Reimagining E-Money:
Its Conceptual Unity with other Retail Payment Systems[*]

By: **Benjamin Geva**[**] **and Muharem Kianieff**[***]
August 8, 2002

Contents: *[1] The product in a context [2] Does e-money constitute "money"? [3] Is the SVP a "payment mechanism"? [4] Does the debt owed by the issuer constitute a "deposit"? [5] Does monetary value on SVP qualify for deposit insurance? [6]Does payment by SVP involve a "funds transfer"? [7] Could e-money nevertheless be "money" and is the SVP different from the debit card? [8] Does payment by SVP constitute "credit- push" or "debit-pull", and does it matter? [9] An outline of the payment law applicable [10] The need to balance privacy with law enforcement objectives [11] Consumer protection issues and principles [12] Concluding observations.*
=+=

1. The product in a context

The term "electronic money" or "e-money" is used to denote value paid in conjunction with a wide variety of electronic retail payment mechanisms, often described as "stored-value" products ("SVPs"). On each such product, a record of the value available to the consumer is stored on an electronic device kept in the consumer's possession. SVPs are contrasted with access products that allow consumers to access "value", or more specifically, funds, kept in their accounts, a record of which is retained by the bank. Such access is given by instructions either embodied in paper, e.g. the

[*] This Paper is developed from an earlier one presented by Professor Geva at *A Global Legal Framework for E-Finance* of the Centre for Commercial Law Studies (International Financial Law Unit) Queen Mary College, University of London and the British Institute of International and Comparative Law to be published in the 2001-2002 Yearbook of International Financial and Economic Law.

[**] Professor of Law. Osgoode Hall Law School of York University, Toronto, Canada. Email: bgeva@yorku.ca

[***] D. Jur. Candidate. Osgoode Hall Law School of York University, Toronto, Canada. Email: muharemkianieff@osgoode.yorku.ca

[****] Financial support through a Faculty Grant of Centre for Innovation Law and Policy, University of Toronto Faculty of Law, and research assistance of Osgoode student, James R.G. Cook is acknowledged with gratitude.

cheque, or by electronic means, e.g. the debit-card, initiating an electronic funds transfer ("EFT"). An SVP may be in the form of either "electronic purse", in which the value is "loaded" on a card, or "digital cash", in which value is "loaded" on computer-software. Typically, a card-based product provides the consumer with an integrated-circuit (IC) card containing a microprocessor chip, namely a "smart card", which is used at a public-access terminal, such as an ATM/ABM or at a point of sale (POS). At the same time, a software-based product operates via a personal computer, namely, a terminal to which the consumer has proprietary access.[1]

An SVP product may either be single or multi-purpose, may operate in either closed or open systems, may or may not be restricted to a geographic area (small or big), may be single or multi-currency, and may be issued by either a single or multiple-issuer. As well, an SVP product may be offline unaccountable, offline accountable, or online accountable.[2] When neither transaction information nor resulting balance is transmitted from the product to a central facility, the product is ***offline unaccountable***. Where transmission to a central facility occurs, the product is accountable; it is ***online accountable*** when transmission is simultaneous with each use and is ***offline accountable*** when information is transmitted to the central facility only periodically. In fact, an online accountable is indistinguishable from an access product. It is only an offline unaccountable system that is fully stored-value and is not an access product. An offline accountable system is hybrid, combining features of both types of products.

---

[1] See in general, Bank for International Settlements, "Security of Electronic Money", (CPSS Publications No. 18) (Basle: Aug . 1996); Bank for International Settlements, "Implications for Central Banks of the Development of Electronic Money" (Basle: Oct. 1996); and S. Chinoy, "Electronic Money in Electronic Purses and Wallets" (1997), 12 BFLR 15.

[2] This division follows that which was proposed by the US Federal Reserve Board in Electronic Fund Transfers (Proposed Rules), 61 Fed. Reg. 19, 696 (May 2, 1996).

Parties to an e-money payment are the issuer, the payor, the payee and the acquirer. Other participants in the transaction are a system operator and, possibly, one or more intermediary institutions. In a single issuer system the issuer is usually also the system operator. In a typical scenario, value issued by the issuer (possibly through a participating institution) and loaded on the payor's device is transmitted to the payee's device or terminal from which it can be deposited to the acquirer and ultimately presented to the issuer for redemption through normal banking channels. The payee may be either a merchant or, in a "person-to-person" payment, another consumer.

Some view the SVP as the ultimate saviour to deliver the long-waited cashless society.[3] At the same time, market penetration of e-money products has not been all that impressive and decisive as originally hoped by their promoters. Undoubtedly, confidence in the reliability and security of the products, in conjunction with adequate legal protections, are likely to enhance the level of acceptance. Nevertheless, doubts persist as to the strength of the business case underlying the SVP. Possibly, particularly in developed economies, consumer needs are well met by the existing mix of access devices, credit and debit facilities, and cash, so that the need for stored-value products are not all that obvious. Presumably, SVPs are likely to flourish in circumstances where inadequate communication facilities preclude the efficient development and use of access products.[4] Or else, they are likely to be popular where cash in correct denominations is

[3] For e-money as the culmination of the evolutionary process of payment media see e.g. O.E. Akindemowo, "The Fading Rustle, Chink and Jingle: Electronic Value and the Concept of Money" (1998), 21 UNSW LJ 466. A visionary view of private electronic currency systems is presented by KL. Macintosh, "How to Encourage Global Economic Commerce: The Case for Private Currencies on the Internet" (1998), 11 Harvard Journal of Law and Technology 733. See also M. Kianieff, "Show Me the Money! A Critical Evaluation of Laissez-Faire Internet Currencies" (2002), 17 BFLR 215.

[4] Generally speaking, inadequacy of communication facilities may reflect the general situation in a given economy. Alternatively, it may be inherent in the nature of the particular business establishment, as for

not easily available, whether as a means of payment or receipt of change. As well, as a repetition of the historical evolution of the multi-purpose credit card, a business case for a multi-purpose product may be substantiated in an environment in which single purpose products, such as telephone and subway cards proliferate. Finally, SVPs may be given a chance to prove their efficiency in an environment where payment mechanisms, including cash, are priced and respective users are made to bear their full cost.[5]

Regardless, the operation of SVPs has raised interesting legal issues. The significance of these issues goes beyond the products themselves and underlies fundamentals relating to payment mechanisms, particularly in the context of retail payment systems.[6] The ensuing discussion is an analysis of such issues and will attempt to use existing legal concepts to show how they can be used in the context of E-Money and where they may have difficulty being used. Issues to be explored relate to the concept of money, the meaning and scope of the payment mechanism, the legal nature of the deposit as well as of the funds transfer, whether deposit insurance can be applied to SVPs, the distinction between credit-push and debit-pull funds transfers, payment laws which apply to SVPs (in this context, the feature of a guaranteed payment is highlighted), consumer privacy, needs for law enforcement and consumer protection principles that can be applied.

---

example, a moving one, such as a taxi. Finally, the cost of communication may be prohibitive due to either distance or low value of the transaction.

[5] In fact, costs are associated with all payment mechanisms. This includes the cash payment system, as the distribution and upkeep of cash in quantity and quality required to meet actual demand is quite an extensive operation. However, the cost of the cash system is not borne directly by cash users and it is conceded here that whatever economic justification may exist, it may politically be inconceivable to envision such costs being passed on to users.

[6] For e-money products and selected review of issues see also ABA's Task Force on Stored-Value Cards, "A Commercial Lawyer's Take on the Electronic Purse: An Analysis of Commercial Law Issues Associated with Stored-Value Cards and Electronic Money" (1997), 52 Bus. Law. 653; and L. Edgar

2. Does e-money constitute "money"?[7]

Economists define money as anything that is widely accepted in payment for goods, used as a medium of exchange, and expressed as a standard unit in which prices and debts are measured.[8] Such a conception[9] was favourably received in *Moss v. Hancock*[10], in which "money" was defined to mean "that which passes freely from hand to hand throughout the community in final discharge of debts … being accepted equally without reference to the character or credit of the person who offers it and without the intention of the person who receives it to consume it …".

Mann finds the adoption by lawyers of the economic point view as unsatisfactory. In his view, the economic definition is broad enough to cover mere bank account balances, which is unacceptable to the lawyer. For Mann, "in law, the quality of money is to be attributed to all chattels which, issued by the authority of the law and denominated with reference to a unit of account, are meant to serve as universal means of exchange in the State of issue".[11] E-money is not a chattel, and if for this reason alone it will not fit into Mann's definition.

Nonetheless, it seems that Mann unjustifiably both expands the economic definition and restricts the legal one. Thereby, he introduces an unnecessary gap that does not really exist. The economic inclusion of balances in demand deposits focuses on their

---

"Electronic Money", in C. Reed, I. Walden and L. Edgar (eds.), *Cross-Border Electronic Banking* 2nd ed (London, Hong Kong: LLP, 2000), 201.

[7] For this aspect, see B. Crawford, "Is Electronic Money Really Money?" (1997), 12 BFLR 399.

[8] See for example, D.H. Robertson, *Money* (Chicago: University of Chicago Press, 1962), 2-3.

[9] As specifically taken from the "Money" entry in the Encyclopaedia Britanica, citing F.A. Walker, "Money, Trade, and Industry" p. 4.

[10] [1899] 2 QB 111, 116.

[11] F.A. Mann, *The Legal Aspect of Money*, 5th ed. (Oxford: Clarendon Press, 1992), 8, and see in general, at 5-28.

availability for immediate withdrawal as money. In other words, it refers to the quantity of money and not the quality of what constitutes money; it does not address the mechanism that converts such balances to a medium of exchange. As for the legal definition, the chattel requirement is quite unfortunate. It may be a good description of what has been money from its inception to the present era. Nevertheless, it does not follow that this feature is inherent in the concept of money, particularly in an era in which we move into the electronic age.[12] Similarly, the issue of "money" by the State is a culmination of a historical process. Yet, historically, money has not always been issued by the State, so that even more than the chattel feature, the State issue is not necessarily a feature inherent in the concept of money.[13] True, as the culmination of a historical process, money currently consists of coins and bank notes issued by the State or its central bank.[14] This fact should not colour our own understanding of the concept of money as transcending any particular historical stage in its actual evolution.

Accordingly, the adoption of the economic definition by *Moss v. Hancock*[15] appears to us to be satisfactory. To this end, prima facie, a third party's obligation whose acceptance in payment of a debt confers an absolute discharge on the debt meets this definition, provided it circulates, namely, passes freely from hand to hand, for the sole

---

[12] Similarly, repeated references in earlier cases to the banker's duty to comply with customer's orders on paper instruments such as cheques or other types of bills of exchange should not be taken to exclude a bank's duty to comply with customer's orders submitted electronically. Rather, such references correspond to the particular technology of the time. See e.g. *Joachimson v. Swiss Bank* [1921] 3 KB 110 (CA) where Atkin LJ speaks at 127 of the "added, or superadded … obligation of the bank to honour the customer's *drafts* …", as well as *United Dominions Trust, Ltd, v. Kirkwood* [1966] 1 All ER 968 (CA) where Lord Denning MR states at 975 that "no person can be considered a banker unless he handles *cheques* as freely as cash". Emphasis is added.

[13] For a critical discussion of the state theory of money, see A. Nussbaum, *Money in the Law*: *National and International* (Brooklyn: The Foundation Press, 1950), at 5-10.

[14] For this evolutionary process see B. Geva, "From Commodity to Currency in Ancient History – on Commerce, Tyranny, and the Modern Law of Money" (1987), 25 Osgoode Hall LJ 115.

[15] See text around notes 8-10, above.

purpose of discharging debts.[16] Potentially, e-money could meet these requirements. The fact that it is a medium of exchange only for small denomination transactions is not an obstacle; ceilings for the use of certain currency denominations issued by the State may even be provided by law.[17]

However, for each e-money product to be "money", the stored or loaded value must be a universal medium of exchange, as measured by wide acceptance among creditors. Obviously, the degree of acceptability of each e-money product in the market place is a question of degree, not always easily ascertainable. To that end, a few observations could be made. First, value loaded on a single-purpose product should not be regarded as "money"; rather it is an advance payment for the goods or services to be bought with it. A telephone or New York subway card is a case to the point. Conversely, and this is the second observation, value stored in a multi-purpose product, accepted across a country by numerous merchants, is likely to constitute money.

Third, by itself, the free convertibility of stored value to cash or its equivalent, such as a cash balance in a demand deposit in a bank, does not necessarily indicate that the product is "money". Free convertibility may however be taken into account as part of the overall picture in border cases of restricted or limited use products, in that their value may not otherwise qualify as money. Relevant restrictions or limits relating to the use of an e-money product may be either geographic, such as acceptance solely in one shopping mall or one small town, or by reference to the number of participating creditors. When the degree of restrictions or limits is not considered to be substantial, free convertibility may arguably support the conclusion that the value is "money", even if by itself, the wide

[16] The fulfilment of this "circulation" requirement is re-visited in Section 7, below.
[17] See e.g. in Canada, s. 8(2) of the Currency Act, RSC, 1985, c. C-52, as am. by S.C. 1999, c.4, s.12(2).

acceptability of the e-money product has not been satisfactorily established. Nevertheless, in determining whether stored value of a given e-money product is "money", we submit that in connection with single-use e-money products redeemability to cash will not suffice, while for widely used multi-purpose products it will not be necessary.

Against the view that e-money may be considered money several principal objections are raised. First, e-money does not provide a distinct unit of account. Second, payment with e-money may not be anonymous since the third party obligor may keep a record of each transfer. Third, e-money may be created other than by withdrawal from a reservable deposit with a commercial bank so as to undermine the central bank's hold on monetary policy. Fourth, e-money cannot constitute "legal tender".

All four objections can however be met. Regarding the first two, neither "unit of account" nor anonymity are fundamental requirements for something to constitute "money", as opposed to salient features of what is traditionally recognized today as "money". First, the unit of account could be external to the money itself; that is, money may be required to be stated quantitatively, though possibly by reference to a yardstick that may be external, and not inherent in the money itself. Accordingly, the denomination of e-money in standard units of a national currency does not diminish its position as "money" in its own right. Second, regarding anonymity, historically, the transition from coins to paper money involved a degree of loss of anonymity, since individual banknotes may be identified by number and recorded by a party to a payment transaction. True, in an e-money situation the potential recording is by a third party; this increases the loss of anonymity but such loss may be a mere question of degree. Furthermore, loss of anonymity may not be substantial in the "offline unaccountable" products. On the other

hand, as technology advances, anonymity may further be eroded even with regard to payment in paper money. Such will be the case if individual banknotes are to be identified with radio-frequency identification tags ("RFIDS"), each consisting of a (batteryless) microchip and antenna encapsulated in plastic, capable of being "interrogated" and tracked by a remote reading machine operating at the right radio frequency.[18] Thus, loss of anonymity is quite a precarious test for whether something does constitute "money".

The third objection is based on the thesis that the electronic revolution may lead to a "decoupling" of the operations of the central bank from markets in which financial claims are created and transacted. Stated otherwise, the thesis is that claims people use in order to execute transactions may no longer be restricted to claims backed one-for-one by bank deposits. Rather, they expand to cover claims against commercial players whose issuance is not influenced by the monetary policy of the central bank.[19] However, even if realistic, this objection fails to address the possible transformation of "money". In the process, "money" is being transformed from predominantly an obligation of a central bank to that of any other creditworthy issuer. For example, such an issuer could be the telephone company, assuming value loaded on its cards may be used to purchase goods and services from other retailers.[20] True, the central bank's position may be affected with the evolution of technologies facilitating an increasing expansion of e-money; most

[18] *The Economist* February 9th 2002, p. 69.
[19] See for example, *The Economist* April 27th 2002, p. 75, as to the use of mobile-phone account balances as "stored-value" used to pay for purchases of unrelated goods and services.
[20] For the development of this line of argument see B.M. Friedman, "The Future of Monetary Policy: The Central Bank as an Army with Only a Signal Corps?" (Nov. 1999) 2:3 International Finance 321; B.M. Friedman, "Decoupling at the Margin: The Threat to Monetary Policy from the Electronic Revolution in Banking" (July 2000) 3:2 International Finance 261.

notably, a substantial loss of seigniorage is to be involved.[21] This impact is however no different than that of all non-cash payment systems; it will require the introduction of innovations in the implementation of monetary policy,[22] but does not undermine the character of e-money as "money".

Finally, the fourth objection states that e-money is not "legal tender". Possibly, the identification between legal tender and money is based on Mann who states that "[i]n the absence of the creditor's consent, express or implied, debts cannot be discharged otherwise than by the payment of what the law considers as money, namely legal tender".[23] Nonetheless, not all money is "legal tender"[24]; as explained by Nussbaum, "[l]egal tender … is money which a creditor is not privileged to refuse if it is tendered by a debtor in payment of his debt".[25] While Nussbaum overlooks the creditor's right to stipulate in advance, expressly or by implication, a mode of discharge that excludes payment by legal tender, he correctly points out that there could be "money" which is not legal tender. Historically, banknotes became "money" before they were elevated to "legal

[21] "Seigniorage" is the monopoly profit of the issuer of currency. "When central banks came to be monopoly suppliers of banknotes, seigniorage came to be reflected in the profits made by them and ultimately remitted to their major or only shareholder, the government. Seigniorage can be estimated by multiplying notes and coin outstanding (non-interest central bank liabilities) by the long-term rate of interest on government securities (a proxy for the return on central bank assets)". See BIS, "Implications" (Oct. 1996), above note 1 at 15.

[22] For the broader question of the central bank and monetary policy in the electronic age see in general, C.A.E. Goodhart, "Can Central Banking Survive the IT Revolution" (July 2000) 3:2 International Finance 189.

[23] Mann, above note 11 at 5-6.

[24] See a statement to that effect in *Reference re Alberta Legislation*, [1938] SCR 100, [1938] 2 DLR 81 at 116 (SCR) (Canada). Interestingly enough, under the Canadian Constitution Act, 1867, currency and coinage, the issue of paper money, and legal tender, are enumerated as three distinct headings of federal legislative power. See Constitution Act, 1867 (UK), 30 & 31 Vict., c.3, ss. 91(14), (15) and (20), reprinted in RSC 1985, App. II, No.5. This reflects the distinct nature of each concept.

[25] Nussbaum, above note 13, at 45-46.

tender",[26] and the analogy between the historical private banknote issuing[27] and e-money issuing is anyway quite tempting.

In any event, it is interesting to note that, as concepts, "e-money" and "legal tender" are not inherently incompatible.[28] A case to the point is the decision by Singapore to embrace e-money as legal tender in 2008. Under an "electronic legal-tender system" every merchant and service provider will be required to accept e-money no matter what the price of the goods or services in question.[29] Fundamental features of the plan have not been unveiled yet. For example, it is unclear whether e-money will exclusively be legal tender, so that coins and bank notes are to be eliminated altogether. Furthermore, no information has been provided to identify the issuer of the e-money serving as legal tender. It is possible that the issuer could be the State or one of its organs. The interesting possibility of e-money issued by the State will meet the second objection to viewing e-money as money. However, the scenario of a state-issued e-money is outside the present discussion that focuses on privately issued e-money. For our purposes here, suffice it to say that "e-money" could be "money" without being "legal tender"; actually, it is not inconceivable to have "e-money" as "legal tender", which by itself is "money".

3. Is the SVP a "payment mechanism"?

Elsewhere, one of the co-authors has described a payment mechanism as "any machinery facilitating the transmission of money in the payment of a debt, which enables

[26] Geva, above note 14, at 149 – 151.
[27] Macintosh, above note 3, at 744.
[28] See e.g. J.B. Konvisser, "Coins, Notes and Bits: The Case for Legal Tender on the Internet" (1997), 10 Harvard Journal of Law and Technology 321, proposing government issued e-money as legal tender currency.
[29] See A. Creed, "E-Money to be Made Legal Tender in Singapore", Newsbytes (20001226/Wires Asia, Online, Legal/Singapore/Photo) (26 Dec. 2000), online: www.newsbytes.com.

the debtor to avoid the transportation of money and its physical delivery to the creditor in the discharge of the debt." Its operation was stated to be "premised on the discharge of a debt by virtue of an authorized payment made by a third party, frequently a debtor's debtor", whose debt to the debtor has been simultaneously discharged as well. Payment by the third party may or may not be in specie. While it "is fundamentally a three-party arrangement", a payment mechanism can be expanded to include more participants, thereby "bringing about a further reduction of the physical transportation of money".[30]

The SVP appears to fall into this broad definition. Fundamentally, it operates to discharge the debt owed by the payor to the payee by means of payment to the payee, carried out by means of discharging a debt of the issuer to the payor, and generating a debt owed by the acquirer to the payee.[31]

The view that the SVP is a "payment mechanism" can consistently be held with the position that the e-money loaded on it is "money". Indeed, as indicated, for something to constitute money, it must confer "final discharge" so as to be accepted in payment "without reference to the character or credit of the person who offers it …".[32] Effectively, this means that to be by itself money, a payment mechanism must confer absolute discharge, so that no recourse against the payor is to be available to the payee upon the default of the third party/pay master, in our case, the e-money issuer. For example, no such absolute discharge is presumed to exist in connection with cheques, bills of exchange and letters of credit; "[i]t is common ground that where a debt is 'paid' by cheque … there is a presumption that such payment is conditional on the cheque … being honoured. If it is not honoured, the condition is not satisfied and the liability of the

[30] B. Geva, "The Concept of Payment Mechanism" (1986), 24 Osgoode Hall LJ 1, 3-10.
[31] See A.L. Tyree, "The legal nature of electronic money" (1999), 10 JBFLP, 273.

[payor] to pay … remains".[33] There is however no general presumption of conditional payment, and "[e]ach method of payment has to be considered in the light of the consequences and other circumstances attending that type of payment."[34] As in connection with the credit card[35], it is reasonable to assume that parties intend an e-money product to provide absolute discharge of the underlying debt so that no recourse against the payor is available to the payee upon the default by the issuer. Consequently, as a payment mechanism providing for an absolute discharge, value loaded on an SVP ("e-money") could simultaneously be money as well.

In fact, this is exactly like the case of the traveller's cheque; the latter is a payment mechanism, facilitating the non-cash transmission of money between a traveller and a merchant, which circulates in the discharge of debts so as to constitute "money". As well, historically, one could argue that up to the end of the period during which convertibility to gold or another precious metal had been available, the banknote, that is paper money, was a payment mechanism. And while instruments such as the bank draft or certified cheque may provide an absolute discharge, they do not constitute "money" since they do not circulate.

4. Does the debt owed by the issuer constitute a "deposit"?

With regard to the bank deposit, it is recognized that "[t]he money placed in the custody of a banker is, for all intents and purposes, the money of the banker, to do with it as he pleases", so that "the relation between banker and customer, as far as the pecuniary

---

[32] *Moss v. Hancock*, supra note 10 at 116. See text at n. 9 above.
[33] *Re Charge Card Services Ltd.* [1988] 3 All ER 702 (CA) at 707.
[34] *Id*.
[35] For the credit card as conferring an absolute discharge, see *Charge Card, id.*

dealings are concerned, [is] that of debtor and creditor."[36] As well, with regard to the contract underlying the bank deposit, " it is admitted that there is added, or superadded, an obligation of the bank to honour the customer's [instructions] to any amount not exceeding the credit balance at any material time".[37] This obligation is however subject to the customer's undertaking "to exercise reasonable care in executing his [instructions] …"[38]

Arguably, this description fits e-money loaded on an SVP in the same way that it fits the traditional situation of monetary value deposited to a bank account, except that for value recorded on an SVP the account is "decentralized" or "distributed".[39] To the extent that e-money constitutes "money", it ought to be regarded as deposited in an account with the issuer. It is only in connection with the single-purpose e-money products, and to a point, restricted or limited-use such products, that e-money is to be regarded as an advance payment, or prepayment, for relevant goods or services.[40]

Moreover, one ought to bear in mind that the obligation represented on a SVP is one that is held by an issuer and can be decreased in increments as opposed to being an instrument for which the payee must accept the entire amount. This facet of SVPs has already found expression in a number of U.S. states. For example, the State Banking Department of Texas has stated that it will consider Smart Cards to be subject to the Texas Sale of Checks Act since the issuer will be holding the funds of consumers who will rely on the issuer to ensure that the card will be honoured by merchants when it is

[36] *Foley v. Hill* (1848), 2 HLC 28 at 36 and 45; 9 ER 1002, at 1005 and 1009 (HL).
[37] *Joachimson v. Swiss Bank*, above n. 12 at 127.

[38] *Ibid.*
[39] Tyree, above note 31 at 276.
[40] For e-money as "money", see Section 2, above.

presented for payment.[41] In addition, the State of Oregon has defined an electronic instrument in its Sale of Checks Act as a card or tangible object "for the storage of information, that is prefunded and for which the value is decrement upon each use."[42] These definitions further reinforce the notion of the SVP as a "distributed" account.

From this perspective, it is regrettable that the European Union adopted the position that "the issuance of electronic money does not constitute in itself … a deposit-taking activity", but rather the sale of a fully redeemable monetary value represented by a claim on the issuer.[43] As applied to widely accepted e-money products[44], and particularly in light of the required convertibility under the Directive, the EU position appears to be unpersuasive. Moreover, one is rather hard pressed to see the difference between recognizing deposit-taking as a debtor creditor relationship while attempting to differentiate stored value on what would appear to be a variant of this concept. In other words, how is a claim against an issuer any different than a claim against any other debtor?

This is not to say that the issue of e-money should be restricted to banks or deposit-taking institutions. The scheme put forward by the EU, namely that of e-money institutions which compared to banks are subject to less cumbersome capital regulation side by side with more stringent requirements regarding business powers, is not

[41] See the Remarks of Catherine A. Ghiglieri, Texas Department of Banking to the PULSE EFT Assoc. Member Conference (October 11, 1996) located at: < http://www.banking.state.tx.us/exec/speech10a.htm > (date accessed: 4 June 2001).
[42] Or. Rev. Stat. Section 717.200(7) (West 1999).
[43] EC Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions (OJ L 275, 27/10/2000, p. 0039 – 0043), preamble s.(7).
[44] The Directive is however not limited to widely accepted e-money products. It does not apply to a single-purpose product but applies whenever an e-money product is accepted in payment for goods or services by someone "other than the issuer". See *id.*, Art. 1(3)(b)(iii). It follows that the Directive may apply to restricted/limited-purpose products with respect to which value would not necessarily qualify as "money".

indefensible; it could however be carried out by recognizing e-money institutions as "special purpose" banks, rather than by introducing a distorted conceptual framework

The question then arises as to whether or not the activities of issuers ought to be considered to be analogous to deposit-taking and hence subject to conventional banking regulations. As we have seen, in the EU express provisions have been made in order to ensure that a regulatory framework applies specifically to stored value. However, in other jurisdictions, the issue may not be as clear. For example in Canada, banking is largely defined through the operation of statutes passed by the Government of Canada which tend to define which activities fall under the auspices of banking.[45] Whether or not regulations will be extended to SVPs will largely be in response to the public / judicial perception of whether or not the activities carried out by issuers amount to deposit-taking or other activities which one would associate with banks.[46]

It ought to be remembered that the issuance of banknotes is a function that was at one time considered to be one of the cornerstones of banking. For example, in 1833, the Bank Commissioner of New York State declared: "The legitimate use of banks is not for the purpose of loaning capital, but for the purpose of furnishing currency to be used instead of specie."[47] Thus, the view that the issuance of e-money is not fundamentally

---

[45] See M.H. Ogilvie, *Canadian Banking Law* 2nd ed. (Toronto: Carswell, 1998) at 24. Also, in the UK bankers are seen as those who (1) accept money from and collect cheques for, their customers and place them to their credit; (2) that honour cheques or orders drawn on them by their customers when presented for payment and debit their customers accordingly; and (3) that keep current accounts in their books in which the credits and debits are entered. See *United Dominions Trust Ltd.* above note 12 per Lord Denning M.R.. However, it should be pointed out that this list is not exhaustive and that transactions which lack the above characteristics may nevertheless be usual banking transactions. See *Royal Bank of Canada v. IRC* [1972] 1 All E.R. 225 at 235 where other activities such as money transmissions, the issuance of travellor's cheques and the operation of credit and cash cards were all held to be transactions undertaken at present day by banks. This also would give credence to the argument that conventional banking regulations ought to be extended to e-money issuers as an analogous activity.

[46] Ogilvie, above note 45, at 19.

[47] As quoted in T.F. Wilson, *The Power " to Coin" Money: The Exercise of Monetary Powers by the Congress* (Armonk, New York: M.E. Sharpe Inc., 1992) at 127.

different from deposit-taking, facilitates the application in principle of banking and payment law to the related area of the issuance of and payment in e-money.

Indeed one may wish to further develop this argument. At its inception, the banknote was a receipt issued by banks to depositors of gold held by a bank. The note was payable to bearer and as such, could circulate throughout the economy as a currency.[48] The issuing bank was liable for the deposits that they maintained, a fraction of which was transferred between individuals by way of the banknote[49]. On the surface, many parallels can be drawn with SVPs. Differences do arise however as a result of the nature of the SVP as compared to the banknote. For example, in the former banks had no control over the negotiation of the note outside of the banking system. Under stored value, the issuer is responsible for maintaining the system whereby stored value can actually circulate from a technical perspective. Moreover, under the banknote regime, there was no transmission of part of a note. The issue of a "distributed account" did not arise in the banknote context in this regard as they were instruments payable to bearer in the amount stated on the face of the note itself. However, the issue of liability with respect to the actual product itself is a feature that both systems have in common. As was the case with customers in the banknote context, holders of stored value are to be reassured of the stability and reliability of the system by way of the holdings of cash and securities that issuers will maintain in order to redeem their obligations as they become due. As a result then, all issuers of stored value including non-banks can be said to have a shadow (but not double) liability on the "deposits" of cash that purchasers of SVPs will make to them so that issuers can meet their obligations.

[48] See generally Geva above note 14. See also A. Khan, "The Evolution of Money: A Story of Constitutional Nullification." (1999) 67 University of Cincinnati Law Review 393, 398.

5. Does monetary value on SVP qualify for deposit insurance?

If we accept the notion that SVP is simply a "distribution" of an existing account relationship with a bank / issuer, and hence does in fact constitute a deposit, one would be tempted to ask if such deposits were subject to deposit insurance. After all, if conceptually speaking we are dealing with an analogous product to existing bank accounts, should they not also have the protections afforded by deposit insurance?

Current deposit insurance laws tend to focus on safeguarding funds which customer's have placed in the custody of a financial institution / intermediary against the threat of its failure. Legislation tends to be interpreted broadly in order to take the development of new financial products into account.[50] Jurisdictions in North America have tended to define deposits (for insurance purposes) as an unpaid balance of money received or held by a financial institution in the usual course of business for which it is obliged to give credit or is evidenced by an instrument on which the institution is primarily liable or is obliged to repay on demand.[51] One of the rationales behind deposit insurance as cited in the common law is the desire to protect the "hard earnings" of consumers that was entrusted to financial institutions would not lead to a tangible loss in the event of failure.[52] Dicta in a Canadian case would extend this concept further arguing that the raison d'être of deposit insurance is to promote economic stability and confidence in the face of an economic crisis.[53]

---

[49] Geva above note 14 at 146.
[50] *FDIC v. European American Bank and Trust Co.*, 576 F. Supp. 950, (S.D.N.Y., 1983) at 953.
[51] See respectively, 12 USC § 1813 (*l*) (1) in the United States and in Canada, the *Canadian Deposit Insurance Corporation Act* RSC, 1985, C-3. Schedule 1 s.2. Online: *Department of Justice website*. < http://lois.justice.gc.ca/en/C-3/text.html > in Canada. (date accessed: 6 June 2002).
[52] *FDIC v. Philadelphia Gear Corp.*, 476 U.S. 426 (1986) at 435.
[53] *Banque Nationale Du Canada c. Sous-Ministre Du Revenu Du Québec* [1994] R.J.Q. 2700 at 2702.

The nature of the product is such that the concerns articulated in the common law towards conventional bank deposits deserves to be replicated in the SVP context. Moreover, it is submitted that coverage ought to be extended to non-bank issuers of SVP as well. The risks involved in maintaining funds on SVPs can be said in someway to be analogous to risks involved in traditional banking deposits. In both scenarios, funds are advanced to a party with the expectation that they will be held on their behalf. In SVP, issuers maintain a block of funds in order to redeem claims made by presentment of the stored value. The amount of this fund must presumably correspond to the amount of stored value that is outstanding. This pool of funds may either take the form of residing in individual accounts that correspond to each purchaser or take the form of an aggregate pool of funds that will satisfy all claims. Theoretically, these accounts do not exist for the issuer's personal use or benefit, but rather fulfill the implicit warranty it makes towards its consumers that adequate funds will be available to satisfy their claims.

The FDIC opinion governing SVP states that under existing regulations, deposit insurance can be extended to Bank Primary-Customer Account Systems.[54] Deposits that qualify for deposit insurance are also created in Bank Secondary-Advance systems[55] although these deposits are considered to be those of the issuer for the duration that they remain in an issuer's bank account. It is regrettable that the FDIC did not consider

[54] See generally, General Counsel's Opinion No. 8; Stored Value Cards, 61 Fed. Reg. 40490 (1996) (notice Aug. 2, 1996). In these systems, the funds underlying a stored value card remain in a customer's deposit account until the value is transferred to a merchant or an acquirer who collects the funds from the customer's bank. Until the funds are collected, liability for them remains with the customer's bank as is the case with a traditional access product.

[55] Under this system, the issuer creates electronic value which is then provided to an institution who sells it to their customers who exchange funds for such value. The institution then holds the funds briefly before it is forwarded to the issuer as payment for the electronic value for which the issuer is liable to the consumer.

deposits to be insured under Bank Primary-Reserve systems.[56] In it's reasoning, the FDIC stated that these types of arrangements did not fall within the statutory meaning of deposit since the funds were not held for a "specific purpose."[57] The FDIC concluded that funds in these systems could be associated with general or miscellaneous unrelated transactions and as a result, would not fall under the auspices of the Federal Deposit Insurance Act (FDIA).[58]

It is respectfully submitted that insurance coverage ought to be extended towards Bank Primary-Reserve systems both as a means of adhering to the spirit of the law governing deposit insurance outlined above and as a recognition of the "distributed" account nature of SVP. By not recognizing Bank Primary-Reserve systems, consumers could be placed at a disadvantage and be denied deposit insurance mainly through no fault of their own but rather as a result of internal accounting policies undertaken for the convenience of the issuer.

This in turn could result in various legal liabilities being associated with SVP as a function of the technology / accounting choices made by the issuer that may be at odds with public policy and established legal doctrines. While it is true that the funds placed in the pool do not relate to a particular transaction per sé, they are held for the sole purpose of satisfying obligations of the issuer to their customers as they become due. As was mentioned earlier, the amount in these pools should correspond to the amount of

[56] These are systems whereby consumer funds are placed into a pool by the issuer that is used to satisfy claims as they are presented for redemption. The FDIC also stated in its opinion that deposits are not created in Bank Secondary Pre-Acquisition Systems where financial institutions advance funds to an issuer in order to receive stored value which they sell to their own customers in turn.
[57] SVC Opinion, 61 Fed. Reg. at 40 492.
[58] *Id.* at 40 493.

stored value that is outstanding and hence extending deposit insurance to these pools of funds would not result in serious accounting difficulties.

Moreover, the specific purpose argument made against Primary-Reserve systems seems to be at odds with other financial instruments that are specifically mentioned in the legislation. For example, the FDIA extends deposit insurance coverage to instruments such as cashier's cheques and money orders.[59] When one purchases an instrument such as a personal money order, the funds used to purchase the instrument are placed in a special reserve account as is the case with bank drafts and certified cheques[60] which are also covered by deposit insurance. Conceptually speaking, in the case of the aforementioned products, deposit insurance seeks to insure the guarantee of the financial institution / issuer to satisfy claims presented to them by means of these products.[61] This same rationale could be use to justify extending deposit insurance to SVP.

One objection that could be raised is that with respect to offline unaccountable stored value, an issuer may have no way of knowing where its stored value has circulated. The issuer may not discover the legal owner of the stored value until it has received the stored value when it is presented for redemption. Despite the evidentiary problem posed by the nature of the product, it is submitted that this ought not to detract from the fact that despite the fact that not every holder of stored value is known to the issuer, the aggregate pool ought to be insured. Indeed, not knowing the holder of a

---

[59] 12 USC § 1813 (*l*) (4). See also *FDIC v. McKnight*, 769 F.2d 658, 661-62 (10th Cir. 1985) which held that outstanding and unpaid cashier's checks of a failed institution are converted into deposits by operation of law under Section 1813 (*l*) (4) upon the appointment of the FDIC as receiver. As quoted in T. Vartanian et al. *21st Century Money, Banking and Commerce*. (Washington: Fried, Frank, Harris, Shriver and Jacobson, 1998) at 188 note 18.

[60] B. Geva. "Irrevocability of Bank Drafts, Certified Cheques and Money Orders." (1986), 65 Canadian Bar Review 107, 131.

[61] See also B. Geva. "Insolvent Bank's Irrevocable Credit as Priority Payment Instrument: *Barclays Bank v. Price Waterhouse*." (2000) 15 BFLR 351, 353 – 354.

financial product is insufficient to deny insurance coverage for other instruments such as travellor's cheques and money orders. In the case of personal money orders, there is no requirement for the issuing institution to fill in the name of the payee on the instrument itself – such discretion is left to the sender.[62] Thus even in the case of offline unaccountable products that utilize a Bank Secondary – Advance system, an argument can be made in favour of extending deposit insurance to these products.

6. Does payment by SVP involve a "funds transfer"?

"Funds transfer" is a generic name for a non-cash payment carried out through the banking system under the instructions of a customer. Its operation results in a credit balance being transferred from one bank account to another, irrespective of whether the two accounts are in one or two banks, and regardless of whether the two accounts belong to the same or two distinct persons.[63]

Still, notwithstanding dicta in one American case,[64] it may be inappropriate to speak of a funds transfer as the assignment to the payee of the credit balance, namely of the debt owed by the bank to the payor. A legal assignment must be absolute, in writing and must be advised to the debtor. It has also been held that it must be for the entire debt.[65] In a funds transfer, the instruction given to the debtor, namely, the payor's bank, is usually not for the entire debt. Also, particularly in non-retail networks, no advice needs to be given to the payee (assignee) by the payor (assignor), in conjunction with the latter's instruction to the payor's bank. Requirements of the legal assignment are thus

[62] *Id.*
[63] *Royal Product Ltd. v. Midland Bank Ltd*. [1981] 2 Lloyd's L. Rep. 194 (QB) at 198.
[64] *Delbrueck & Co. v. Manufacturers Hanover Trust Co.,* 609 F. 2d 1047 (2d Cir. 1979) at 1051.
[65] *Steel Wing Co. Ltd., Re*, [1921] 1 Ch. 349.

unlikely to be fulfilled. But even the less formal equitable assignment could hardly be accommodated in the usual case, involving not only the replacement of the creditor by the assignee, but also the replacement of the debtor. Stated otherwise, in inter-bank funds transfer, the debt owed to the payor (alleged assignor) that 'shifts' to the payee (alleged assignee), becomes that of the payee's bank, replacing the payor's bank as debtor. Indeed, it is specifically provided that the bill of exchange is not an assignment of funds,[66] and it is hard to see why that rule should not be extended.

There is also a pragmatic reason. If the funds transfer is an assignment of the debt owed by the bank to the payor, it must be taken to pass with it all defences available to the bank against the payor and make them available against the payee. For policy reasons this is unacceptable; hence, the better view is to see the operation of the funds transfer as premised on the extinction of the debt owed to the payor and the creation of a new debt owed to the payee. Accordingly, in connection with a funds transfer, "'transfer may be a somewhat misleading word, since the original obligation is not assigned"; rather, it "is extinguished or reduced pro tanto", while "a new obligation [possibly] by a new debtor is created".[67] In this framework, defences available against the payor do not become available against the payee since the debt owed to the payee is not the one originally owed to the payor.

The e-money payment can thus be regarded as a transfer of funds, in which the issuer's debt to the payor extinguishes while a new debt from the issuer to the payee is created.

[66] In the UK, see Section 53(1) of the Bills of Exchange Act 1882, (45 & 46 Vict. c.61). See also in Canada the Bills of Exchange Act RSC, 1985, c. B-4 s. 126 and in the United States UCC § 3 – 408.

7. Could e-money nevertheless be "money" and is the SVP different from the debit card?

The foregoing analysis entails a re-visit of two fundamentals. First, can e-money truly be "money"? Second, is an SVP really substantially different from an access device, so that particularly in the retail area, is the law governing the smart card entirely separate from that applicable to the debit card?

Regarding the first question, that of the definition of "money", the issue is that of "circulation". If the issuer's obligation is not being transferred, how can it be said to "circulate"? Interestingly enough, "central bank money", namely the central bank deposit obligations, "circulates" in the same manner. Being an obligation of the central bank, it is indistinguishable from banknotes in discharging debts. Yet, when one bank pays another with central bank money, the process entails a debit to the paying bank's account and a credit to the payee-bank's account, so as to extinguish or reduce the central bank's obligation to the former, and create or increase another central bank's obligation to the latter. Still, the central bank deposit obligation is fundamentally the same as that on the banknote so as to be "money".[68]

It is submitted here that the objection based on lack of true transferability is met by following the same logic as that facilitating the treatment of "central bank money" as "money". "Circulation" has to be viewed as feasible not only in the context of actual "transferability" or concrete assignment. Rather, substance ought to be allowed to prevail over form. This is particularly true in light of the mechanism facilitating the defence-free

---

[67] *Libyan Arab Foreign Bank v. Bankers Trust Co*. [1988] 1 Lloyd's L. Rep. 259 (QB) at 273.

[68] In fact, the "monetary base" of money, being the net monetary liabilities of the government that are held by the public, consists of bank reserves, that is, reserve obligations of the central bank, plus "currency", comprised of coin and paper money (namely, banknotes issued by the central bank) in circulation. For example, see P.A. Samuelson and W.D. Nordhaus, *Economics* 17th ed. (NY: McGraw-Hill, 2001) at 760 and 770 (Glossary of Terms). See also at 545.

position of the payee with regard to defences available against the payor, as outlined in Section 6 above. Accordingly, any mechanism that facilitates the smooth operation of the extinction and corresponding creation of interchangeable obligations accepted in full discharge of debts is to be viewed as establishing "circulation". In turn, when other requirements are met,[69] this enables us to view such obligations as "money".[70]

It could nevertheless be paused here to observe that this conclusion might be of a limited utility. As indicated, the payee under a funds transfer takes the issuer's claim free of the payor's defences, irrespective of whether the payee received "money". As well, statutes and even contracts requiring payment in "money"[71] may anyway be interpreted to include payment mechanisms settled in "money". On the other hand, it is arguable that for the debt owed by the issuer to be treated as a "deposit" it is essential that the "deposited" e-money be "money".

The second question concerns the debit card and the relationship between its underlying concepts and those underlying the smart card. It appears indeed that from a legal perspective, the two instruments are not all that far apart. As discussed, the fundamental difference lies in the accounting system. In an access device such as the debit card, the account is maintained and activity is recorded centrally, with the bank itself. In an SVP, including the smart card, the account is maintained and activity is recorded on the device itself; the accounting system is said to be "distributed". Obviously, this leads to a few changes in the governing legal regime; for example, duties

[69] For what meet necessary requirements to be "money", and the fulfilment of such requirements by e-money, see Section 2, above.
[70] For another perspective please see Crawford, above note 7, at 402.
[71] As for example, the UK Sale of Goods Act 1979, c.54 defining (in Section 2(1)) a contract for sale to be "a contract by which the seller transfers or agrees to transfer the property in goods to the buyer for a *money* consideration, called the price". Emphasis added.

regarding periodical statements do not exist with regard to the value recorded on the SVP. Yet, as a payment mechanism, both the access device and the SVP, namely, both the debit card and the smart card, are subject to the same law governing the transmission of messages between sender and receiver and the movement of value or funds from payor to the payee. In addition, since the operation of a "centralized" accounting system requires the recording of each transfer at the bank and an ensuing statement, current practices preclude anonymity in debit card transfers. This may undermine the actual treatment of funds transferred by debit cards as "money"; yet, in theory, it does not negate such characterization, as long as parties are prepared to accept the obligation of the card issuer in an absolute discharge of debts.[72]

8. Does payment by SVP constitute "credit- push" or "debit-pull", and does it matter?

Depending on the manner in which instructions are communicated so as to affect banking, or more generally, accounting operations, funds transfers are either credit or debit transfers. In a credit transfer the payor's instructions are sent to the payor's bank, which then "pushes" the funds to the payee's account. Conversely, a debit transfer is initiated by instructions communicated by the payee to the payee's bank, and is carried out by "pulling" the funds from the payor's account. Here lies the distinction between "credit-push" and "debit-pull" transfers. In a credit transfer, communication is in the same direction as the movement of funds. Conversely, in a debit transfer, communication is in the reverse direction. Accordingly, in a credit transfer, the sender of the first message is the payor, and the ultimate receiver, or destination party, is the payee; in a

[72] For legal aspects pertaining to the debit card see B. Geva, "The E.F.T Debit Card" (1989), 15 Can. Bus. LJ 406. (hereafter: Geva, "EFT Card").

debit transfer, conversely, the first sender is the payee, and the ultimate receiver, or destination party, is the payor.[73]

Effectively, this means that in a credit transfer, the first impact on the banking or accounting system is the debit to the payor's account, and the concluding event is that of a credit to the payee, which is final and unconditional. At the same time, in a debit transfer, the first impact on the banking or accounting system could be a credit to the payee's account, and the concluding event is the debit to the payor's account; credit to the payee's account is provisional and conditional on the debit in the payor's account, most typically, on the availability of funds in the payor's account, and possibly, also on the lack of revocation of authority by the payor. Thus, in contrast to the credit in the payee's account in a credit transfer, the credit posted to the payee's account in a debit transfer is not accorded finality.

Regarding payment system risks, credit transfers are safer to the inter-bank payment system than debit transfers. This is so since credit transfer operations involve neither float nor the risk of insufficient funds in the payor's account.[74] This results from the fact that in a credit transfer, as opposed to the debit transfer, debit to the payor precedes the credit to the payee. There are also some important distinctions between the rules of law governing credit and debit transfers, all stemming from the different direction between the flow of messages in each type of payment mechanism. For example, in the credit transfer, the moment of payment is determined according to events occurring at the payee's bank. Conversely, in a debit transfer, the crucial events

[73] See B. Geva, "International Funds Transfers: Mechanisms and Law", in *Cross-Border Electronic Banking*, above n.6 at 1.

determining the moment of payment take place at the payor's bank. As well, due to the inverse directions of messages, the engagement of each sender in a credit transfer is fundamentally different than that of a sender in a debit transfer. Briefly stated, in a credit transfer a sender undertakes to pay, while in a debit transfer the sender's undertakings essentially amount to warranties of authority and validity. Another example is the more extensive scope of liability for consequential loss for an improper execution or non-execution of a credit transfer.[75]

Retail payment systems could operate as either credit-push or debit-pull systems. Stated otherwise, the message from the payee's terminal could be communicated to the payee's bank that will "pull" the funds from the payor's account. At the same time, the message from the payee's terminal could be communicated through the network to the payor's bank, and will be followed by funds "pushed" to the payee's account.[76] True, a POS retail payment is initiated by the payor who, with the consent of the payee, inserts a card at a POS terminal, and requests the acceptance of the request, so as to possibly give an appearance of a credit transfer. Nevertheless, the communication from the POS terminal, which is under the payee's control, may be viewed as the payee's collection order, as in the collection of a cheque.

---

[74] For the increased risk in relation to debit instruments, particularly cheques, see, Bank for International Settlements, "*Core Principles for Systematically Important Payment Systems*," Report of the Task Force on Payment System Principles and Practices (CPSS Publications No. 43) (Basle: January 2001) at 70 –75.

[75] On these differences between debit and credit transfers consider the following provisions of the American Uniform Commercial Code. The determination of the moment of payment is governed by Section 4A-406 for credit transfers and by Section 4-215 for cheques and other paper-based debit items. For the sender's payment engagement in a credit transfer see Section 4A-402 while for the sender's warranty undertakings in the collection of cheques and other paper-based debit items see Sections 4-207 and -208. The potentially extensive liability of a bank executing a credit transfer under *Evra Corp. v. Swiss Bank Corp.*, 673 F. 2d 951 (7th Cir. 1982) is specifically not followed in Section 4A-305.

[76] A previous discussion by one of the authors on debit card retail network architecture is Geva, "The EFT Card", above note 72 at 419-427.

Indeed, retail payment systems may thus not be amenable to a universal classification; this may give the impression that no single body of law applies. A retail payment system will be characterized as either a debit-pull or credit-push transfer, and depending on the architecture of the underlying network, be subject to the law applicable to each such a transfer. Furthermore, the system operator may act as a third-party processor or agent for either payor's or payee's bank, so that messages sent to it cannot always be easily interpreted as necessarily or exclusively directed to, or meant to reach, any specific bank.

Regardless, however, the principal feature of both the debit and the stored-value card is the instant guarantee of payment accorded to the payee, even in a debit pull, and at the time of the communication of the first instructions, even in a credit push. It is submitted that this feature overshadows the difference between debit and credit transfers that otherwise would have been crucial in the determination of the law applicable.

We shall endeavour to demonstrate in the following section that the law governing retail payment systems evolves around the payment guarantee feature so as to neutralize the usually very important division between credit and debit transfers.

9. An outline of the payment law applicable

As indicated, both the debit and stored-value card are guaranteed payment mechanisms. Participants are the payor, payee, the payor's bank ("issuer"), the payee's bank ("acquirer"), and possibly one or more intermediary banks. The system operator may act as a third-party processor, or agent on behalf of participants. "Bank" is broadly used here to include an authorized issuer of e-money. An intermediary bank provides a

communication pathway between the acquirer and the issuer with or without a banking or funds-transfer link. Regardless, the intermediary bank's position does not affect that of either the payor or the payee, since in the guaranteed payment environment, these parties interact directly with each other as well as with each other's bank.

Governing legal principles may be summarized as follows:

1. Payment over a retail payment system network ("RPSN") may be either a credit or a debit transfer. Either way, it is initiated by the payor who, with the consent of the payee, inserts a card at a POS terminal, and requests the acceptance of the request, as provided in applicable contracts. The communication of such request over the RPSN constitutes the transmittal of the payment instruction.

2. The payor's request may either be accepted or rejected by the issuer/payor's bank. It shall be accepted if made according to the contract between the payor and the issuer/payor's bank and there is adequate cover (including under any approved credit line) in the payor's account. Rejection or non-acceptance in breach of this provision charges the payor's bank with liability to the payor for the wrongful dishonour of the payor's payment instruction.[77] Non-acceptance caused either by system malfunction not attributed to the fault of any participating bank, or by system maintenance at reasonable intervals, will not constitute such breach.

[77] It is a question of policy, then, whether the scope of liability for such wrongful dishonour is to be restricted to a particular amount.

3. No acceptance by the issuer/payor's bank of the payor's request will be given without first asking the payor to confirm or approve the amount of payment. Upon the confirmation or approval of the amount of payment so given by the payor, the payment instruction becomes irrevocable and cannot be cancelled. The request for confirmation or approval sent by the issuer/payor's bank, the payor's confirmation or approval, and the acceptance or rejection by the issuer/payor's bank are to be advised per RPSN rules and applicable contracts, in immediate response to the payment instruction under Paragraph 1.

4. Acceptance by the issuer/payor's bank of the payment instruction, when received by the payee, to the extent of its amount as accepted upon the payor's confirmation or approval:

   (i) entitles the payee towards the acquirer/payee's bank[78] to unconditionally obtain credit to the payee's account;

   (ii) binds the issuer/payor's bank to pay the acquirer/payee's bank;

   (iii) binds the payor to pay the issuer/payor's bank and entitles the issuer/payor's bank to have the payor's account debited or otherwise obtain reimbursement from the payor; and

   (iv) constitutes an absolute discharge of the debt paid by the payor to the payee.

[78] It seems to be unnecessary to provide the payee with an additional right directly against the payor's bank. Adequate protection is given to the payee as the payee is provided with a right against the payee's bank, which in turn, becomes entitled to recover from the payor's bank. It is thus the obligation of the payor's bank to pay the payee's bank which constitutes "money" with which payment is made to the payee and with which the payor's obligation is discharged. Yet, the actual risk of default by the payor's bank does not fall on the payee, but rather, on the payee's bank. This may be necessary for the maintenance of the

Time, manner, and charges for carrying out these obligations are governed by RPSN rules and applicable bilateral contracts.

5. In initiating payment over an RPSN, the payor warrants to the payee and each participating bank that the card to be used is valid and that value to be applied in payment is genuine.[79]

6. A person to whom a device was issued is responsible under Paragraph 4(iii) for any communication either over an RPSN or per its governing rules or procedures, given by him or her, under his or her authority, or that has been authenticated under a commercially reasonable security procedure agreed upon between the issuer of the device and that person.[80]

10. The need to balance privacy with law enforcement objectives

The ease with which automation has allowed information to be processed and compiled has wide ranging effects when one considers the potential threat to personal privacy that results from the use of SVPs. While total anonymity may be desirable from a consumer's perspective, the anonymous nature of SVPs may hinder transactional reporting which is key to anti-money laundering law enforcement objectives. As a result,

---

integrity of the system since the payee may not have had any dealing with the payor's bank and is likely to rely on the payee's bank.

[79] This warranty is analogous to an undertaking by a payor that banknotes and coins used in cash payment are genuine.

[80] This rule does not exclude a consumer protection type regulation setting a ceiling to customer's exposure.

regulators are faced with the uneasy task of balancing these two seemingly conflicting objectives.

Looking first to the issue of consumer privacy, the increased automation prevalent in Stored Value systems brings the potential for unscrupulous issuers / retailers to document an individual's spending habits which they can either sell to interested third parties or retain for their own use in seeking to boost sales of products they may be promoting. The potential for this to occur is equally prevalent in both online and offline systems. In the former information could be compiled by an issuer / retailer through terminals that process transactions, correlating the anonymous identifiers used by SVPs with customer lists, building databases and engaging in data mining techniques which are either used to supplement existing issuer / merchant marketing efforts or sold to third parties (such as marketing firms or reference services). In the latter, this threat is still present although only at the merchant level. Even if consumers are not identified by name but rather by number, informational value can still be generated from their behaviour.

Existing regulations and common law doctrines should provide adequate protections to consumers so that personal information is not disclosed without their consent except where absolutely necessary in extraordinary circumstances. Thus there is no reason to suppose that in the case of recognised financial institutions which sell SVPs, that they will not be subject to existing common law doctrines that mandate confidentiality towards their customers with certain public policy exemptions.[81]

[81] The leading case on this issue is the English case of *Tournier v. National Provincial and Union Bank of England* 1 K.B. 461 (1924). See also the U.S. cases of *Peterson v. Idaho National Bank*, 367 P.2d 284 (Idaho 1964) which held that an implied duty of confidentiality exists between a bank and its depositor and *Barnett Bank of West Florida v. Hooper*, 498 So. 2d 923, 925 (Florida 1986) (where it was held that

One area of concern which the common law has yet to evaluate are the circumstances in which a financial institution could be liable when an individual could break into their computer networks without their knowledge.[82] Moreover, it is not certain what the standard of care would be applicable in this context.[83] It is respectfully submitted that liability with respect to breaches of privacy ought to fall on the issuer in order to serve as an incentive to ensure that systems are designed to respect individual privacy rights. Moreover, in light of the fact that issuers are the chief beneficiaries of the pecuniary benefits associated with stored value, that they ought to be the party which should bear these risks.

Recent statutory developments have brought a variety of regulatory responses, some of which will be of great benefit to consumers worldwide. In light of the threat to individual rights of privacy it is regrettable that the United States has opted to move slowly on this issue.[84] Canada has implemented regulations[85] although the relative lack of remedial powers granted to its implementing authority has hindered the legislation's ability to live up to its potential.[86] The European approach represents the most forceful approach to date that recognises privacy as a political right and uses an approach which relies upon the principles of notice and consent.[87] Indeed, such an approach will likely

---

exceptions to the general rule include disclosures under compulsion of law, pursuant to the public interest, pursuant to a bank's interest, and where expressly or impliedly authorized by the customer).

[82] Vartanian, above note 59, at 298.

[83] *Id.*

[84] For a critique of current U.S. approaches to privacy protection see M. Rotenberg. "Fair Information Practices and the Architecture of Privacy: (What Larry Doesn't Get)." 2001 Stanford Technology Law Review 1.

[85] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5. Available online at < http://www.justice.gc.ca/en/P-8.6/text.html >

[86] See T. Scassa. "Text and Context: Making Sense of Canada's New Personal Information Protection Legislation." (2000 / 2001), 32 Ottawa Law Review 1.

[87] Council Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and On the Free Movement of Such Data, 1995 O.J. (L 281) 31

prove to be the most successful in implementing stringent standards that will boost consumer confidence and ultimately allow SVP to reach a critical mass.

The European Privacy Directive contains a provision that prohibits EU firms from transferring data to be processed in an entity in a non-EU country, unless the receiving country has adequate privacy laws[88] subject to certain exceptions.[89] This provision has encouraged the United States despite its laissez-faire position; to negotiate a safe harbour agreement[90] with the European Union that encompasses many of the principles required to comply with the EU regulations. One of the unsettling aspects of the Privacy Directive is the perceived extra-territoriality of its application. Conversely however, the Directive has been successful in functioning as a business incentive for compliance that has resulted in increased consumer privacy protection worldwide by providing standards that have raised the status quo.

Regulators have been confronted with the question of how to regulate in such a manner that balances consumer rights to privacy with the objectives of law enforcement officials who wish to combat money laundering. Consumers may prefer to have total cash-like anonymity yet such an approach would make it virtually impossible to trace the movement of funds that are used in illicit activities. The converse would be equally harmful is the sense that individuals may be subject to constant public / private surveillance recording their every activity and which could potentially be exploited for commercial gain. Privacy must be regarded as a political right that consumers enjoy and

---

[88] *Id.* at Article 25.
[89] *Id.* at Article 26.
[90] Issuance of Safe Harbor Privacy Principles and Transmission to European Commission, 65 Fed. Reg. 45666, 45667 (July 24, 2000), available at < http://export.gov/safeharbor/SHPRINCIPLESFINAL.htm >. See also A.E. Shimanek. "Do You Want Milk With Those Cookies?: Complying With The Safe Harbour Privacy Principles." (2001), 26 Journal of Corporation Law 455.

should be respected as such however at the same time, precautions need to be put in place to ensure that SVPs are not used as a means to circumvent existing laws.

SVP presents a particular challenge to existing anti-money laundering schemes by allowing illicit funds to pass through traditional chokepoints / reporting requirements which are crucial to the operation of these statutes. Features present in Internet funds transfers which make them attractive for money launderers are the anonymity and speed of transfer it affords in addition to the ability to transfer virtually unlimited amounts.[91] Issues arise not only in the context of consumer uses for stored value but also for merchant uses as well.[92]

For example, many issuers state that consumer cards will be subject to limits on the amount of value that may be placed on them at any one time. Yet this approach does not address the fact that money launderers could circumvent these limits by engaging in a multitude of transactions to launder a large amount (smurfing). While this may make it inconvenient for launderers, the speed at which transactions can be conducted (ie. Multiple units of stored value can be bought instantly) coupled with the economic incentives of being able to launder funds online may prove to be an irresistible proposition. Moreover, criminals could get around the consumer limits of SVPs by taking advantage of money laundering businesses that would be able to utilize merchant smartcards that have higher limits in order to accommodate the value of retail

[91] S.N. Welling and A.G. Rickman. "Cyberlaundering: The Risks, The Responses." (1998) 50 Florida Law Review 295 at 320.
[92] See also Vartanian, above note 59, at 225 – 243.

transactions.[93] Inevitably, the only effective way to combat money-laundering is through the creation of an audit trail that exists, is readable and is followable.[94]

One of the largest impediments to reporting requirements is the fact that SVPs can provide for peer-to-peer transactions. The distributed nature of the account placed upon a smartcard for example would make it difficult to track stored value movements in peer-to-peer transactions without access to the card itself[95] in the case of offline unaccountable transactions. While this aspect allows stored value to circulate in a cash-like manner, it can also serve as a powerful tool for those seeking to launder money.

Solutions to combat money laundering have included the creation of regulations that seek to extend conventional inspection and licensing regimes to SVPs such as the Uniform Money Services Act[96] in the United States. Other approaches have included taking a more proactive approach towards overcoming difficulties imposed by the nature of the technology itself such as key escrow requirements. However such an approach may have the undesirable effect of mandating technical standards that may be unsuitable for the long term development of the technology and hinder its acceptance / viability.

Instead, a better solution may be one that was proposed by Timothy Ehrlich. Ehrlich argues that steps ought to be taken now before the technology has taken hold in

---

[93] T. Ehrlich. "To Regulate or Not? Managing the Risks of E-Money and Its Potential Application in Money Laundering Schemes." (1998), 11 (3) Harvard Journal of Law and Technology 833, at 847.
[94] Welling, above note 91, at 320
[95] This facet relates to another set of concerns in the privacy field. For example, when it was first launched, it was claimed that Mondex would be an anonymous system since it did not create central records. Following a compliant made by a privacy advocacy association, officials in the U.K. noted that card readers used by merchants who accepted Mondex value maintained a record of the last 300 card transactions. Merchant lists identified purchasers by card number and not by name. However, it was noted that the issuer could supply merchants with identifying information that could allow for the creation of informational databases that could be used for commercial purposes. See T.S. Onyshko and R.C. Owens. "Debit Cards and Stored Value Cards: Legal Regulation and Privacy Concerns." (1997), 16 (5) National Banking Law Review 65, at Paras. 21 – 22.
[96] Uniform Money Services Act. Online: *National Conference of Commissioners on Uniform State Laws* < http://www.law.upenn.edu/bll/ulc/moneyserv/UMSA2001Final.htm > (date accessed 24 January 2002).

order to prevent SVPs from being used as a conduit to launder money and minimize the risk of financial loss to issuers themselves.[97] Ehrlich's proposal would regulate the ability of issuers to develop untraceable currency products and would require that transactions be processed through an intermediary (either governmental, the issuer themselves or a third party).[98] Issuers would be required to maintain a registry of the identity and addresses of the users of their products that they could give to law enforcement officials when necessary.[99] Access to such information would be subject to existing legal safeguards such as requiring a warrant before access can be granted to the information thereby safeguarding consumer privacy interests.[100] Indeed, one may wish to go a step further and argue that investigators should demonstrate reasonable grounds prior to commencing investigations. Moreover, in cases where issuers themselves are acting as processors, Chinese Walls ought to be set up between their marketing and informational security departments to ensure that privacy rights are not infringed.

A restriction of peer-to-peer transactions would not necessarily restrict the "circulation" of stored value. As was mentioned previously, substance ought to prevail over form and nothing in this proposal would hinder the ability of a payee to receive stored value free from the payor's defences.

11. Consumer protection issues and principles

A crucial factor governing the ability of SVPs to reach a critical mass is the issue of the consumer protection provisions that will apply to SVPs. In some cases different financial products have similar legal regimes that are applicable to them with very

[97] Ehrlich, above note 93, at 853.
[98] *Id.* at 857.
[99] *Id.*

different repercussions for consumers.[101] Yet it may still be possible to synthesize current legal doctrines with new developments in SVPs that could guide future regulatory efforts.

Of main interest to consumers is the issue of loss allocation in the event of an unauthorized transaction. Usually security procedures with respect to smart cards merely involve card insertion and validation[102] and in some cases do not require consumers to enter a PIN.[103] In the event of a dispute for an unauthorized transfer, one is confronted with the issue of the burden of proof to be met by each party in asserting the other's liability. For example, the question arises as to whether or not proof of compliance with security procedures and demonstrations of the reliability of the payment media will be sufficient to fasten liability on to consumers. The answer to this question will in large part be determined by the context in which the loss occurs. While numerous scenarios can be put forth, we will briefly focus on some of the more problematic ones.

One such scenario is where the issuer is asked for a refund of value for a lost or stolen card. The issuer's typical point of view is that e-money is the equivalent to cash so that such value is not refundable. It is hard to see how this point can be justified in the context of all accountable[104] systems where the issuer could conceivably act upon a stop

---

[100] *Id.*

[101] Consider the difference in the treatment of credit and debit cards in the United States for instance. Regulation Z 14 C.F.R. pt. 226 (1998) imposes a minimum liability $50 for consumers for unauthorized transfers involving credit cards. The same concept applies in Regulation E 12 C.F.R. pt. 205 (1996) however, over time consumer liability increases eventually until it encompasses the entire amount in dispute.

[102] D. O'Mahony et al. *Electronic Payment Systems for E-Commerce*. 2nd Edition. (Norwood MA: Artech House, 2001) at 59.

[103] Consider the case of offline unaccountable systems such as Visa Cash. See O'Mahony *Supra* note 102 at 217 – 218.

[104] Even in the case of offline accountable systems (see the text around notes 2 –3, above), an issuer could conceivably act to save the remaining value on a card once information has been sent to it as part of a periodic update. At the same time, apart from systems utilizing online authorization, there would appear to be no way for an issuer to control the subsequent use of its issue.

payment order made by the payor following a loss, with respect to the remaining value on their cards. Where the position of non-refundability may hold true is in the case of offline unaccountable systems where an issuer has no means of disabling stored value until it is presented for redemption.

Yet even within the context of lost cards, one must still address the question of loss allocation when a consumer either has or has not complied with security procedures established by the issuer. For example, if a consumer were to lose a stored value card that they had left unlocked and that card was found by an innocent third party, it may be an unreasonable proposition to assert that the issuer ought to bear the responsibility to track the stored value down. This situation could have been avoided but for the consumer's negligence and the remedy would place an unreasonable burden on the issuer.

Conversely however, suppose an individual did comply with security procedures and subsequently lost their card. Issuers claim that third parties cannot access the value on a locked card. As a result, there is no value that could potentially fall into the hands of an innocent third party if issuer's claims are to be believed. In such a scenario, we submit that the loss ought to be absorbed by the issuer who ought to be liable for any outstanding stored value issued to the customer that has not been redeemed after its expiry date in the form of rendering an account. In order to encourage consumers to adequately safeguard their cards and PINs some consumer liability subject to a low ceiling should be established with the balance to be absorbed by the issuer.

Another issue that warrants some consideration is the question of who ought to bear responsibility for stored value that is lost as a result of media failure. Analogously,

one would have to ask what were to happen if an individual's stored value were to be erased as a result of a physical act (ie. a thunderstorm whose magnetic field causes a SVP to fail) or technological malfunction that is beyond the consumer's control (ie. walking through a security terminal through an airport that erases the value on a card). While issuers maintain that their products are built to withstand such possibilities the legal nature of this question ought to be examined further.

Any claims of a loss resulting from media failure or unauthorized use loss made by a consumer would have to be weighed and assessed against evidence adduced by the issuer relating to the technical soundness of its system, the reliability of its records and the reliability of its security / authentication procedures. Whether such proof will suffice to shift losses to the consumer is another issue, not different than that existing in connection with unauthorized electronic funds transfers that utilize access products.[105] However, in a consumer setting, it is highly unlikely that consumers will be sufficiently sophisticated to challenge the issuer's technical claims. Moreover, the availability of evidence may be compromised in an offline unaccountable setting as a result of the decentralized nature of the account in question. We submit that losses in this regard also be placed upon issuers in order to create pecuniary incentives for them to update their products and make the necessary investments to ensure that such losses do not occur. The onus of proof on the part of issuers should extend beyond demonstrating compliance with security procedures and move to the civil standard of a balance of probabilities[106] establishing that the losses were the result of a consumer's actions before losses can be

[105] For the latter issue, see in great detail, Bohm, Brown and Gladman. "Electronic Commerce: Who Carries the Risk of Fraud?", 2000(3) The Journal of Information, Law and Technology, online: <http://elj.warwick.ac.uk/jilt/00-3/bohm.html> (date accessed: March 8, 2002).

shifted to them. While the standard of compliance with security procedures may be adequate in a business context as is the case with the American Article 4A,[107] such a standard is not sufficient in the consumer context.

An additional consumer protection issue that surfaces with respect to SVPs is the issue of disclosure in the form of transaction receipts provided to the consumer after each purchase. While this may result in considerable expenses for some issuers particularly those who provide offline unaccountable systems, it is submitted that disclosure is key to protecting consumers and fostering their acceptance so much so that it overrides issuer concerns of high operating costs. Disclosure helps avoid "black box" transactions whereby consumers are not provided with a method of ascertaining the amount of value that has been deducted from their card following each use, which can then be used as evidence in a dispute with an issuer. An unscrupulous individual could thereby defraud a consumer by extracting the entire value of their card unbeknownst to the consumer.[108] Even within the context of SVPs that utilize low amounts, consumers may attribute negative experiences with these transactions to all SVP systems that could have the undesirable effect of hindering the long-term development of stored value. Despite the high costs associated with paper disclosure, there is no reason why issuers could not supply a digital receipt as a substitute at low cost.

---

[106] For a description of this standard, see J. Sopinka, S.N. Lederman, and A.W. Bryant. *The Law of Evidence in Canada*, 2nd ed. (Toronto: Butterworths, 1999) at 154.

[107] See in particular U.C.C. § 4A-202. Under this scheme, the risk of an unauthorized payment order initially falls on the bank. The risk is then shifted to the consumer if the bank proves its compliance with an agreed upon commercially reasonable security procedure. The risk is then shifted back onto the bank where the loss is proved by the consumer to be caused by an interloper, or is allocated to the bank by agreement.

[108] See S.M. O'Connor, "The De Minimis Exemption of Stored Value Cards from Regulation E: An Invitation to Fraud?" (1998), 5 Richmond Journal of Law and Technology 6, Para. 16.

Furthermore, cases of "black box" transactions are not analogous to normal cash transactions. It ought to be borne in mind that when a consumer engages in an SVP transaction, they are relying upon a third party to deduct the proper value from their electronic purse. Without disclosure, there is no means of ascertaining the amount that is deducted. Hardly any individuals would be prepared to engage in cash transactions where one gives their wallet to a merchant and asks them to "take what is necessary and return the rest." We see no reason why such transactions should occur in the electronic context either.

Thus it is submitted that in the case of fraudulent transactions of this nature, liability ought to fall on merchants / issuers to ensure that steps are taken to prevent fraud in light of the fact that consumers are relying upon issuers and their agents to deduct the proper amount. While issuers claim that the distributed nature of SVPs hinders attempts to trace fraudulent transactions in the retail context, having them place a time and date stamp on the consumer SVP (which many currently do on the merchant SVP) would enhance a consumer's ability to demonstrate that an amount was deducted from their SVP which did not correspond to the amount on their invoice.

Other issues that need to be addressed in the consumer context include the issue of the voluntary surrender of an SVP by the consumer to an individual who acts either without or in excess of their authority. There is also the issue of consumer negligence in the safekeeping of a card and facilitating its unauthorized access and use. Space considerations do not allow us to discuss these issues here however suffice it to say that existing legal doctrines in relation to conventional access products (such as imposing

minimum levels of consumer liability) could serve as a useful guideline in setting rules in the SVP context.

12. Concluding Observations

The foregoing analysis demonstrates the existence of a conceptual unity among retail payment systems, regardless of whether they utilise debit (access) or smart (SVP) cards, so as to rationalize the application of common legal principles to all such retail payment systems. In fact, the conceptual unity may be broader so as to encompass all closed network systems, connecting participating banks and their customers, so as to facilitate a guaranteed payment. Possibly, the framework may further be expanded to cover guaranteed payments in open systems as well.

It is vehemently argued that the development of stored-value products ought not to be arrested by pre-mature over-restrictive regulation.[109] The counter argument is however that legal certainty is needed for both consumer and investor confidence. Moreover, while e-money products may defy traditional strict categories of regulation, it is imperative to secure they do not become no-man's land attracting predators seeking to act free of any form of regulation. The proper development of stored-value products by legitimate enterprises to meet genuine market needs will be hampered if they are used by others strictly as a means for law evasion.

[109] See generally, President W.J. Clinton and Vice President A. Gore Jr. "A Framework for Global Electronic Commerce." Online: <http://www.iitf.nist.gov/eleccomm/ecomm.htm> (date accessed: July 1, 1997).

Authors' Biography

Benjamin Geva

Benjamin Geva is a Professor of Law at Osgoode Hall Law School in Toronto. He specializes in commercial, financial and banking law, particularly in payment and credit instruments, electronic banking, and the regulation of the payment system. He obtained his LL.B. (cum laude) at the Hebrew University of Jerusalem (1970) and his LL.M. and S.J.D. at Harvard. He practised in Israel and Canada and held visiting positions at various universities in the United States, Israel, Australia and France. Under the IMF technical assistance program, he has advised authorities in several countries on payment and banking law matters.

Professor Geva is the founding editor-in-chief of the *Banking and Finance Law Review* and the author of several books on payment instruments and electronic funds transfers published in Canada, US and UK. He has been involved in law reform projects in Canada on secured transactions, the transfer of securities, and electronic funds transfers.

Muharem Kianieff

Muharem Kianieff is currently a D. Jur. candidate at Osgoode Hall Law School of York University in Toronto, Canada. He is currently writing his dissertation on consumer electronic payments with an emphasis on electronic commerce. He holds an LL.B. from Osgoode Hall and a B.A. (Hons.) in Politics and Economics from Trent University in Peterborough, Canada.