CONSUMER PROTECTION AND STORED VALUE FACILITIES

LYNDEN GRIGGS*

Stored Value Facilities are becoming increasingly available for Australian consumers. But what are the consumer protections offered to users of these facilities. This article examines and outlines what is a stored value facility, considers their advantages and disadvantages and the current role of the Electronic Funds Transfer Code of Conduct. The paper will conclude with a summary of the consumer protection norms that should guide future development of this area.

I INTRODUCTION

In 1995, it was predicted[1] that within 10 to 15 years, stored value facilities[2] (SVF) such as electronic or digital cash would be the primary way in which consumers would pay for routine consumable goods and services of small value. With the prescience of hindsight, and the dawn of 2010 nearly upon us, we can now say with some degree of certainty that SVF will not be, at least immediately for Australian consumers, the currency of choice for the purchase of low value products, or micro payments (outside possibly of the transport sector).[3] However, at the risk of being proven wrong, the submission is that government initiatives, market reality, and global pressures are likely to see the establishment of the infrastructure necessary to promote the use of electronic payments through SVF,[4] and that perhaps rather glacially, the revolution, or at least the

* Senior Lecturer, University of Tasmania <Lynden.Griggs@utas.edu.au>.

1 For example, G Stuber, *The Electronic Purse: An Overview of Recent Developments and Policy Issues,* (Technical Report No 74, Bank of Canada, Ottawa, 1996) suggested that within 15 years of 1996, 60% of cash transactions worldwide would be undertaken using an electronic purse.

2 Stored value facility (SVF) is defined by the Australian Securities and Investments Commission (ASIC) as follows: ASIC, *Electronic Funds Transfer Code of Conduct* (2008) 11.2: '"stored value facility" means a facility (for example software) which:
(a) is designed to control:
(i) the storage of value; and
(ii) the release of that stored value from the facility in the course of making a payment using that stored value;
(b) is intended to be in the possession and control of a user; and
(c) contains a value control record.'
In this article, I propose an even wider definition that would encompass products where the card does not contain a value control record. For example, most gift cards, prepaid cards today do not use the stored value on the card, but rely on remote authorisation to ascertain the value. At present, these are not covered by either Part A or Part B of the Code.

3 However, it is recognised that SVFs are in use for transport schemes and the like. For example, the Victorian smartcard transport system known as Myki <http://www.myki.com.au/> at 13 August 2009.

4 For example, a report prepared by the Centre for International Economics, *Exploration of Future Electronic Payment Markets* (2006) for the Department of Communications, Information

evolution predicted some 15 years ago,[5] will come to fruition in this country in the not too distant future. This development will be driven by the demands of a more tech-savvy generation, improved reliability, and the success of SVF in other jurisdictions, decreasing costs, and increasing confidence in the global market.[6] Current and likely uses of this type of product include the following:

- Transport;
- Retail;
- Road toll tags;
- Electronic passports;
- Telephone calling cards;
- Healthcare;
- Payroll;
- Closed loop facilities such as cards available to pay for purchases within a particular sector (such as a University);
- Identification cards;
- Fobs such as contactless entry keys;
- Virtual cards for internet/phone purchases; and
- Mobile Phone SIMS facilities.[7]

Specific illustrations already currently in use nationally and internationally include, with the focus largely in the transport sector:[8]

Technology and the Arts, highlighted the economic benefits associated with an expansion of non-cash electronic payment systems. Cited in ASIC, *Reviewing the EFT Code* (2007) 17.

5 On a global level, the two countries that widely use stored value products are Germany and Singapore. In 2006, 65.91ml cards were issued in Germany with 12.04ml issued in Singapore. Many of these relate to the transport systems in operation in those jurisdictions. E Akindemowo, 'Contract, Deposit or E-Value? Reconsidering Stored Value Products for a Modernized Payments Framework' (2009) 7 *DePaul Business and Commercial Law Journal* 275, 276, fn 8.

6 As of 2008, there was 7.23ml Internet subscribers in Australia, ¾ of these were broadband (Australian Bureau of Statistics, *Internet Activity in Australia*, 2008).

7 Australian Government, Department of Finance and Deregulation, *National Smartcard Framework: Smartcard Handbook* (2008) 4, for a wider list of possible applications.

8 Extracted from Australian Government, Department of Finance and Deregulation, *National Smartcard Framework, Case Studies* (2008) 6. A number of other cities are also featured in the report.

Location	Project	Sectors	Cards issued to December 2006	Transactions per day
Hong Kong	Octupus	Transport, retail, parking	13ml	30ml
Rome	ATC/Cotral Metrebus	Transport, parking	500k	4ml
Singapore	EZ-Link	Transport, retail	9ml	4ml+
London	Oyster	Transport, retail	5ml	2ml+
Washington	Wamata/SmartTrip	Transport, parking	2.2ml	500k
Seoul	T-money	Transport, parking, retail	5ml	500k
Sydney	Tcard (this system was abandoned and is set to be replaced by a new electronic ticketing system)	Transport	250k+	Not available
Brisbane	Translink	Transport	<500k	Not available
Melbourne	MyKi (now being progressively introduced)	Transport, retail	0	N/A
Perth	Smartrider	Transport	450k	>100k

A *A Specific Illustration – the Octopus Card of Hong Kong*

The most widely used SVF in the world is the Octopus card of Hong Kong.[9] For an adult this card can be purchased for $50 (HK), and can have a reloaded value of up to $1 000 (HK). It can be used at over 2 000 service providers, and within Hong Kong there is in excess of 50 000 card readers, with some readers displaying the last 10 transactions. Widely used on the transport system including buses, trains, trams and light rail, the card can also be used at the large fast food chains such as Café de Coral, Fairwood, and MacDonalds. All major supermarkets (Vanguard, Park and Shop, Wellcome and Taste) as well as most convenience stores (for example 7 Eleven) will accept the card, with some supermarkets having Octopus card express lanes. The card can also be used at some providers whereby the consumable (such as a newspaper) is simply collected by the consumer, and the consumer then swipes their card against the reader without intervention of shop assistants. An industry of Octopus Card accessories has also arisen with, for example, the electronic chip of the card now inserted into female and male watches. Cards can be reloaded at many outlets, and it is also possible to link ones card to a credit card, so that when the stored value on the Octopus card

[9] Octopus <http://www.octopus.com.hk/home/tc/index.html> at 21 August 2009.

reaches a certain level, the card is reloaded from the credit card – in effect an endless line of credit.

This growth in the adoption and use of SVF inherently leads to one question. What consumer protections are embedded for the users of these products? And, perhaps more importantly, what should be the consumer protection norms? The importance of this cannot be underestimated. Up to now, the analysis has largely centred on the theoretical legal framework and the system risk associated with the payment systems of SVF. The critique, so far, has not been undertaken from the consumer perspective. If we ask the following question: What consumer protection principles and values should guide the legal and regulatory regime that will be built around SVF, what answer is given? As Akindemowo[10] notes: 'If the concern is possible risks to the payments system, then the card issuer perspective will be the appropriate one to adopt. If the concern relates to consumer protection, then the cardholder's perspective is key.' On a macro level, without an appropriate legal and regulatory regime in place the advantages offered by them, and the economic growth to which SVF can contribute will be greatly stifled – Australia will be left at a competitive disadvantage relevant to its global partners. On a micro level, if modern consumer protection norms are not adopted, then the imbalance between the initiators of this system as against the users will be stark and likely to exploitation – consumer interests will be captured by industry. Critically, it is important to note that both sides of the transacting divide will benefit from improved consumer norms. Systemic security will be enhanced, confidence within the process heightened, with both these factors leading to higher usage of SVF.[11] Further, with payment fraud on the increase, with this driven specifically by credit and charge card fraud,[12] a facility that offers both convenience and security offers clear advantages to all concerned. Government will benefit from a rise in consumer activity, merchants will add revenue through another stream of business with quality producers able to package their wares to the world, and consumers will have opportunities to access goods and services otherwise not possible. The importance of this analysis recognised by the ongoing review conducted by ASIC into the *Electronic Funds Transfer Code of Conduct,* with this influencing the regulation of SVF.[13] With this background in mind, this paper will be structured in the following way:

(i) What is a SVF?
(ii) What advantages and disadvantages do they offer to a consumer?
(iii) What is the current consumer protection regime?
(iv) What are the consumer protection norms that should inform the regulatory regime?

---

10 Akindemowo, above n 5, 341.

11 The lack of standardisation in the software and hardware used by industry is something that could be remedied by industry working together for the benefit of consumers.

12 Australian Payments Clearing Association, *Media Release: Payments Fraud In Australia* (2008) <http://www.apca.com.au/> at 1 August 2009, indicates that the total rate of fraud has increased by 5.9 cents (in 2007) to 7.2 cents of every $1 000 of payments. Cheque fraud declined (1.4 cents to 0.8 cents); debit card fraud slightly increased (7.1 cents to 7.4 cents), whereas credit and charge card fraud increased from 38.6 cents to 50.2 cents in every $1 000 of payments.

13 A revised EFT Code is expected to be released sometime in 2009. At the time of writing this has not occurred. The ASIC's proposals for amendment are discussed (ASIC, *Review of the Electronic Funds Transfer Code of Conduct 2007/08: ASIC proposals,* Consultation Paper 90 (2008)).

II WHAT IS A SVF

A SVF is a prepaid card/electronic wallet that, as the name suggests simply stores value on that instrument. A person (consumer) will buy a SVF that will contain a certain value from an issuer. The consumer will use the facility to purchase goods or services from commercial entities that are part of the scheme attached to the facility. The entities will then redeem from the issuer the value of the transaction that has been undertaken with the consumer. SVF can come in many forms, including Internet accounts, smartcards, contact-less instruments and magnetic strip cards. Some SVF will also allow for the value of the card to be reloaded. Explained in this way, SVF are currently wider than the definition provided by the *Electronic Funds Transfer Code of Conduct.*[14] With this expansive view in mind, some examples are as follows:

A *Gift Card*

A simple example of a non-reloadable SVF that can only be used once is a gift card from a retailer. This will contain either a magnetic strip or a microprocessor chip. The gift card will be inserted into the terminal that allows information to pass between the terminal and the card. Rarely would the identity of the gift cardholder be checked. This is also known as a closed loop system – acceptable only to a single entity.

B *Reloadable Stored Cards*

The next step in the continuum from the once-off gift card was to allow reloading, with an example being a photocopier card designed for use within a particular entity, such as a library, or a university card that can be utilised with the precinct of the specific college. When attached to something like a university they are regarded as a semi-closed system, with cards issued by organisations such as MasterCard and Visa regarded as open-loop. Open loop cards able to be used at any retailer accepting the issuing card. Technically, reloadable stored cards operate in a similar way to the gift card, but provide for value to be added via the issuing institution.

C *Reloadable Contact-Less Stored Cards*

The next generation from the reloadable card was the arrival of the contact-less card able to be used by a variety of different merchants, such as the Octopus Card in Hong Kong. In addition, we see some countries such as Russia and United States of America using SVF as a means by which to load the salary and wages of their employees.[15] These cards allow for purchases that require neither a signature nor a PIN number to access. They have the functional equivalency of cash. In Australia, for example, ANZ has recently released the ANZ Stadium Visa PayWave card, which is both reloadable and no authentication is involved for transactions under $35.[16] Another example available in Australia is the Technocash Card.[17] With this card, individuals are able to

---

14 See ASIC, above n 2.

15 For a discussion of this see AS Rosenberg, 'Better than Cash? Global Proliferation of Payment Cards and Consumer Protection Policy' (2006) 60 *Consumer Finance Law Quarterly Report* 426.

16 See ANZ, *ANZ Stadium Australia's Home Ground* <https://your.prepaidcardsupport.net/stadium/index.do> at 3 August 2009.

17 See Technocash <http://www.technocash.com/> at 17 August 2009.

hold monies in multiple currencies, easily transfer money internationally with this free for a transfer to another Technocash card, as well as securely make Internet purchases.

D *Card-less Facilities*

In Australia, we have recently seen the arrival of the virtual visa card,[18] which does not involve the issue of a physical card, but the delivery to the consumer of a prepaid single load product that can be used for shopping on the Internet, by phone or mail order. The process involves the encryption and decryption of information between the consumer, the issuer, and the merchant. It is not necessary that the merchant be aware of the identity of the consumer.

E *Mobile Payments*

Used extensively in Japan and South Korea, mobile phones embedded with microprocessor chips can be used as payment devices.

F *Digital Cheques*

The process is similar to the writing and authenticating of paper based cheques. However, it adds the feature of a digital signature[19] that has been encoded onto the electronic signal.[20]

G *Digital Cash*

The ultimate goal in the development of SFV would be the arrival of an alternative currency – this being digital cash. This product, which allows storage of money as a computer code whereby a person seeking to receive a digital coin sends a coded message to the bank. The bank decodes this and then sends a message with the digital coin attached. This digital coin has the bank's security features embedded. The coin is then used to purchase goods on the Internet. As noted by ASIC, 'this type of product has not been successfully commercialised in Australia (or, generally, elsewhere) to date'.[21] Despite the differences between the various types of products, diagrammatically, the relationship between consumers, merchants, and issuers of all SVF products can be reduced to the following illustration:[22]

---

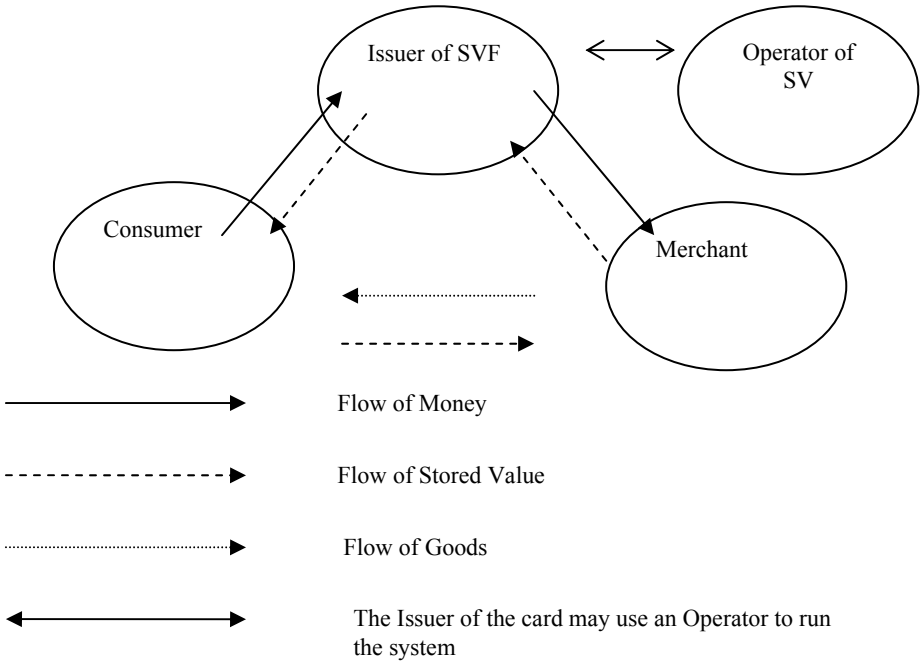
18 For example, see the Product Disclosure Statement of the V-Card issued by Visa. VCARD, *Now You Can Shop on the Internet and Pay by Visa Without Using a Credit Card* <http://www.virtualvcard.com.au/> at 11 August 2009. In Australia, one issuer of the product is the Heritage Building Society based in Toowoomba, Queensland.

19 A digital signature is 'appended date or a cryptographic transformation of a data unit'. Standards Australia, *Health Informatics – Public Key Infrastructure Part 1: Framework and Overview*, AS ISO 17090.1-2003 (2003) [7.3]. Digital signatures use asymmetric cryptography. The signer of the document adds their private key to a document (this is a string of letter, numbers and/or symbols). This key is attached to a computer-generated code resulting in a different signature for each document. A third party such as a certifying agency then confirms that the public key is a match to the private key and that the private key is attached to a designated person or individual. The certifying agency then uses its own key to verify the document signer. The other party associated with the transaction is then able to decrypt the sender's signature and verify the sender.

20 As to the dangers associated with a digital signature, see J Winn, 'The Emperor's New Clothes: The Shocking Truth about Digital Signatures and Internet Commerce' (2001) 37 *Idaho Law Review* 353.

21 ASIC, *Reviewing the EFT Code,* Consultation Paper 78 (2007) [2.14].

22 Adapted from Monetary Authority of Singapore, *Stored Value Facility Guidelines* (2006) 3.



As outlined, the question posed by this article is not so much how the underlying theoretical legal framework is to operate. These views are largely polarised. On the one hand, there is the accounts based analogy of SVF that sees it as a deposit made by a consumer, the operation of an account, and a relationship between customer and issuer similar to that of principal and agent.[23] By contrast, some speak of SVF as electronic impulses embodying underlying legal rights without resort to some central provider.[24] With this matter possibly intractable, the matter can, and should be considered from a different perspective – that is the perspective of the consumer. What are the consumer values and principles that will drive this form of business? If we get this right, and recognise the practical and contextual use of the SVF, then the consumer norms adopted can inform both systemic security and the underlying risks to the consumer. By undertaking the analysis from this direction, the objectives and utility of SVF can be fulfilled. There is no doubt that systemic security (or the perspective of the issuer of the SVF) can inform consumer norms, but on occasions, the critique may well be different. For example, where disclosure of the terms and conditions associated with these products present terms that are inherently one-sided, no issue of systemic insecurity is raised, yet the same issue may direct attention to consumer concerns.

---

23 See A Tyree, *Digital Cash* (Butterworths, 1997); R Bollen, 'The Development and Legal Nature of Payment Facilities' (2004) *Murdoch University Electronic Journal of Law* 19.

24 D Kreltszheim, 'The Legal Nature of Electronic Money – Part 1' (2003) 14 *Journal of Banking and Finance Law and Practice* 161; D Kreltszheim, 'The Legal Nature of Electronic Money – Part 2' (2003) 14 *Journal of Banking and Finance Law and Practice* 261; Akindemowo, above n 5, 275. Akindemowo states: 'Conceptualizing the [Stored value product] as a deposit is oxymoronic. Stored value transactions proceed on the basis that a prepayment has been made and deposited in an account belonging to a party other than the cardholder. The merchant is reimbursed by the card issuer arranging a transfer of funds from the underlying account to the merchant's account. The underlying funds do not usually belong to the cardholder. In cases where the underlying funds do belong to the cardholder as her deposit, the card functions as an access, not a stored value, device.'

III THE ADVANTAGES AND DISADVANTAGES OF SVF

The advantages are intuitively obvious. First, depending on the extent of disclosure within the particular type of SVF, the seller may not know the identity of the consumer. Whereas credit and debit card companies are able to trace the spending habits of a consumer, with certain types of stored value products (such as digital cash), this will not be possible. The privacy and confidentiality of the consumer will be assured. Second, as noted, SVF may well present a more secure platform than what presently exists. Cryptographic technology should ensure that systemic security is minimised with multinationals such as Visa and MasterCard[25] looking to implement non-jurisdictional specific safeguards. Third, some stored value products such as smart cards are extraordinarily resistant to counterfeiting. This can be contrasted with magnetic stripe cards that enable the skimming of data from the strip and the replication of many cards. Fourth, SVF present a counterattack to the dangers of phishing or 'man-in-the-middle' fraud. In this scenario, information sent via electronic means to a supposedly authentic looking financial institution is intercepted, with this phished information then used for fraudulent purposes. Smart card technology has the potential to remove the 'middle man' as no connection to a bank or financial institution is necessarily required at the time of transacting.

Conversely, SVF do come with a number of disadvantages. First, where the stored value product involves a card that does not require authentication at the point of purchase, the card itself will then be as good as cash. Loss of the card may well see loss of the stored value. Second, and perhaps more threatening is sophisticated criminal fraud through intentional hacking into a person's computer and through this being able to access an electronic wallet of digital cash. The criminal's task is, on the one hand, made simpler by the paperless and transferable nature of many SVF, yet the digital DNA left by some of these products may well allow some level of government tracking and intervention (which equally may reduce some of the confidentiality and privacy associated with SVF). The consumer (as will the merchant) will also face two specific security issues. The first is one of identification integrity – how does each party verify that the person with whom they are dealing is the person they say they are. Second, how does each party ensure that the messages sent and received (the critical offer and acceptance in traditional contract law analysis) are in fact the intended message by each party to the transaction. Again, encryption represents the somewhat bland answer, though no doubt behind this there is a complex technical solution. Those with an economic interest to ensure that the dangers of misidentification can be minimised must invest appropriate technology. To date, secure socket layer (SSL) has been the worldwide standard for authentication, encryption and privacy protection. Visa and MasterCard have also jointly developed Secure Electronic Transaction (SET) protocols to assist with electronic commerce. Further investment in this area is needed.

Finally, a specific problem associated with electronic currency is the potential for the 'money' to be double spent – a consideration not possible to the traditional physical

[25] An example is the Mondex, part of the MasterCard suite of smartcard products. This product can be used to purchase goods over the Internet, via interactive television or through the mobile phone. Money can be stored in a number of different currencies with no limit (subject to national regulation) as to how much cash can be transferred. A consumer will insert their card into a reader attached to the particular device, with the card then verifying that a Mondex reader is present at the supplier's end. The value is then transferred across.

form of banknotes and coins. For example if digital coins are generated and held on a hard drive, and then spent with a merchant who does not verify the legitimacy of those coins, it may be possible for the consumer to double-spend the coins. This problem can easily be overcome. First, the financial institutions may only issue single-use coins with these verified through the issuing financial institution. For example, Akindemowo[26] describes how a transaction may occur through digital cash, with appropriate safeguards against double spending:

1) a request for digital coin is made of a bank by a consumer;
2) the bank attaches its verification to the digital coin;
3) the coin is stored on the consumer's hard disk until needed;
4) the consumer having made a purchase spends the coin with a business entity;
5) the vendor will verify the digital signature of the bank;
6) the vendor checks that the money has not previously been spent;
7) the goods are transmitted to the consumer;
8) the merchant will surrender the coin to the bank in exchange for new coin, or credit for an equivalent amount.

IV WHAT ARE THE CURRENT CONSUMER PROTECTION NORMS?

In Australia, Part B of the Electronic Funds Transfer Code of Conduct[27] applies to SVF and stored value transactions – though it has a significant limitation in only applying to those who subscribe to the Code[28] as well as providing a limiting definition.[29] Despite these limitations, an overview of the Code will highlight current government regulatory thinking in this area.

Stored value is defined to mean:
'a representation of value that:
(a) is intended to be used to make a payment (for example digital cash or units of value recorded in a computer chip on a card); and
(b) may or may not be dominated by reference to units of a currency.'

Stored value facility means:
'a facility (for example software) which:
(a) is designed to control:
  (i) the storage of stored value; and
  (ii) the release of that stored value from the facility in the course of making a payment using that stored value;
(b) is intended to be in the possession and control of a user; and
(c) contains a control value record.'

---

26 OE Akindemowo, 'The Fading Rustle, Chink and Jingle: Electronic Value and the Concept of Money' (1998) *University of New South Wales Law Journal* 24, 11 of online version.

27 ASIC, *Electronic Funds Transfer Code of Conduct* (issued 1 April 2001, amended 18 March 2002 and 1 November 2008).

28 Signatories to the Code include almost all banks, building societies and credit unions as well as a number of other entities that are involved in finance services (for example American Express International, LinkLoan Services Pty Limited, Money Switch Limited, Rural Finance Corporation of Victoria, Baptists Investment and Finance Ltd, Technocash, Territory Insurance Office).

29 It currently would not apply to most toll cards, prepaid cards, and the like, as they do not have a self-contained record of the value left on the card. This can only be found by access to remote infrastructure.

The ethos associated with the Code is drawn, not surprisingly, from the type of protection provided to investors, rather than consumers. Empowerment by way of disclosure is seen as sufficient, intervention an unnecessary impediment to the market. Those to whom the Code applies are required to prepare and provide unambiguous terms and conditions,[30] with a focus on disclosure surrounding the charges imposed, the expiry date, the user's right to a replacement, the capacity to exchange stored value for money, and the process involved in reporting a loss.[31] Any changes, such as increased fees, must be notified to users, with at least 20 days notice before the change takes effect.[32] A user is able to obtain a record of the available balance, with rights to exchange stored value established as well as a refund of lost or stolen stored value outlined under the Code.[33] Two points of contrast can initially be made between Part B of the Code, which applies to stored value operators, and Part A, which applies to electronic funds transfer transactions.[34] Under Part A, clause 4.2(a), the account institution is required to provide a record of account every six months, whereas stored value operators need only provide a process by which the account balance can be checked.[35] The second difference is, from a consumer perspective, more fundamental. Under Part A of the Code, liability for unauthorised transactions is strictly controlled. For example, clause 5 (applying to EFT transactions) provides that the user is will not be liable for:

- Losses caused by the fraudulent or negligent conduct of the employees or agents of the institution;
- Losses that result from an access method that is faulty;
- Losses that result from the use of a device or code forming part of the user's access method, with critically, the account institution having the onus of showing that the user received the device or code. Proof of delivery to the user's postal address not meeting this requirement;
- Losses caused by a double debit.

Under Part A, the account holder is also not liable for transactions that occur after notification of loss of access method or device[36] or where it is clear that the user has not contributed to the loss.[37] The account holder will be liable where the institution is able to show, on the balance of probabilities, that the losses resulted from the fraud of the user, an unreasonable delay in notification of loss of access method[38] or where the user voluntarily discloses the codes, keeps a record of the code near the access device (such as a card) or where the user is instructed not to use birth date or part of the name as the

30 ASIC, *Electronic Funds Transfer Code of Conduct*, above n 27, [12.1].
31 Ibid [12.3].
32 Ibid [13].
33 Ibid [15]-[16].
34 Electronic Funds Transfer is defined as follows: 'funds transfers initiated by giving an instruction, through electronic equipment and using an access method, to an account institution (directly or indirectly) to debit or credit an EFT account maintained by the account institution.' Ibid [1.1(a)].
35 Ibid [14]. 'Stored value operates must ensure that an undamaged stored value facility (either by itself) or together with other equipment reasonably available to users) enables a user to ascertain the amount of stored value controlled by the stored value facility, which is available for use.'
36 Ibid [5.3].
37 Ibid [5.4].
38 If a code was required to perform the electronic funds transaction, and the user did not engage in fraud, or delay notification, the most the user will be liable for is $150. Ibid [5.5(c)].

access code.[39] By contrast to Part A, liability under Part B for unauthorised stored value transactions is far less prescriptively stated and which more heavily favours the stored value facilitator. Clause 16 provides as follows:

> Where:
> a stored value operator, together with relevant system participants, has or can create a reliable record of the amount of the stored value controlled by a stored value facility from time to time; and
> the stored value operator and any relevant system participants can prevent any further transfers of stored value from the facility;
> the stored value operator must:
> provides a means for a user to notify the stored value operator (or other entity specified by the stored value operator) at any time of the loss or theft of the stored value facility; and
> where a user gives notice under paragraph 16(1)(c), pay the user the amount of the stored value which the stored value operator could have prevented from being transferred from the facility.

In furtherance of these aims, the stored value operator must be able to inform the user whether anything can be done to prevent unauthorised use and whether a refund will be made. The Code indicates that the capacity to provide a refund will depend on the technical capabilities of being able to prevent unauthorised use and the ability to be able to determine the balance at any given time.[40] In effect, unlike Part A, there is no broad consumer protection given to users of SVF – the onus of responsible use and protection is placed very strongly on the user, rather than the issuer.

As noted in the consultation paper prepared by ASIC[41] on the *Electronic Funds Transfer Code of Conduct* the lesser standards for unauthorised transactions of a SVF represent the dictates of the marketplace, rather than the 'higher standards of consumer protection.' Due to the these deficiencies and the evidence that stored value operators are unlikely to subscribe to the Code,[42] a joint submission of Choice, Consumer Action Law Centre, and the Centre for Credit and Commercial Law-Griffith University, submitted that Part B be removed from the Code and re-published as a best practice guideline to be adopted by the industry on a voluntary basis. It was suggested in this submission that 'If stored value products become widespread, Part B could be used as the basis for a more specific Code of Conduct for stored value products, not linked to the EFT Code.'[43]

The suggestion is that, as a first step, the time for doing this is now. If the regulatory infrastructure is put in place at the outset, the advantage is that it will ensure that the appropriate consumer protections are highlighted, and not hijacked by industry. With

---

39 Ibid [5.6]. This is a subjective test, the user means the actual user and in determining whether an instruction was given, the capacity of the user to understand the warning must be taken into account. Ibid [5.6].

40 Ibid [fn 39 of the Code].

41 ASIC, *Reviewing the EFT Code*, above n 21, 81.

42 Ibid 79.

43 Choice, Consumer Action Law Centre and Centre for Credit and Commercial Law Griffith University, *Electronic Funds Transfer (EFT) Code of Conduct Submission (v20 Public – 30 May 2007)* to the 2007 ASIC Review of the EFT Code <http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/Galexia.pdf/$file/Galexia.pdf> at 19 February 2010.

new products such as 'prepaid electronic gift cards and online payment products'[44] now entering the market, it is critical that the regulatory regime be designed to promote innovation, yet still provide appropriate consumer safeguards. Accordingly, the next section considers the broad principles or norms that should govern consumer protection for stored value products.

V WHAT ARE THE CONSUMER PROTECTION NORMS THAT SHOULD INFORM THE REGULATORY REGIME?

At the outset, it is important to recognise that any level of interventionist consumer protection will have costs. In this respect, the so-far light-handed approach to regulation may be considered appropriate given the nature of the products with which we are dealing. Consumer expectations with many of these types of products will intuitively be less than associated with a traditional deposit facility provided by a financial institution. In looking to meet consumer expectations, the diverse nature of these types of products, and the difficulty in definition presents a foundation stone difficulty. The simplest example of a SVF, (gift card), encompasses a number of characteristics that have relatively different levels of importance to the consumer. For example, one may purchase a gift card as a present – ease of transferability is critical, the card is the equivalent of cash. Another may see the time limit for expiration as vital, another the range of stores at which the card can be used, a further the possibility of using it for online purchases, another the chance to re-load value onto that card. In other words, there may be competing values in play when consumers purchase the gift card. Accordingly, any regulation needs to reflect this and not overly inhibit innovation or restrict consumer choice by the impediments of government regulation. What then is important is to identify the core underlying expectations of every consumer when purchasing a SVF and use these as a minimum in expressing the values that must guide any future directives. Beyond this, and there is a risk that consumer choice will be effected and the dynamic efficiency demanded of a contemporary economy may be stifled - an outcome obviously undesirable. For this reason, and seeking to balance the expectations of consumers with industry, it is suggested that the following norms be adopted, with this incorporating both best practice guidelines as well as the canons that will inform the package of consumer reforms needed.[45]

1 *SVF must be Categorised by Product Rather than Payment Authorisation*

The current definition within the *Electronic Funds Transfer Code of Conduct* highlights the difficulties in attempting to define how these types of products evolve. Because of this ASIC has proposed that the current two-part structure to the *Code of Conduct* be

---

44 ASIC, *Review of the Electronic Funds Transfer Code of Conduct 2007/08: ASIC Proposals,* above n 13, 8.

45 See also Monetary Authority of Singapore, *Stored Value Facility Guidelines* (2006). There has been limited academic discussion of the consumer protection norms associated with the new forms of consumer transactions. In the European context, with a particular emphasis on online auctions, see I Barral, 'Consumers and New Technologies: Information Requirements in E-commerce and New Contracting Practices on the Internet' (2009) 27 *Penn State International Law Review* 609; C Riefa, 'Consumer Protection on Online Auction Sites: Just an Illusion' (2005) 16(3) *Computers & Law* 34; C Riefa, 'To be or Not to be an Auctioneer? Some Thoughts on the Legal Nature of On-Line 'Ebay' Auctions and the Protection of Consumers' (2008) 31 *Journal of Consumer Policy* 169; C Riefa, 'Consumers and Electronic Communication Laws in Europe and England: Reaping the Rewards of the New Regulatory Framework' (2006) 61(7-8) *Annales des telecommunications* 924.

replaced with a one-part structure, with a tailoring of the requirements for certain types of products. The reason for this was the little impact that Part B has had on the issuers of the new products (who do not subscribe to the Code), and that some suppliers of new products would, in any event, fall within Part A of the *Code*.[46] Whilst I agree that the new products do compete with traditional banking products and the starting point should be one that sees them treated no differently,[47] my submission is that this proposal does not go far enough, and is unlikely to be in a position to quickly respond to new products as they develop. Whilst we continue to focus on payment systems, the view will be issuer facing. With a focus on products, the view becomes consumer centred. With some types of SVF containing a record of its value (such as a electronic purse and some smartcards), yet with others only possible to determine this by way of remote access (and thus not within the definition of Part B of the Code), the advantages of defining by product allows for comprehensive coverage and swift alteration as new products come on the market. The advantages of definition by product rather than payment are numerous for the consumer. With consumer expectations altering as the product changes (for example consumer expectations may be that the purchase and redemption of a gift card should be anonymous), yet in other scenarios, some level of protection and identification (at least by code) of the owner of the SVF may be considered appropriate (for example a travel card holding thousands of dollars of stored value). ASIC in its proposals do attempt to take account of this by providing that the general requirements under the Code would not apply for products where the issuer is not able to cancel the product if lost or stolen, there is no electronic authorisation and the maximum value held on the product is less than $100. The rationale for this exemption is that low value products of this nature represent lower risks to consumers, whereas cards that store significant sums should be subject to the general rules that allocate liability for unauthorised transactions.[48] Whilst laudable in its aim, and given that businesses that offered newer electronic products did not submit to the review, it may be possible that, short of making the Code mandatory, such steps would have little effect.[49] For consumer benefit, regulation by product is required.

2 *Reliable, Safe Infrastructure (Hardware/Software/Regulatory)*

Industry must meet consumer expectations that the infrastructure has the capacity to meet the reasonable expectations of consumers. This would involve appropriate design, testing and redress measures for consumers should the system fail to operate as expected. Each issuer of a SVF should ensure that they have regular testing and independent auditing of the system. This system should have adequate security including authentication procedures when required, ant-counterfeit technology and anti-money laundering guidelines.[50] However, reliable, safe infrastructure is not just a reference to the technology that underlies the system. Whilst operational risk is

---

46 ASIC, *Review of the Electronic Funds Transfer Code of Conduct 2007/08: ASIC Proposals*, above n 13, 14.

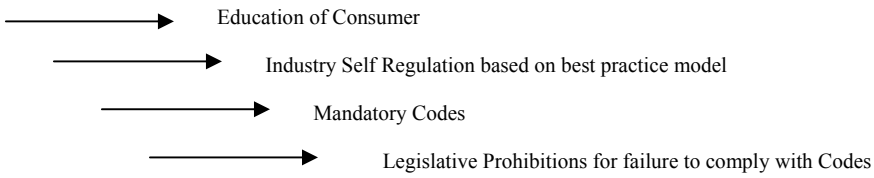
47 Ibid 15.

48 Ibid 19-20.

49 Ibid 24, recognise that promotion of the Code to potential subscribers and increasing consumer awareness is likely to have little impact. 'Behavioural economics research shows that consumers tend to be overoptimistic when choosing providers, in the sense that they discount the likelihood of adverse events such as a dispute with their provider over an unauthorised transaction.'

50 Such as the USA guidelines of the industry association: Network Branded Prepaid Card Association, *Recommended Practices for Anti-Money Laundering Compliance for US based Prepaid Card Programs* (2008).

important, regulatory risk must also be managed. Consumers must not be misled into thinking that safeguards are in place when this is not the case. For this reason, a model is required which works on cascading levels of penetration by government into the marketplace to safeguard the consumer needs of an inexpensive, safe, reliable stored value system that sees the technology utilised to provide, in an economic sense, consumer surplus. This model would require extensive consumer education of the risks associated with SVF and industry self-regulation through a best practice model. Should this prove unsatisfactory, legislative interference with a mandatory code accompanied by statutory prohibitions would be required.[51]



3 *Disclosure must be made Prior to Sale/Terms must be Fair*

Consumer expectations are that full disclosure of all terms and conditions, including fees, charges, redemption rights, dispute resolution rights must be expressly articulated and outlined to the consumer. These must be brought to the consumer's attention prior to the sale of the product, with particular emphasis on expiration dates, liability for unauthorised transactions, and the right to redeem stored value.[52] Examples of the types of clauses that may catch the consumer unaware can be seen in the ANZ Stadium Visa PayWave Card. This SVF allows for purchases of less than $35 without authorisation and a maximum reloadable limit of $700. Unlike Part A of the *Electronic Funds Transfer Code of Conduct,* the conditions associated with unauthorised transactions are far narrower. The terms and conditions provide that: 'The Card user is liable for all transactions on this card except where there has been fraud or negligence by ANZ.'[53] In addition, a $15 administration fee is imposed to issue a replacement card when it expires.[54] Perhaps even more starkly, the Visa VCard highlights the consumer risks associated with the purchase of a SVF.[55] This product is a Visa prepaid single load card number that can be used to purchase goods and services online or by mail order. Whilst it is in its incipiency in Australia, its worth has been proven in other jurisdictions.[56] It is not a credit card and the only value that can be accessed is the stored value on the card.

---

51 Such as enforcement through s 51AD of the *Trade Practices Act 1974* (Cth).

52 See ASIC, *Review of the Electronic Funds Transfer Code of Conduct 2007/08: ASIC Proposals*, above n 13, 18 where in the case of low value products they suggest that at a minimum, consumers must be given a summary and notice as to how they might find out the terms and conditions.

53 ANZ Stadium Card, *Terms and Conditions*, cl 13 <https://your.prepaidcardsupport.net/stadium/terms.do> at 3 August 2009.

54 Ibid cl 9, provided that at least $15 remains on the card at expiry. Presumably if less than $15 remains on the card no replacement card is issued.

55 The product disclosure statement for this product can be accessed at VCARD, above n 18. In Australia, one issuer of the product is the Heritage Building Society Limited, based in Toowoomba, Queensland.

56 A visa virtual prepaid card was launched in Ireland in 2005, and by the end of March 2007, there was 100 000 active cards, representing 15% of the national online purchasing population. Visa, *Card-less Visa Payment Launches in Australia* (2007) <http://www.visa-asia.com/ap/au/mediacenter/pressrelease/NR_AU_151107.shtml> at 3 August 2009.

The consumer can choose how much to load onto the card (within a range of $50-$1 000), and there is no restriction on the number of cards that can be purchased by an individual consumer. On the expiration of the VCARD, the fee charged is the remaining balance left on the card. Thus, a person who buys a card and loads $700 on it, but then has $300 left remaining at expiry, will have a fee charged of $300.[57] No prior notice will be given of this extraction nor do the funds attract any interest. The VCARD is not backed by a deposit account with the issuing institution. Whilst the terms in both the PayWave card and the VCARD are in the respective documents, the operation of these terms may well not meet best practice guidelines and demand a more interventionist strategy. For example, it is difficult to see how the refusal to provide a refund of the balance remaining could be reasonably necessary to protect the legitimate interests of the issuer of the card.[58] It would seem simple to notify that consumer that this will occur and provide a reasonable time for the money to be spent. Similarly, the heightened responsibility placed on the consumer to protect against misuse may well be seen as a significant imbalance in the respective rights of the parties.[59] Another example of a term that intuitively seems unfair is that contained within the Technocash Card where on some of its products, if there has been no login activity for a year, the monies become the sole property of Technocash.[60]

VI CONCLUSION

Consumer, consumers law scholars, practitioners, policy makers all face a world where the dam to halt technological advancement has not yet been constructed. SVF are no different. Increasingly, almost imperceptibly, these sorts of products are becoming increasingly available, and whilst we may not see a significant change in our purchasing habits a year from now, it would be a courageous individual who would suggest that the lack of development that has occurred since the original epiphany of the mid 90's would be replicated over the next decade. Increasing standardisation by the institutions behind these products and the rise of a generation to whom technology is simply another form of social outlet will increasingly demand from the marketplace the suite of products that come within the broad rubric of SVF. The critical challenge is to be proactive, rather than reactive. Law must lead science and provide the regulatory framework that encourages innovation, competition efficiency, and fairness. Our goal is not to favour regulation over liberty but to balance the sometimes-competing ideals. By doing this, the regulation will in fact promote efficient market practices, encourage uptake by consumers and establish an industry driven by best practice of fairness, transparency, education, reliability and safety. As recognised through the review process of the *Electronic Funds Transfer Code of Conduct,* the present feathery touch of regulation for this product merely needs to be tweaked, with a focus on a watching brief. If education of the consumer and industry self-regulation fails to match these consumer goals, the call for a more interventionist strategy should be heard loud and clear.

---

57 VCARD, above n 18, cl 7.

58 For this reason it may fall foul of the proposed national unfair terms legislation (see Trade Practices Amendment (Australian Consumer Law) Bill 2009 (Cth)).

59 See Trade Practices Amendment (Australian Consumer Law) Bill 2009 (Cth).

60 See Technocash, above n 17 and link to terms and conditions.