MATTHEW FARRINGTON

PHISHING, PHARMING AND PHRAUD: ONLINE BANKING AND UNAUTHORISED TRANSACTIONS

LLM PAPER
E-COMMERCE (LAWS525)

FACULTY OF LAW
VICTORIA UNIVERSITY OF WELLINGTON

2005-2006

TABLE OF CONTENTS

ABSTRACT

This paper considers the contractual terms that govern the bank-customer relationship for online banking that operates in New Zealand and their practical effect on the customer. These contractual terms are analysed against the backdrop of the technical security measures adopted by banks in their online banking services. This paper highlights flaws in the online banking security systems and argues that these flaws, combined with the contractual terms, mean that customers face a disproportionate burden when trying to seek recompense for unauthorised transactions. This paper therefore offers some advice to customers seeking to challenge unauthorised transactions debited to their accounts. Customers may be able to resort to a combination of evidential, legal and public policy arguments. However, some of these arguments are such that fraudulent customers may be able to take advantage of them too. The paper therefore also offers some advice to banks. It conducts a survey of various comparative overseas jurisdictions. The practices of these overseas jurisdictions show that it is not necessary for contractual terms to be weighted so heavily in favour of banks. It suggests some technical measures that banks should adopt to address the potential vulnerabilities of the current security systems. Combining the legal and technical suggestions of this paper would potentially insulate banks against challenges by customers, while also ensuring greater practical security for online banking and a fairer and more balanced approach for both customers and banks.

STATEMENT ON WORD LENGTH

The text of this paper (excluding table of contents, abstract, footnotes, appendices and bibliography) comprises approximately 15,765 words.

Electronic commerce – Banking law – Online banking – Internet banking

I INTRODUCTION

Banking, like most other aspects of commerce, has warmed to electronic mediums for carrying out business. "Electronic banking" – the "automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels"[1] – allows bank customers to quickly and conveniently carry out routine banking transactions. Electronic banking may be via such methods as the telephone or mobile phone "texting". However, probably the most important form of electronic banking today is online or internet banking.[2]

With little more than a website address, a username and a password, bank customers can check their account balances, transfer funds between their accounts and update their contact details. Customers may also be able to communicate with their bank through secure email, set up facilities to pay bills and even make investments or trade securities. Moreover, this convenience is portable – customers can initiate transactions from anywhere with an internet connection.

Banks can also make significant cost savings through processing such transactions online. Banks may reduce their need for staff to answer questions, tally amounts and re-key data. These cost savings usually flow to the customer in the form of lower costs for the transactions processed online.

The cost, convenience and effectiveness of online banking have made it a significant factor in the banking environment. The level of customer acceptance of online banking can be measured through its use. Statistics published by the New Zealand Bankers' Association[3] show that in 2000 there

---

[1] Federal Financial Institutions Examination Council *Information Technology Examination Handbook: E-Banking* (Washington DC, USA, 2003) 1. Available at <http://www.ffiec.gov> (last accessed 4 February 2006).

[2] A number of other terms, including "remote banking", "cyber banking" and similar, have been used interchangeably by various authors. This paper has attempted to use the term "online banking" throughout for the sake of consistency, other than where making direct quotations.

[3] New Zealand Bankers' Association *Payment Statistics 2004* (Wellington, 2004). Available at <http://www.nzba.org.nz> (last accessed 4 February 2006).

were approximately 94 million uses of "Personal Computer" banking.[4] In 2004, this figure had nearly doubled to approximately 183 million uses.[5]

However, online banking remains a relatively recent development. The implications of its various aspects have not yet been fully explored. The Banking Ombudsman,[6] in her most recent annual report, stated:[7]

> Internet banking fraud is new, however, with the consequence that neither existing legislation nor the Code [of Banking Practice] is able to offer clear guidance concerning the allocation of risk between banks and their customers... my office is principally guided by the specific form of contract between banks and their individual customers...
>
> Unfortunately, some banks appear to have updated and amended only some sections of their standard contracts when they introduced internet banking services, with the consequence that we sometimes identify fundamental inconsistencies between different parts of the same contract, making it difficult if not impossible to apply their terms in a coherent manner.

The Law Commission has also observed that the allocation of risk between customers and banks may not be appropriate.[8] The Commission concluded that while legislative change would not be appropriate, the 2001 review of the Code of Banking Practice should take into account the concerns.[9] The 2001 review having apparently not done so, the Banking Ombudsman has expressed her

---

[4] It is not clear what transactions are covered by this figure, however, it does appear to include bill payments, funds transfer, credit transactions and debit transactions.

[5] Note that the New Zealand Bankers' Association splits its "Personal Computer" banking into "Internet Banking" and "PC Banking" from 2003 onwards.

[6] The Office of the Banking Ombudsman is an independent, private and free alternative dispute resolution scheme. The Banking Ombudsman acts under terms of reference established by participating banks (most of the major trading banks). Under those terms of reference, the Banking Ombudsman may receive and consider complaints against participating banks, and has the power to award limited damages for actual loss as well as stress and inconvenience. See Office of the Banking Ombudsman of New Zealand *Banking Ombudsman Terms of Reference* (Wellington, 2002). The Banking Ombudsman also publishes case notes annually to provide an indication to banks and the public of areas of concern or in need of improvement. See generally Office of the Banking Ombudsman of New Zealand <http://www.bankombudsman.org.nz> (last accessed 4 February 2006).

[7] Office of the Banking Ombudsman of New Zealand *Annual Report 2004-2005* (Wellington, 2005), 4.

[8] New Zealand Law Commission *Electronic Commerce Part Three: Remaining Issues* (NZLC R68, Wellington, 2000), para 63.

[9] New Zealand Law Commission *Electronic Commerce Part Three: Remaining Issues*, above n 8, paras 62-69. See also New Zealand Law Commission *Electronic Commerce Part Two: A Basic Legal Framework* (NZLC R58, Wellington, 1999), paras 294-312.

hope that the 2005 review of the Code "will help to remove uncertainties and to establish standards in this increasingly important area of banking practice."[10]

This paper conducts its own review of the provisions and issues associated with online banking. In doing so, it focuses on the direct relationship between bank and customer, and situations where the two parties "transact" with each other, rather than third party merchants. It also does not consider situations involving fraud that happen to be carried out the through the medium of online banking.[11]

This paper begins by setting out some background material relating to the technical and legal aspects of online banking. The technical background includes a basic framework for considering the risks associated with electronic transactions such as online banking (the "PAIN" risks) and an outline of the security measures used by New Zealand banks to address these risks. The legal background sets out various elements of the bank-customer relationship, including the three basic sub-relationships, some common law affecting the boundaries of the relationship, and a brief summary of the general contractual terms agreed between banks and customers for the provision of banking services.

The paper then turns to the specific contractual terms that govern the bank-customer relationship for online banking. It first sets out a summary of the relevant clauses, then goes on to analyse their apparent practical effect. As indicated by the Banking Ombudsman,[12] there is almost no precedent relating to online banking to assist in determining the outcome of any given fact situation. However, the similar contractual terms from other related areas of banking law and disputes relating to these terms provide a useful comparison.

This analysis leads to the conclusion that the express terms related to online banking are unfortunately heavily weighted in favour of banks over their customers. The paper takes issue with this approach, pointing out the

---

[10] Office of the Banking Ombudsman of New Zealand *Annual Report 2004-2005*, above n 7, 4.
[11] See, for example, Office of the Banking Ombudsman *Case Note Compendium 2004-2005* (Wellington, 2005) 11, case 3.
[12] Office of the Banking Ombudsman of New Zealand *Annual Report 2004-2005*, above n 7, 4.

difficulties faced by a customer who is in the invidious position of trying to have an unauthorised withdrawal refunded. It then moves on to discussing some of the potential vulnerabilities in the technical security measures of online banking and uses these, along with some legal arguments, to proffer some advice to customers with the aim of redressing the balance between bank and customer.

Finally, this paper seeks to offer some advice to banks that could potentially be incorporated into the current review of the Code of Banking Practice. In doing so, the paper undertakes a comparative assessment of the online banking regimes of the United Kingdom, Australia and the United States. The paper concludes by suggesting some legal and technical measures that could usefully be incorporated in New Zealand to ensure greater practical security for online banking and a fairer and more balanced approach for both customers and banks.

II TECHNICAL BACKGROUND: ONLINE BANKING SECURITY

A PAIN

Four security risks have been identified with e-business transactions: privacy, authentication, integrity, and non-repudiation ("PAIN").[13] Any system seeking to conduct e-business securely must address these risks, although the degree to which each is addressed will depend on the nature of the specific transaction.

Online banking has elements of each of these risks. The exchange of sensitive information (such as account balances) should be kept private. Only the authentic customer should be able to access information and provide instructions in relation to his or her accounts. Information exchanged between a customer and the bank should be protected in such a way that it cannot be interfered with while in transit. Finally (although of less relevance for the purposes of this paper), information and instructions should be recorded in such a way that prevents subsequent alteration so disputes may be resolved impartially. This paper considers the first three security risks.

---

[13] Stacy Cannady and Thomas Stockton "Easing the PAIN" (IBM, New York NY, USA, 2001) <http://www.ibm.com> (last accessed 10 January 2006).

B Technical Security Measures

Personal online banking in New Zealand today is invariably delivered over the worldwide web through the use of an ordinary internet browser. The major trading banks (ANZ, [14] National Bank, [15] the Bank of New Zealand, [16] Westpac,[17] ASB Bank,[18] TSB Bank,[19] HSBC,[20] Superbank[21] and Kiwibank[22]) all offer online banking access in essentially the same manner: customers access the website of their particular bank and enter a distinct user log-on and password.[23]

All the major trading banks surveyed use 128 bit Secure Sockets Layer ("SSL") encryption for online banking. SSL is a series of protocols developed to provide secure communications over the internet. In the context of banking, it enables customers and banks to exchange confidential information (for example, passwords or account balances) with a much reduced risk that information can be intercepted in transit.

1 How SSL works

A secure SSL communication link is established whenever a customer accesses his or her bank's website. All the customer has to do is enter the bank's website address. [24] However, a number of more technical steps are carried out automatically by the customer's and bank's computer systems after the

---

[14] ANZ National Bank Limited, trading as ANZ New Zealand <http://www.anz.co.nz> (last accessed 4 February 2006).
[15] ANZ National Bank Limited, trading as the National Bank of New Zealand <http://www.nbnz.co.nz> (last accessed 4 February 2006).
[16] Bank of New Zealand <http://www.bnz.co.nz> (last accessed 4 February 2006).
[17] Westpac Banking Corporation (New Zealand division) <http://www.westpac.co.nz> (last accessed 4 February 2006).
[18] ASB Bank Limited <http://www.asb.co.nz> (last accessed 4 February 2006).
[19] TSB Bank Limited <http://www.tsb.co.nz> (last accessed 4 February 2006).
[20] The Hongkong and Shanghai Banking Corporation Limited <http://www.hsbc.co.nz> (last accessed 4 February 2006).
[21] St George Bank New Zealand Limited, trading as Superbank <http://www.superbank.co.nz> (last accessed 4 February 2006).
[22] Kiwibank Limited <http://www.kiwibank.co.nz> (last accessed 4 February 2006).
[23] Some banks do have additional security measures. These are discussed in greater detail below.
[24] More technically, its Uniform Resource Locator or "URL" – see *Wikipedia* (Wikimedia Foundation Inc, St Petersburg FL, USA, 2006) "Uniform Resource Locator" <http://en.wikipedia.org> (last accessed 4 February 2006).

customer accesses the bank's online banking website. Most customers will not be aware of these steps:[25]

1. The customer sends to the bank a list of information relating to the type of encryption methods he or she is able to use.

2. The bank chooses the encryption methods and parameters from the list sent to it by the customer.

3. The bank sends a certificate from a certificate authority[26] to the customer.

4. The customer checks the certificate against the list published by the relevant certificate authority to ensure it is valid.

5. The customer and the bank negotiate a common "master secret".[27]

This is known as the "handshake" protocol. Once the above steps have been completed, the "record" protocol takes over. At its most basic level, the record protocol takes the shared master secret and uses it to create a key. The record protocol then uses this to encrypt information that is sent to the other party. Because the other party also knows the master secret, he or she is able to work out the key and decrypt the information.

This process is most clearly demonstrated by way of a non-internet analogy. Suppose Alice needs to exchange some private information with Bob so she telephones him (accessing the bank's online banking website). Alice suggests a number of ways they might exchange information securely (step 1 above). Bob selects one of Alice's suggested methods, locking a letter in a box with a combination lock (step 2). However, at this point, Alice realises that she has

---

[25] Note that "customer" and "bank" have been substituted for the more technical "client" and "server".

[26] The role of certificates and certificate authorities is discussed in greater detail at page 8, below.

[27] This master secret can itself be kept confidential through the use of another cryptographic method known as "asymmetric" or "public-key cryptography." A detailed discussion of asymmetric cryptography is beyond the scope of this paper. However, for further information, see, for example, *Wikipedia*, above n 24, "Public-Key Cryptography" and "Diffie-Hellman Key Exchange".

never met Bob and wants to be sure of his identity. Bob suggests that she talk to his friend, Chris, who will vouch for his identity (step 3). Alice knows Chris is trustworthy, so is willing to accept his word that Bob is in fact who he says he is (step 4). Assured of Bob's identity, Alice and Bob then agree the combination will be "1234" plus the numerical date and month on which she sends the letter – for example 0402 for 4 February (step 5 – the "master secret"). Alice then writes Bob a letter, locks it in the box with the combination 1636 (the "key") and sends it to Bob. Bob, who already knows the master secret and therefore how to work out the key, adds 1234 to the date of the postmark on the box, opens the lock and reads the letter. He can then write back to Alice using the same method (the record protocol).

As the name suggests, the handshake protocol essentially involves the customer and the bank identifying themselves to each other and working out the framework for their future communications. The record protocol then utilises the agreed framework to encrypt information exchanged so that one party is able to decrypt information encrypted by the other.[28]

When a secure SSL communications link has been established using a standard browser, a padlock or key symbol appears at the bottom of the browser window and the URL changes from "http://..." to "https://...".[29]

2 Privacy

Information exchanged during an SSL connection is encrypted using a key based on the master secret. No one can determine any of the information exchanged unless they know the key to decrypt the information. Ordinarily this should only be the customer and the bank. However, ultimately it would be possible for a third party "cracker"[30] to try and determine the key simply by

---

[28] Two additional SSL protocols, the "alert" and "cipher change" protocols play more minor roles that are not necessary to discuss for the purposes of this paper.

[29] *Wikipedia*, above n 27, "Transport Layer Security" and Tomasz Onyszko "Secure Socket Layer" [sic] (WindowSecurity.com, 2004) <http://www.windowsecurity.com> (last accessed 10 January 2006).

[30] The term "cracker" is used to denote a computer "hacker" with malicious intent. See *Wikipedia*, above n 27, "Hacker", "Hacker (computer security)" and "Hacker Definition Controversy".

trying every possible combination. The security of the key is therefore critical to minimise the risks to privacy.

New Zealand banks all use "strong 128 bit"[31] encryption. A bit is a binary digit, either 1 or 0. The number of bits refers to the length of the key used to encrypt and decrypt information, based on the master secret.[32] A 128 bit key is therefore a string of 128 digits – for example:

> 01001010101011010101010101111010000101000101000001000101010100
> 00011011011111001010100000001101001010010101101010010101000101
> 0100

A 128 bit key has 2^{128} possible combinations. That is, 3.4×10^{38} or 340 trillion trillion trillion combinations. The world's current fastest supercomputer has been recorded as performing 280.6 trillion floating point operations per second ("teraflops").[33] Although this performance would not actually flow through to calculating a 128 bit key, even at this speed it would take approximately 3.8×10^{16} or 38 thousand trillion years to try all the possible key combinations by "brute force". A 128 bit key would therefore appear to be very secure.

3 Authentication

The identity of the bank is authenticated in the SSL protocol by use of certificates. Certificates are issued by certificate authorities, which are usually private companies. A certificate authority certificate essentially provides a guarantee from the authority to the customer that the bank (the provider of the certificate) is genuine. If they are not, the theory behind the certificate system is that the certificate authority will compensate for any loss suffered by the person.[34]

---

[31] Westpac Banking Corporation (New Zealand division) "How secure is online banking?" <http://www.westpac.co.nz> (last accessed 4 February 2006).

[32] See *Wikipedia*, above n 27, "Transport Layer Security".

[33] The BlueGene/L of the Lawrence Livermore National Laboratory. See Top500.org <http://top500.org> (last accessed 10 January 2006).

[34] *Wikipedia*, above n 27, "Certificate Authority". However, it should also be noted that while all certificate authorities provide "guarantees" of identity, the liability of certificate authorities that issue certificates erroneously is unclear. Most certificate authorities provide for some form of contractual liability, normally seeking to limit liability to a maximum sum. However, customers that have suffered loss due to reliance on erroneous certificates may be able to take

However, the SSL protocol does not confirm the identity of the customer. Only the bank provides a certificate from a certificate authority verifying its validity. It is functionally possible within the SSL handshake protocol for both parties to provide certificates to each other. However, this is not done for online banking. The process for obtaining a valid certificate is likely to be too technical for the average banking customer.

Instead, banks issue customers with unique log-ons and passwords. The customer must enter these correctly before being able to use online banking. This is to authenticate the identity of the customer. Most banks recommend or require[35] a password of at least six characters that includes a mix of upper and lowercase letters and numbers.[36] There are around 72^6 possible combinations for such a six-character password.[37] That is, 1.39×10^{11} or nearly 140 billion possible combinations. The number of combinations increases markedly for each additional character added to the password. The chance of a cracker randomly guessing an appropriately chosen password is therefore remote. Further, some banks disable an online banking account following three unsuccessful log-on attempts.[38] Only having three guesses makes it even more unlikely a cracker could randomly guess a log-on and password.

However, the log-on and password process is separate from the SSL protocols. In fact, an SSL connection is already in place when the customer sends their log-on and password to the bank. This prevents third parties from intercepting log-on and password details.

---

other actions, for example, a claim in tort for negligent misstatement. Full consideration of the liability of certificate authorities is beyond the scope of this paper.

[35] Some banks appear to do this technically by only allowing customers to enter a password that satisfies the criteria. Others provide for this criterion in the express terms relating to the use of online banking.

[36] See, for example, ANZ National Bank Limited, trading as the National Bank of New Zealand "Change my password" <http://www.nbnz.co.nz> (last accessed 4 February 2006).

[37] 26 letters plus 10 numerals multiplied by 2 for upper and lowercase equals 72. This may be greater or lesser for some banks, depending on whether they allow certain characters such as punctuation marks or the special characters obtained by pressing "shift" and a numeral.

[38] The banks surveyed by this paper do not appear to publish information relating to unsuccessful log-ons and it was not possible to confirm how many observe this practice. Anecdotally, however, it seems widespread.

4 *Integrity*

SSL provides privacy by encrypting information that is to be exchanged between customer and bank. Although it would be difficult to decrypt and read information encrypted using 128 bit SSL encryption, it is possible to interfere with it encrypted. Computer data, even encrypted, is ultimately no more than strings of 1s and 0s. It is possible to change some of these digits (even if only destructively) or prevent the exchange of data at all.

SSL also addresses this risk. All information to be exchanged is divided up into smaller blocks before being encrypted. Each block is numbered sequentially, enabling the receiver of the information to determine whether any blocks have been intercepted.[39] Further, each block contains a "hash" of itself. A hash is a one-way mathematical algorithm that converts a set of data into (typically) an alphanumeric string. The fundamental property of hash functions is that different outputs are produced for each different input, even if the inputs vary only slightly. For example, hashing the previous sentence in this paragraph using the common SHA-1 hash function[40] produces the result:[41]

a93b4112e474108ab50ca16ed3ac66035814d652

But even as small a variation as changing the capital "T" at the start of the sentence to lowercase produces quite a different hash:

65adc962520310c58d4112d6e4c6f7fd48a4aa19

By passing the information received through the same hash function and comparing the result with the hash received, it is possible to determine whether any changes have been made while the information was in transit.[42]

The combination of sequential numbering and hashing ensures data cannot easily be intercepted or altered without detection. Both the sequential number

---

[39] *Wikipedia*, above n 27, "Transport Layer Security", and Onyszko, above n 29.
[40] The SHA-1 hash function has recently been cracked and so can no longer be considered fully secure (see *Wikipedia*, above n 27, "SHA Hash Functions"). However, it is still in common use and provides a demonstration of how hash functions work.
[41] Hash calculators are freely available on the internet. See, for example, Serversniff.net <http://serversniff.net> (last accessed 11 January 2006).
[42] *Wikipedia*, above n 27, "Hash Function".

and the hash are also encrypted to ensure the privacy of this important information.

5 Advantages

In addition to the level of security described above, SSL has the major advantage of being widely accepted. SSL can provide security for many different sorts of applications, including the World Wide Web (the HTTP protocol). There is no need to implement separate security measures for different applications and protocols.

The acceptance of SSL has been extended to internet browsing software. SSL encryption is supported natively (that is, without the need to install additional software) in all recent internet browsers.

Because of this general acceptance, the fact that there is no need to install additional software, and its relative security, 128 bit SSL encryption is the preferred means of securing electronic commerce transactions, including online banking.[43]

III LEGAL BACKGROUND: THE BANK-CUSTOMER RELATIONSHIP

A The Basic Sub-relationships

The legal relationship between banks and their customers involves a number of separate sub-relationships. Take the simple example of a customer that has deposited funds with a bank. Firstly, the bank is the debtor of the customer, owing a debt equal to the amount of the deposit. Correspondingly, the customer is the creditor of the bank. Secondly, there is a contractual relationship associated with the creditor-debtor relationship. The bank agrees to honour the customer's instructions (or "mandate") for the repayment of the debt the bank owes to the customer. Finally, the bank is the agent of the customer. This sub-

[43] *Wikipedia*, above n 27, "Transport Layer Security", and Onyszko, above n 29.

relationship arises when the bank acts on behalf of the customer in making payments from, or receiving deposits into, the customer's account.[44]

B Implied Terms: the Customer's Duty of Care

The debtor and agency relationships between a bank and its customers are essentially unilateral. A bank assumes obligations in respect of its customers. However, the contractual relationship necessarily involves mutual obligations. The bank agrees to obey the customer's mandate, while the customer assumes a number of obligations in respect of the bank. These are usually contained in the express terms of the agreement between bank and customer and are discussed further below.

Perhaps the most significant of these obligations is the customer's duty of care in respect of the bank. This may arise from the express terms of the bank-customer agreement. However, even if it does not, the courts have introduced a duty of care as an implied term of the contractual relationship between banks and customers.

In a line of cases culminating in *Tai Hing Cotton Mill Limited v Liu Chong Hing Bank Limited and Others*,[45] a case concerning unauthorised transactions due to cheque fraud, the courts examined the extent of the duties customers owe to their banks. Earlier judgments had introduced what was described as the "narrow" duty of care – that a customer "must exercise due care in drawing his cheques so as not to facilitate fraud or forgery and he must inform his bank at once of any unauthorised cheques of which he becomes aware."[46] The customer argued that this was the proper extent of the duty. Under this

---

[44] *Electronic Business and Technology Law (NZ)* (Service 12, LexisNexis NZ Limited, March 2005) Introduction to Electronic Banking para 20.5 <http://www.lexisnexis.co.nz> (last accessed 10 January 2006).

[45] [1986] AC 80 (PC) Lord Scarman for their Lordships [*Tai Hing*].

[46] *Tai Hing*, above n 45, 108 Lord Scarman for their Lordships, affirming the earlier decisions of *London Joint Stock Bank Limited v Macmillan* [1918] AC 777 (HL) and *Greenwood v Martins Bank Limited* [1933] AC 51 (HL). This position was essentially adopted in New Zealand in *Bank of New Zealand v The Auckland Information Bureau (Incorporated)* [1996] 1 NZLR 420 (CA).

approach, the customer would be entitled to recover the value of the unauthorised transactions.

On the other hand, the bank argued that customers owed their banks a "wider" duty of care to:[47]

> exercise such precautions as a reasonable customer in his position would take to prevent forged cheques being presented to the bank... or, at the very least to check his monthly... bank statements so as to be able to notify the bank of any items which were not, or may not have been, authorised by him.

If this were accepted, the customer would be estopped from denying the authority of the payments from its account and the bank would not have to repay the amount of the unauthorised transactions.

Their Lordships ultimately decided that customers do not owe their banks any wider duty, only the narrow duty.[48] The customer therefore recovered the amount of the unauthorised transactions.

The *Tai Hing* line of cases was in relation to a specific form of instruction or mandate of a customer to the bank, that of a cheque. However, the reasoning seems equally applicable to any form of mandate. For example, New Zealand courts have applied *Tai Hing* to direct credits.[49]

C Express Terms: Conditions for the Provision of Banking Services

The Judicial Committee of the Privy Council held in *Tai Hing* that customers owe their banks a duty of care as an implied term of the contractual relationship. However, an implied term can be superseded by an express term dealing with the same matter. Indeed, one of the rationales in *Tai Hing* for refusing to extend a wider *implied* duty of care to customers was that banks are perfectly free to dictate their *express* terms of business if "the banking business

---

[47] *Tai Hing*, above n 45, 97 Lord Scarman for their Lordships.
[48] *Tai Hing*, above n 45, 108 Lord Scarman for their Lordships.
[49] *Bank of New Zealand v The Auckland Information Bureau (Incorporated)*, above n 46. In this case the direct credits were regular salary payments by the Auckland Information Bureau to its employees.

[has become] so burdensome that [there] should be... a reciprocal increase of responsibility placed upon the customer".[50]

New Zealand does not have any statutory regulation of the bank-customer relationship. Rather, banks in New Zealand have adopted detailed sets of terms and conditions to regulate the provision of banking services, including online banking. However, through the New Zealand Bankers' Association the major trading banks in New Zealand have produced the Code of Banking Practice.[51] The Code guides many of the matters that are addressed in individual bank's express terms. It is binding on member banks, and compliance is monitored by the Banking Ombudsman.[52]

The standard terms and conditions for the provision of banking services include a number of express terms. To the average customer, the most obvious is probably the obligation to pay bank fees. However, a number of other matters are included as well. For example, and particularly relevant in light of the decision in *Tai Hing*,[53] customers must check their account statements for accuracy and advise their bank of any discrepancies as soon as possible.[54] The express terms will also include clauses governing the use of specific accounts or transaction services such as "EFTPOS"[55] cards, cheques and automatic payments.[56]

---

[50] *Tai Hing*, above n 45, 105-106 Lord Scarman for their Lordships.
[51] New Zealand Bankers' Association *Code of Banking Practice* (Third Edition, Wellington, 2002). Available at <http://www.nzba.org.nz> (last accessed 4 February 2006) [*New Zealand Code of Banking Practice*].
[52] *New Zealand Code of Banking Practice*, above n 51, cl 1.1.
[53] Above n 45.
[54] *New Zealand Code of Banking Practice*, above n 51, cl 4(c). See also, for example, Bank of New Zealand "Standard Terms and Conditions", cl 6 <http://www.bnz.co.nz> (last accessed 4 February 2006) and ASB Bank Limited "Personal Banking Terms and Conditions", 2 <http://www.asb.co.nz> (last accessed 4 February 2006).
[55] EFTPOS stands for "Electronic Funds Transfer at Point-Of-Sale". See Reserve Bank of New Zealand *Payment and Settlement Systems in New Zealand* (Wellington, 2003). Available at <http://www.rbnz.govt.nz> (last accessed 4 February 2006).
[56] *New Zealand Code of Banking Practice*, above n 51. See also, for example, Bank of New Zealand Limited "Standard Terms and Conditions", above n 54 and ASB Bank Limited "Personal Banking Terms and Conditions", above n 54.

IV EXPRESS TERMS FOR ONLINE BANKING

The express term approach is also used in the context of online banking. This paper addresses these express terms in three broad categories: mandate, security and liability.

A Mandate

Hard copy signatures (in the sense of squiggles on paper) have been the essential element for authorising instructions for many centuries.[57] Express terms in bank-customer agreements attempt to import a similar sense of authorisation to transactions in the electronic environment.

Mandate is not addressed by the Code of Banking Practice. However, the current practice among New Zealand banks is to provide that using an online banking log-on and password essentially provides sufficient mandate to process transactions (the "mandate clause"[58]). An example of this clause is:[59]

> Anyone using your Customer ID and Internet password will be allowed access to your accounts, whether they are authorised by you to do so or not. [The bank] will have no obligation, or take any further steps, to verify any instruction received from you or appearing to be sent by you via Online Banking.

B Liability

Banks also include express terms relating to liability arising from the use of online banking.[60]

---

[57] Currently embodied in New Zealand in the Bills of Exchange Act 1908. This was itself a consolidation of a number of earlier statutes. The requirements for negotiable instruments generally can be traced back to the law merchant – see *Goodson v Hawera Lawn Tennis and Croquet Club Inc* [1931] NZLR 1096, 1100 – 1101 (Supreme Court) Reed J.

[58] Appendix 1 sets out a list of the concepts that are defined and used by this paper. See page I, below.

[59] Westpac Banking Corporation (New Zealand division) "Online Banking Terms and Conditions" <http://www.westpac.co.nz/> (last accessed 4 February 2006).

[60] The following terms are based largely on the *New Zealand Code of Banking Practice*, above n 51, cl 3.9. However, see also, for example, ANZ National Bank Limited, trading as the National Bank of New Zealand "Online Banking Conditions of Use (Version 11)" <http://http://www.nbnz.co.nz> (last accessed 4 February 2006), ASB Bank Limited "FastNet Classic: Terms and Conditions" <http://www.asb.co.nz/> (last accessed 4 February 2006) and Westpac Banking Corporation "Online Banking Terms and Condition's, above n 59.

1 Notification clause

First, the express terms provide an incentive for customers to notify banks of potential issues early. The "notification clause" provides that a customer is not liable for any loss occurring after the customer notifies that bank of any actual or possible security breach. Security breaches may include such things as unauthorised transactions.[61]

2 No liability clause

Second, the terms provide that the customer will not be liable for the following (the "no liability clause"):[62]

- Unauthorised transactions that occur before the customer is registered to use online banking;
- Fraudulent or negligent conduct by the bank's employees or agents (the "no liability (fraud) clause");
- Faults or errors that occur in the online banking systems or software, other than errors that are obvious or advised by message or notice on display (the "no liability (error) clause"); or
- Any other unauthorised transaction where the customer could not have contributed to the loss.

3 Limited liability clause

Finally, where neither of the above clauses apply, the terms provide that the customer will only be liable for $50 or the actual loss (whichever is lower) stemming from an unauthorised transaction (the "limited liability clause"). However, the limited liability clause does not apply where the customer has acted fraudulently, negligently, breached the express terms or otherwise contributed to the loss.[63]

---

[61] *New Zealand Code of Banking Practice*, above n 51, cl 3.9(c).
[62] *New Zealand Code of Banking Practice*, above n 51, cls 3.9(a) and (f).
[63] *New Zealand Code of Banking Practice*, above n 51, cl 3.9(d).

(a) Fraud

Where the customer has acted fraudulently, the express terms provide that he or she will be absolutely liable for any loss, including loss suffered by others.[64]

(b) Negligence

Where a customer has acted negligently, he or she will be not be able to take advantage of the limited liability clause.[65] Instead, the maximum liability will be the lesser of:[66]

- The actual loss;
- The maximum amount that should have been allowed by the daily transaction limit;[67] or
- The loss up to the balance of the customer's account (including overdraft facilities).

There is no further definition of negligence. It can therefore presumably be taken to have its ordinary meaning.

(c) Breaching terms and conditions / otherwise contributing to the loss

Although treated separately in the Code of Banking Practice, several banks treat these elements the same. In any event, the examples given for otherwise contributing to the loss (such as selecting inappropriate passwords and keeping written records of passwords) amount to breaching the terms and conditions – specifically, the password clause (this is discussed further below).[68] The maximum liability is the same as for negligence.

---

[64] *New Zealand Code of Banking Practice*, above n 51, cl 3.9(d)(i). See also, in particular, ANZ National Bank Limited, trading as the National Bank of New Zealand "Online Banking Conditions of Use (Version 11)", above n 60.
[65] *New Zealand Code of Banking Practice*, above n 51, cl 3.9(d)(i).
[66] *New Zealand Code of Banking Practice*, above n 51, cl 3.9(d).
[67] Most banks impose a daily transaction limit for online banking to minimise potential losses stemming from security breaches.
[68] *New Zealand Code of Banking Practice*, above n 51, cls 3.9(d)(ii) and 3.9(d)(iii). See also, in particular, ANZ National Bank Limited, trading as the National Bank of New Zealand "Online Banking Conditions of Use (Version 11)", above n 60.

C Security

Finally, the express terms contain a number of provisos relating to passwords (the "password clause").[69] The customer is obliged to generally "safeguard" his or her password. This includes committing it to memory, taking care when entering it so as not to be observed and regularly changing it. Further, the customer must not:[70]

- Choose an obvious or easily-guessed password (such as names, sequential numbers, birthdays, telephone numbers, addresses);
- Store the password anywhere, in written or electronic form;
- Keep any record of the password in a form that can be readily identified;
- Disclose his or her password to any other person; or
- Leave his or her computer unattended while logged on to online banking.

Finally, the customer is also required to contact the bank as soon as possible if any record containing his or her password is lost, stolen or becomes known to someone else.

Where the customer breaches the password clause, he or she will not be able to take advantage of the limited liability clause.

V PRACTICAL EFFECT

A For Example

Suppose that a customer, Gus Tommer, logs on to his bank's online banking service and authorises a transaction of $10. However, when he checks his bank statement later that month, he notices that an additional $1,000 has been

---

[69] The following terms are again based largely on the New Zealand Bankers' Association *New Zealand Code of Banking Practice*, above n 51, cl 3.7. However, they also incorporate elements of banks' terms and Conditions. See, for example, Westpac Banking Corporation "Online Banking Terms and Conditions", above n 59, ANZ National Bank Limited, trading as the National Bank of New Zealand "Online Banking Conditions of Use (Version 11)", above n 60, and ASB Bank Limited "FastNet Classic: Terms and Conditions", above n 60.

[70] *New Zealand Code of Banking Practice*, above n 51, cls 3.7(c) and (d).

debited from his account. Gus did not authorise the $1,000 transaction and complains to his bank. The bank, relying on the express terms, refuses to refund him.

B Precedent

There is little precedent relating to online banking to assist in determining the practical effect of the express terms applied to any given fact situation. However, the online banking clauses appear to be closely modelled on the terms and conditions relating to the use of EFTPOS and credit cards[71] and telephone banking,[72] particularly in relation to "PINs".[73] The Code of Banking Practice even covers most of the online banking provisions within the same clauses as EFTPOS, credit cards and telephone banking.[74]

The effect of these EFTPOS and credit card and telephone banking terms have frequently been considered by the Banking Ombudsman.[75] These decisions provide some valuable guidance as to the practical effect of the express terms associated with online banking.

C Security Assumptions

Much of the following is based on the premise that online banking is "secure" due to the technical security measures implemented by banks. While this paper takes issue with this premise (discussed further below), assume for the purpose

---

[71] Credit cards have some slightly different provisions relating to unauthorised transactions with third parties. In certain circumstances, it is possible to "chargeback" disputed transactions through the international credit card organisation that issued the card. Although the process is complicated, in certain circumstances it is easier to reverse a disputed transaction made with a credit card than the same transaction made with a debit card. However, this relates to transactions with third-parties. It is therefore beyond the scope of this paper. For more information on the chargeback regime, see Office of the Banking Ombudsman *Case Note Compendium 2001-2002* (Wellington, 2002), 3 and Office of the Banking Ombudsman *Case Note Compendium 2002-2003* (Wellington, 2003), 26.

[72] See, for example, ANZ National Bank Limited, trading as the National Bank of New Zealand *Cashpoint Card: Conditions of Use* (Wellington, 2005) and ANZ National Bank Limited, trading as the National Bank of New Zealand *Thoroughbred, Visa and Freestyle: Conditions of Use* (Wellington, 2005).

[73] "PIN" stands for Personal Identification Number.

[74] New Zealand Bankers' Association *New Zealand Code of Banking Practice*, above n 51, cls 3.7 and 3.9.

[75] Office of the Banking Ombudsman of New Zealand case notes. See above, n 6.

of this section that the use of 128 bit SSL encryption does in fact make online banking secure. This leads to the following propositions:

S1. The technical security measures implemented by banks make online banking secure.

Therefore:

S2. There is no way to send the bank an instruction to make a transaction, other than by using the customer's password.

The presumption that the only way to make transactions is by use of a customer's password (the "security presumption") is important. It plays a crucial role in considering both the mandate and liability clauses discussed below.

D Mandate

The mandate clause provides legal authority that logging on equals mandate. When the security presumption discussed above is combined with the mandate clause, the following line of reasoning applies:

S2. There is no way to send the bank an instruction to make a transaction, other than by using the customer's password.

So if:

M1. The bank has received an instruction to make a transaction.

Then S2 + M1 =

M2. The transaction must have been made using the customer's password.

Therefore, by virtue of the mandate clause:

M3. The transaction is authorised by the customer.

The security presumption appears to provide a foundation for the mandate clause. However, a further outcome emerges when the security presumption is combined with the password clause:

M4. Only the customer knows his or her password.

Therefore M2 + M4 =

M5. The instruction to make a transaction must have come from the customer.

This latter line of reasoning provides an important practical consideration. By creating a presumption that the customer authorised the transaction, banks are able to shift the burden of proof to the customer to raise sufficient evidence to show that the transactions were not authorised. There are therefore both legal and evidential presumptions that a transaction has been authorised by the customer (the "authorisation presumption"). In order to recover the value of his unauthorised transaction, Gus would have to raise sufficient evidence to rebut this presumption.

This is demonstrated in a 2001-2002 decision of the Banking Ombudsman.[76] Mr C was adamant that he was the victim of unauthorised transactions. However, Mr C was unable to provide evidence that he had not initiated the transactions himself and the transactions did not conform to the usual pattern of fraud. The Banking Ombudsman therefore concluded that the most likely explanation was that Mr C was responsible for the transactions himself.

E Limited Liability

The limited liability clause seems to loosen some of the apparent harshness of the authorisation presumption. The bank may have received an ostensible mandate from Gus to debit his account $1,000. But if Gus can rebut the authorisation presumption by raising sufficient evidence to prove that the

[76] Office of the Banking Ombudsman *Case Note Compendium 2001-2002*, above n 71, 40, case 40.

ostensible mandate was not really authorised by him, the liability clauses may be triggered.

Under the limited liability clause, Gus will only be liable for $50 (that is, the bank will re-credit him the $950 balance), subject to the provisos of the clause. However, these provisos are important. Gus would not able to limit his liability to $50 if he had acted negligently or otherwise contributed to the loss. In practice, "otherwise contributing to the loss" amounts to breach of the express terms, particularly the password clause.

Some of the terms of the password clause may be difficult for the average customer to comply with on their face. For example, the password clause requires customers not to choose obvious passwords and not to write passwords down. But there are many sorts of services (both online and offline) that require passwords or identification codes that have similar requirements. It is likely to be impossible for customers to remember such a wide array of unique passwords, particularly if the service or password is not used often. Many customers may struggle to comply with these requirements.

Such terms appear harsh on their face. However, when combined with the security presumption, even more significant implications arise.

1 Limited liability and technology – the fault presumption

The security presumption gives rise to a line of reasoning that leads to the authorisation presumption. This means that the onus is on Gus to raise sufficient evidence to rebut the presumption of authorisation. However, the security presumption, combined with Gus' own rebuttal of authorisation and the provisions of the password clause, leads to a further line of reasoning:

S2. There is no way to send the bank an instruction to make a transaction, other than by using the customer's password.

So if:

L1. The transaction is unauthorised (Gus' rebuttal of the authorisation presumption).

Then S2 + L1 =

L2. Someone other than the customer knows the customer's password.

But:

L3. The customer is responsible for his or her password (the password clause).

Therefore L2 + L3 =

L4. The customer must be responsible for someone else learning his or her password.

This creates a res ipsa loquitur[77] ("the facts speak for themselves") evidential presumption that the customer is at fault, either by being negligent in his or her security practices or breaching the password clause (the "fault presumption"). This again shifts the evidential burden to Gus to show that he was not at fault, rather than the bank to show that he was.

2 Banking Ombudsman

The Banking Ombudsman has described the approach she takes to such matters as:[78]

> There is often no direct evidence as to how the offender became aware of the PIN. I am satisfied that it cannot be obtained from the card itself and I have no evidence of deficiencies in the security of banks' technology. Accordingly, in the absence of any other explanation, it is most likely that an offender has obtained knowledge of the PIN from the cardholder. The question therefore is whether, on the balance of probabilities, the offender

---

[77] *Scott v London and St Katherine Docks Company* (1865) 3 H & C 596; 159 ER 665 (Exchequer Chamber). See generally DL Mathieson QC (ed) *Cross on Evidence (NZ)* (Service 40, LexisNexis NZ Limited, December 2005) para 4.27 – Res ipsa loquitur <http://lexisnexis.co.nz> (last accessed 13 January 2006).

[78] Office of the Banking Ombudsman *Case Note Compendium 2001-2002*, above n 71, 37.

> was able to obtain knowledge of the PIN through a breach by the customer of the conditions of use on which the card was issued. Generally speaking, if there is a reasonable explanation for the offender's access to the PIN and the explanation does not involve a breach of the conditions of use, then the cardholder is entitled to reimbursement. If there is no reasonable explanation that does not involve a breach of the conditions of use, then the cardholder is not entitled to reimbursement.

This shows the logical progression that leads from the security presumption to the fault presumption. Because the Banking Ombudsman has no evidence of deficiencies in security technology, the most likely reason for an unauthorised transaction is a breach of the express terms by the customer. The phrasing "in the absence of any other explanation…" also demonstrates that the onus is on the customer to show he or she was not at fault.

And if the reverse burden of proof were not enough of itself, the Banking Ombudsman has concluded there are also several elements to it.

3 *Fault presumption part 1: breach of the password clause*

Gus must firstly show that he did not breach the password clause. However, this is not likely to be easy, given the fault presumption's reverse burden of proof.

This presumption is clearly demonstrated in a 2002-2003 decision of the Banking Ombudsman.[79] A customer, V, had her credit card stolen. Before she reported it stolen, the thief used it to withdraw $2,000 cash, using V's PIN correctly at the first attempt. V's bank refused to reimburse her, saying that she must have breached the terms of the card by not taking reasonable care of it and the associated PIN.

Due to the circumstances of the case, the Banking Ombudsman concluded that the only way the thief could have obtained V's PIN was due to V breaching the terms and conditions of the card by choosing either an easily guessed PIN or having a written record of the PIN with the card. V, unable to raise any evidence to the contrary, was liable for the full $2,000.

---

[79] Office of the Banking Ombudsman *Case Note Compendium 2002-2003*, above n 71, 34, case 31.

The burden was upon V to show that she did not breach the terms and conditions of the card, not on the bank to show that she did.

4 Fault presumption part 2: reasonable explanation required

Because the list of prohibited acts in the password clause is not exhaustive, banks include a catchall proviso in the form of negligence as a part of the limited liability clause. This covers circumstances where a password or access code is learnt from a customer without that customer necessarily breaching the password clause. If the password has been disclosed negligently, the customer will be liable even if they have not breached the password clause. Again, the fault presumption means that the burden of proof lies with Gus.

However, under the Banking Ombudsman's approach discussed above, the burden on Gus is potentially even greater than that under the password clause. Under the password clause, Gus "merely" has to show that he did not do one of the prohibited acts. To disprove negligence, Gus has to put forward positive evidence showing that there was a reasonable explanation for the unauthorised transaction.

This element of the fault presumption is demonstrated in another 2002-2003 decision.[80] Mr K was the victim of a purportedly professional scam in London. Immediately after making a withdrawal from an "ATM",[81] a thief approached him and tapped him on the shoulder, saying he had dropped some money. When Mr K bent down to look, the thief stole the card and later made some $6,000 of withdrawals. Mr K's bank refused to refund him, maintaining that he must not have taken reasonable care, as the offender was able to steal both card and PIN.

In the circumstances of the case, the Banking Ombudsman concluded that Mr K's PIN must have been observed by the thief "shoulder surfing" Mr K as he

---

[80] Office of the Banking Ombudsman *Case Note Compendium 2002-2003*, above n 71, 38, case 38.

[81] "ATM" stands for Automated Teller Machine.

entered his PIN at the ATM just before the theft. Being shoulder surfed is not included on the list of prohibited acts in the password clause.

Mr K claimed that he was always very careful because he was aware of the increasing prevalence of ATM crime in London. However, the Banking Ombudsman concluded that Mr K cannot have been careful enough. If he were, "it seemed likely the offenders would have targeted someone else." The offender must have obtained the PIN somehow (by virtue of the security presumption), and therefore Mr K must have failed to take reasonable care (the fault presumption).[82]

This is further compounded by the security presumption. This provides that the only way for a transaction to be made is by the use of the customer's log-on and password. Gus cannot therefore raise evidence of any explanation for how the unauthorised transaction came about – for example, some sort of technology-based breach. Gus must admit that his password was disclosed, and put forward a reasonable explanation as to how it came to be disclosed.

5 Causation

Finally, there does not even have to be a demonstrable link between the breach and the unauthorised transaction.

Another 2002-2003 decision provides a useful example.[83] Mr and Mrs S were burgled. Shortly after the burglary, a number of unauthorised telephone banking transactions were made, totalling some $15,000.

Mr and Mrs S admitted that their PIN had been written down amongst other personal documents, however in disguised form. There was no evidence that the burglar had discovered the PIN, let alone decoded it. However, the Banking

---

[82] Mr K was, however, able to recover some money due to the Banking Ombudsman applying a contributory negligence approach. Under this approach, loss is apportioned depending on the degree of fault. This approach of apportioning loss is somewhat curious, given that the bank wears the portion of the loss that a third party causes. However, a detailed analysis of this approach is beyond the scope of this paper.

[83] Office of the Banking Ombudsman *Case Note Compendium 2002-2003*, above n 71, 55, case 56.

Ombudsman found Mr and Mrs S had breached the password clause, and would therefore be liable.[84]

F No Liability

In addition to the limited liability clause, the express terms also provide for no liability where there has been fraud on the part of bank staff or due to technical errors with the online banking systems.[85]

It will probably be difficult for Gus to take advantage of the no liability (fraud) provision. Fraud is always a difficult matter to prove, and it is likely to be difficult for Gus to obtain the necessary evidence.

It will also be difficult for Gus to utilise the no liability (error) clause. The security presumption applies equally to this situation. Since online banking systems are secure, there is a presumption that there cannot be any errors that someone could exploit to make unauthorised transactions. Therefore there is no way for Gus to rebut the bank's assertion there were no technical faults at the time of the transaction. The Banking Ombudsman herself has stated that "I have no evidence of deficiencies in the security of banks' technology."[86] This is similar to the fault presumption in the context of the limited liability clause.

G Net Effect

The view could be taken that the net effect of the express terms of the contractual arrangements between banks and customers is to enable a useful new service for the benefits of both parties. And such contractual provision is necessary because the government has not seen fit to provide legal certainty around the legal status of private electronic transactions.[87] At the same time, the express terms ensure that an honest and diligent customer will only ever be

---

[84] Mr and Mrs S actually managed to recover some of the money from the bank, however this was due to an unrelated technicality.

[85] Assuming the unauthorised transactions did not occur before Gus registered for online banking.

[86] Office of the Banking Ombudsman *Case Note Compendium 2001-2002*, above n 71, 37.

[87] Electronic Transactions Act 2002, s 14. Contrast with the United States – see 15 USC § 1693 and page 54, below.

liable for $50 of unauthorised transactions prior to notifying the bank, and not liable at all for any transactions that occur after notification. The default position is that the bank voluntarily assumes liability for unauthorised transactions. The customer is only liable in a specific range of circumstances where he or she is at fault. Customers, as the weak link in the security arrangements, should rightly face the consequences of their own lax security.

However, taking quite a different perspective, the express terms could also be viewed as unduly favouring the interests of banks at the expense of their customers. This paper contends that this is the correct perspective to take of existing online banking terms and conditions. The real net effect of the express terms is to shift essential elements of the burden of proof from the bank to the customer. Shifting these elements means that a customer must negotiate a difficult series of hurdles to claim back funds debited in an unauthorised transaction.

Firstly, Gus is obliged to check his statements regularly for any unauthorised transactions.[88] The obligation is on Gus to bring any potentially unauthorised transactions to his bank's attention. If he fails to do so, he would breach his implied duty of care and be estopped from claiming the transactions were unauthorised.[89]

Next, Gus faces an evidential burden to show that the transactions were not authorised. The authorisation presumption, built on the security presumption and the mandate and password clauses, means that Gus must raise sufficient evidence to rebut the presumption that the transaction was not authorised.

However, Gus may find that his rebuttal of the authorisation presumption works against him in determining whether he is entitled to take advantage of the limited liability clause. The security presumption, combined with the password clause and Gus' rebuttal leads to the fault presumption. This means Gus will be deemed responsible for unauthorised transactions unless he can

---

[88] The notification clauses precluding any further liability post notification adds some incentives here too.

[89] *Tai Hing*, above n 45. See also above n 46, and accompanying text.

meet a further reverse burden of proof. Discharging this burden is likely to be extremely difficult. Gus must show that there is both a reasonable explanation for how his password came to be disclosed (the security presumption means he must admit that it was disclosed), and that he did not breach the terms of the password clause. However, there is a real risk that he will find himself in a "catch-22" situation trying to satisfy both limbs. Admitting that his password was disclosed may expose him to allegations that he breached the password clause. Even if he had behaved entirely reasonably, but still breached one of the terms of the password clause, he will be liable. Similarly, if he had scrupulously adhered to the password clause, but was otherwise found to be negligent, he will be liable.

Moreover, it must not be forgotten that the limited liability clause limits Gus' liability to $50. So even if Gus is able to detect and report the unauthorised $1,000 transaction, prove that he did not authorise it and further prove that there is a reasonable explanation for how his password came to be disclosed that doesn't breach the password clause, the bank will charge him $50 for his trouble.

The no liability (error) clause is, if anything, even more unlikely to be of assistance to Gus. The security presumption also makes it impossible for Gus to maintain that there was an error with online banking security.

VI BUT IS ONLINE BANKING "SECURE"?

The previous section of this paper criticised the practical effect of the express terms governing the use of online banking. However, if online banking is in fact secure, and there are no other possible ways the security of online banking can be compromised, the presumptions would be well-founded and the criticisms unjustified. Unfortunately, that does not appear to be the case.

This section of the paper presents a number of possible flaws in online banking security. It outlines some of the limitations of SSL, banks' primary technical

security measure. These limitations are such that weaknesses arise in two broad areas: bank practices and attacks by "crackers".[90]

A Limitations of SSL

SSL is generally very good at what it does: protecting the privacy and integrity of information exchanged between bank and customer. However, privacy and integrity are not really all that important for unauthorised transactions.

1 Customer authentication

Assume the counterfactual: that SSL is not used and communications between bank and customer are not encrypted (other than the initial log-on and password). A cracker seeking to steal funds would not actually be able to affect either the customer or the bank directly. Rather, he or she would be limited to viewing and changing information and instructions in transit. This would certainly mean that the customer's privacy would be compromised. While of concern to the customer, it is not actually likely to be of much interest to a cracker concerned with theft. The integrity of the information may also be affected. However, the very best result for the cracker in this regard would be intercepting an instruction to pay funds to someone, and altering the payee's name and account number to the cracker's own (and probably increasing the amount). Compromising the privacy and integrity of information (other than a password) does not necessarily give a cracker the ability to instruct the bank to make unauthorised transactions.

In the PAIN framework, it is rather authenticity (mandate) that is of most interest to crackers. But SSL does not provide any technical security guarantee that information and instructions apparently coming from the customer are actually from that customer. Authenticity is rather the realm of the customer's log-on and password. SSL does provide a guarantee that the password is private during transit, but no more than that. The technical security method adopted by the banking industry (and prominently advertised as providing

[90] As to the meaning of "cracker", see n 30, above.

security[91]) actually provides no technical guarantees that the origin of any instructions to the bank is the genuine customer rather than a cracker. While the information exchanged in an SSL communication is private and uncorrupted, it will be private and uncorrupted regardless of its source.

2 Bank authentication

In addition to customer authentication issues, there are also bank authentication issues. SSL does provide a mechanism whereby the bank can verify its identity – the use of certificates from a certificate authority.[92]

Providing a certificate is a necessary precursor to forming a secure SSL communication. However, a customer may not notice that a communication with the cracker is not secure (through the absence of the padlock or key symbol in the browser window). It may even be possible for advanced crackers to make a session appear secure by "layering" a picture of a padlock in the right place on the screen.[93] This is possible because browser applications normally (depending on the user's choice of setting) do not prompt users when they receive a valid certificate. Nor is there usually any prompt when users do not receive any certificate. Therefore there may be nothing observable by a customer that confirms whether the communication is secure or not.

Alternatively, a cracker attempting to masquerade as a legitimate bank could send a certificate as part of creating a genuine SSL connection. Certificates are issued by certificate authorities, which are private companies. It is conceivable that a less reputable certificate authority could issue certificates to crackers intent on fraud.

In this regard, it is worth noting that several banks have begun to advertise how SSL and certificates work. One bank, for example, points out that the SSL padlock icon should appear and that double-clicking on the icon will show the

---

[91] See, for example, Bank of New Zealand "Internet Banking and Internet Banking for Business Security" <http://www.bnz.co.nz> (last accessed 4 February 2006).
[92] See above page 5 and following.
[93] *Wikipedia*, above n 27, "Phishing".

certificate. It also provides instructions of what to look for on the certificate, such as the correct URL and the certificate authority.[94]

The certificate process is quite technical and is not likely to be widely understood by customers. However, more advanced cracker attacks may fool even technology-literate customers. This makes it possible for crackers to fool customers into believing a forged website they are viewing is valid.

B Weaknesses due to Bank Practices

Ross Anderson is a computer cryptography expert who has appeared as an expert witness in several unauthorised transaction cases.[95] Anderson's "Why Cryptosystems Fail"[96] is perhaps the seminal article on cryptographic systems and security. Although the article considers ATM fraud specifically, it is equally applicable to other systems, including online banking. Anderson points out a number of technical flaws with ATM security.[97] This demonstrates that bank systems are not secure. It is entirely possible similar such flaws exist with online banking security. However, there is no evidence either way on this.

Anderson's more important conclusion is that most unauthorised transactions are not caused by technical attacks, but rather by implementation errors and management failures.[98]

1 Security of banks' systems

There are a number of possible methods to fraudulently obtain user log-ons and passwords from bank customers (these are discussed below). From a cracker's

---

[94] See Superbank "Security Information" <http://www.superbank.co.nz> (last accessed 4 February 2006).

[95] See the papers associated with *Diners Club (SA) Pty Limited v Singh*, available at <http://www.cl.cam.ac.uk/> (last accessed 20 January 2006). See also, for example, John Leyden "How to get an ATM PIN in 15 guesses" (21 February 2003) *The Register* United Kingdom <http://www.theregister.co.uk> (last accessed 20 January 2006).

[96] (University of Cambridge, 1993) <http://www.cl.cam.ac.uk/> (last accessed 20 January 2006) ["Why Cryptosystems Fail"].

[97] Anderson "Why Cryptosystems Fail", above n 96, 2-7. See also Mike Bond and Piotr Zieliński "Decimalisation table attacks for PIN cracking" (University of Cambridge, 2003) <http://www.cl.cam.ac.uk/> (last accessed 20 January 2006).

[98] Anderson "Why Cryptosystems Fail", above n 96, 9 and 12.

point-of-view, however, they are inefficient. Customers will only ever know their own details. Banks, on the other hand, need to know the details of all their customers, including log-ons and passwords. They are therefore a far more enticing target, even if this information is protected by bank security systems.

It appears that no such attacks have occurred in New Zealand. However, similar incidents have occurred internationally. For example, companies that process credit card data have been targeted. Some high-profile incidents have netted millions of customers' details, including credit card numbers.[99]

Banks in New Zealand advertise that they operate common practices like firewalls.[100] However, the actual level of technical security does not appear to have been tested or made public as yet. If the security systems implemented by banks are not adequate, customer log-ons and passwords could be stolen by crackers.

Any cracker using a stolen log-on and password would be able to access a customer's account. This is because SSL does not provide any guarantee of customer authenticity as discussed above. This vulnerability is compounded by the fact that customers must always enter the same log-on and password.

2 Security of bank procedures

Similarly, Anderson points out a number of flaws among security procedures of bank staff and contractors. Even where the procedures themselves are adequate, sometimes the execution may be lacking. Anderson outlines a number of examples, including cases where security systems were installed incorrectly, where bank security staff failed to implement necessary security

---

[99] See, for example, Jonathan Krim and Michael Barbaro "40 Million Credit Card Numbers Hacked" (18 June 2005) *The Washington Post* Washington DC, USA <http://www.washingtonpost.com> (last accessed 20 January 2006) and Fred Katayama "Hacker hits up to 8M credit cards" (27 February 2003) *CNNMoney.com* United States <http://www.cnnmoney.com> (last accessed 20 January 2006).

[100] See, for example, Bank of New Zealand "Internet Banking and Internet Banking for Business Security", above n 91.

measures, and even where the installers of security systems left themselves a "back door" (a hidden way of accessing the system).[101]

Again, such weaknesses may leave banks vulnerable to crackers and even fraudulent staff stealing customer log-ons and passwords. Again, online banking is susceptible to such attacks as the security measures for confirming customer authenticity are limited.

C Weaknesses to Cracker Attacks

While it is far more efficient to target banks, customers are often less technology and security-literate. There are a number of attacks by which crackers may attempt to gain customers' log-ons and passwords.

1 Spoofing and phishing

"Spoofing" refers to the practice by which one person sends another an email, but the email appears to the recipient to be from someone other than the sender.[102] "Phishing" is a similar practice, but refers more specifically to emails that seek to extract personal information from the recipient, such as online banking log-ons and passwords.[103] This attack is able to work due to weaknesses in the email protocols. It is possible to change the apparent sender of an email without detection.

In the context of online banking, phishing involves a cracker preparing an email that appears as if it comes from a legitimate bank email address. The email has a message to the effect that the recipient needs to verify their customer details. The email suggests that the customer click on a link in the email to do this. Clicking on the link takes you to an official-looking website with instructions for the customer to enter their log-on and password. The site is, of course, not legitimate, but rather serves as a way for the cracker to obtain

---

[101] Anderson "Why Cryptosystems Fail", above n 96, 2-4 and 9-10.
[102] *Wikipedia*, above n 27, "Spoofing Attack".
[103] *Wikipedia*, above n 27, "Phishing".

customers' log-ons and passwords.[104] There have been several of this type of phishing email sent recently.[105]

Unlike the weaknesses due to bank practices, which are due to weaknesses in customer authentication, phishing is possible because of the weaknesses in bank authentication. Because customers may not be sure whether the bank website they are accessing is genuine, they can be deceived into disclosing their log-ons and passwords.

2 Pharming

Like phishing, pharming is an attack that is possible due to weaknesses in a protocol, this time the "Domain Name System" protocol ("DNS"). The DNS protocol is also applicable to other applications such as email, but in the context of pharming relates to assigning "URLs".[106]

Entering a URL into a browser usually involves entering something such as http://www.examplebank.com. The user is then taken to the examplebank.com website. However, the "real" address for a website actually consists of a set of four numbers between 0 and 255, separated by full stops – for example, 123.45.67.89 (its "IP address"). Linking the easy-to-remember company or brand name to its actual IP address is done by DNS servers.[107]

If a cracker were able to access examplebank.com's DNS server, he or she would be able to reassign its URL to a different IP address that the cracker controls. This can be achieved either through technical means (cracking the DNS server's own security measures), or by fooling the DNS server's staff into believing that the cracker has legitimate authority to instruct the URL to be reassigned to a different IP address. A customer then entering the URL http://www.examplebank.com would not be directed to the genuine examplebank.com website, but rather the cracker's website, forged to look like

---

[104] *Wikipedia*, above n 27, "Phishing".
[105] See, for example "Phishing scam continues to hit Westpac" (4 January 2006) *National Business Review* New Zealand <http://www.nbr.co.nz> (last accessed 20 January 2006).
[106] "Uniform Resource Locator", above n 24.
[107] *Wikipedia*, above n 27, "Uniform Resource Locator" and "Domain Name System".

examplebank.com website. Customers entering their log-ons and passwords to the site would actually be sending them to the cracker, who would then be able to use them at the genuine examplebank.com website to authorise transactions.[108]

Pharming is similar to phishing in that customers enter their own log-ons and passwords into a forged website. Only the means by which the customer is tricked into accessing that forged website differ. Like phishing, the attack is possible because of the weaknesses in bank authentication. Customers can never be quite sure whether the website they are accessing is the genuine bank website.

Unlike phishing, pharming does not appear to have been used to target online banking customers to date.[109]

3 Keystroke logging

Phishing and pharming attacks rely on deceiving customers. Keystroke logging, on the other hand, is a "Trojan". This is a type of malicious programme that is often spread by means of a virus or by masquerading as a different sort of programme (hence the name "Trojan"). When a Trojan is downloaded, it installs itself without the knowledge of the user. A keystroke logger is a type of Trojan that records all the keystrokes of a user as he or she enters them. This can be used to record log-ons and passwords as they are typed by a bank customer.[110] The keystroke logger then automatically sends information back to the cracker that distributed it.

Unlike phishing and pharming, keystroke loggers do not exploit vulnerabilities in bank authentication. Rather, they exploit the customer authentication weaknesses. SSL does not provide any surety as to the actual identity of a person entering a log-on and password. The protection it does provide, making information private, only comes into play once the information has left a user's

---

[108] See *Wikipedia*, above n 27, "Pharming".
[109] See *Wikipedia*, above n 27, "Pharming".
[110] *Wikipedia*, above n 27, "Keystroke Logging".

computer. However, keystroke loggers essentially record information "inside" the user's computer, before it is encrypted. This lack of authentication, combined with the fact that customers must always enter the same log-on and password, make online banking vulnerable to a keystroke logger attack.

VII SOME ADVICE FOR CUSTOMERS

The previous section of this paper presented some flaws in the technical security measures of online banking. These flaws should allow Gus to mount a number of challenges to the validity of the unauthorised transaction as follows.

A Evidential Matters

Any of the weaknesses in bank practices described could potentially represent a "reasonable explanation for the offender's access to the [password] and the explanation does not involve a breach of the conditions of use".[111] This would bring Gus within the limited liability clause and recover from his bank the unauthorised transaction. However, whether any of these particular flaws exist in Gus' case would need to be determined. And, as indicated earlier in this paper, the onus is on Gus to prove them.

Anderson points out that Gus is unlikely to succeed if he is required to bring specific evidence that shows the precise flaw in the bank's security systems or practices. Rather, Anderson suggests the best approach for Gus would be to demand copies of things such as:[112]

> the bank's security and quality documentation, including security policies and standards, crypto key management procedures and logs, audit and insurance inspectors' reports, test and bug reports... balancing records and logs, and details of all customer complaints in the last seven years.

To this may be added matters such as whether any attacks have been made against the banks security systems, when such attacks were made, whether any have succeeded, whether there have been any other security compromises, the

---

[111] Office of the Banking Ombudsman *Case Note Compendium 2001-2002*, above n 71, 37.

[112] Ross Anderson "Liability and Computer Security: Nine Principles" (University of Cambridge, 1994) <http://www.cl.cam.ac.uk/> (last accessed 20 January 2006), 3 ["Nine Principles"].

banks information technology policy and whether there have been any disciplinary actions taken against staff.

This would enable Gus to determine whether there are any matters relating to bank security practices that may give rise to his unauthorised transaction.[113] For example, if a successful attack had recently been made against the bank's system, Gus' log-on and password may have been stolen. Other complaints or discrepancies in balancing records may show that a number of other customers have suffered unauthorised transactions too, perhaps indicating more systemic problems. This sort of information may provide a "reasonable explanation" for Gus' unauthorised transaction, bringing Gus within the limited liability clause.[114]

Gus may also be able to take advantage of the no liability clause. This clause provides that Gus is not liable for fraud on the part of bank staff or agents. Information relating to the bank's management procedures and disciplinary actions against staff may show potential fraudulent actions on the part of the bank's employees. Similarly, the bank's information technology policy would show what procedures are in place to, for example, stop fraudulent staff installing keystroke logging software on the computers that banks make available in branches to access their own online banking websites. Information to this effect could enable Gus to take advantage of the no liability (fraud) clause.

However, Anderson points out that similar questions in the United Kingdom do not usually results in banks actually disclosing information. Rather, banks tend to refund customers the amounts of the unauthorised transaction without further argument.[115]

It should be noted that this approach may not be available under the Banking Ombudsman scheme, Gus' likely first avenue of redress. While the Banking

---

[113] See above page 32.
[114] See above page 16.
[115] Anderson "Nine Principles", above n 112, 3.

Ombudsman does have the power to request that banks provide information,[116] and that information is normally shared with the customer,[117] banks are entitled to assert confidentiality[118] and the Banking Ombudsman must respect that confidentiality.[119] Gus may therefore have to result to court action. This would enable him to take advantage of the much more rigorous discovery[120] and inspections processes.[121] Gus is therefore more likely to get the information under the discovery process than the Banking Ombudsman scheme. However, the expense of a court action is only likely to be justified in the case of significant unauthorised transactions.

B Consumer Protection

The preceding section discussed how evidence of weaknesses in bank practices may allow Gus to recover the amount of the unauthorised transaction. On the other hand, weaknesses to cracker attacks may provide Gus with legal arguments against the bank under the Consumer Guarantees Act 1993 or the Fair Trading Act 1986.

1 Consumer Guarantees Act

The Consumer Guarantees Act is a major component of New Zealand's consumer protection regime. The Act applies to all contracts for the acquisition of goods and services[122] by a consumer.[123] The Act operates by implying

---

[116] Banking Ombudsman of New Zealand *Banking Ombudsman Terms of Reference*, above n 6, art 5.
[117] Banking Ombudsman of New Zealand *Banking Ombudsman Terms of Reference*, above n 6, art 7.
[118] Banking Ombudsman of New Zealand *Banking Ombudsman Terms of Reference*, above n 6, art 6.
[119] Banking Ombudsman of New Zealand *Banking Ombudsman Terms of Reference*, above n 6, art 29.
[120] See High Court Rules, rules 293-317A. While banks may attempt to resist discovery on the grounds of confidentiality, it is not likely the court would accept this in totality. The court may, for example, order discovery on a limited basis such as to counsel only. This approach recognises the growing view that while some documents may be confidential, it may be necessary for the other party to have access to the information to pursue its claim – see High Court Rules, rules 297 and 307 and *McGechan on Procedure* (Brookers Limited, Wellington, February 2006) HCR307.17 <http://www.brookers.co.nz> (last accessed 19 February 2006).
[121] See High Court Rules, rules 322-323.
[122] Consumer Guarantees Act 1993, long title.

certain terms (in the form of guarantees) into contracts relating to the provision of goods and services. Among other things, "services" includes facilities that are provided under a contract between a bank and customer.[124] The Consumer Guarantees Act therefore applies to online banking. It is also not possible to contract out of the Consumer Guarantees Act, unless the consumer acquires a good or service for business purposes.[125] This would not apply to Gus.

For the purposes of this paper, the most important guarantee is that of fitness for purpose.[126] The service must be of such a nature and quality that it can reasonably be expected to achieve the outcome(s) desired by the consumer.[127] For online banking, this means that the online banking facility (the systems and software) must satisfy the reasonable expectations of the customer. Most fundamentally, the customer expects the facility to be secure and not to facilitate unauthorised transactions.

Gus would be able to argue that the systems adopted by banks in the provision of online banking do not meet this expectation. The key component of online banking "security" is SSL. While SSL carries out it functions admirably, those functions are limited to privacy and integrity. It provides no guarantee as to customer authenticity, and only limited guarantees at best for bank authenticity.[128] These limitations are demonstrated in the weaknesses to cracker attacks.[129]

Moreover, banks could make their systems more secure by providing greater certainty as to authenticity. "Two-factor authentication" is particularly noteworthy in this regard. Two-factor authentication relies on a combination of mechanisms for identifying a person. Something a person knows (for example, a password) is one such mechanism. Other factors may include something a

---

[123] "Consumers" are retail customers, that is, not business or trade customers – Consumer Guarantees Act 1993, s 2.
[124] Consumer Guarantees Act 1993, s 2.
[125] Consumer Guarantees Act 1993, s 43.
[126] Consumer Guarantees Act 1993, s 29.
[127] *Laws of New Zealand* (Service 36, LexisNexis NZ Limited, September 2005) Consumer Protection para 28 <http://www.lexisnexis.co.nz> (last accessed 10 January 2006).
[128] See above page 30 and following.
[129] See above page 34 and following.

person has (for example, an EFTPOS card) or something a person is (for example, biometric identification). For banking, the most common form of two-factor authentication adopted to date utilises a device that generates a number when the customer presses a button. In addition to the customer's log-on and password, the code generated by the device must be entered to log on to online banking or authorise transactions. The code changes each time the button is pressed, and is only valid for a short period of time. As the device code is different for every log-on, crackers cannot use recorded information to access a customer's online banking. This protects against the phishing, pharming and keystroke logging attacks described above. This is an example of two-factor authentication utilising something the customer knows (his or her password) and something the customer has (the device).

It is becoming standard banking industry practice internationally to utilise two factor authentication. In particular, United States banks will be required to strengthen their security measures beyond single-factor authentication by the end of 2006 (although the exact method of this strengthening is not prescribed).[130] Two New Zealand banks have already adopted two-factor authentication using the devices described above.[131] Banks that have not may be more vulnerable to challenges that their online banking service is not fit for purpose.

Similarly, the Basel Committee on Banking Supervision[132] has published *Risk management principles for electronic banking*.[133] The Basel Committee principles are accepted practice in the banking industry and are usually adopted by domestic prudential supervisors as part of the regulatory framework for

---

[130] Federal Financial Institutions Examination Council *Authentication in an Internet Banking Environment* (Washington DC, USA, 2005). Available at <http://www.ffiec.gov> (last accessed 4 February 2006). This technically has the status of "guidance" only, but will likely be adopted by all United States banks.

[131] ASB Bank Limited, above n 18, and Hongkong and Shanghai Banking Corporation Limited, above n 20.

[132] The primary standard-setting body for banking supervision – see Bank for International Settlements "About the Basel Committee" <http://www.bis.org> (last accessed 23 January 2006).

[133] (Basel, Switzerland, 2003). Available at <http://www.bis.org> (last accessed 23 January 2006) [*Basel Committee Electronic Banking Principles*].

banks subject to their supervision.[134] While the electronic banking principles are specifically put forward as guidance only and not definitive requirements, [135] they nevertheless provide some valuable assistance to determine good banking practice. In particular, the electronic banking principles state:[136]

> ... e-banking... needs special management attention because of the enhanced security challenges posed by e-banking. This should include establishing appropriate authorisation privileges and authentication measures, logical and physical access controls, adequate infrastructure security to maintain appropriate boundaries and restrictions on both internal and external user activities and data integrity of transactions, records and information...

While not binding, and only general in nature, failure to meet the accepted banking industry practice as embodied in the Basel Committee principles may again indicate that the online banking services provided are not fit for purpose.

The weaknesses of (most) New Zealand banks existing systems to cracker attacks, and failure to implement readily-available and internationally-accepted additional security measures leave those banks open to challenges that their measures to ensure authenticity are not sufficient. Given authenticity is a key component of the PAIN risks, it would certainly be open to argue that the current systems for online banking are not "fit for purpose".

If online banking is not fit for purpose, Gus is entitled to claim damages from the bank for any loss that resulted from this shortcoming that was reasonably foreseeable. [137] This would include loss suffered due to unauthorised transactions. Alternatively, if the breach were deemed "substantial",[138] Gus would be entitled to cancel the contract for the provision of online banking services. Setting aside those terms would mean that the mandate clause (which gives the bank authority to debit Gus' account) did not apply and that Gus' bank debited his account without authority. In turn, this means that the bank's

---

[134] See, for example, Reserve Bank of New Zealand "Implementation of Basel II capital rules in New Zealand" (18 March 2005) Press Release <http://www.rbnz.govt.nz> (last accessed 23 January 2006).
[135] *Basel Committee Electronic Banking Principles*, above n 133, 1.
[136] *Basel Committee Electronic Banking Principles*, above n 133, 2.
[137] Consumer Guarantees Act 1993, s 32(c).
[138] Consumer Guarantees Act 1993, ss 32 and 36.

debt to Gus would still exist and the bank would need to re-credit Gus' account. However, both damages and cancelling the contract would result in the same outcome.

The Consumer Guarantees Act also provides a guarantee that services will be carried out with reasonable care and skill.[139] In the same manner as the guarantee of fit for purpose, Gus may be able to argue that banks are not providing online banking with reasonable care and skill. The "reasonable bank" may adopt, for example, two-factor authentication so as to address the concerns with current online banking systems as described above.

2 *Fair Trading Act*

The Consumer Guarantees Act covers agreements for services that have already been concluded. This contrasts with the Fair Trading Act, which covers the pre-contract period. In particular, the Fair Trading Act prohibits businesses from engaging in false and misleading conduct in advertising their goods. For the purposes of this paper, this includes conduct that may mislead customers as to the nature, characteristics or suitability of purpose of a particular service.[140] It also includes false and misleading representations that services are of a particular kind, standard, or quality.[141]

Banks advertise their systems as secure and refer to the benefits of SSL.[142] However, this could amount to misleading conduct, given the weaknesses to cracker attacks described above. This may provide grounds for Gus to take action under the Fair Trading Act. Breach of the Fair Trading Act can result in both criminal[143] and civil[144] action. For Gus this includes the possibility of actions for damages for loss suffered,[145] or cancellation of the contract.[146] Like

---

[139] Consumer Guarantees Act 1993, s 28.
[140] Fair Trading Act 1986, s 11.
[141] Fair Trading Act 1986, s 13(b).
[142] See, for example, ASB Bank "Precautions we take" <http://www.asb.co.nz> (last accessed 4 February 2006) and Bank of New Zealand "Internet Banking and Internet Banking for Business Security", above n 91.
[143] Fair Trading Act 1986, s 40.
[144] Fair Trading Act 1986, ss 41-46.
[145] Fair Trading Act 1986, s 43(2)(d).

the Consumer Guarantees Act, both of these would result in Gus being refunded the amount of the unauthorised transaction.

In addition to the courts, the Banking Ombudsman may be able to apply the provisions of the Consumer Guarantees Act and Fair Trading Act. The Banking Ombudsman may apply "any applicable rule of law or relevant judicial authority" when considering complaints.[147] Depending on the amount of the claim, Gus would also be able to take his complaint to the Disputes Tribunal.[148]

C No Liability for Faults in the Online System

The no liability (error) clause provides that Gus is not liable where the unauthorised transaction is the result of faults or errors that occur in the online banking system. The other category of weaknesses, cracker attacks, may allow Gus to argue that this clause applies. Gus would, however, need to show that the weaknesses are of such a scale that they amount to fundamental faults or errors with the online system. This would be an interesting argument, but there does not appear to be any guidance that assists in determining this question.

Even if he could prove that the weaknesses amounted to faults, Gus would also need to show that the faults do not fall within the proviso to the no liability (error) clause – that is that the errors are not obvious or previously notified by the bank.[149] Some banks are starting to advertise extra steps a customer can take to ensure the authenticity of the bank website.[150]

However, United States precedent may help Gus here. In a case involving ATM fraud, it was held that a bank, having knowledge of a specific type of fraud, is negligent if it does not provide sufficient information to warn its customers of that type of fraud and how to take precautions to guard against it. Moreover, this burden is not discharged by publishing general warning notices

---

[146] Fair Trading Act 1986, s 43(2)(a).
[147] Banking Ombudsman of New Zealand *Banking Ombudsman Terms of Reference*, above n 6, art 16(a).
[148] Disputes Tribunals Act 1988, s 10(2) and Schedule 1 Part 2, Consumer Guarantees Act 1993, ss 39 and 47 and Fair Trading Act 1986 ss 39 and 43.
[149] See above page 16.
[150] See Superbank "Security Information" above n 94.

to the effect of "Beware of ATM fraud" or "Do not let your card be used for any transaction but your own".[151] If this were to be followed in New Zealand, general warnings of the type currently published would not be sufficient.

On the other hand, some sorts of cracker attack have received specific security warnings from banks. In particular, the recent spate of phishing attacks has resulted in action by the banking industry, at least in some places.[152] Such a warning would preclude any arguments that the no liability (error) clause should apply in respect of weaknesses in online banking systems to cracker attacks.

This argument could potentially be made before the Banking Ombudsman. However, if specific non-public evidence is required, Gus may be required to resort to the court so as to take advantage of the discovery process.[153]

D Tai Hing */ Public Policy*

Finally, Gus would be able to ask the court[154] to set aside the terms of the contract on the basis of *Tai Hing* or general public policy grounds. The Judicial Committee of the Privy Council in *Tai Hing* stated:[155]

> If banks wish to impose upon their customers an express obligation... the burden... must be brought home to the customer... this [is an] undoubtedly rigorous test. The test is rigorous because the bankers would have their terms of business so construed as to exclude the rights which the customer would enjoy if they were not excluded by express agreement... Clear and unambiguous provision is needed...

It would be possible to argue that Gus' bank had not met the "rigorous test" of "bringing home" the effect of the express terms to Gus. While their Lordships

---

[151] *Ognibene v Citibank* (1981) 112 Misc 2d 219, 223; (1981) 446 NYS 2d 845, 848; [1981] NY Misc LEXIS 3417, 9-10 (Civil Court of the City of New York, New York County) Mara T Thorpe J.

[152] See Westpac Banking Corporation "Latest hoax email scam" <http://www.westpac.com.au> (last accessed 23 January 2006). Note however, that this is the website of the Australian division of Westpac.

[153] See above n 120, and accompanying text.

[154] The Banking Ombudsman or the Disputes Tribunal may also be able to apply public policy concerns (see Banking Ombudsman of New Zealand *Banking Ombudsman Terms of Reference*, above n 6, art 16(a) and Disputes Tribunals Act 1988, s 19(1)(e)). However reasoning on the basis of public policy will have more authority coming from the court.

[155] *Tai Hing*, above n 45, 110 Lord Scarman for their Lordships.

were concerned with the obligation to check bank statements, it seems the reasoning could be extended to apply to online banking. The net practical effect of the terms is to shift essential elements of the burden of proof from the bank on to the customer. This effect is not apparent on the face of the express terms, nor does it appear to be communicated anywhere else.[156]

VIII SOME ADVICE FOR BANKS

In its advice to customers, this paper presented a number of possible arguments that may be available to a customer who has been the victim of unauthorised transactions. However, as pointed out by Armstrong, some of these arguments are open to fraudulent as well as legitimate customers.[157] It would therefore be in the interests of banks, as well as customers, for banks to revise the express terms, systems and practices relating to online banking. This may include both legal and technical matters. There is a review of the Code of Banking Practice underway at the moment.[158]

This paper compares New Zealand's online banking regime with that of several international jurisdictions. All reveal slightly different approaches. This paper attempts go outline these various approaches, before making some suggestions about a revised legal regime for online banking. It also makes some technical suggestions that banks could consider.

A The United Kingdom

1 Banking Code

The approach in the United Kingdom is similar to that in New Zealand. There is no legislative framework governing the contractual arrangements between

---

[156] One United Kingdom commentator has suggested that the equivalent contractual terms in the United Kingdom could be subject to scrutiny under the Unfair Terms in Consumer Contracts Regulations 1999 – see Ahmad Azzouni "Internet Banking and the Law: A Critical Examination of the Legal Controls over Internet Banking in the UK and their Ability to Frame, Regulate and Secure Banking on the Net" (2003) 18 JIBLR 351. Although New Zealand does not have an equivalent statutory regime, the same effect could be achieved under public policy grounds.

[157] Armstrong "Nine Principles", above n 112, 4.

[158] New Zealand Bankers' Association "Review of the Code of Banking Practice" <http://www.nzba.org.nz> (last accessed 4 February 2006).

banks and their customers for the provision of banking services. Rather, the bank-customer relationship is left to the express terms and conditions associated with particular banking products. However, like New Zealand, the United Kingdom has a voluntary self-regulatory Banking Code[159] providing guidance to banks as to the terms and conditions they should adopt for provisions relating to the use of online banking.

2 Mandate

Like New Zealand, the mandate clause is not covered in the United Kingdom Banking Code. Rather, banks presume that an online transaction initiated by a customer's correct log-on and password is authorised.[160]

3 Liability and security

The United Kingdom also limits liability for unauthorised transactions. The Banking Code provides that customer liability is limited to £50 for any unauthorised transactions prior to notification, so long as the customer has not acted fraudulently or not taken reasonable care (discussed below).[161] However, not all United Kingdom banks appear to have adopted the £50 limited liability clause for unauthorised online transactions. Some banks actually accept the entire risk for unauthorised online transactions (that is, customer liability is limited to £0) where there is no fraud or negligence.[162]

---

[159] British Bankers' Association, the Building Societies Association and the Association for Payment Clearing Services *The Banking Code* (London, United Kingdom, 2003). Available at <http://www.bankingcode.org.uk> (last accessed 4 February 2006) [*United Kingdom Banking Code*].

[160] See, for example, Royal Bank of Scotland "Direct and Digital Banking Services: Terms and Conditions" <http://www.rbs.co.uk> (last accessed 14 January 2006), cl 1 and Hongkong and Shanghai Banking Corporation Limited "Internet Banking Terms and Conditions" <http://www.hsbc.co.uk> (last accessed 14 January 2006), cls 3.1-3.3.

[161] *United Kingdom Banking Code*, above n 159, cl 12.10.

[162] See, for example, Royal Bank of Scotland "Direct and Digital Banking Services: Terms and Conditions", above n 160, cl 6 and Hongkong and Shanghai Banking Corporation Limited "Internet Banking Terms and Conditions", above n 160, cl 4.1. See also Nicholas Bohm, Ian Brown and Brian Gladman "Electronic Commerce: Who Carries the Risk of Fraud?" 2000(3) Journal of Information, Law and Technology, part 4.2. Available at the University of Warwick's Electronic Law Journals project <http://www2.warwick.ac.uk> (last accessed 14 January 2006).

The United Kingdom Banking Code also provides that the limited liability clause does not apply where customers have acted fraudulently or have not taken reasonable care.[163] Lack of reasonable care may include breach of the password clause. Again like New Zealand, the password clause includes requirements to keep passwords confidential, not write passwords down and choose appropriate passwords.[164]

This is somewhat more favourable to the customer than the New Zealand approach. New Zealand also excludes limited liability where customers are generally fraudulent or negligent, as well as where they have breached the password clause.[165] It would appear that any breach of the password clause in New Zealand would exclude the limited liability clause.[166] However, by tying breach of the password clause to negligence, it would seem that a United Kingdom customer would have to *unreasonably* breach the password clause. This may allow, for example, a customer to write down his or her password, so long as he or she takes reasonable care in doing so. Reasonable care may include, for example, making reasonable efforts to disguise the password, or keeping it physically secure such as locked in a safe and/or away from a computer.[167]

4 Presumptions and the burden of proof

Very differently to New Zealand, the United Kingdom does not appear to place the burden of proof regarding unauthorised transactions on the customer. The current version of the United Kingdom Banking Code states "Unless *we* [the bank] can show that *you* [the customer] have acted fraudulently or without reasonable care, your liability for the misuse of your card will be limited as

---

[163] *United Kingdom Banking Code*, above n 159, cl 12.9. See also, for example, Royal Bank of Scotland "Direct and Digital Banking Services: Terms and Conditions", above n 160, cls 3-7 and Hongkong and Shanghai Banking Corporation Limited "Internet Banking Terms and Conditions", above n 160, cls 2.1-2.3 and 4.2.

[164] *United Kingdom Banking Code*, above n 159, cl 12.5.

[165] *New Zealand Code of Banking Practice*, above n 51, cl 3.9(d). See also page 15, above.

[166] See above page 24.

[167] Note, however, that Bohm, above n 162 and Azzouni, above n 156, argue that customers face potentially unlimited liability due to the mandate clause. However, this argument appears to have been made without reference to the qualifications provided by the liability clause.

follows... [*emphasis added*]".[168] This is the reverse of the New Zealand situation, where the presumption is that the customer breached the password clause unless the customer is able to prove otherwise.

However, it should also be noted that while some banks seem to adopt this approach, others do not. These banks require the customer to prove absence of fault and negligence.[169]

Anderson, however, dismisses this as a "cosmetic change" to the previous situation,[170] which seems to have been more akin to the current New Zealand approach. There do not appear to be any recent United Kingdom cases which would directly address this issue. There is, however, an online forum whereby customers can complain of unauthorised withdrawals from their accounts.[171] Although this online forum cannot be considered definitive, there are a number of recently-reported instances where banks have sought to rely on a presumption of authorisation and/or fault where the correct password or PIN is used.[172] On the other hand, there are some instances where banks have refunded customers upon receiving a complaint regarding an unauthorised withdrawal,[173] although some with difficulty.[174]

---

[168] *United Kingdom Banking Code*, above n 159, cl 12.10. See also Azzouni, above n 156, 359-360 and Bohm, above n 162, part 4.2.

[169] Contrast Hongkong and Shanghai Banking Corporation Limited "Internet Banking Terms and Conditions", above n 160, cl 4.3 (however note that cl 4.2 is more vague) with Royal Bank of Scotland "Direct and Digital Banking Services: Terms and Conditions", above n 160, cl 7.

[170] Anderson "Nine Principles", above n 112, 7.

[171] Mike Bond "Phantom Withdrawals: on-line resources for victims of ATM fraud" <http://www.cl.cam.ac.uk> (last accessed 20 January 2006).

[172] See, for example, Bond "Phantom Withdrawals: on-line resources for victims of ATM fraud", above n 171, "Camm Case" (Case Number 17, 24 October 2004) and "Sexton Case" (Case Number 21, 25 October 2005).

[173] See, for example, Bond "Phantom Withdrawals: on-line resources for victims of ATM fraud", above n 171, "Hardy Case" (Case Number 16, 17 December 2004).

[174] See, for example, Bond "Phantom Withdrawals: on-line resources for victims of ATM fraud", above n 171, "Anon1 Case" (Case Number 12, 14 May 2004) and "Bolton Case" (Case Number 14, 17 October 2004).

B Australia

1 EFT Code

Like the United Kingdom and New Zealand, Australia also operates a non-statutory scheme for governing the bank-customer relationship. However, unlike the United Kingdom and New Zealand, the Australian scheme is not wholly self-regulatory. Instead, the Australian Securities and Investments Commission ("ASIC")[175] established an Electronic Funds Transfer Working Group. The Working Group produced an Electronic Funds Transfer Code of Conduct (the "EFT Code").[176] Choosing to participate in the scheme is voluntary for financial institutions, but once a financial institution has opted to participate, it must comply with the requirements of the EFT Code.

2 Mandate

Mandate is not covered by the EFT Code. However, perhaps unsurprisingly given the Australian domination of the New Zealand banking environment, the mandate clauses adopted by Australian banks follow the same model adopted by their New Zealand counterparts. Once again, a correct log-on and password are deemed sufficient mandate.[177]

---

[175] ASIC is the Australian regulatory body for financial services and markets, companies, and consumer protection in superannuation, insurance, deposit taking and credit. See the Australian Securities and Investments Commission Act 2001 and <http://www.asic.gov.au> (last accessed 15 January 2006). See also ASIC's consumer protection website, <http://www.fido.asic.gov.au> (last accessed 15 January 2006).

[176] ASIC *Electronic Funds Transfer Code of Conduct* (Canberra ACT, Australia, 2002). Available at <http://www.fido.asic.gov.au> (last accessed 15 January 2006) [*Australian EFT Code*].

[177] See, for example, Westpac Banking Corporation "Terms and Conditions for Internet Banking and BPAY" <http://www.westpac.com.au> (last accessed 23 January 2006), cls 6 and 7 and National Australia Bank "National Internet Banking Product Disclosure Statement including Terms and Conditions" <http://www.national.com.au> (last accessed 15 January 2006), cl 21.

3 *Liability*

Like New Zealand, the EFT Code provides for a range of situations where the customer will not be liable for any unauthorised transactions.[178] These situations include, for example, where the bank's agents or employees have acted fraudulently[179] or where the unauthorised transaction occurs after the customer has notified the bank of the loss of his or her password.[180]

The EFT Code also provides for a limited liability clause. Where the no liability clause does not apply, a customer will be liable for, at most, A$150.[181] Similar to the United Kingdom and New Zealand, this limited liability will not apply where the customer has acted fraudulently or failed to comply with the required security measures.[182]

4 *Security*

The required Australian security measures are less onerous on customers than the equivalent United Kingdom and New Zealand requirements. An Australian customer will not be liable for security breaches unless he or she has acted with

---

[178] *Australian EFT Code*, above n 176, cls 5.2-5.4. See also, for example, Westpac Banking Corporation "Terms and Conditions for Internet Banking and BPAY", above n 177, cl 10 and National Australia Bank "National Internet Banking Product Disclosure Statement including Terms and Conditions", above n 177, cl 27.1.

[179] *Australian EFT Code*, above n 176, cl 5.2(a). See also, for example, Westpac Banking Corporation "Terms and Conditions for Internet Banking and BPAY", above n 177, cl 10 and National Australia Bank "National Internet Banking Product Disclosure Statement including Terms and Conditions", above n 177, cl 27.1(a).

[180] *Australian EFT Code*, above n 176, cl 5.3. See also, for example, Westpac Banking Corporation "Terms and Conditions for Internet Banking and BPAY", above n 177, cl 10 and National Australia Bank "National Internet Banking Product Disclosure Statement including Terms and Conditions", above n 177, cl 27.1(e).

[181] *Australian EFT Code*, above n 176, cl 5.5(c). See also, for example, Westpac Banking Corporation "Terms and Conditions for Internet Banking and BPAY", above n 177, cl 12 and National Australia Bank "National Internet Banking Product Disclosure Statement including Terms and Conditions", above n 177, cl 27.2(c)(i).

[182] *Australian EFT Code*, above n 176, cl 5.5(a). See also, for example, Westpac Banking Corporation "Terms and Conditions for Internet Banking and BPAY", above n 177, cl 11 and National Australia Bank "National Internet Banking Product Disclosure Statement including Terms and Conditions", above n 177, cls 27.2(a) and 27.3.

"extreme carelessness" in failing to protect his or her security measures (such as passwords).[183] "Extreme carelessness" is defined as:[184]

> a degree of carelessness with the security of the codes which greatly exceeds what would normally be considered careless behaviour. For example storing the user's username and password for Internet banking in a diary or personal organiser or computer (not locked with a PIN) under the heading "Internet banking codes".

Also less onerously, Australia does not prohibit keeping written records of passwords. The EFT Code only requires that reasonable attempts are made to protect the security of the record.[185] This may include making reasonable efforts to disguise the password or keeping passwords physically secure.[186]

An Australian customer will also be liable if he or she has "voluntarily" disclosed a password[187] or chosen an inappropriate password (such as the customer's name or date of birth).[188]

5 *Presumptions and the burden of proof*

The Australian approach regarding presumptions and the burden of proof is also more favourable to the customer than the New Zealand approach. Like the United Kingdom, Australia requires the bank to show that the customer was

---

[183] *Australian EFT Code*, above n 176, cl 5.6(e). See also, for example, Westpac Banking Corporation "Terms and Conditions for Internet Banking and BPAY", above n 177, cl 11 and National Australia Bank "National Internet Banking Product Disclosure Statement including Terms and Conditions", above n 177, cl 27.3(a)(ii).

[184] *Australian EFT Code*, above n 176, cl 5.6(e) and endnote 17.

[185] *Australian EFT Code*, above n 176, cl 5.6(c). See also Australian EFT Code, cl 5.6(b) and also, for example, Westpac Banking Corporation "Terms and Conditions for Internet Banking and BPAY", above n 177, cl 8 and National Australia Bank "National Internet Banking Product Disclosure Statement including Terms and Conditions", above n 177, cl 27.3(a)(iii).

[186] For some examples of what one bank considers do not amount to "reasonable efforts", see Westpac Banking Corporation "Terms and Conditions for Internet Banking and BPAY", above n 177, cl 8.

[187] *Australian EFT Code*, above n 176, cl 5.6(a). See also, for example, Westpac Banking Corporation "Terms and Conditions for Internet Banking and BPAY", above n 177, cl 8 and National Australia Bank "National Internet Banking Product Disclosure Statement including Terms and Conditions", above n 177, cl 27.3(a)(i).

[188] *Australian EFT Code*, above n 176, cl 5.6(d). See also, for example, Westpac Banking Corporation "Terms and Conditions for Internet Banking and BPAY", above n 177, cl 8 and National Australia Bank "National Internet Banking Product Disclosure Statement including Terms and Conditions", above n 177, cl 27.3(b).

negligent or failed to comply with the security requirements.[189] However, in terms of evidence, the EFT Code provides that "all reasonable evidence must be considered, including all reasonable explanations for the transactions occurring."[190] Requirements for "reasonable explanations for the transactions occurring" may shift the balance somewhat back towards the bank, as it would appear to exclude more far-fetched customer explanations. Banks would not have to rebut such explanations.

However, perhaps most significantly, the EFT Code states:[191]

> The fact that the account has been accessed with the correct [password] while significant, will not of itself constitute proof on the balance of probability that the [customer] has contributed to losses through the [customer's] fraud or through the [customer] contravening the [security requirements or password clause].

This means that banks are not allowed to maintain the fault presumption – that customers must be responsible for transactions, merely because the technology is secure. This provides a significant advantage for Australian customers compared to their New Zealand counterparts.

Unfortunately, it is not possible to test this theoretical position by application to decided cases in Australia. No cases appear to have been decided. Further, the EFT Code provides for private external dispute resolution schemes.[192] It does not appear that such schemes publish decisions in a readily-available format.

---

[189] *Australian EFT Code*, above n 176, cl 5.5(a). See also *Australian EFT Code* cl 5.5(b) and, for example, National Australia Bank "National Internet Banking Product Disclosure Statement including Terms and Conditions", above n 177, cl 27.2(b). However note that Westpac is more vague as to the required standard – see Westpac Banking Corporation "Terms and Conditions for Internet Banking and BPAY", above n 177, cl 10.

[190] *Australian EFT Code*, above n 176, cl 5.5.

[191] *Australian EFT Code*, above n 176, cl 5.5.

[192] *Australian EFT Code*, above n 176, cl 10.8 and following.

C *The United States*

1 *Electronic Fund Transfer Act*

Unlike the United Kingdom, Australia, and New Zealand, the United States has implemented statutory rules governing the relationship between banks and their customers. The Electronic Fund Transfer Act 1982[193] was enacted in response to concerns that electronic funds transfers were such that the rights and liabilities of customers (particularly) and banks were unclear.[194] The Act applies to all transactions "initiated through an electronic terminal, telephonic instrument or computer or magnetic tape".[195]

2 *Mandate*

The Electronic Fund Transfer Act provides that a customer is not liable for an electronic transaction, other than a transaction that has been initiated by a card, code or other means of access that can be identified as relating to that customer.[196] The Act does not provide guidance as to what does amount to mandate. Rather, it means that a bank cannot construe mandate from a means of access that does not identify the individual customer.

Instead, as for the other jurisdictions considered, mandate for online banking is covered by the contractual terms and conditions agreed between banks and customers. The general approach once again seems to be that logging in with the correct password amounts to mandate.[197]

3 *Authorisation*

Unlike the other jurisdictions considered in this paper, the Electronic Fund Transfer Act does not provide that a customer will face liability if he or she failed to observe some security provisions or satisfy a reasonable person

---

[193] 15 USC § 1693.
[194] 15 USC § 1693 Congressional findings and declaration of purpose.
[195] 15 USC § 1693a(6).
[196] 15 USC § 1693g(a) and 1693g(e).
[197] See, for example, Wells Fargo "Online Access Agreement for Wells Fargo Online and Wells Fargo Business Online Services" <http://www.wellsfargo.com> (last accessed 15 January 2006), cl X.

standard. Instead, the Act focuses on the concept of an "unauthorised" transaction. If a transaction is authorised, the customer is fully liable. If it is unauthorised, the customer is able to take advantage of the limited liability provision discussed below.

An unauthorised transaction is defined as a "transfer from a [customer's] account initiated by a person other than the [customer] without actual authority to initiate such transfer and from which the [customer] receives no benefit".[198] The definition goes on to exclude fraudulent transactions[199] and transactions where the customer has "furnished" his or her password to another person.[200]

The meaning of "furnished" has been considered in some early cases relating to ATM withdrawals. These cases specifically considered whether a customer who was tricked into disclosing his or her PIN to a fraudster has "furnished" it. It would appear that being unwittingly tricked into disclosing a PIN does not amount to "furnishing", even where customers were warned (although perhaps not obviously) to be careful with their PIN numbers.[201]

4 Liability

The Electronic Fund Transfer Act creates a tiered limited liability regime for unauthorised transactions based on the time it takes a customer to notify his or her bank. A customer's liability is limited to US$50 if he or she reports an unauthorised transaction within two business days of first noticing the unauthorised transaction. This rises to US$500 if the customer delays more than two business days but still reports the unauthorised transaction within sixty days of receiving his or her periodic account statement. After sixty days,

---

[198] 15 USC § 1693a(11).
[199] 15 USC § 1693a(11)(B).
[200] 15 USC § 1693a(11)(A).
[201] *Ognibene v Citibank*, above n 151. This contrasts with the position prior to the Electronic Fund Transfer Act – see *Feldman v Citibank* (1981) 110 Misc 2d 838; (1981) 443 NYS 2d 43; [1981] NY Misc LEXIS 3172 (Civil Court of City of New York, Queens County, NY, USA), where the plaintiff was not able to recover in an identical scam to *Ognibene*. See also Jeff Sovern "The Jewel of their Souls: Preventing Identity Theft through Loss Allocation Rules" (2003) 64 U Pitt L Rev 343, 376 and footnote 128.

the customer is liable for the entire amount of the unauthorised transaction.[202] Provision is made for the time limits to be extended in extenuating circumstances such as travel or hospitalisation.[203]

5 Security

In quite a different approach from the other jurisdictions considered in this paper, the Electronic Fund Transfer Act provides that customers have no liability for any unauthorised transactions,[204] other than the $50/$500 discussed above. It does not appear as though there is any particular standard of care required of the customer.

Provided that the transaction was unauthorised, and reported to the bank within the statutory timeframes, even negligent customers would not be liable for any unauthorised transactions, other than the relevant limited liability amount depending on the delay in reporting the transaction.[205]

6 Presumptions and the burden of proof

The United States provides the clearest rules about the burden of proof. The customer has the initial "burden of going forward" to detect and report unauthorised transactions.[206] However, once that burden is discharged, the bank is solely responsible for showing that the transaction was authorised.[207] If they are unable to do so, the bank must refund the customer the amount of the unauthorised transaction, less the $50/$500 statutory limit.

---

[202] Subject to some causation matters that are beyond the scope of this paper – see 15 USC § 1693g(a).
[203] 15 USC § 1693g(a). See also, for example, Wells Fargo "Online Access Agreement for Wells Fargo Online and Wells Fargo Business Online Services", above n 197, cl IX(B).
[204] 15 USC § 1693g(e).
[205] Clayton P Gillette "Rules, Standards, and Precautions in Payment Systems" (1996) 82 Va L Rev 181, 183 and footnote 7.
[206] 15 USC § 1693g(a) and *Ognibene v Citibank*, above n 151, 222 Mara T Thorpe J. See also "ATM Crime: Expanding the Judicial Approach to a Bank's Liability for Third Party Crimes against ATM Patrons" (1995) 30 Val UL Rev 99, 111-112 and footnote 69.
[207] 15 USC § 1693g(b).

General United States case law also reflects this position. The case of *Judd v Citibank*[208] was decided before the Electronic Fund Transfer Act came into force. However, the result would have been the same following the passage of the Act. The case also provides some interesting guidance about witness evidence and the reliability of machine or computer evidence. The Court essentially held that computer evidence cannot be considered conclusive in and of itself. The opposing evidence of a credible witness must be given due weight.[209] The Court held that to do otherwise would be to subject the customer to an "unmeetable burden of proof".[210]

D The Jurisdictions Compared

New Zealand, the United Kingdom, Australia and the United States have adopted different approaches towards regulating online banking.[211] The United States offers the most favourable terms to the customer (and correspondingly, least favourable to the bank), followed in order by Australia and the United Kingdom, with New Zealand the least favourable.

It is perhaps a sign of the interests involved that the two jurisdictions with entirely self-regulatory approaches (New Zealand and the United Kingdom) provide banks the most comfort, while the two jurisdictions that have seen government intervention (Australia and the United States) are more customer-centric. However, this customer-focus has not prevented the expansion of online banking in those jurisdictions. In fact, as Anderson points out, that while United States banks inevitably pay out a certain amount due to customer complaints that are fraudulent, it is not substantial.[212] This is reflected in an

---

[208] (1980) 107 Misc 2d 526; (1980) 435 NYS 2d 210; [1980] NY Misc. LEXIS 2882 (Civil Court of the City of New York, Queens County, NY, USA).
[209] *Judd v Citibank*, above n 208, 527-528 John Marmarellis J.
[210] *Judd v Citibank*, above n 208, 529 John Marmarellis J.
[211] Appendix 2 to this paper sets out a tabular comparison of the regimes of New Zealand, the United Kingdom, Australia and the United States. See page III, below.
[212] Anderson "Nine Principles", above n 112, 6. However, note this paper was written in 1994 and the amounts quoted are now out-of-date.

early United States case considering unauthorised electronic transactions. There the Judge stated:[213]

> ...the court is not unmindful of the possibility of fraudulent suits. However, this fear exists in many areas of the law and the history of jurisprudence has not indicated that courts have been unable to competently (although certainly not perfectly) deal with such challenges.

Moreover, Anderson states that United Kingdom banks pay substantially more on security measures than their United States counterparts.[214] This is presumably to provide better security in an attempt to ensure the mandate and fault presumptions apply. Given the similarities of the United Kingdom and New Zealand approaches, similar conclusions could be drawn for New Zealand.

E Some Legal Conclusions

We can therefore conclude that lessening some of the burden on the customer would not spell the end of online banking. Such a readjustment in the current review of the Code of Banking Practice[215] may therefore be appropriate. This would also pre-empt the possibility that Parliament may decide to enact more extreme legislative measures, as happened in the United States.

While the exact distribution of bank and customer rights and obligations will always be open to debate, this paper considers that one measure in particular should be adopted in New Zealand: merging the provisos to the limited liability clause (negligence and breach of password clause), so that a customer must unreasonably breach the password clause before being held liable. Only holding customers liable for such "blameworthy breaches" is the approach of the United Kingdom and Australia. This approach would be fairer to customers, in that technical breaches[216] would not attract liability unless it was proved the breach led to the loss. However, perhaps more importantly, it would potentially

---

[213] *Porter v Citibank* (1984) 123 Misc 2d 28, 30; 472 NYS 2d 582, 583; 1984 NY Misc LEXIS 2961, 6 (Civil Court of the City of New York, New York County, NY, USA) Edward H Lehner J.

[214] Anderson "Nine Principles", above n 112, 6.

[215] New Zealand Bankers' Association "Review of the Code of Banking Practice", above n 158.

[216] See, for example, the case of Mr and Mrs S, above n 83, and accompanying text.

allow for greater practical security, assisting both banks and customers. There are many sorts of services (both online and offline) that require passwords or identification codes. The advice offered to customers by many of these service-providers is not to choose a password that the customer uses elsewhere. Similarly, many instruct customers not to write down the password.[217] Yet it is impossible for customers to remember such a wide array of unique passwords, particularly if the service or password is not used often. Customers are therefore always likely to write passwords down, use the same password on less-secure websites or pick easy-to-guess passwords. This paper suggests that banks would attract greater security by instructing customers on suitable ways to disguise written passwords so that they cannot be deciphered readily. However, New Zealand banks cannot provide this advice in light of their current express terms. To do so would encourage customers to breach the password clause.

As a secondary measure, one favouring customers, banks should assume the burden to prove that a customer breached the terms, rather than shifting the burden on to the customer to prove that he or she did not. This would provide a fairer approach, in that the burden would be placed on that best-placed to bear it. Banks have far more resources to investigate complaints than customers. In the event that both parties are innocent, banks are also much-better placed to bear any loss. It would also incentivise banks to do everything (economically) possible to reduce the risk of unauthorised transactions in online banking.

These two measures would make New Zealand's online banking provisions very similar to Australia's. Generally, this paper considers that the Australian model provides a good starting point for the current review of the Code of Banking Practice. It seems to provide an appropriate balance between the interests of banks and customers. It would also be easy to implement, given the Australian-dominance of the New Zealand banking industry and their existing experience with the EFT Code.

---

[217] See the password clause, above page 18.

F Technical Measures

This paper also considers that New Zealand banks should increase the rigour of their technical security measures. This paper's analysis of SSL, banks primary security mechanism, shows its weaknesses. These are due to a misunderstanding as to SSL's purpose. It is not designed to provide any guarantee as to customer authenticity. Additional security measures keyed to individual customers would provide far greater certainty as to customer authenticity.

Such measures may include biometric measures such as retina scans, thumb prints or voice recognition.[218] Perhaps more likely in the near future, the two-factor authentication devices[219] adopted by some banks should be adopted by those that have not yet done so. Even more low-tech would be to adopt Transaction Authentication Numbers ("TANs").[220] TANs essentially consist of a sheet of paper containing numerous codes. Each time a customer wishes to log on to online banking, a TAN must be entered. Once that TAN is used, the customer crosses it off the list and cannot use it again. Once all the numbers are used, the customer must go into his or her bank and collect another sheet. Again, this provides two-factor authentication, as the customer must both know something (the password) and have something (the sheet of TANs). Like the two-factor authentication devices, TANs would ensure that customers are not vulnerable to cracker attacks, as obtaining a log-on, password and one-use code from a device or TAN sheet would not necessarily provide a cracker access to the customer's account. The one-use codes constantly change. Similar results could be achieved by issuing customers a card with an indexed grid on it. To log on to online banking, a customer would need to look up grid references and enter the corresponding character. Because the grid reference would be

---

[218] See, for example, *Wikipedia*, above n 27, "Biometrics".
[219] See above n 131, and accompanying text.
[220] See, for example, *Wikipedia*, above n 27, "TAN (banking)".

different each time, this would amount to a one-use code that would prevent cracker attacks.[221]

Any of the above approaches would provide much greater security. This would obviously benefit customers, who currently wear the large majority of the risk for unauthorised transactions. But it is also likely to benefit banks too. By providing much greater technical security, banks are better-insulated from the potential legal and evidential challenges of a fraudster attempting to exploit the advice for customers discussed above.[222] Better security measures may also enable banks to argue that, in fact, the security, authorisation and fault presumptions *do* apply. If online banking is in fact secure, and there are no other possible ways the security of online banking can be compromised, these presumptions would be well-founded and the criticisms levelled in this paper unjustified.

IX CONCLUSION

This paper considered the regime for online banking that operates in New Zealand. An analysis of the contractual terms that govern the bank-customer relationship revealed that the current framework is heavily weighted in favour of banks at the expense of their customers. The purpose of the terms is to create presumptions that shift essential elements of the burden of proof from the bank to the customer. This paper endeavoured to point out the difficulties this framework poses for a customer trying to have an unauthorised withdrawal refunded.

Shifting this burden of proof is based on the premise that online banking is secure. But this paper argues that this is an incorrect premise. Online banking is not secure. It is subject to weaknesses in both bank practices and cracker attacks. However, the potential vulnerabilities and the fundamental misunderstanding of the purpose of the technical security measures adopted by online banking means that customers may not be without redress. This paper

---

[221] See, for example, Entrust Inc. <http://www.entrust.com> (last accessed 25 January 2006).
[222] See above page 37 and following.

presented some advice to customers in the position of Gus Tommer, a victim of an unauthorised transaction. The weaknesses due to bank practices and bank security measures may enable Gus to challenge his unauthorised transaction.

The paper also offered some advice for banks. A survey of some comparative overseas jurisdictions showed that it is not necessary for contractual terms to be weighted so heavily in favour of banks. It is hoped that some of these considerations will be adopted in the current review of the Code of Banking Practice. In particular, this paper has pointed out the need to provide that customers are only liable for "blameworthy breaches". Shifting elements of the burden of proof back to banks would also be desirable. Banks are far better placed than customers to bear the risk of unauthorised transactions. It would also incentivise banks to do everything (economically) possible to reduce the risk of unauthorised transactions in online banking.

This paper also suggested some technical measures that banks should adopt. These measures would go a long way towards addressing the potential vulnerabilities of current systems raised in this paper. In doing so, banks may be able to insulate themselves against potential challenges to the current system as well as providing a greater security for customers. Two-factor authentication is a major enhancement that could be readily adopted. Greater technical security *may* overcome the need to make the sort of legal changes canvassed by this paper. However, technical security measures do not yet seem to have reached a point where they can absolutely guarantee the integrity of online banking and guard against every conceivable cracker attack.

Combining the legal and technical suggestions of this paper would potentially insulate banks against challenges by customers, while also ensuring greater practical security for online banking and a fairer and more-balanced approach for both customers and banks.

APPENDIX 1: LIST OF DEFINED CONCEPTS USED IN THIS PAPER

The following concepts (in order of occurrence) are defined and used by this paper:

Mandate clause: clause in online banking express terms providing that use of a customer's log-on and password amounts to mandate. See page 15.

Notification clause: clause in online banking express terms providing that a customer is not liable for any unauthorised transactions that occur after notifying the bank of a potential security breach. See page 16.

No liability clause: clause in online banking express terms providing the range of circumstances where customers will not be liable for unauthorised transactions. Includes provisions relating to transactions occurring before registration, fraud on the part of bank staff ("no liability (fraud)") or where there are technical faults or errors in the online banking systems ("no liability (error)"). See page 16.

Limited liability clause: clause in online banking express terms proving the range of circumstances where a customer will be able to limit his or her liability for unauthorised transactions. Includes provisos relating to fraud, negligence and breaching terms and conditions (the provisos to the limited liability clause) See page 16.

Password clause: clause in online banking express terms providing that a customer is obliged to safeguard passwords. In the context of EFTPOS and credit cards, also includes physical security of the card. See page 18.

Security presumption: presumption that an instruction to make a transaction on a customer's account has been made using that customer's log-on and password. Stems from the proposition that the technical security measures implemented by banks make online banking secure. See page 19.

Authorisation presumption: presumption that transactions are authorised by the customer if the correct log-on and password are used. Combination of mandate clause and security presumption. See page 20.

Fault presumption: presumption that the customer is at fault for unauthorised transactions, either by being negligent in his or her security practices or breaching the password clause. Combination of security presumption, rebuttal of authorisation presumption and password clause. See page 22.

APPENDIX 2: TABULAR COMPARISON OF JURISDICTIONS

	New Zealand	The United Kingdom	Australia	The United States
Regime	Contract, self regulatory code	Contract, self regulatory code	Contract, government-sponsored code	Primarily statute, some contractual terms
Mandate	Presumption that correct log-on and password amounts to mandate			
Liability for unauthorised transactions (other than those where no liability applies, e.g. fraud of bank staff)	Limited to NZ$50, other than where fraudulent, negligent, breached terms and conditions or otherwise contributed to the loss (e.g. breach of password clauses)	Limited to £50, other than where fraudulent or failed to take reasonable care (e.g. breach of password clauses)	Limited to A$150, other than where fraudulent or failed to comply with password clauses	Limited to US$50 if reported to bank within two days of noticing unauthorised transaction or $500 if reported to bank within sixty days of periodic account statement
Security	Must (absolutely) keep password confidential, choose appropriate password, not write password down etc.	Must take reasonable care to keep password confidential, choose appropriate password, not write password down etc.	Must not act with "extreme carelessness", must make reasonable attempts to protect security of written record of password	Must not "furnish" password
Presumptions / burden of proof	Correct log-on and password amounts to mandate Customer to detect and report unauthorised transactions			
	System secure, therefore an unauthorised transaction must be result of customer's fraud or negligence unless the customer proves otherwise	Bank must show customer's fraud or negligence (though note that approach not universally adopted), possible presumption that unauthorised transaction must be result of customer's fraud or negligence	Bank must show customer's fraud or negligence, all reasonable evidence, including reasonable explanations for transactions, must be considered	Bank must show transaction authorised, evidence of machine / computer record not conclusive evidence in itself

APPENDIX 3: BIBILOGRAPHY

A Primary Sources

1 Legislation

New Zealand

- Bills of Exchange Act 1908
- Cheques Act 1960
- Consumer Guarantees Act 1993
- Disputes Tribunals Act 1988
- Electronic Transactions Act 2002
- Fair Trading Act 1986
- High Court Rules

Australia

- Australian Securities and Investments Commission Act 2001

United States of America

- Electronic Fund Transfer Act 1982 15 USC § 1693

2 Cases

New Zealand

- *Bank of New Zealand v The Auckland Information Bureau (Incorporated)* [1996] 1 NZLR 420 (CA)
- *Goodson v Hawera Lawn Tennis and Croquet Club Inc* [1931] NZLR 1096 (Supreme Court)
- *Westpac Banking Corporation v MM Kembla New Zealand Limited* [2001] 2 NZLR 298 (CA)

United Kingdom

- *Greenwood v Martins Bank Limited* [1933] AC 51 (HL)

- *Joachimson v Swiss Bank Corporation* [1921] 3 KB 110 (CA)
- *London Joint Stock Bank Limited v Macmillan* [1918] AC 777 (HL)
- *Scott v London and St Katherine Docks Company* (1865) 3 H & C 596; 159 ER 665 (Exchequer Chamber)
- *Tai Hing Cotton Mill Limited v Liu Chong Hing Bank Limited and Others* [1986] AC 80 (PC)
- *Young v Grote and Others* (1827) 4 Bing 253; 130 ER 764 (CP)

United States of America

- *Feldman v Citibank* (1981) 110 Misc 2d 838; (1981) 443 NYS 2d 43; [1981] NY Misc LEXIS 3172 (Civil Court of City of New York, Queens County, NY, USA)
- *Judd v Citibank* (1980) 107 Misc 2d 526; (1980) 435 NYS 2d 210; [1980] NY Misc. LEXIS 2882 (Civil Court of the City of New York, Queens County, NY, USA)
- *Ognibene v Citibank* (1981) 112 Misc 2d 219; (1981) 446 NYS 2d 845; [1981] NY Misc LEXIS 3417 (Civil Court of the City of New York, New York County)
- *Porter v Citibank* (1984) 123 Misc 2d 28; 472 NYS 2d 582; 1984 NY Misc LEXIS 2961 (Civil Court of the City of New York, New York County, NY, USA)

3 Bank documents and websites

New Zealand

- ANZ National Bank Limited, trading as the National Bank of New Zealand *Cashpoint Card: Conditions of Use* (Wellington, 2005)
- ANZ National Bank Limited, trading as the National Bank of New Zealand *Thoroughbred, Visa and Freestyle: Conditions of Use* (Wellington, 2005)
- ANZ National Bank Limited, trading as ANZ New Zealand <http://www.anz.co.nz> (last accessed 4 February 2006)

- ANZ National Bank Limited, trading as the National Bank of New Zealand <http://www.nbnz.co.nz> (last accessed 4 February 2006)
  - "Change my password"
  - "Online Banking Conditions of Use (Version 11)"
- ASB Bank Limited <http://www.asb.co.nz> (last accessed 4 February 2006)
  - "FastNet Classic: Terms and Conditions"
  - "Personal Banking Terms and Conditions"
  - "Precautions we take"
- Bank of New Zealand <http://www.bnz.co.nz> (last accessed 4 February 2006)
  - "Internet Banking and Internet Banking for Business Security"
  - "Standard Terms and Conditions"
- Kiwibank Limited <http://www.kiwibank.co.nz> (last accessed 4 February 2006)
- St George Bank New Zealand Limited, trading as Superbank <http://www.superbank.co.nz> (last accessed 4 February 2006)
  - "Security Information"
- The Hongkong and Shanghai Banking Corporation Limited <http://www.hsbc.co.nz> (last accessed 4 February 2006)
- TSB Bank Limited <http://www.tsb.co.nz> (last accessed 4 February 2006)
- Westpac Banking Corporation (New Zealand division) <http://www.westpac.co.nz> (last accessed 4 February 2006):
  - "How secure is online banking?"
  - "Online Banking Terms and Conditions"

United Kingdom

- Royal Bank of Scotland <http://www.rbs.co.uk> (last accessed 14 January 2006)
  - "Direct and Digital Banking Services: Terms and Conditions"
- Hongkong and Shanghai Banking Corporation Limited <http://www.hsbc.co.uk> (last accessed 14 January 2006)

- "Internet Banking Terms and Conditions"

Australia

- Westpac Banking Corporation <http://www.westpac.com.au> (last accessed 23 January 2006)
  - "Latest hoax email scam"
  - "Terms and Conditions for Internet Banking and BPAY"
- National Australia Bank <http://www.national.com.au> (last accessed 15 January 2006)
  - "National Internet Banking Product Disclosure Statement including Terms and Conditions"

United States

- Wells Fargo <http://www.wellsfargo.com> (last accessed 15 January 2006)
  - "Online Access Agreement for Wells Fargo Online and Wells Fargo Business Online Services"

4 Other official/quasi-official banking sources

New Zealand

- New Zealand Bankers' Association <http://www.nzba.org.nz> (last accessed 4 February 2006)
- New Zealand Bankers' Association "Review of the Code of Banking Practice" <http://www.nzba.org.nz> (last accessed 4 February 2006)
- New Zealand Bankers' Association *Code of Banking Practice* (Third Edition, Wellington, 2002). Available at <http://www.nzba.org.nz> (last accessed 4 February 2006)
- New Zealand Bankers' Association *Payment Statistics 2004* (Wellington, 2004). Available at <http://www.nzba.org.nz> (last accessed 4 February 2006)
- Office of the Banking Ombudsman of New Zealand <http://www.bankombudsman.org.nz> (last accessed 4 February 2006)

- Office of the Banking Ombudsman *Case Note Compendium 2000-2001* (Wellington, 2001)
- Office of the Banking Ombudsman *Case Note Compendium 2001-2002* (Wellington, 2002)
- Office of the Banking Ombudsman *Case Note Compendium 2002-2003* (Wellington, 2003)
- Office of the Banking Ombudsman *Case Note Compendium 2003-2004* (Wellington, 2004)
- Office of the Banking Ombudsman *Case Note Compendium 2004-2005* (Wellington, 2005)
- Office of the Banking Ombudsman of New Zealand *Annual Report 2000-2001* (Wellington, 2001)
- Office of the Banking Ombudsman of New Zealand *Annual Report 2001-2002* (Wellington, 2002)
- Office of the Banking Ombudsman of New Zealand *Annual Report 2002-2003* (Wellington, 2003)
- Office of the Banking Ombudsman of New Zealand *Annual Report 2003-2004* (Wellington, 2004)
- Office of the Banking Ombudsman of New Zealand *Annual Report 2004-2005* (Wellington, 2005)
- Office of the Banking Ombudsman of New Zealand *Banking Ombudsman Terms of Reference* (Wellington, 2002).
- Reserve Bank of New Zealand <http://www.rbnz.govt.nz> (last accessed 4 February 2006)
- Reserve Bank of New Zealand "Implementation of Basel II capital rules in New Zealand" (18 March 2005) Press Release <http://www.rbnz.govt.nz> (last accessed 23 January 2006)
- Reserve Bank of New Zealand *Payment and Settlement Systems in New Zealand* (Wellington, 2003). Available at <http://www.rbnz.govt.nz> (last accessed 4 February 2006)

United Kingdom

- British Bankers' Association, the Building Societies Association and the Association for Payment Clearing Services *The Banking Code* (London, United Kingdom, 2003). Available at <http://www.bankingcode.org.uk> (last accessed 4 February 2006)

Australia

- Australian Securities and Investments Commission <http://www.asic.gov.au> (last accessed 15 January 2006).
- Australian Securities and Investments Commission consumer protection website <http://www.fido.asic.gov.au> (last accessed 15 January 2006)
- Australian Securities and Investments Commission *Electronic Funds Transfer Code of Conduct* (Canberra ACT, Australia, 2002). Available at <http://www.fido.asic.gov.au> (last accessed 15 January 2006)

United States

- Federal Financial Institutions Examination Council *Information Technology Examination Handbook: E-Banking* (Washington DC, USA, 2003) 1. Available at <http://www.ffiec.gov> (last accessed 4 February 2006)

International

- Bank for International Settlements "About the Basel Committee" <http://www.bis.org> (last accessed 23 January 2006)
- Basel Committee on Banking Supervision *Risk management principles for electronic banking* (Basel, Switzerland, 2003). Available at <http://www.bis.org> (last accessed 23 January 2006)

5 *Other primary sources*

- New Zealand Law Commission *Electronic Commerce Part Two: A Basic Legal Framework* (NZLC R58, Wellington, 1999)

- New Zealand Law Commission *Electronic Commerce Part Three: Remaining Issues* (NZLC R68, Wellington, 2000)
- Entrust Inc. <http://www.entrust.com> (last accessed 25 January 2006)
- Serversniff.net <http://serversniff.net> (last accessed 11 January 2006)
- Top500.org <http://top500.org> (last accessed 10 January 2006)

B Secondary Sources

1 Texts

- *Electronic Business and Technology Law (NZ)* (Service 12, LexisNexis NZ Limited, March 2005) <http://www.lexisnexis.co.nz> (last accessed 10 January 2006)
- *Laws of New Zealand* (Service 36, LexisNexis NZ Limited, September 2005) <http://www.lexisnexis.co.nz>
  - Consumer Protection
  - Negotiable Instruments
- Mathieson QC, DL (ed) *Cross on Evidence (NZ)* (Service 40, LexisNexis NZ Limited, December 2005) <http://lexisnexis.co.nz> (last accessed 13 January 2006)
- *McGechan on Procedure* (Brookers Limited, Wellington, February 2006) <http://www.brookers.co.nz> (last accessed 19 February 2006)
- *Wikipedia* (Wikimedia Foundation Inc, St Petersburg FL, USA, 2006) <http://en.wikipedia.org> (last accessed 4 February 2006)
  - "Biometrics"
  - "Certificate Authority"
  - "Diffie-Hellman Key Exchange"
  - "Domain Name System"
  - "Hacker"
  - "Hacker (computer security)"
  - "Hacker Definition Controversy"
  - "Hash Function"
  - "Keystroke Logging"
  - "Pharming"

- "Phishing"
- "Public-Key Cryptography"
- "SHA Hash Functions"
- "Spoofing Attack"
- "TAN (banking)"
- "Transport Layer Security"
- "Uniform Resource Locator"

2 *Journals and articles*

- "ATM Crime: Expanding the Judicial Approach to a Bank's Liability for Third Party Crimes against ATM Patrons" (1995) 30 Val UL Rev 99
- "E-commerce" [2003] Legal Information Access Centre – Hot Topics 1 <http://www.austlii.edu.au> (last accessed 4 February 2006)
- Anderson, Ross "Liability and Computer Security: Nine Principles" (University of Cambridge, 1994) <http://www.cl.cam.ac.uk/> (last accessed 20 January 2006)
- Anderson, Ross "Why Cryptosystems Fail" (University of Cambridge, 1993) <http://www.cl.cam.ac.uk/> (last accessed 20 January 2006)
- Arora, Anu "Unfair Contract Terms in International Banking Contracts" [2001] JBL 553
- Azzouni, Ahmad "Internet Banking and the Law" (2003) 18 JIBLR 351
- Batalla, Enrique J "Electronic Commerce: Online Payments" (2001) 7 CTLR 80
- Bohm, Nicholas, Brown, Ian and Gladman, Brian "Electronic Commerce: Who Carries the Risk of Fraud?" 2000(3) Journal of Information, Law and Technology. Available at the University of Warwick's Electronic Law Journals project <http://www2.warwick.ac.uk> (last accessed 14 January 2006)
- Bond, Mike and Zieliński, Piotr "Decimalisation table attacks for PIN cracking" (University of Cambridge, 2003) <http://www.cl.cam.ac.uk/> (last accessed 20 January 2006)

- Cannady, Stacy and Stockton, Thomas "Easing the PAIN" (IBM, New York NY, USA, 2001) <http://www.ibm.com> (last accessed 10 January 2006)
- Gillette, Clayton P "Rules, Standards, and Precautions in Payment Systems" (1996) 82 Va L Rev 181
- Gkoutzinis, Apostolos "The Prudential Supervision of Internet Banking in the United Kingdom – is the 'Basel Approach' Finding its way through National Regulations" (2002) 17 JIBL 249
- Maysami, Ramin Cooper and Mills, Kim "Regulation and Supervision of Online Banking Services in the United States: An Integrated Approach" (2004) 19 JIBLR 447
- Onyszko, Tomasz "Secure Socket Layer" [sic] (WindowSecurity.com, 2004) <http://www.windowsecurity.com> (last accessed 10 January 2006)
- Shum, Clement and Ko, Sai-hong "The Legal Significance of PINs in Banking" 30 Hong Kong LJ 194
- Sovern, Jeff "The Jewel of their Souls: Preventing Identity Theft through Loss Allocation Rules" (2003) 64 U Pitt L Rev 343
- Teo, Jack C C "A Stitch in Time Saves Nine" (1998) 13 JIBL 370
- Tripe, David "Technology, Banking and Risk" (2001) 1 TLF 61

3 *Other*

- Bond, Mike "Phantom Withdrawals: on-line resources for victims of ATM fraud" <http://www.cl.cam.ac.uk/> (last accessed 20 January 2006)
- Katayama, Fred "Hacker hits up to 8M credit cards" (27 February 2003) *CNNMoney.com* United States <http://www.cnnmoney.com> (last accessed 20 January 2006)
- Krim, Jonathan and Barbaro, Michael "40 Million Credit Card Numbers Hacked" (18 June 2005) *The Washington Post* Washington DC, USA <http://www.washingtonpost.com> (last accessed 20 January 2006)

- Leyden, John "How to get an ATM PIN in 15 guesses" (21 February 2003) *The Register* United Kingdom <http://www.theregister.co.uk> (last accessed 20 January 2006)
- "Phishing scam continues to hit Westpac" (4 January 2006) *National Business Review* New Zealand <http://www.nbr.co.nz> (last accessed 20 January 2006)
- University of Cambridge Computer Laboratory <http://www.cl.cam.ac.uk/> (last accessed 20 January 2006)
  - Documentation associated with *Diners Club (SA) Pty Limited v Singh*