, or unless as a matter of a business arrangement, the NSF risk has been assumed by another participant. No assurance of payment is provided by the account holder in the course of the communication process.

The implementation of both smart-card technology and nonbank's verification faces hurdles and is open to several objec-

[22] On smart cards (and related topics) see in general, Martres, *supra*, footnote 2; and Chorafas, *supra*, footnote 2, at pp. 343-50.

[23] The risk includes the nonexistence as well as the closure of the account.

tions. First, the smart card itself is quite expensive. Further, prepayment is an unattractive proposition to consumers. Their aversion is directed to prepayment itself as well as to the attendant risk of losing a prepaid card. At the same time, the need for authorization cannot be eliminated except where there is prepayment or the credit risks are low. Overall, in connection with consumer payments, smart cards do not appear to present a viable alternative to second generation magnetic-stripe cards.[24]

For its part, a nonbank's verification facilitates access to funds under a verification process which is outside the account holder's control.[25] This exposes the account holder to the risk of unauthorized debit leading to the subsequent wrongful dishonour of valid payment orders. It further leaves the account holder with no evidence of its own as to the authenticity of payment instructions.[26]

A nonbank PIN controlled verification may be a possible enhancement to a credit card system. In such environment, authenticated card instructions dispense with the need for a signed sales draft. Online authorization triggers an electronic deposit to the merchant's account and payment by the nonbank card issuer to the bank of deposit. No cardholder's funds are accessed in the course of this process. Payment is made by the cardholder to the nonbank issuer separately and for items charged to his credit account and billed to him periodically.[27] No funds are thus accessed on the basis of the nonbank PIN controlled verification.

Nevertheless, in some U.S. systems, a nonbank PIN controlled verification facilitates access to cardholder's funds. The account

[24] For a pessimistic outlook for the smart card in payment systems, see, *e.g.*, Chorafas, *supra*, footnote 2, at pp. 345 and 347. None the less, the smart card's prospects look brighter in countries where the telecommunication system is inefficient. See L. Rosenthal, "Italy's Smart Card Systems: Alternatives to On-line Eftpos", *Electronic Payments International*, issue 32, p. 9, May, 1989 (A Lafferty Group Publication).

[25] The Canadian Payments Association is opposed to such procedures. See statement of February 10, 1986, "The Framework for the Evolution of the Payments System", being Appendix A to EFTPOS Consultative Process, *supra*, footnote 13.

[26] Risks to which the account holder is exposed in the absence of control over verification are set out in the text around footnotes 5 and 6, *supra*.

[27] *Cf.*discussion around footnote 8, *supra* (a paper-based credit card system). A PIN controlled credit card system may be cost effective only for unattended terminals (such as for the sale of traveller's cheques) as well as for circumstances where, in the issuer's judgment, merchant's safekeeping of sales drafts is an unsafe or otherwise unworkable verification system (*cf.* discussion which follows footnote 10, *supra*). An unattended terminal for traveller's cheques works like a cash dispenser.

holder protects itself by means of appropriate contractual provisions designed to insulate itself from any dispute as to the authenticity of the instructions. However, since access to funds is involved, it is questionable whether entrusting the verification process to someone other than a regulated depositary financial institution is in the cardholders' interest.

Furthermore, all offline options are premised on overnight processing of batched messages. Computerized facilities at bank data centres are under heavy demand during night hours, when cheque processing takes place. There is less demand on these facilities during daytime hours. Consequently, an increase in the nightime and diminished daytime demand on computerized facilities is not consistent with the most efficient use of processing equipment.

A further difficulty is that in an offline environment procedures must be set to deal with the return of dishonoured items. Such procedures are costly and may outweigh any saving realized from the elimination of an online stage. For all these reasons banks in Canada tend to disfavour all offline options.

A model allowing retailers to control retail data as well as maintain their cardholder base while entrusting banks with the PIN controlled verification is being worked out in Canada. PIN information is to be stored by the account holder in the magnetic stripe of a retailer issued card. So far as the payment process is concerned, the card is to be treated as an EFT bank issued debit card. Bank controlled online verification/authorization is thus to be fully exercised.

For the time being, the development of the payment card has not run its full course. It seems though that the magnetic-stripe technology holds the key to future large scale developments. Within this framework, cash disbursements at cash dispensers must be premised on interactive verification as well as online authorization. For point-of-sale terminals, online authorization may be dispensed with. However, for a debit card, such a course may not be desirable and is disfavoured by banks in Canada. Indeed, if the objective is to assimilate the card funds transfer to cash payment, online authorization is to be exercised in point-of-sale transactions as well.

3. The Network — Terminals, Computers and Sharing Models

A retail payment system in which the communication and transfer of value in economic exchange depend wholly, or in large part, upon electronics is known as a retail EFT system.[28] The public access terminal, known also as an automated banking machine ("ABM") or automated teller machine ("ATM"), which includes the cash dispenser ("CD"),[29] and POS equipment, are two of the "three pillars" of a retail consumer-oriented EFT system.[30] However, the terminals at the point of origin are only the tip of the iceberg. The network interconnecting the terminals and connecting them to the appropriate databases is most important.[31] Typically, a comprehensive system includes a card, a terminal, communication lines, a switching computer, and databases that maintain the individual account information.[32] Ideally, such a retail EFT system may operate in a realtime environment,[33] and in any event is more than a collection of stand-alone electronic cash registers.[34]

ABM and POS terminals are card reading terminal devices. Except in conjunction with cash registers at large department stores where the embossed credit card numbers are keyed in by the clerk at the point of sale, only second and third generation cards, storing data either in magnetic stripes or as smart cards, and capable of being used as EFT debit cards, can be activated by such terminals. In the context of magnetic-stripe technology, each terminal is connected by telecommunication links to a host computer facility. A cardholder activates an ABM by inserting the

---

[28] See Chorafas, *supra*, footnote 2, at p. 237.

[29] More accurately, the CD, ATM and ABM are three generations of the public access terminal. *Cf.* Chorafas, *ibid.*, at pp. 192-5. In the Canadian terminology, "ABM" denotes "ATM".

[30] Chorafas, *ibid.*, at p. 87. The third pillar is home banking, facilitating communication from the customer's home. As a rule, third party payments initiated from home proceed offline, except that the payer's account may be debited online. For a skeptic assessment on the future of home banking, see Chorafas, *ibid.*, Chapter 15. Home banking has not taken off in Canada. For a positive outlook, see "The Impact of Home Information Systems on Canada's Payment System: A Call for Action", a paper by W. Javor of Bell Canada, May 1989, circulated in the 1989 Conference of the Canadian Payments Association (Quebec City, May 29-30, 1989) where (at pp. 5 and 6) the home computer is expressly analogized to a POS terminal.

[31] Chorafas, *ibid.*, at p. 332.

[32] *Ibid.*, at p. 235.

[33] *Ibid.*

[34] *Ibid.*, at p. 308.

card into a card entry slot at the terminal. First he enters his PIN. He then requests the cash withdrawal and selects the account by pressing appropriate buttons. Ultimately the cardholder enters the amount of the requested cash disbursement. Withdrawal limits and designated accounts are provided for in the cardholder agreement. Step by step instructions are displayed on a screen throughout the entire transaction.[35]

A POS terminal is activated by the insertion of the card by the cardholder followed by the merchant keying in the amount at the terminal and by the cardholder entering the account number and the PIN on a PIN pad. This amounts to a request for payment to the seller's account.[36]

In an online environment, a terminal so activated is capable of communicating with the host computer facility to execute the request. Terminals may be equipped with processors capable of performing at-the-terminal verification for cards issued by the bank operating that particular terminal. Some POS terminals are incapable of performing this function and the verification is conducted at a host computer. However, the PIN is always encrypted at the terminal prior to transmission. Authorization for requests made at ABM as well as POS terminals is universally performed at a host computer. In a smart card environment, verification is conducted at the terminal; authorization is usually bypassed, except when it is made at the terminal solely on the basis of limits stored in the card.

Terminals linked to one or more host computers constitute a network. Networks are either self-contained or shared. Self-contained networks are also known as unitary, proprietary, or one party networks. A more refined thinking currently prevailing in Europe and the United Kingdom as to POS networks is that of a "common highway". The concept aims at integrity and flexibility so as to ensure a high level of integration, facilitate smooth

[35] This is a general description, subject to possible variations. See, Goldstein, *supra*, footnote 3, at Chapter VII. Other services which can be obtained at an ABM, such as an online transfer from one account to another, obtaining up-to-date balance information, as well as initiating payment to designated third parties (usually online as to the payer's debit but offline as to the payee's credit), are outside the scope of this article. In facilitating such services the ABM provides similar services to that of home banking (see footnote 30, *supra*).

[36] Again, this is a general description, subject to possible variations. See Goldstein, *ibid.*, Chapter VIII. The separate PIN pad in a POS terminal is designed to maintain cardholder's privacy in entering the PIN.

operation and accommodate a broad range of compatibility among technologies. This requires the establishment of an agreed high standard of security and strict adherence to common technical standards among all participants of the shared network. Each consists of terminals linked to a host computer and is owned and operated by one institution only.[37] For the time being, the POS environment in Canada is characterized by proprietary networks, mostly operating as pilot projects.

"Sharing" is defined as participation in the use, possession or enjoyment of a terminal and some portion of the telecommunication links in common with others.[38] A typical shared environment is created by the merger of two or more proprietary networks.

The host computers of participating institutions in a shared network are connected to each other by telecommunication links either directly or through a central switching computer so as to form a network of the host computers. A shared network thus facilitates the use of a terminal of one institution by the customer of another institution. The respective networks cease to be proprietary since the use of terminals and telecommunication links is shared by all participating institutions.[39]

A shared network is characterized by interbank communication. Where a terminal is linked either directly or through a controller to the host computer of each of several banks,[40] the

[37] Two qualifications ought to be made. First, this definition identifies the ownership and operation of the host computer with ownership and operation of the system. In fact every POS network involves the merchants operating the terminals and cannot be exclusively owned and operated by a bank like ABM networks. However, in most cases, except in connection with large retailers who own terminals which are used also as cash registers, terminals are owned by banks. Second, in a POS network the connection between a terminal operated by a large retailer and the bank host computer may be intermediated by the retailer's own host computer. This intermediation is irrelevant for our purposes.

[38] See two documents issued by the Canadian Payments Association (collectively referred to hereafter as "CPA ABM documents"): (1) *Report on Standards Applicable to Networks of Shared Automated Teller Machines* (June 4, 1986), p. 3 (hereafter "ATM Report"); and (2) *Standards Applicable to Networks of Shared Automated Banking Machines* (March 4, 1987), p. 1 (hereafter "ABM Standards Document").

[39] In principle, networks can be owned and operated exclusively by retailers or other nonbanks. In such systems, only periodic inter-institution settlement is made through the banking system. Cardholders pay either periodically, as in a credit card system, or by authorizing issuers to access accounts (usually periodically and offline). The only nonbank ABM network operating in Canada is operated by a large retailer and is connected to a bank. Most transactions are handled online. In some networks in the United States some large retailers share equally with banks. To keep the analysis relatively simple, these variations are excluded from the scope of this article.

[40] Possibly through the retailer's own host computer, as indicated in footnote 37 (second qualification).

entire design consists of clustered but separate proprietary networks and is not a shared network. Indeed, in such a setting the use and enjoyment of a terminal are shared by more than one bank. Nevertheless, each card transaction does not involve interbank communication. In a POS system falling into such design, the merchant operating the terminal maintains an account with each bank linked to the terminal so that no communication between the terminal and a bank other than that of the merchant is involved. In this sense, no portion of the communication links is possessed, enjoyed or used by one bank in common with others so that, from a transactional point of view, no shared network exists.

A shared network is delineated by its constituent communication links. The institutions running the network must abide by a common set of rules and are referred to as network members. In general, the host computers of the participating network members may be linked to each other either through a central switch or, in a gateway system, by means of direct computer-to-computer communication.[41]

A central switch system is premised on the imposition of minimum bilateral compatibility requirements between each participant and the central computer, and on a centralized organizational structure. A gateway architecture requires a higher degree of multilateral compatibility among all participants, and is more decentralized in its organization. It is more flexible and more responsive to technological enhancements. A central switch system better accommodates an open access policy and is consistent with a fragmented banking system consisting of numerous and diverse institutions. At the same time, the gateway architecture is likely to accommodate a banking system dominated by a small number of large banks.[42]

A variant of the central switch design may offer a direct communication link between a terminal and a card issuer,[43] via the central

---

[41] This is the same as in large-value computerized payment systems. Thus, the New York-based CHIPS is a central switch system. The London-based CHAPS is a gateway system. See B. Geva, "CHIPS Transfer of Funds", [1987] J.I.B.L. 208; and B. Geva, "CHAPS Transfer of Funds", [1988] Lloyd's Mar. & Com. L.Q. 477.

[42] Accordingly, networks in the United States are usually central switch systems, while networks developed in Canada and Australia are gateway systems. As well, the "present thinking" in the United Kingdom was reported in 1984 as in effect premised on a gateway system. See Members of the Bankers' Clearing House, *Payment Clearing Systems: Review of Organization, Membership and Control* (London, Banking Information Service, 1984) (known as "the Child Report"), Appendix 3, at p. 44.

[43] But *cf.* footnote 40, *supra*. The retailer's own host computer may intermediate.

switch, without the intermediation of the host computer of the bank operating the terminal. Such a "direct central switch" design shortens the terminal-to-issuer's communication. However, in this design, control of access is given to a third party rather than to the terminal bank. Since the bank operating the terminal is excluded from the communication route, neither its right against the card issuer nor, in a POS payment, the merchant's right against the bank, is generated in the course of the authorization process. The establishment of both rights requires further communication to the bank operating the terminal: from the switch, usually online; from the terminal, usually in batched messages; or from the card issuer, by means of a wire or any other mode of communication. Furthermore, the exclusion of the bank operating the terminal from the authorization communication route may spell trouble in case of a transmittal error resulting in an amount communicated to the bank being different from the amount received earlier at the terminal. Finally, in the "direct central switch" design, a bank operating POS terminals does not have immediate access to, or control over, retail data. Nor does the terminal bank control the level of service given to the merchant. Consequently, this is not a popular network architecture among banks.

In a shared environment, there are no direct communication links between a terminal of one institution and the host computer of another. Except for in the "direct central switch" design, each terminal is linked to its own institution's host computer. All institutions' host computers are linked to each other, whether in a gateway or central switch system. In the "direct central switch" design, all terminals are linked to the central switch. The central switch is linked to host computers of participating institutions.

In a shared system, network architecture may require, at least in some cases, the intermediation of one or more members in the communication between two member institutions. A shared network may further expand to give access to nonmember participating institutions. Each of them ought to establish its own individual correspondent relationship linking it to a member sponsoring it and intermediating between itself and the network. However, sponsored institutions usually are members since they have a right to use the trademarked logo of the network. In general, intermediation is more likely to occur in a gateway system than in a central switch architecture.

A shared network allows a cardholder of a participating insti-

tution to use a terminal of any participating institution. However, it does not follow that every participating institution operates terminals as well as acts as a card issuer. It is quite common for an institution to be solely a card issuer.

In a shared environment, network rules provide for clearing and settlement among participating members. A member sponsoring a participant clears and settles also for the sponsored institution. As a rule, each participant settles with its sponsor via a correspondent account.

The most comprehensive ABM network of shared terminals in Canada is Interac.[44] It is a "two tiered" gateway system open only to members of the Canadian Payments Association ("CPA")[45] covering more than 6,000 ABMs from coast to coast.[46] It is expected that by 1990 Interac will also encompass POS terminals.

Members of the Interac Association are either chartered or sponsored.[47] Chartered members have developed a system to link their respective proprietary terminal networks by installing a switching device at the computer of each institution. The switching devices act as communication gateways between members' networks of terminals. Each device receives information from its own institution's terminals and passes or receives coded messages to and from other switching devices. A sponsored institution must establish an individual relationship with a sponsoring chartered member. The former can transmit and receive messages only

---

[44] For a general description of the system see "Coast to Coast Convenience" 2:3 Forum (Canadian Payments Association, September, 1986).

[45] Members of the Canadian Payments Association are the Bank of Canada, every bank, every savings bank to which the Quebec Savings Banks Act, R.S.C. 1970, c. B-4 applies, and other depositary financial institutions, such as a central co-operative credit society or a trust company. See s. 4 of the Canadian Payments Association Act, R.S.C. 1985, c. C-21 (hereafter "CPA Act"). Members must meet certain requirements as to financial stability (s. 30).

[46] According to Interac, at the end of December, 1988, there were 6,468 ABMs installed: letter from Interac to the author (February 27, 1989). According to a recent published ABM survey of distribution of terminals by province (as well as types of depositary financial institution), at January 31, 1989, there were altogether 6,176 ABMs. See 5:1 Forum (Canadian Payments Association, March, 1989). As each financial institution keeps installing ABMs, the total is a changing number.

[47] The original 10 chartered members are: Bank of Montreal, Bank of Nova Scotia, Canadian Cooperative Credit Society, La Confederation des caisses populaires et d'economie Desjardins du Québec, Canadian Imperial Bank of Commerce, Canada Trust, Laurentian Bank, National Bank, Royal Bank, and Toronto Dominion Bank. At present there are eight sponsored members: Hong Kong Bank, National Trust, Royal Trust, Caisses Acadienne, Caisses Ontario, Central Trust, Lloyds Bank, and Montreal Trust. Source: letter from Interac to the author (February 27, 1989).

through the latter's gateway. Some sponsored members act only as card issuers.

Interac operates on the basis of online verification and authorization. An immediate cardholder's account adjustment is not necessarily an indispensable feature of the system. Each institution member is free either to act on a realtime basis or to delay action by initially "memoposting" a transaction for an overnight batch update.

Clearing and settlement for transactions exchanged through Interac takes place in the framework of the national clearing and settlement system run by the CPA.[48] Chartered members must be direct clearers.[49] Each charter member debits each other charter member for the daily value of cash dispensed to the latter's customers, including those of its sponsored member(s), at the former's, as well as its sponsored member(s)' ABMs. The debits are entered on the ACSS, and charter members' accounts are adjusted at the Bank of Canada.[50] A sponsored member settles with the charter member acting for it in a correspondent account.

An Interac transaction may thus involve up to four members: two charter and two sponsored members. The charter member which communicates either its own or its sponsored member's authorization guarantees funds to the recipient charter member. Whether funds are guaranteed to the recipient sponsored member is a matter to be agreed upon between that institution and its correspondent charter member.

Institutions which are neither chartered nor sponsored members cannot send or receive payments in Interac. The network exclusively serves Interac Association members.

---

[48] Under the statutory authority "to establish and operate a national clearings and settlements system" provided for by s. 5 of the CPA Act.

[49] "Direct Clearer" is a CPA member that settles for items drawn on or payable by it through a settlement account at the Bank of Canada. It must satisfy certain requirements as to volume and must participate directly in the exchange of items at least at one regional settlement point. "Indirect Clearer" settles through a settlement account with a "Direct Clearer" acting as its Clearing Agent. See definitions in s. 1.01 of By-law No. 3 — Clearing By-law, *Can. Gaz.*, *Part 1*, Vol. 117, No. 3, January 15, 1983, made by the CPA pursuant to authority under (what is now) s. 18(1)(*d*) (and possibly (*e*)) of the CPA Act. At present (June, 1989), there are 15 Direct Clearers (7 of which do not currently act as clearing agents for any other institution) and 129 Indirect Clearers (altogether 144 CPA members). Membership statistics is according to a letter from CPA to the author (June 7, 1989).

[50] ACSS stands for the Automated Clearing Settlement System. Its major functions are logging, reconciling, balancing and reporting the daily exchanges of payment items in the clearing. For an overview, see "Drawdowns and Redeposits", 2:3 Forum (Canadian Payments Association, September, 1986).

A different model for a shared ABM network is that of *Cirrus* and of *Plus*. Each may operate as a cross border network in Canada and the United States. Institution members communicate through a central switch. Network architecture is not that of the "direct central switch" variety. Communication from a terminal to the central switch is intermediated by the host computer to which the terminal is linked. The switch bank holds accounts for directly connected institution members. Settlement is made at the switch bank where accounts are adjusted daily. A Canadian bank may use its U.S. office to transmit funds to the switch bank. Such a network allows a Canadian cardholder to access his account via an ABM of an American bank located in the United States, and increasingly, in other parts of the world.

A universal national POS system exists in Australia. This is a gateway system operated by the four large main trading banks. Any other institution must establish an individual correspondent relationship with a main trading bank. At present, institutions other than the main trading banks participate solely as card issuers. The main trading banks settle daily at the Reserve Bank. A sponsored institution settles in its sponsoring main trading bank in a correspondent account. The system operates in a full realtime environment. It is premised on online authorization followed by realtime debit and credit to cardholder's and merchant's respective accounts.[51]

The environment envisaged by the Canadian Payments Association for POS transactions "is one in which Debit Cards and PINs, whose issuance is controlled by CPA members, employing magnetic stripe technology, are used to initiate on-line authorization and realtime data capture".[52] Instantaneous account adjustment is not required. A similar environment already exists for ABM transactions.[53] The overall framework for ABM a well as for POS transactions is that of a "two tiered" gateway system. Sponsoring institutions must be Direct Clearers which settle at the

---

[51] For a brief reference to this structure see "Payments System Developments in Australia", Reserve Bank of Australia Bulletin 1, July 4, 1988.

[52] EFTPOS Fundamentals, *supra*, footnote 13, at p. 3. For the present experimentation in Canada, along the lines described in the text which follows footnote 37, *supra*, see T. Reiman, "Debut of the Debit Cards" (1989), 96 Canadian Banker 4:18.

[53] For a blueprint, see ATM Report, *supra*, footnote 38, at pp. 5-6. The suggested scenario refers to a debit in the cardholder's account as preceding the cash disbursement.

Bank of Canada and are fully responsible for transactions of their sponsored institutions.[54]

4. Legal Framework for EFT Debit Card Transactions

There is no legislation in Canada governing debit card transactions. Clearing arrangements and settlements fall into the sphere governed by by-laws and rules made by the Canadian Payments Association.[55] Contract governs the respective cardholder-bank, merchant-bank, and cardholder-merchant relationships. Interbank relationships may be governed by contract and network rules. Apart from public law regulation, the rest is common law which may supersede contractual provisions and apply to spheres falling outside the reach of contract, that is, as between parties not privy to a contract.[56]

Pertinent common law rules may be derived from the law applicable to the banker and customer relationship as well as from principles applicable to consumer protection. They may further be dependent on the classification of the debit card transaction into a recognized category of payment mechanisms.

In general, payment mechanisms are either credit or debit transfers. Where the payment instructions are communicated by the paying party directly to this bank, there is a credit transfer. Where the paying party's instructions are communicated to his own bank via the payee, there is a debit transfer. In a credit transfer, the first impact of the payment instructions is a debit to the paying party's account. Funds are subsequently "pushed" to the payee. In a debit transfer, the first impact of the payment instructions is a credit, though usually provisional, to the payee's account. Funds are then "pulled" from the paying party's account.[57]

The cheque payment is a typical debit transfer. Having received the cheque from the drawer, the payee deposits it in his own bank and receives provisional credit. The cheque is then forwarded for collection to the drawer's account from which funds are "pulled".[58]

---

[54] See in general EFT/POS and ABM documents, *supra*, footnotes 13 and 38 respectively.

[55] CPA Act, ss. 18(1)(*d*) (and possibly (*e*)) and 19(1).

[56] Whether CPA by-laws and rules may supersede common law or even statutory rules is outside the scope of the present article.

[57] See in general, B. Geva, "The Concept of Payment Mechanism" (1986), 24 Osgoode Hall L.J. 1, at pp. 6-7.

[58] For cheque clearing in Canada, see Geva, *supra*, footnote 9, at pp. 303-5.

The wire payment is the example par excellence of a credit transfer. It is initiated by the communication of payment instructions from the paying party to his bank. The latter debits the former's account and "pushes" funds which are paid to the credit of the payee's account.[59]

The EFT debit card transaction does not lend itself easily to such classification. Thus, in a POS payment,[60] instructions are communicated to the paying party's bank via a terminal installed by the merchant's bank at the merchant's place of business. Except in the "direct central switch" design, communication to the cardholder's bank is via the merchant's bank. This is consistent with the channels of communication in a debit transfer. At the same time, where the transaction is completed on a realtime basis, the debit to the cardholder's account precedes the credit to the merchant's account, as in a credit transfer. Otherwise, where only online authorization but no realtime account adjustment is involved, the sequence of credit and debit may vary. Where a nonbank issuer verification is involved or in the case of a smart card, credit will precede debit, as in a debit transfer.

In the final analysis, whenever the debit to the cardholder's account is posted on the basis of online authorization and not in response to the credit posted to the merchant's account, the POS payment may be regarded as a credit transfer, regardless of the actual sequence of the respective debit and credit. This analysis distinguishes between the request made through the terminal bank and the payment made by the paying party's bank. Stated otherwise, in transmitting the cardholder's payment request to his bank, in every configuration except the "direct central switch" design (where it is not involved at all), the merchant's bank serves as a mere messenger. Unlike in the cheque deposit, no provisional credit is posted to the merchant's account. The account is only credited upon receipt by the merchant's bank of the online authorization. The original online communication from the terminal ought thus to be understood as instructions from the cardholder directly to his bank which "pushes" funds to the merchant's account. In this scenario no electronic deposit is involved and the

[59] See in general, B. Geva, "The Evolving Law of Payment by Wire Transfer — An Outsider's View of Draft UCC Article 4A" (1988), 14 C.B.L.J. 186, at p. 187.

[60] The classification applies solely to third party payments. Hence, ABM cash disbursements are excluded.

online authorization is an indication of the existence of a credit transfer.

On the other hand, whenever collection from the cardholder is made by means of batch processing, which is always the case where no online authorization exists, the POS payment is a debit transfer. In such a case, credit is posted to the merchant's account and funds are collected or "pulled" from the cardholder's bank.

Unfortunately, the proper categorization of an EFT debit card transaction, either as a credit or debit transfer, does not bring with it a comprehensive identifiable body of law automatically applicable to all facets of the particular debit card payment. Classification may assist us to bring and apply analogies. At the same time, the technological components of a retail EFT system may impact the legal regime in a way that is likely to supersede the initial categorization.

The analysis which follows identifies the function served by each participant in an EFT debit card transaction. Sources of law and substantive applicable rules will then be examined in pertinent interparticipant relationships.

Participants in an EFT debit card transaction may act in various capacities:[61]

1. *Card Issuer:* the institution that issues a card and controls the PIN used to access the account.
2. *Cardholder:* a customer of the card issuer to whom the card and PIN are issued by the card issuer.
3. *Account holder:* the institution that holds the cardholder's deposit account to be accessed by means of the card.
4. *Acceptor:* the person operating the terminal at the point of origin.
5. *Acquirer:* an institution which acquires the data relating to the payment following its entry at the terminal at the point of origin, then passes the data to the card issuer and communicates back the latter's response in the form of either authorization or rejection.
6. *Intermediate Network Connector:* an institution providing communications pathways between the card issuer and the acquirer.

[61] The ensuing definitions draw on POS and ABM documents, *supra*, footnotes 13 and 38, respectively.

The following observations should be made about this definitional framework:

1. In the environment envisaged by the CPA for Canada, the card issuer must be the account holder.[62] It ought to be a depositary financial institution.[63]
2. In a POS payment the acceptor is the merchant and the acquirer is the merchant's bank. In an ABM cash disbursement transaction, the acceptor is likely to be a depositary financial institution.[64] Where such an acceptor is a network member, no separate acquirer exists.
3. In a proprietary network, the card issuer/account holder is the same as the acquirer in POS payment, and the same as the acceptor/acquirer in an ABM transaction.
4. An EFT debit card transaction in a shared network may involve intermediate network connector(s). In the definitional framework, the intermediate network connector is always a depositary financial institution. Any other intermediary, such as a communication carrier, is to be regarded as an agent of its employer.[65]

As indicated, clearing arrangements and settlements constitute a sphere subject to by-laws and rules made by the Canadian Payments Association. Contract and network rules govern all aspects of interbank relationships not governed by CPA by-laws and rules, including the positions of the operator of a central switch, clearing house, or communication carrier. In general, norms adopted by interbank contracts, network rules, and CPA by-laws and rules are likely to be comprehensive and detailed. Furthermore, interbank relationships are typically reciprocal and are subject to an autonomous regime. Accordingly, general law has little to say about interbank relationships.[66]

---

[62] But this is not necessarily the case in the United States. See the paragraph which follows the one containing footnote 27, *supra*.

[63] For an explanation, see footnote 25 and the text around it. Two exceptions are recognized. First, the issuer can be one related with the account holder such as a central cooperative society. Second, as discussed in the paragraph preceding the last one in Part 1, a depositary financial institution may provide (and control) a PIN to a card issued by a retailer. In the context of the payment system, the bank ought to be regarded as the issuer of the card. The two exceptions are thus more apparent than real.

[64] That is in a depositary financial institution-operated system such as Interac. *Cf.* footnote 39, *supra*.

[65] *Cf.* Geva, *supra*, footnote 59, at p. 212 (on Draft UCC Article 4A).

[66] Except perhaps in relation to competition. *Cf.* B.R. Campbell, "The Competition Act — The Special Case of Banks" (1986-87), 1 B.F. L. Rev. 225.

Contract governs the cardholder-acceptor relationship. However, so far as the debit card transaction is concerned, most contract terms are likely to be implied and derived from the other relationships whose regulation is quite detailed.

The merchant-acquirer and the cardholder-card issuer/account holder relationships are governed by the law of banker and customer. This branch of law focuses on the bank account and the banker's responsibility in following the customer's instructions as to incoming and outgoing funds to and from the account. In this branch of law, common law rules are supplanted and even superseded by detailed contractual provisions.[67]

The merchant-acquirer relationship is thus predominantly contractual. However, it is not characterized by intensive mutuality and is not autonomous in the same way as the interbank relationship is. Hence, contractual terms may be subject to some scrutiny. To some extent, the bargaining power of banks may be offset by the combined power of retail organizations. In the final analysis, the merchant-acquirer contractual relationship is not immune from legal scrutiny. In practice, however, the scrutiny may be quite minimal.

The cardholder-card issuer/account holder relationship is governed by contract. In some countries it is also subject to a detailed regulatory scheme which either supersedes or imposes contract terms. In the United States it is done by statute[68] and by regulation.[69] In New Zealand there is a binding Code of Practice negotiated by the government. In Australia the banks voluntarily abide by a set of procedures recommended by the government.[70] These procedures provide standards for the availability and disclosure of terms and conditions applicable to the use of debit cards, as well as to changing such terms and conditions; the availability of paper records and periodical statements for debit card transactions; cardholder's liability for an unauthorized transac-

---

[67] Recognition of the contractual nature of the banker-customer relationship goes back to *N. Joachimson v. Swiss Bank Corp.*, [1921] 3 K.B. 110 (C.A.), at p. 127, *per* Atkin L.J.

[68] Electronic Fund Transfer Act, 15 U.S.C.S. (Supp., 1978), §§ 1693 *et seq.*

[69] Regulation E, 12 C.F.R, Part 205.

[70] The Australian perspective (with a reference to New Zealand as well) is set out by D. Harland in "Developments in Electronic Funds Transfer Systems and the Consumer — an Australian Perspective" (1989), 15 C.B.L.J. 259. The text of the Recommended Procedures is reproduced in the *Second Report of the Working Group Examining the Rights and Obligations of the Users and Providers of Electronic Funds Transfer Systems* (Canberra, Australian Government Publishing Service, 1986), pp. 32-44.

tion; card issuer's liability in cases of technical malfunction; error and dispute resolution procedures; deposits in electronic terminals; inability of networking arrangements to deny cardholders direct remedies against card issuers; audit trails; and privacy. No regulatory scheme of any nature exists in Canada. As a result, the cardholder-card issuer/account holder relationship remains predominantly contractual.[71]

Five contentious consumer protection areas relating to the cardholder's position have been identified. They are disclosure and billing practices, countermand of payment, liability for unauthorized use of the card, recovery of loss resulting from communication breakdown, and dispute resolution.

Disclosure and billing practices are traditional concerns of consumer protection legislation. These concerns are not unique to debit card transactions and have long been recognized in the credit cards area.

As for countermand of payment, it is almost universally accepted that once authorization is given, or at least communicated to the terminal, a debit card payment to a merchant cannot be countermanded. Similarly, any debit card payment with respect to which the NSF risk is assumed by the card issuer ought to be irrevocable. No such certainty exists in relation to a debit card payment for which the card issuer only guarantees authenticity of the card use, that is, provides verification alone. In principle, such payments ought to be countermandable until collection, exactly like cheque payments are.[72] However, no specific legislation covers it.

On a policy level, one may raise the question whether even an irrevocable debit card payment ought not to be subject to charge-back powers in a specified set of circumstances, as for example where there is a dispute between the cardholder and the merchant. No regulation to that effect is known to me in the debit card area.[73] In general, such a scheme would be inconsistent with the finality of the debit card payment, that is, to its assimilation to payment in cash.

The third point, that of liability for unauthorized use,[74] may be

---

[71] See in general A. Chant,"The Automated Teller Machine — A New Consumer Bank Relationship" (1986-87), 1 B.F. L. Rev. 99

[72] Under s. 167(*a*) of the Bills of Exchange Act.

[73] This is unlike the credit card area: see, *e.g.*, s. 170 of the federal Fair Credit Billing Act of 1974, 15 U.S.C.S. (1975), § 1666i.

[74] In general, and without purporting to define the term comprehensively, "unauthorized

regarded as the most contentious. So far as a card issuer is concerned, the insertion of the card at the terminal, accompanied by entering the correct PIN, is a valid authentication of the payment instructions subsequently given. Since prudence requires that the PIN should not be recorded by the cardholder on the card or next to it, any knowledge by an unauthorized user of the PIN must have come from the cardholder, either willingly or by negligence. This reasoning leads to the allocation of losses incurred by the unauthorized use to the cardholder. There is however a broad consensus today that even assuming cardholder's responsibility notice given to the card issuer of the loss or theft of the card should block the possibility of subsequent use of the card. Accordingly, loss incurred by virtue of unauthorized use subsequent to the notice ought to be borne by the card issuer.

However, consumer advocates question whether the mere existence of unauthorized use is necessarily the cardholder's fault. Some question reliability of bank handling procedures of PIN information as well as the level of integrity of bank systems.[75] A more broadly shared conviction is that if fault is to determine responsibility, the bank's behavior must also be taken into account. Sophisticated crime may be facilitated by bank negligence. Moreover, the mere ability of a stanger to learn a PIN by observing the dialling pattern of a cardholder may be the result of a defective terminal design.

Consumer advocates also argue that losses created by a sophisticated criminal victimizing an innocent cardholder cannot be attributed to the latter's fault and ought to be fully absorbed by banks as better risk bearers. One such case is that of obtaining the card by false pretence from an unsuspecting cardholder by a criminal who has learned the PIN by observing the dialling pattern of the cardholder.[76] Another case is the installation of a bogus terminal.[77]

---

use" corresponds to the use of a stolen card by an unlawful possessor. In fact, there is the additional problem, not discussed here, of use in excess of authority.

[75] For allegations of "robotic thefts", that is "episodes involving the erroneous debiting of cards in apparently inexplicable circumstances", in the early days of ATMs in the United Kingdom, see M. Karmel, "Procedure and Evidence: The Maintenance of Transaction Records: Proving the State of Account in EFT Transactions", in R.M. Goode, ed., *Electronic Banking* (London, Institute of Bankers and Centre for Commercial Law Studies of Queen Mary College, 1985), at pp. 50-1, quoting from the National Consumer Council's 1983 report on banking services and the consumer.

[76] See, *e.g.*, *Ognibene v. Citibank, N.A.*, 446 N.Y.S. 2d 845, (N.Y. City, Civ. Ct., 1981); *State of New York v. Citibank*, 537 F. Supp. 1192 (D.C., S.D., N.Y., 1982).

[77] "A bogus terminal is an unauthorized card-accepting device and PIN entry device used

In the final analysis, consumer advocates challenge altogether the application of fault notions to the determination of cardholder's exposure. First, they argue, litigating negligence issues with respect to relatively small amounts may lead to gross inefficiency. Second, human shortcomings are not to be overlooked even in the electronic age. Thus, they argue, some cardholders are bound to be forgetful and sloppy in handling PIN information. Banks ought to treat losses created thereby as part of the costs of the electronic revolution and be willing to absorb them. In fact, the argument continues, the allocation of fraud losses to banks would provide them with further inducement[78] to improve security and identification procedures[79] and thereby reduce losses altogether. A variant of this school of thought would be prepared to fasten on the customer liability for a relatively small amount out of the initial loss up to notification as an incentive for better card and PIN protection as well as prompt loss notification.

Solutions to the problem of unauthorized use vary. They reflect different compromises between competing approaches. The American statutory solution is the most favourable to consumers. The cardholder's exposure is limited either to $50 or to $500, depending on the time when the card issuer is notified of the loss of the card.[80] Exposure extends solely for loss from unauthorized use occurring prior to notification of the loss to the card issuer. These limits exist irrespective of the cardholder's negligence in

---

for fraudulent purposes to capture card information and a customer's PIN. This information can then be used to manufacture a fraudulent card, which in conjunction with the correct PIN, could then be used to access a customer's account". See EFTPOS Consultative Process, *supra*, footnote 13, at p. 16.

[78] Indeed, loss minimization may be high on the agenda of banks under any regime for the allocation of unauthorized use losses, if for marketing purposes alone.

[79] Alternatives to PIN technology capable of identifying an individual user which are currently known include voice or photograph recognition systems, fingerprint or handprint verification, and signature dynamics (where the characteristics of the signature are digitized and stored for comparison in the computer system). All are technologically feasible though not necessarily cost effective. As well, they may be perceived as a threat to cardholders' privacy. See, J.V. Vergari and V.V. Shue, *Checks, Payments and Electronic Banking* (New York, Practising Law Institute, 1986), pp. 542-3.

[80] Reg. E., *supra*, footnote 69, § 205.6. Exposure is unlimited only for unauthorized transfers which follow the failure to notify earlier unauthorized transfers that appear in a periodic statement.

maintaining PIN secrecy, but not where the cardholder furnished the wrongdoer the "means of access" to the account.[81]

The Australian Recommended Procedures limit the cardholder's exposure to $50 prior to notification of the loss, provided the cardholder has not contributed to the loss, as for example, by failing to maintain PIN secrecy.[82] The Canadian contractual position is not uniform. Under one standard contract, consumer exposure extends to the amount of the actual loss incurred by the unauthorized use up to notification. Under another, it is limited to $50 up to notification, though subject to PIN confidentiality being maintained by the cardholder.[83]

The fourth point, that of the cardholder's right to recover for loss resulting from communication breakdown, raises the question of liability for consequential loss. The Australian Recommended Procedures allow recovery for consequential damage except where "the cardholder should have been aware that the system or equipment was unavailable for use or malfunctioning".[84] In principle, American common law recognizes liability for foreseeable consequential loss resulting from interbank communication breakdown.[85] This exposure will be eliminated in nonconsumer wire payments if UCC Article 4A becomes law.[86]

The final contentious issue relates to dispute resolution. Two separate questions arise. The first involves access to justice due to economies of scale. Many disputes are likely to involve amounts that are too small to justify legal costs. At the same time, the potential for aggravation and ill feeling is quite enormous. Second, there is a serious question about the onus of proof. Does the bank computer printout indicating an authenticated card use constitute *prima facie* evidence of such use? How can such evidence be challenged by an aggrieved consumer alleging unauthorized use, and how can he prove maintenance of complete confidentiality as to the PIN? In *Judd v. Citibank*[87] a cardholder

---

[81] According to *Ognibene*, *supra*, footnote 76, at pp. 847-8, "means of access" include the card and the PIN.

[82] Sec. 5.5 of the Recommended Procedures, *supra* footnote 70.

[83] This is based on Chant, *supra*, footnote 71, at p. 102 and Appendix. No independent survey has been made in connection with this article.

[84] Section 6.2 of the Recommended Procedures, *supra*, footnote 70.

[85] *Evra Corp. v. Swiss Bank Corp.*, 673 F. 2d 951 (7th Cir., 1982), revg 522 F. Supp. 820 (D.C. N.D. Ill., 1981).

[86] See Geva, *supra*, footnote 59, at pp. 223-4.

[87] 435 N.Y.S. 2d 210 (N.Y. City, Civ. Ct., 1980).

sued her bank for the return of moneys allegedly charged to her account erroneously. Bank computer printouts documenting cash withdrawals were met by the cardholder's alibi as to all relevant times. She further testified that the card had always been in her possession and that she had maintained complete PIN confidentiality. The court held in her favour and "[was] not prepared to go so far as to rule that where a credible witness is faced with the adverse testimony of a machine, he is as a matter of law faced also with an unmeetable burden of proof". Taking into account "the tales of computer malfunctions that we hear daily" and the testimony of the bank's own witness confirming "physical malfunctions of the very system in issue", the court held for the cardholder.[88] Nevertheless, the question cannot be considered as being finally resolved along these lines.[89]

Contract law is quite inadequate in explaining the position of the cardholder or the merchant against an institution[90] other than his own respective bank. Indeed, a transmittal error as well as the failure to communicate either a payment request or positive verification/authorization may be attributed to technical malfunction or any other factor which may happen to be outside the control of a bank with which the party at loss is in privity. Under those circumstances, may the merchant sue such parties as the card issuer or an intermediate network connector? May the cardholder sue parties such as the acceptor, acquirer or an intermediate network connector? Alternatively, is the merchant limited to an action against the acquirer, and may the cardholder sue only the card issuer?

The common law has not answered these questions with great precision. Indeed, in a debit transfer, an intermediary bank is an agent of the bank of deposit.[91] In a credit transfer, an intermediate transmitting bank is an agent of the originating bank. It was held in England, in the latter context, that the paying customer may not sue the intermediate transmitting bank. That is, a principal may

---

[88] *Ibid.*, at p. 212.

[89] For example, the cardholder's testimony as to circumstances surrounding the use of the card was not accepted in *Feldman v. Citibank*, 443 N.Y.S. 2d 43 (N.Y. City, Civ. Ct., 1981).

[90] As well as against the switch, any intermediate clearing facility, or a communication carrier.

[91] *Cf.* in general, *Barclays Bank plc. v. Bank of England*, [1985] 1 All E.R. 385 at p. 392, *per* Bingham J.: paying bank as a subagent of the presenting bank in a cheque collection.

not recover directly from a subagent employed by his own (the principal's) agent.[92] The contrary view has prevailed in the United States.[93]

The better view appears to be the one limiting the number of potential defendants. That is, except for when bank insolvency is involved, no policy is served by allowing a bank customer, be it the cardholder or the merchant, to sue a bank other than his own. Among themselves banks may set their own rules designed to assign liability to the bank at fault. This should be of no concern to the customer who has suffered loss. Needless to say, such a scheme presupposes two conditions. First, that banks are not allowed to disclaim liability by contract for fault of their own or for the fault of other network participants. Second, rules of evidence must assist a plaintiff-customer suing his bank on the basis of an occurrence for which another bank is responsible. Thus, in the final analysis, liability for communication breakdown and interruption may require legislation.

Another area involving no direct contractual privity is that of the verification/authorization communication. Is the acceptor/-merchant entitled to the benefit of this communication and can he fasten liability on the card issuer, on the intermediate network connector, or only on the acquirer? Does liability depend on the chain of communication as determined by each network configuration? Under theories of collateral warranties as well as of liability for negligent statements, avenues of recovery may also be constructed against parties not in contractual privity.[94] At the same time, in the context of the EFT debit card transaction, each bank's liability is discharged by payment along settlement lines and not directly to the merchant, even as the beneficiary of the promises under the verification/authorization. Except for the "direct central switch" design, the gains from other sources of liability, besides that of the acquirer, are far from clear. Still, in all configurations, are intermediate connectors more than conduits for messages? Does the acquirer guarantee payment prior to receiving settlement?

---

[92] *Royal Products Ltd. v. Midland Bank*, [1981] 2 Ll. L. Rep. 194 (Q.B.). See also Geva, *supra*, footnote 59, at pp. 190-1 and references there.

[93] *Evra*, *supra*, footnote 85.

[94] See, *e.g.*, *Shanklin Pier Ltd. v. Detel Products Ltd.*, [1951] 2 K.B. 854 (collateral warranty); *Hedley Byrne & Co. Ltd. v. Heller & Partners Ltd.* [1964] A.C. 465 (H.L.) (negligent statement).

No obvious answers exist. The common law may provide a framework for dealing with these questions. However, legislation is likely to provide a more comprehensive and carefully tailored solution.

Finally, issues concerning discharge and time of payment ought to be considered.

To begin with, the reliability and the operationability of a POS system ought not to be warranted by either party to a POS payment. Stated otherwise, the failure to complete a POS payment due to system failure should not be regarded as a breach of contract by either cardholder or merchant. Upon such a failure, an alternative mode of payment ought to be pursued, failing which a fully executory transaction ought to be cancelled. Loss generated by either side may be recoverable from his respective bank.[95]

Once a POS payment is carried out so that a confirmation is obtained at the terminal, what are the respective rights of the cardholder and merchant? Has the cardholder been discharged, either conditionally or absolutely? What are the merchant's rights and against whom? The law governing these questions has not so far been fully developed.[96] The following is a tentative outline setting out a proposed optimal model.

The receipt at the terminal of a confirmation of a guaranteed debit card payment generates an absolute discharge of the cardholder's indebtedness to the merchant. When the acquirer receives settlement for the guaranteed debit card payment, its amount becomes part of the funds in the merchant's bank account and any claim to it as a separate item is fully discharged. Whether the merchant stands in a similar position even earlier, by obtaining an absolute right but exclusively against the acquirer, is a question yet to be resolved. The determination of this issue depends on the merchant's position towards the authorization originating from the card issuer.[97] Is he entitled to its benefit? Until what point? Is this entitlement affected by such circumstances as bank failure?

The receipt at the terminal of a nonguaranteed debit card payment generates a conditional discharge of the cardholder's

---

[95] For bank liability for communication breakdown see the paragraph containing footnotes 84 to 86, *supra*.

[96] For a credit card payment as an absolute discharge of the cardholder's indebtedness to the merchant, see *Re Charge Card Services Ltd.*, [1988] 3 W.L.R. 764 (C.A.).

[97] As discussed in text around footnote 94, *supra*.

indebtedness to the merchant. The item is then deposited by the merchant to his account at the acquirer for collection from the card issuer/account holder. A provisional credit may be posted to the merchant's account upon deposit. It firms up upon the obtainment of settlement by the acquirer. In principle, a nonguaranteed card payment is the equivalent of a cheque payment.[98] It is thus governed by similar rules.[99]

5. Conclusion

In a historical process which started with coins and bank notes and continued with cheques and credit cards, the EFT debit card is the newest method of retail payment.[100] It is likely to expand primarily as a mode of payment to retailers who normally do not accept credit cards, such as grocers, as well as among some consumers. Such consumers may not qualify to receive credit cards. Others hold credit cards but prefer to use them selectively in order not to exhaust available credit lines or for any other reason. In retail transactions, the debit card is capable of serving as cash. It is considerably more sophisticated than the bank note or the coin, but is nevertheless not subject to a comprehensively developed body of law.[101]

In selecting the appropriate avenue for the development of debit card law two extremes should be avoided. First, there is no need to rush in with a detailed statute that, by being geared solely to existing technology, may arrest development. Flexibility is an important feature to be retained in this area of law. Second, the case by case process of the common law may be too slow to be trusted in such a fast-moving area.

In substantive matters, the by-law and rule-making power of the CPA is limited to the operation of the national clearing and settlement system.[102] However, the association is also entrusted with a statutory mandate "to plan the evolution of the national payments system".[103] Needless to say, such a mandate can be

---

[98] Though with one enhancement, that is the card authentication serving as the verification of the cardholder's authority.

[99] This does not ensure certainty. For an effective return of a dishonoured cheque after the time permitted under clearing rules, see *National Slag v. C.I.B.C.* (1982), 140 D.L.R. (3d) 473 (Ont. H.C.J.), affd 19 D.L.R. (4th) 383*n* (C.A.).

[100] For this observation see Chorafas, *supra*, footnote 2, at p. 294.

[101] *Ibid.*, at pp.336-7.

[102] See ss. 18 and 19 of the CPA Act. Other enumerated items relate to the administration of the association itself.

[103] CPA Act, s. 5.

carried out successfully only as a genuinely co-operative effort between the CPA and its member depositary financial institutions on the one hand, and the other participants in the payment system (such as retailers and consumers) on the other. In fact, a co-operative process is well underway. It should produce an agreed set of rules and terms to be introduced in standard form agreements. It should also generate interbank rules and practices in areas not exclusively limited to clearing and settlement. The process is thus a welcome development.

Whether a CPA dominated process is the most appropriate broadly based framework to generate consensus on the rules applicable to debit cards, and whether other government departments, such as Consumer and Corporate Affairs ought not to participate, are questions outside the scope of this article. Furthermore, it remains to be seen whether the outcome of any voluntary process will eliminate the need for compulsory regulation. None the less, any proposed scheme should not bypass but be the culmination of such a process, taking into account and building on what has been achieved through it.