Joint submission to the 2007 Review of the Electronic Funds Transfer (EFT) Code of Conduct

CHOICE

Consumer Action Law Centre

Centre for Credit and Consumer Law

(30 May 2007)

Prepared by: Galexia
Suite 95 Jones Bay Wharf, 26-32 Pirrama Road,
Pyrmont (Sydney) NSW 2009, Australia
ACN: 087 459 989
Ph: +61 2 9660 1111
Fax: +61 2 9660 7611
WWW: www.galexia.com

Document Control

Client

This report has been written for CHOICE, the Consumer Action Law Centre and the Centre for Credit and Consumer Law.

Document Purpose

This document is a joint submission to the 2007 Review of the Electronic Funds Transfer (EFT) Code of Conduct from CHOICE, the Consumer Action Law Centre and the Centre for Credit and Consumer Law.

Document Production

This Document was prepared by Galexia. Guidance, input and comments were received from a small reference group consisting of representatives of CHOICE, the Consumer Action Law Centre, the Centre for Credit and Consumer Law, the Australian Privacy Foundation, the Consumer Credit Legal Centre (NSW), Care Inc. Financial Counseling Service and Consumer Law Centre of the ACT. Funding assistance was received from the Australian Securities and Investments Commission Consumer Advisory Panel (ASIC CAP).

Consultant Contact:

Chris Connolly (Director)
Galexia
Suite 95 Jones Bay Wharf
26-32 Pirrama Road, Pyrmont NSW 2009
Phone: +612 9660 1111
Fax: +612 9660 7611

Copyright

Contents

1. Executive Summary

This document is a joint submission from CHOICE, the Consumer Action Law Centre and the Centre for Credit and Consumer Law to the Australian Securities and Investments Commission in respect of the 2007 Review of the Electronic Funds Transfer (EFT) Code of Conduct.

This Document was prepared by Galexia. Guidance, input and comments were received from a small reference group consisting of representatives of:

— CHOICE;

— Consumer Action Law Centre;

— Centre for Credit and Consumer Law;

— Australian Privacy Foundation;

— Consumer Credit Legal Centre (NSW); and

— Care Inc. (Financial Counseling Service and Consumer Law Centre of the ACT).

Funding assistance was received from the Australian Securities and Investments Commission Consumer Advisory Panel (ASIC CAP).

As ASIC would be aware, many consumer and community groups have limited resources to participate in reviews of this size and import. With greater resourcing capacity, it might have been possible for other organisations to have also had a direct input into the preparation of this submission.

Consumer stakeholders see this review as an opportunity to dramatically improve the EFT Code. This submission attempts to answer every question raised in the ASIC Consultation paper and also provides additional comments and suggestions.

The core of this submission is a proposed five-step approach to improving the Code:

Step 1: Retaining a fair liability approach

The current liability approach in Clause 5 of the Code is working well. Although there have been some changes in the vulnerability of Internet banking since the last review of the Code (for example the growth in social engineering attacks), there is no justification for changing the overall liability regime in the Code. Financial institutions remain in the best position to address security issues in Internet banking and the responsibility of consumers is already fairly addressed in the Code.

Two key suggested liability reforms are firmly rejected in this submission:

— **Increased liability for consumers who fail to secure their personal computers**
This submission presents detailed arguments outlining policy and practical issues which would be faced if this reform was to proceed.

— **Increased liability for consumers who respond to social engineering attacks**
Although there are measures that can be taken by banking customers in order to combat phishing attacks, this submission describes how these measures are considerably less effective than the technologies that can be utilised by financial institutions to deal with phishing.

Step 2: Improving the dispute resolution experience for consumers

This submission presents some suggested improvements to ensure internal and external dispute resolution processes are meeting the needs of consumers. Reference is made to the *Consumer Caseworker Submission* which contains detailed case studies of EFT related complaints. This submission endorses the recommendations contained in the *Consumer Caseworker Submission*.

Step 3: Shortening the Code

The Code has become long and unwieldy and this is having a negative impact on Code subscription, compliance, education and complaints management. Code length has a knock on impact on the length of terms and conditions as all clauses tend to be repeated by financial institutions in their terms and conditions – making them difficult to digest for consumers.

This submission recommends some significant changes to the Code in the interest of shortening the Code:

- The complete removal of Part B of the Code;
- Moving specific scenarios set out in the text to examples in notes rather than including them all as separate Clauses in the Code, and relying on common sense interpretation by internal and external dispute resolution; and
- The removal of a number of minor Clauses (described in further detail in the submission).

Step 4: Simplifying the Code

The Code has become complex and difficult to interpret. This is having a negative impact on Code subscription and complaints management. Code complaints often relate to small value transactions and it is difficult to justify the expense of legal advice in interpreting the Code. Simplifying the Code will benefit all stakeholders.

This submission recommends some significant changes to the Code in the interest of simplifying the Code:

- Removal of the business / consumer account distinction so that the Code can be more simply applied to all transactions. This will simplify terms and conditions, implementation, complaints management and data collection;
- Removal of Part B from the Code will simplify the Code. Part B is technically complex and has delivered little benefit;
- Removal of Part B and the collapse of Part A and Part C into one section will simplify the Code. There will be no requirement to refer to 'Parts' in the text;
- Relocation of endnotes to short footnotes so that they can be read together with the text; and
- Relocation of all Clauses on interpretation and scope into one section at the front of the Code (e.g. moving Clauses 8 and 20 to the beginning of the Code).

Step 5: Commissioning a Technology Neutrality Review of the final Code text

In addition to reviewing the Code content, this submission recommends a thorough Technology Neutrality Review of the Code text. This review should ensure that the terms used in the Code are defined broadly enough to encompass the wide range of technology that might be used to complete an EFT transaction. The key terms that require review are:

— Electronic equipment;

— Device;

— Identifier; and

— Code.

This issue is discussed in further detail in response to *Q73 – Are there other issues not covered in this consultation paper that the review should address?* below.

2. Marketplace Developments

Q1 – What do you see as the emerging trends or developments in the consumer payments marketplace in Australia over the next few years?

Three emerging trends in the marketplace are of interest in relation to the EFT Code review:

- **1. Growth in use of third party direct electronic transfers**
  Internet banking appears to have entered a new phase where it is common for customers to arrange direct transfer of funds to a third party using their BSB and Account Number. This service is now offered for all accounts – whereas at the time of the last review of the EFT Code this service was only available for a small number of account holders. Some financial institutions require additional security or authentication for direct transfers (e.g. there may be an extra security question before the transfer is confirmed).

- **2. Emergence of new Internet only payment services**
  A small number of new, Internet based payment systems are operating. Two of these services – PayPal and Checkout – have become quite prevalent and are widely used in Australia. They are not traditional payment systems or financial institutions but they do share many characteristics with credit cards and Internet banking. This type of service was not in widespread use at the time of the last EFT Code review.

- **3. Convergence / confusion of consumer banking and business banking**
  Although this development was also considered during the previous review of the EFT Code, there appears to now be even greater convergence of consumer banking and business banking. This is due to the growth in the home business and micro business sectors, and the need for micro-businesses (e.g. eBay sellers) to offer electronic payment systems to consumers. It is unlikely that all home businesses and micro businesses operate a strict division between their personal banking and their business banking, so determining which accounts are personal accounts may be difficult.

Q2 – Are there trends or developments that the Review Working Group should particularly consider in reviewing the EFT Code? What implications might these have for the regulatory scheme of the Code?

The convergence / confusion of consumer banking and business banking has significant implications. This issue is important because financial institution terms and conditions continue to be considerably harsher for those accounts not protected by the EFT Code. Terms and conditions provided by financial institutions are currently divided into Code compliant and non-compliant sections depending on the 'business' nature of the transaction. This issue may also have implications for the complexity of dispute resolution processes.

Q3 – What are the issues associated with the emergence of 'non-contact' payment facilities?

This does not appear to be a significant issue at this time. However, two minor issues may be raised by non-contact payment facilities:

— **Privacy**
Non-contact payment systems are not widespread and appear to be limited to stored value applications in the transport sector where their speed and convenience is appreciated by consumers. However, privacy and security issues may emerge if applications combine non-contact products with higher risk personal information (i.e. if the product can be accessed without authorisation and valuable personal information is revealed.). We note, for example, that this issue was a particular concern during the upgrading of passports to include non-contact functionality.

— **Absence of a PIN or Password**
Non-contact payment facilities may, in some circumstances, result in an electronic transfer without use of a PIN, password or other code. However, this does not appear to be an issue that requires detailed consideration in the Review of the EFT Code at this stage.

3. Growth in Online Fraud

Q4 – What do you see as the main challenges in relation to online fraud over the next few years? Are there trends or developments that the Review Working Group should particularly consider in reviewing the EFT Code?

There has been steady growth in the sophistication of fraud and this is matched by rising complexity in preventing fraud.

Fraud can take place through a variety of technical and social engineering techniques designed to compromise communication channels used to exchange sensitive data or to coax consumers into disclosing this data.

These techniques are constantly evolving. Some common forms include:

- **Phishing**
  Phishing involves the use of socially engineered ('spoofed') websites that are designed to appear as if they belong to legitimate and reputable businesses and financial institutions.[1] Users are lured to these websites by congruently designed emails. Once at the spoofed website, the user is deceived into providing confidential data such as usernames and passwords.

- **Pharming**
  Pharming occurs when a fraudulent party interferes with the domain name resolution process used to map a URL requested by an Internet user to its corresponding IP address. Pharming typically takes one of two forms:

  - Firstly, a DNS server can be hijacked and its data modified such that when a user enters the URL of a legitimate organisation's website, the server maps the domain name to the IP address of a spoofed website which the user is then forwarded to.[2]

  - The second form of pharming relies on the fact that end-user computers typically store a hosts file containing the IP addresses of certain commonly accessed domains. The hosts file abrogates the need for a DNS server to be contacted when the user wishes to visit those domains. A fraudulent party can, in some circumstances, compromise the data in the hosts file so that it points to the IP address of a spoofed website.[3]

[1] Black P, *Catching a phish: protecting online identity*, Internet Law Bulletin, Vol 8 No 10, 2006, page 133.

[2] Keizer G, *Possible Domain Poisoning Underway*, TechWeb, 4 March 2005, <http://www.techweb.com/wire/security/60405913>.

[3] de la Cuadra F, *Pharming – a new technique for Internet fraud*, eChannelLine Canada, 7 March 2005, <http://www.crime-research.org/news/07.03.2005/1015>.

- **Man-in-the-middle (MITM)**
  Man-in-the-middle attacks take place where a fraudulent party is able to intercept online communications between two innocent parties (such as a website and an end-user). Such attacks may be facilitated through the sending of deceptive emails which contain a link to a proxy server monitored by the fraudulent party. The proxy server undertakes the task of routing communications between the end-user and the actual website the user intends to deal with. Since all communications are routed via the proxy, the fraudulent party is able to covertly read and modify communications made between the website and end-user.

- **Replay Attacks**
  A replay attack is an extension of the conventional MITM attack in which the fraudulent party uses data they have obtained by eavesdropping on the communications between the website and end-user to assume the identity of either at a later date.

- **Spyware**
  Spyware refers to software covertly installed on an end-user's machine that then proceeds to monitor and collect information about the user's activities. More malignant versions may perform tasks such as redirecting users and stealing confidential information belonging to the user and distributing it to fraudulent parties. Common forms of spyware include keystroke loggers, screen loggers and pop-up window generators. Despite the availability of software utilities to detect and remove many types of spyware, it has become an extremely troublesome issue for Internet users. A 2004 survey of US Internet users revealed that 80% of respondents' computers were infected with spyware, with close to 90% of those respondents being unaware of the spyware's presence. Another study found that 85 million spyware programs were installed on the computers of a sample of Internet users, a clear indication of the magnitude of the problem.[4]

The increasing frequency with which these various attacks have begun to occur has precipitated a need for Internet users to be able to reliably verify the identity of websites they are visiting and the integrity of communications channels they use to communicate with web servers. In response to this need, a variety of authentication approaches have been proposed and/or developed. These are discussed further in the response to Question 30 (*Potential Responses to Phishing Attacks and other forms of Online Fraud*).

In reviewing the EFT Code, the Working Group should consider the fact that financial institutions are in the best position to implement many of these authentication technologies. This is a factor which largely undermines suggestions that the liability of account holders for losses resulting from online fraud should be increased compared with the current version of the Code.

[4] Commonwealth of Australia, *Senate - Official Hansard,* 12 May 2005, <http://www.aph.gov.au/hansard/senate/dailys/ds120505.pdf>, page 5.

Q5 – What information can you provide to the Working Group about online fraud countermeasures being considered or deployed by Australian financial institutions? How does the Australian response compare with that of other comparable countries, in your view?

There is no established industry recommendation or mandate which specifically requires Australian financial institutions to implement authentication technologies that are more advanced than the conventional username and password approach. However, several Australian banks (including Commonwealth Bank,[5] National Australia Bank,[6] Bendigo Bank,[7] ANZ,[8] Westpac[9] and HSBC[10]) have implemented some form of two-factor authentication for their Internet banking services.

However, two-factor authentication provides only minimal protection against phishing attacks.[11] For this reason, financial institutions need to consider deploying technologies that enable them to authenticate their websites to customers.

Nevertheless, there are examples of recommendations and mandates being issued in other jurisdictions regarding the use of two-factor authentication by financial institutions. These include:

— **United Kingdom**
APACS, the UK trade association for payments and for institutions who deliver payment services to customers, currently has 31 members whose payment traffic volumes account for 97% of the total UK payments market.[12] APACS is working with a number of UK banks on a trial to implement a form of two-factor authentication known as 'remote card authentication'. Using this form of authentication, account holders seeking to use Internet banking services must first swipe their card through a hand-held reader provided by their bank, and then enter their PIN. Once the bank has confirmed the PIN is correct, the account holder is provided with a dynamically generated passcode which they then use to log in. It is expected the trial will commence at some stage in 2007.[13]

[5] Woodhead B, *Stronger security for Commonwealth's retail users*, Australian IT, 27 March 2007, <http://australianit.news.com.au/articles/0,7204,21449009^15318^^nbv^,00.html>.

[6] National Australia Bank, *SMS payment security*, <http://www.nab.com.au/Personal_Finance/0,,82833,00.html>.

[7] Bendigo Bank, *Bendigo e-Banking Security Tokens*, <http://www.bendigobank.com.au/public/personal/e-banking_security_tokens.asp>.

[8] Carreker, *ANZ Recognised for Internet Banking Security*, 9 March 2007, <http://www.carreker.com/main/media/press_releases/releases2007/03-09-07-ANZ-IB-Award.htm>.

[9] Westpac, *Discover a level of banking convenience you may never have thought possible...*, January 2006, <http://www.westpac.com.au/manage/pdf.nsf/1FFDBA6706FA99F0CA2572A2007C30B8/$File/Token_Instruction.pdf>.

[10] HSBC, *HSBC launches second factor authentication for retail customers*, 25 October 2005, <http://www.hsbc.com.au/information/news/051025.html>.

[11] This is explained further in the response to Question 30, Potential Responses to Phishing Attacks and other forms of Online Fraud at page 29.

[12] <http://www.apacs.org.uk/>.

[13] APACS, *Remote Card Authentication*, 2005, <http://www.apacs.org.uk/payments_industry/new_technology2.html>.

— **United States**
The Federal Financial Institutions Examination Council (FFIEC) is empowered to establish principles and standards for US financial institutions.[14] In October 2005, the FFIEC released a guidance document for financial institutions regarding authentication mechanisms necessary for the verifying the identity of customers who access online financial services. The document states that financial institutions should implement effective methods of authentication that are commensurate with the risk associated with online banking. The FFIEC states that it does not consider single-factor authentication sufficient in circumstances where transactions are high-risk,[15] which would appear to cover Internet banking transactions. US financial institutions were expected to have conformed with the requirements of the guidance documents by the end of 2006.[16]

The Federal Deposit Insurance Corporation (FDIC), an independent agency of the US federal government, has also recommended that financial institutions consider deploying two-factor authentication in response to the increased incidence of online fraud.[17]

— **Hong Kong**
In May 2005 the Hong Kong Monetary Authority, Hong Kong Police Force and Hong Kong Association of Banks jointly announced that banks would make two-factor authentication mechanisms available to customers engaging in high-risk Internet transactions.[18]

— **Singapore**
The Monetary Authority of Singapore has released risk management guidelines for financial institutions. The guidelines advocate the use of two-factor authentication as a means of combating online fraud.[19]

[14] <http://www.ffiec.gov/>.

[15] Federal Financial Institutions Examination Council, *Authentication in an Internet Banking Environment*, 2005, <http://www.ffiec.gov/pdf/authentication_guidance.pdf>, pp 4-5.

[16] Board of Governors of the Federal Reserve System, *Interagency Guidance on Authentication in an Internet Banking Environment*, October 13 2005, <http://www.federalreserve.gov/boarddocs/srletters/2005/sr0519.htm>.

[17] Federal Deposit Insurance Corporation, *Putting an End to Account-Hijacking Identity Theft*, December 14 2004, <http://www.fdic.gov/consumers/consumer/idtheftstudy/index.html>.

[18] Hong Kong Government, *Launch of Two-factor Authentication for Internet Banking*, 30 May 2005, <http://www.info.gov.hk/hkma/eng/press/2005/20050530e3.htm>.

[19] Monetary Authority of Singapore, *Technology Risk Management Guidelines for Financial Institutions*, 11 November 2002, <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN011549.pdf>.

Q6 – Is the growth in, and growing publicity given to, fraud issues having an impact on online transacting in Australia at present?

Online fraud is undoubtedly becoming an increasingly prominent form of identity theft. For example, the Anti-Phishing Working Group (APWG), a worldwide association consisting of over 2600 members (including several prominent financial institutions) received 23 610 reports of phishing attempts on the Internet during February 2007, representing an increase of more than 12 000 compared with the corresponding figure for the same month in 2006.[20] Of particular interest is that of the 16 463 unique phishing websites detected by the APWG during February 2007, over 92% of those sites attempted to falsely identify themselves as belonging to organisations in the financial services industry.[21] This emphasises the necessity for financial institutions to improve their response to the problem of online fraud being perpetrated against their customers.

APACS, the UK trade association for payments and for institutions who deliver payment services to customers, reported that in the first six months of 2006, incidences of online fraud caused the loss of 22.5 million pounds (approximately $54.5 million AUD), representing an increase of 55% compared with the corresponding period in 2005.[22]

The Australian Payments Clearing Association (APCA) has also reported that there were 37 952 incidents of card-not-present fraud (which includes online fraud) perpetrated in Australia on Australian-issued cards during the period from July 2005 to June 2006, with a total value of over eleven million Australian dollars. There were also over 38 000 incidents of card-not-present fraud relating to cards issued outside of Australia with a total value of over ten million Australian dollars.[23] Given the growing incidence of phishing attacks worldwide, it is realistic to expect these already significant figures will continue to rise at a rapid rate. If more is not done by financial institutions to control the growth of online fraud, this will undoubtedly affect the confidence of their customers in using the online channel to perform banking transactions and hence the continued viability of online banking generally.[24]

The fragile nature of consumer confidence in Internet banking and electronic payment systems in Australia appears to be resulting in some financial institutions using phrases such as ‘we guarantee the security of your money’ on Internet banking sites. However, such a claim is usually accompanied by a considerable degree of fine print.

A small selection of ‘guarantees’ are included in the following table:

Institution	Claim
CBA	**The Commonwealth Bank’s Security Guarantee** The Commonwealth Bank’s Security Guarantee guarantees the safety of your money as long as you keep to the NetBank terms and conditions.

[20] Anti-Phishing Working Group, *Phishing Activity Trends Report*, February 2007, <http://www.antiphishing.org/reports/apwg_report_february_2007.pdf>, page 2.

[21] Anti-Phishing Working Group, *Phishing Activity Trends Report*, February 2007, <http://www.antiphishing.org/reports/apwg_report_february_2007.pdf>, page 4.

[22] APACS, *Latest figures show UK card fraud losses continue to decline in first six months of 2006*, 2006, <http://www.apacs.org.uk/media_centre/press/06_07_11.html>.

[23] Australian Payments Clearing Association, *Credit and Charge Card Fraud*, 2006, <http://www.apca.com.au/Public/apca01_live.nsf/WebPageDisplay/FraudStats_2006A_CreditAndChargeCards>.

[24] Tubin G, *The Sky Is Falling: The Need for Stronger Consumer Online Banking Authentication*, TowerGroup, April 2005, <http://www.bnet.com/>, page 3.

Institution	Claim
Westpac	**Our Security Guarantee** Subject to investigation, we guarantee that you will not be personally liable for any unauthorised transactions on your Westpac accounts, provided that you: Were in no way responsible for the unauthorised transaction Did not contribute to the loss Complied with the Westpac Internet Banking terms and conditions
ANZ	**Our guarantee to ANZ Internet Banking customers** When you do your banking with ANZ Internet Banking, we have security measures in place designed to protect your transactions. You will be protected against unauthorised transactions carried out on your account as a result of using ANZ Internet Banking where you have complied with the Electronic Banking Conditions of Use and it is clear that you have not contributed to the loss.
St George	**Our guarantee: St. George Secure** In the unlikely event that an unauthorised transaction does occur on your account, we will refund the full amount. Read more about our commitment to you. (This link then leads to further qualifications but they don't appear on the home page)

The lesson from the use of these 'guarantees' in Internet banking promotional literature is that financial institutions need to convince consumers that they can use Internet banking with confidence. Reliance on these guarantees is conditional on the underlying terms and conditions and subsequently on the standards imposed by the EFT Code.

Q7 – What information can you provide to the Working Group about the online fraud mitigation skills of Australian online users?

There does not appear to be any data readily available on this issue in Australia. Fraud mitigation skills are likely to be extremely low in the general population due to the complex and sophisticated nature of both Internet fraud and suggested remedies. There may also be large pockets of the community where general awareness levels in relation to fraud are very low.

4. Regulatory Developments

Q8 – Are there developments in the regulatory environment that the Review Working Group should particularly consider? What are the implications of those developments for the EFT Code?

Although there has not been time to consider this question in detail, there are several regulatory developments that may be relevant:

— Review of privacy legislation by the Australian Law Reform Commission.

— Productivity Commission review of Australia's Consumer Policy Framework.

Both reviews have a focus on the simplification and harmonisation of regulation in Australia.

5. EFT Code, Part A (Scope and Interpretation)

Q9 – Do you have any suggestions as to how the scope of Part A of the Code might be defined more simply? Should Part A include a non-exhaustive list of the main types of transactions to which it applies?

The definition of scope in Part A appears to remain sufficiently broad enough to cover all target transactions. However, the drafting might be improved if the entire scope was described in Clause 1.1 without any need to refer to later provisions (e.g. 1.3 and 1.4).

Also, Clause 1.1 (B) appears to include a substantive regulatory requirement rather than a statement of scope – in that it requires financial institutions to be responsible for the actions of some third party providers. This Clause has always appeared out of place in a scope section.

A further issue relates to the definitions of some terms. These may need to be reviewed to ensure technology neutrality is maintained. One issue here is that modern access methods now include two-factor authentication approaches resulting in a plethora of new devices – smart cards, one-time password generators, mobile phones, USB tokens – all of which might play a role in providing access.

As a result, some of the definitions (e.g. 'device' and 'electronic equipment') may need to be reviewed for technology neutrality. Some initial observations show the complexity of these definitions in practice:

— A mobile phone is currently defined as both a device and electronic equipment.

— The definition of code means that it must be known to the user, but modern codes (e.g. one-time passwords) are generated by devices and only 'known' to the consumer for a short period.

It may be useful to conduct a thorough Technology Neutrality Review of the definitions in the Code once other clauses are agreed in the Review process.

Q10 – Should biller accounts continue to be excluded or should cl 1.4 be modified or, alternatively, removed altogether?

The reasons for the current exclusion of Biller accounts are unclear. It is preferable to have the coverage of the Code be as broad and simple as possible and the biller exemption has already caused some confusion. Biller accounts are growing in popularity and the exclusion should be removed to ensure that all EFT transactions receive equal treatment.

Q11 – Do small businesses experience problems in relation to their banking services that need to be addressed? Does the EFT Code provide an appropriate framework for addressing any problems identified?

It is essential that in this Review of the EFT Code the distinction between consumer and business transactions in the Code should be removed. This issue was the source of considerable debate during the last Review and it is arguable that the convergence of consumer and business banking has only increased since then. It is now very difficult to distinguish between consumer and business transactions.

There are no policy reasons for not including businesses in a Code that addresses mainly technical issues. Some arguments are presented in the Consultation paper, but they each have clear weaknesses:

— **Argument 1: Small businesses must be given incentives to maintain and improve their systems**
This argument implies that small business must be exposed to losing money via Internet banking fraud as a lesson in security management. In fact, financial institutions receive significant benefits from small businesses migrating to Internet banking from more expensive branch banking, and exposure to losses from fraud provides no incentive at all to improve the security of small business computer systems as they are in a weaker position than financial institutions when it comes to preventative measures.

— **Argument 2: The volume and value of business transactions may expose financial institutions to higher average losses**
This argument fails to recognise that average losses are in direct proportion to daily transaction limits and are not a reflection of the liability provisions. Although overall volume may be higher, income from business banking is also very high and the benefits to financial institutions of attracting more businesses to use Internet banking should still significantly outweigh the risks of including businesses in the EFT Code.

— **Argument 3: Subscribers may demand a reduction in the overall level of protection to the detriment of consumer stakeholders.**
Relief of the confusion over the distinction between consumer and business banking will benefit all stakeholders, including financial institutions, and this benefit is likely to outweigh any perceived detriments from this change. The threat to one group of stakeholders (consumers) appears hollow in this context.

It is also interesting to consider the terms and conditions currently provided by financial institutions. Typically, they are divided into Code compliant and non-compliant sections depending on the ‘business’ nature of the transaction. The non-compliant provisions can be harsher than the compliant provisions – particularly in relation to liability and dispute resolution.

Current terms and conditions also have specific and sometimes peculiar differences between liability for business customers and non-business customers. For example, one bank makes business consumers liable if they use part of their Driver Licence Number as their passcode, but they apply the EFT Code tests (name and birth date) to personal customers. However, a driver’s licence has no particular relevance to a business transaction. It is clear that financial institutions simply extend harsher terms to those customers not protected by the EFT Code, without any reference to the ‘business’ nature of the transaction.

Finally, dispute resolution is very complex if a business transaction is involved (or alleged). It will be simpler for all parties if this unhelpful distinction is removed and all EFT disputes are resolved according to the same rules and procedures.

6. EFT Code, Part A (Requirements)

Q12 – Should the requirement in cl 3.1 to provide written notification in advance of an increase in a fee or charge be replaced by another process? For example, should the notice appear in the national or local media on the day on which the increase starts?

There is no evidence that national media notices are an effective form of disclosure. Newspaper circulation in Australia is not keeping pace with population growth and English-language newspapers do not reach a large proportion of the population. Financial institutions are unlikely to use broadcast media to provide notice of increased bank fees, especially as their argument against the current notice requirement is essentially based on costs.

In practice, EFT Code notices are supplied as part of existing communication with customers (e.g. bank statements) and do not represent an additional burden on institutions.

Q13 – Should cl 4.1(a) be revised to allow users to 'opt-in' to receive a receipt?

Consumers are likely to accept that this is an area where the EFT Code can be made more flexible to reflect the practical realities facing financial institutions across a growing number of delivery channels. The opt-in model proposed in the consultation paper appears suitable.

Q14 – Should cl 4.1(a) be revised to deal with the problem of ATMs or other machines running out of paper for receipts? If so, how should it be amended?

Consumers are likely to accept that this is an area where the EFT Code can be made more flexible to reflect the current practices of ATM operators. The revision of Clause 4.1(a) proposed in the consultation paper appears suitable.

Q15 – Should cl 4.1(b)(v) be changed to allow a receipt for an EFT transaction by voice communication to specify the merchant identification number instead of the name of the merchant to whom the payment was made?

Consumers are likely to accept that this is an area where the EFT Code can be made more flexible to reflect the practical difficulties posed by telephone / voice systems. The revision of Clause 4.1(b)(v) proposed in the consultation paper appears suitable.

Q16 – Should the EFT Code give more guidance on cl 4.1(a)(viii) regarding balance disclosure on receipts? If so, what guidance should be added?

Further guidance on balance disclosures is not a priority. This does not appear to be a significant issue and perhaps resources could be directed at higher priority issues.

Q17 – Is there duplication or inconsistency between Part A of the EFT Code and the requirements of the Corporations Act that should be reviewed? How should any such issues be dealt with?

If the Code was inconsistent with legal requirements this would be cause for concern. However, no significant inconsistencies have been identified. Minor overlaps and duplication between codes and law are common and are not a significant issue. This does not appear to be a significant issue and perhaps resources could be directed at higher priority issues.

Q18 – Are there aspects of the product disclosure regime under the Corporations Act that should be adopted as part of the regulatory framework under Part A of the EFT Code?

It would be inappropriate to extend the Corporations Act approach to ***risk*** to include the security risks posed by EFT systems. A significant body of law is emerging to assist in the interpretation of risks that must be disclosed under the Corporations Act. The security risks posed by EFT systems would appear to be in an entirely different category. It may be more efficient to find another mechanism – elsewhere in the EFT Code – to discuss security risks, without raising any potential confusion with the term 'risk' under the Corporations Act.

Q19 – Should cl 7 be revised to specifically require subscribing institutions to identify and correct discrepancies between amounts recorded on the user's electronic equipment or access method as transferred, and amounts recorded by the institution as received? What are your views on the suggested redrafting?

The use of the word 'deposit' in this Clause does appear to limit the effectiveness of the Clause. The revision of Clause 7 proposed in the consultation paper appears suitable.

The more substantial issue is whether financial institutions should also be obliged to identify the source of the error and to correct it. Most consumers probably already believe that institutions are obliged to carry out this basic task and the EFT Code should reflect this.

Q20 – Should the EFT Code include a definition of the term 'complaint' under cl 10? If so, should it adopt the definition in AS ISO 10002–2006? Does the standard sufficiently address uncertainty about what is a complaint for the purposes of the EFT Code? Are there any other steps that might be taken to assist stakeholders to understand what is meant by a complaint under the Code?

Consumer stakeholders support the broadening of the definition of the term 'complaint'. The parties to this submission have read and endorse the recommendations on this issue contained in the *Consumer Caseworker Submission*.

Q21 – Should AS ISO 10002—2006 become the required standard for internal complaint handling under the EFT Code?

The parties to this submission have read and endorse the recommendations on this issue contained in the *Consumer Caseworker Submission*.

Q22 – Should account institutions be given a brief period within which to investigate a complaint before they must give the complainant written advice on how they investigate and handle complaints (as required under cl 10.3)? If so, what is an appropriate period?

Consumer stakeholders prefer complaint information to be provided immediately. If a brief period is to be allowed for internal consideration it should be restricted to a maximum of one day. The parties to this submission have read and endorse the recommendations on this issue contained in the *Consumer Caseworker Submission*.

Q23 – Should any changes be made to the timeframe for resolving complaints under cl 10 of the EFT Code?

Consumer stakeholders would like to see financial hardship taken into consideration in the application of complaints timeframes. The parties to this submission have read and endorse the recommendations on this issue contained in the *Consumer Caseworker Submission*.

Q24 – Do you have information or views about the level of compliance with cl 10?

Although no additional quantitative data is available, consumer stakeholders are concerned that case studies indicate problems with compliance. The parties to this submission have read and endorse the recommendations on this issue contained in the *Consumer Caseworker Submission*.

Q25 – Has the procedure in cl 10.12 been an effective incentive to compliance? Are further incentives required, and if so what form should they take?

There is no evidence that Clause 10.12 has been used. The parties to this submission have read and endorse the recommendations on this issue contained in the *Consumer Caseworker Submission*.

Q26 – Should the EFT Code be amended to cover situations when the subscribing institution is unable to, or fails to, give the dispute resolution body a copy of the record within a certain time? If yes, should the Code specify that a dispute resolution body is entitled to resolve a factual issue to which a record relates on the basis of the evidence available to it?

Case studies have revealed some significant issues with record keeping by financial institutions. The parties to this submission have read and endorse the recommendations on this issue contained in the *Consumer Caseworker Submission*.

Q27 – Should there be a time after which EFT Code subscribers are no longer required to resolve complaints about EFT transactions on the basis set out in Part A of the Code?

Consumer stakeholders accept that some limitation period should apply. However, it is important that the period only begins when the consumer becomes aware of the breach, and that financial institutions do not unfairly rely on limitation periods to discourage legitimate complaints. For further details please refer to the *Consumer Caseworker Submission*.

7. EFT Code, Part A (Liability)

Q28 – Should account holders be exposed to any additional liability under cl 5 for unauthorised transaction losses resulting from malicious software attacks on their electronic equipment if their equipment does not meet minimum security requirements? Do the benefits and costs of extending account holder liability justify such an extension of cl 5? What implementation issues would have to be addressed?

This is a vital issue to be addressed in the Review. Consumers will be seriously disadvantaged if they are required to accept any additional liability resulting from malicious software attacks and/or failure to adequately secure their computer.

Some financial institutions appear to support (either through submissions to the Review or in terms and conditions) an increase in consumer liability where there is malicious software on their computer. In the absence of clear direction from the EFT Code, terms and conditions are likely to be extremely harsh for consumers. For example, one bank (Westpac) has already included a Spyware Clause in their terms and conditions:

> If you knowingly use a computer that contains software, such as Spyware, that has the ability to compromise access codes and/or customer information, you will be infringing our rules for access code security referred to above and we will not be liable for *any* losses that you may suffer as a result [emphasis added].

Enforcing such a Clause would be difficult, but its presence may be a deterrent to a consumer with a legitimate EFT complaint, if for example they believe their complaint may result in an intrusive investigation into the contents of their personal computer.

It is also difficult to envisage circumstances in which account holders have displayed such a degree of carelessness in ensuring their computer meets minimum security requirements that liability should be imposed upon them for any resultant financial loss from a malicious software attack.

In addition, the task of defining acceptable 'minimum security requirements' is problematic due to a number of practical issues:

— Internet malware is a moving target. Security risks and technical attack vectors change. It is unreasonable to expect that end-users are aware of these risks and attacks, or that they are capable of monitoring and responding to changes. Financial institutions on the other hand have specialised security resources and processes that are dedicated to addressing these risks.

— Consumers access online financial services from a wide variety of computing platforms. These range from mobile devices and the latest desktop operating systems through to legacy systems such as Windows 98. Legacy platforms typically do not support many of the security software tools that provide some protection against the current generation of malware. It may be unreasonable to exclude customers with legacy platforms from access to online financial services. The cost of software and hardware upgrades to an acceptable platform will be prohibitive to some end-users.

— The number and variety of end-user security tools is constantly changing. These tools include browser chrome security enhancements, email filtering software, software-based firewalls, virus scanners and spyware detectors. Software vendors are required to release new versions to address new security threats and to meet their business objectives. It is unrealistic to expect that all end-users will be able to identify the correct combination of tools and versions that must be installed. Moreover, software tools that attempt to combat malware are usually unable to detect the very latest forms since the updates to such software typically lag behind the development of new forms of malware.

— The cost of installing, configuring and maintaining an effective security defence will be prohibitive for some consumers.

— The effectiveness and reliability of end-user security tools is highly variable. Many of these end-user technologies rely on heuristic methods to (either directly or indirectly) detect or avoid malicious software and phishing attacks rather than more dependable techniques.[25] The effectiveness of particular software against malicious software attacks may also be affected by other variables including the operating system used and the specifications of the user's machine. It is unreasonable to expect that, in these circumstances, end-users will be able to evaluate the effectiveness of these tools. These consumer-grade tools are generally inferior to the levels of protection offered by technologies installed at the financial institution end to prevent these attacks affecting an account-holder in the first place. For example, the *State of Spyware* (Q2 2006) Report stated:[26]

> Overall spyware infection rates continue to rise for the third straight quarter. The second quarter of 2006 saw an increase in the share of consumer PCs infected with spyware: from 87 percent in Q1 2006 to 89 percent. This increase in spyware infections suggests that although home computer users are adopting anti-spyware programs, they are choosing inadequate programs to protect their computers or not keeping their programs up-to-date. Before installing an anti-spyware program, home computer users should evaluate the program's ability to detect and remove all types of spyware, especially malicious programs.

— Account holders, even if they have some computer experience, will often have difficulty interpreting messages that the software may display to them regarding the probability they are being subjected to a malicious software attack.

— Microsoft Windows is the predominant end-user platform. Windows is the target of the overwhelming majority of malware released in the wild. This malware continues to exploit critical security flaws. In some cases security fixes are released weeks or months after the vulnerability is found. End-users may conscientiously patch their operating system, but they are dependent on Microsoft to release timely patches.

[25] This is discussed further in the response to Question 30, General weaknesses of client-end website authentication solutions at page 32.

[26] Webroot Software, Inc, *State of Spyware Q2 2006, A Review and Analysis of the Impact of Spyware on Consumers and Corporations*, 2006.

- The effectiveness of software that needs to be installed by account holders on their own machines is dependent on their computing knowledge and motivation to ensure that the software is successfully installed and continually updated. Clearly computing knowledge and motivation would vary amongst account holders. For example, users who only access online banking services on a monthly basis may be less inclined to ensure relevant software is updated regularly than users who access their accounts online on a daily basis.

- Installing software at the user-end would prove particularly impractical in situations where users need to access Internet banking services from public machines or networks (for example, in Internet cafes). It is naive to expect that these machines and networks are protected against malicious software attacks. Financial institutions have promoted the flexibility of Internet banking and the entire system relies on consumers being able to access their accounts from public Internet facilities such as libraries and Internet cafes.

- It is unreasonable to expect that security tools will be installed correctly and optimised to meet the specific threats that affect the financial services industry.

- It may be prohibitively expensive for the financial services industry to maintain an agreed list of technologies, configurations and threats that comprise the ‘minimum security requirement’. It will also be very difficult to effectively communicate that list to consumers, especially if it changes regularly.

Given these considerations, the task of defining what constitutes ‘minimum security requirements’ for the purpose of determining when account holders are liable for financial loss flowing from malicious software attacks is particularly difficult.

It would appear more practical and economically efficient for measures to be implemented at the financial institution end since the protection afforded would then diffuse from a central point to the entire base of consumers utilising Internet banking services. Moreover, many of the developments in security in recent years would not have occurred if the security effort was more diffuse – i.e. in the hands of consumers rather than financial institutions.

Q29 – Should an additional example be included in cl 5.6(e) specifically referring to the situation when an account user acts with extreme carelessness in responding to a deceptive phishing attack?

It may be that there are certain situations in which account users have acted with a degree of carelessness to a phishing attack that is considered ‘extreme’ such that liability should be imposed upon them for any resultant financial loss. However, the notion of ‘carelessness’ should be carefully demarcated with respect to phishing attacks for a number of reasons:

- Firstly, it is important to remember that, although there is a range of authentication technologies available to end-users to assist with detecting phishing attacks, these are generally less effective than technologies that can be implemented by financial institutions.[27]

[27] This is discussed in more detail in the response to Question 30, Potential Responses to Phishing Attacks and other forms of Online Fraud at page 29.

— Secondly, financial institutions have been instrumental for some time in promoting the use of the online channel to their customers. Despite having the option of encouraging, or even compelling, customers to shift to the use of other channels for banking so as to avoid the problem of phishing attacks (including telephone or face-to-face banking), they have avoided doing so. In this regard it must be remembered that financial institutions reap significant benefit in the form of cost savings by encouraging their customers to perform banking transactions online.

— Thirdly, if the financial services community does not know why consumers repeatedly respond to phishing attacks, then it is pointless and unfair to impose liability on them for responding more than once. If consumers genuinely think that they are taking appropriate action, and genuinely think they are responding to a message from their institution, then making them liable in those circumstances would just seem to have the effect of discouraging them from using Internet banking. Further research on why consumers respond to attacks would help design appropriate security defences, rather than simply shifting liability to consumers.

For these reasons, employing a broad definition of 'carelessness' in Clause 5.6(e) in order to impose a greater degree of liability on bank customers in relation to losses flowing from phishing attacks is unwarranted.

Q30 – Apart from this possible clarification, should account holders be exposed to any additional liability under cl 5 for unauthorised transaction losses because of a deception-based phishing attack? Do the benefits and costs of extending account holder liability justify such an extension? What implementation issues would have to be addressed?

The current liability regime for unauthorised transactions should not be modified so as to expand the situations in which account holders will be liable for financial losses flowing from phishing attacks. Although there are measures that can be taken by banking customers in order to combat phishing attacks, for reasons that will be discussed below these are considerably less effective than the technologies that can be utilised by financial institutions to deal with phishing. Hence, it is financial institutions who should bear the primary responsibility for implementing solutions to combat forms of online fraud including deception-based phishing attacks.

Potential Responses to Phishing Attacks and other forms of Online Fraud

There are a host of potential solutions that are available to financial institutions to combat phishing and other attacks their customers may be subjected to online. These include:

— **1.** Two Factor Authentication Solutions; and

— **2.** Website Authentication Solutions which can be installed at either the server (financial institution) or client end.

Each of these types of solutions is discussed below.

Two Factor Authentication Solutions

Two-Factor authentication refers to the use of a dual-layered approach in order to verify the identity of an end-user to a server. For example, an end-user may be required to supplement a password they have memorised (something they know) with something they have (such as a hardware token that produces a random sequence of digits at pre-determined intervals) or something they are (such as a fingerprint or other biometric data). Examples of two-factor authentication technology include RSA's SecurID hardware tokens[28] and Australia Post's joint undertaking with Verisign to produce a two-factor authentication system known as VIP.[29] Both of these technologies involve the use of hardware tokens provided to customers that generate random passcodes at specified intervals of time, which can be used by the customer when logging into the Internet banking section of a financial institution's website. An alternative system adopted by some financial institutions involves sending random passcodes via SMS to an account holder's mobile phone when they attempt to log in and/or initiate a transaction.

Two-factor authentication generally represents the limits of what financial institutions in Australia are currently implementing in response to online fraud such as phishing attacks. However, the technology provides only marginally improved resistance against phishing attacks.[30]

There is, for example, a significant possibility that the passcode displayed to a bank's customer by their hardware token can be intercepted through the use of a spoofed website designed to falsely appear to belong to the customer's financial institution. The website, if a convincing spoof, could cause the customer to provide the passcode displayed on their hardware token. The fraudulent party who created the spoofed website could then immediately use the passcode to login to the customer's account as part of a replay attack (assuming they also know the customer's password and username details). An example of this has occurred recently when account holders with Dutch bank ABN Amro had money stolen from their accounts by fraudulent parties using this very method to circumvent the bank's use of two-factor authentication.[31]

Hence, there is a need for financial institutions to consider deploying some form of website authentication technology to prevent the use of spoofed websites (typically used as part of a phishing attack) undermining the security of customer's login credentials.[32] A variety of these technologies are considered below.

Website Authentication Solutions

It is important to distinguish website authentication from two-factor authentication. While two-factor authentication techniques are typically not concerned with authenticating websites to users, website authentication technologies have been specifically developed to enable Internet users to verify whether the actual identity of a website aligns with the represented identity of the website. Website authentication technologies can be installed at either the client (customer) end or server (financial institution) end.

[28] RSA Security, *Protecting Against Phishing by Implementing Strong Two-Factor Authentication*, 2004, <http://www.indevis.de/dokumente/anti_phishing_rsa.pdf>.

[29] Deare S, *Australia Post tests online identification service*, ZDNet Australia, 6 September 2006, <http://www.zdnet.com.au/news/security/soa/Australia_Post_tests_online_identification_service/0,130061744,339270865,00.htm>.

[30] There have been attempts to improve the effectiveness of two-factor authentication in dealing with online fraud. See in this regard Appendix 1 – Authentication Technologies, Attempts to Strengthen Two-factor Authentication at page 50.

[31] Out-Law.com, *Phishing attack evades ABN Amro's two-factor authentication*, 18 April 2007, <http://www.out-law.com//default.aspx?page=7967>.

[32] Financial Services Technology Consortium, *Financial Industry Recommendations and Requirements for Better Mutual Authentication*, June 12 2006, <http://fstc.org/projects/docs/Recommendations_and_Requirements_for_BMA_v1.0.pdf>, page 12.

- **Server-end website authentication solutions**
  Although several of the authentication technologies outlined in this section do require some level of user involvement, they have been listed as server-end since they are predominantly dependent on the financial institution for their effectiveness.
  - **Shared Secrets**
    A technique that is commonly put forward as a means of achieving authentication of a web server is the sharing of a secret between the server and end-user. The user may, for example, provide the server with a personal image that can then be displayed back to them whenever they wish to access the relevant website. If the wrong image is presented, the user will know that they are interacting with a spoofed website.
  - **Keypad Technology**
    Keypad technology involves presenting an end-user with an mage of a keypad containing a set of symbols that enables them to communicate their password to a web server. One advantage of this technology is that it is not susceptible to keystroke logging malware that may have been covertly installed on a customer's computer by a fraudulent third party in order to capture passwords the user enters via their keyboard. Keypad technology can also be adapted to authenticate the websites of financial institutions to customers. This makes it even more effective at dealing with phishing attacks. An example of this is provided by Tricerion's Strong Mutual Authentication keypad technology.[33]
  - **Secure Remote Password (SRP) Protocol**
    The Secure Remote Password (SRP) protocol prevents a shared secret, such as a password, from being compromised during communications between a financial institution and one of its customers by removing the need for the secret to be sent over a network at all.[34]
  - **Challenge/Response Mechanisms**
    In the context of website authentication, challenge / response mechanisms involve a client presenting a server with a challenge in order to verify the identity of the server. Using a secret previously shared between the client and server, the server calculates a response and presents it to the client. The client is able to use the response to authenticate the server.[35]
  - **Delayed Password Disclosure (DPD)**
    An extension of Secure Remote Password protocol, DPD enhances the effectiveness of SRP as a website authentication technology by stipulating the association of numerous images with a customer's internet banking password. The images are presented sequentially to a customer by the financial institution's server as they enter each character of their password during a login attempt. This process enables the customer to detect when they are dealing with a party other than the financial institution.[36]

[33] Refer to 14. Appendix 1 – Authentication Technologies, Tricerion Strong Mutual Authentication at page 50.

[34] Refer to 14. Appendix 1 – Authentication Technologies, Secure Remote Password Protocol at page 52.

[35] Refer to 14. Appendix 1 – Authentication Technologies, Challenge/Response Mechanisms at page 53.

[36] Refer to 14. Appendix 1 – Authentication Technologies, Delayed Password Disclosure at page 52.

- **Client-end website authentication solutions**
  These technologies are typically installed on the end-user (customer) machine and attempt to detect phishing attacks typically through the use of heuristic analysis techniques. Examples of such solutions include:

  - **Browser Chrome Enhancements**
    There is an emerging trend in attempting to achieve website authentication by adding to the visual cues presented to users in the area surrounding a typical browser window. This area is commonly referred to as the 'browser chrome' and a host of plug-ins can be added to the web browser chrome to assist in the process of detecting spoofed websites, one of the key elements used in a phishing attack. Examples of actual and proposed browser-chrome enhancements include Petname,[37] SpoofGuard.[38] Proposed browser-chrome enhancements include Trusted Password Windows and Dynamic Security Skins.[39]

  - **Email Detection**
    These technologies use either heuristic or collaborative methodologies to analyse emails received by an end-user and determine whether they are likely to be phishing emails. An example of this is provided by the Cloudmark Network Feedback System.[40]

General weaknesses of client-end website authentication solutions

Although, given the inadequacies of two-factor authentication, some form of website authentication is undoubtedly needed for Internet banking in order to more effectively neutralise the threat of phishing attacks, client-end solutions are a less attractive option compared with server-end solutions. One of the reasons for this is that client-end technologies such as those outlined above rely on probabilistic methodologies (such as collaboration and heuristic analysis) in order to detect phishing attacks. This is an inherently less robust fashion of detecting phishing attacks compared to many of the methodologies employed by server-end technologies.

For example, with regard to browser-chrome enhancements the W3C paper on *Limits to Anti-Phishing*[41] notes:

> Adding more trust indicators or more obvious trust indicators (to a web browser user interface) misses the point that an attacker can spoof every part of a user interface, including browser chrome and copy new trust indicators. Some proposals include new UI elements such as new anti-phishing trust icons, company logos in browser chrome, or new authentication popup windows. All of these miss the point that an attacker is capable of spoofing the entire user interface.

[37] Refer to 14. Appendix 1 – Authentication Technologies, Petname at page 55.

[38] Refer to 14. Appendix 1 – Authentication Technologies, SpoofGuard at page 56.

[39] Refer to 14. Appendix 1 – Authentication Technologies, Trusted Password Windows and Dynamic Security Skins at page 58.

[40] Refer to 14. Appendix 1 – Authentication Technologies, Cloudmark Network Feedback System at page 59.

[41] Nelson J and Jeske D, *Limits to Anti-Phishing*, W3C Workshop on Transparency and Usability of Web Authentication, 2006, <http://www.w3.org/2005/Security/usability-ws/papers/37-google>.

The Financial Services Technology Consortium (FSTC) is conducting a Better Mutual Authentication Project. Their recent publication – *Financial Industry Recommendations and Requirements for Better Mutual Authentication*[42] suggests that although modern web browsers have a fairly sophisticated array of security features, those features (particular those that can be used to authenticate websites) are often poorly integrated into the user interface, with security indicators, alerts and dialogue boxes being difficult to understand. Many end-users have difficulty understanding what the browser is telling them, while users are often provided with the option to make security warnings go away permanently.

Moreover, current web browsers allow websites to easily modify the 'browser chrome' – for example, by re-arranging, altering or even concealing certain elements within the browser window. This allows fraudulent parties to mislead users about the site they are viewing.

An additional problem of using browser chrome enhancements to achieve website authentication is evident when one considers that there may be situations in which end-users need to access the same websites from different machines, depending on their location. This means that they will need to install the enhancements on each machine, requiring a degree of effort which many users may simply refuse to invest.[43] Alternatively, different users may elect to install different browser chrome enhancements, each with their own level of effectiveness. Therefore different users accessing the same website may receive differing levels of protection against phenomena such as spoofed websites.

Q31 – To what extent has the restriction on using a user's name or birth date under cl 5.6(d), been relied on?

It does not appear that any data is available on the self selection of name or birth date as user codes. Prior to the last review of the EFT Code there were some incidents where financial institutions used birth dates as the default telephone access code. This practice no longer occurs.

Some anecdotal evidence is available on current practices:

— Self selection screens for changing access codes tend to carry suitable warning messages about the selection of weak access codes.

— A limited number of self selection processes will automatically reject weak access codes (eg sequential numbers), but these are not (yet) designed to reject name or date of birth.

— Clause 5.6 (d) has not been relied on in practice to the extent that it has come to the attention of consumer stakeholders.

— Criminal activity based on 'guessing' common passwords is likely to represent a smaller proportion of criminal activity now that most attacks rely on social engineering or deception to entice the consumer to reveal their password.

Overall, the usefulness of Clause 5.6 (d) is questionable. It never had the support of consumer stakeholders and this Clause is a candidate for removal in the interests of simplifying and shortening the Code.

[42] Financial Services Technology Consortium, *Financial Industry Recommendations and Requirements for Better Mutual Authentication*, 12 June 2006, <http://fstc.org/projects/docs/Recommendations_and_Requirements_for_BMA_v1.0.pdf>.

[43] Fraser N, *The Usability of Picture Passwords*, Tricerion, 2006, http://www.tricerion.com/downloads/Usability-of-picture-passwords.pdf, page 2.

Q32 – Should the restriction on users acting 'with extreme carelessness in failing to protect the security of all the codes' under cl 5.6(e) be further elaborated or extended in some way? Should additional examples of extreme carelessness be given?

The term 'extreme carelessness' was considered necessary in the last Code Review because the drafters could not possibly anticipate all of the potential attacks and vulnerabilities in relation to access codes. It is a useful catch-all term that allows other parts of the Code to remain technology neutral. The Clause has overall merit and should be retained.

Reliance on this Clause is limited in practice.

The addition of examples, however, is more problematic. Typically, the example scenarios need to be debated amongst stakeholders to ensure there is common agreement about when liability might shift due to extreme carelessness. Great care is required in the drafting of such examples.

A suggested approach to improving Clause 5.6 (e) is:

- Retain the 'extreme carelessness' term in Clause 5.6 (e);
- Consider extending the scope of the Clause to include protecting the security of devices in line with the proposed Technology Neutrality Review; and
- Remove or limit the examples provided to scenarios which have clear agreement amongst stakeholders (this is a task for the Working Group).

Q33 – Should the EFT Code specifically address the situation when an unauthorised transaction occurs after a user inadvertently leaves their card in an ATM machine?

There do not appear to be any advantages in codifying this approach. Perhaps, in the interests of simplifying and shortening the Code, this could be provided as an example scenario in notes rather than including it as a specific Clause in the Code.

Q34 – To what extent is unreasonable delay in notification of security breaches by account users currently an issue? Please provide on the frequency and cost of such delays, if possible. (You may wish to provide this information on a confidential basis.)

Consumer stakeholders are not in a position to provide new data on this issue. There is some concern that increased charges by financial institutions for replacement cards / tokens may act as a disincentive for low income and disadvantaged consumers to report security breaches quickly. Consumers spend further time searching for missing cards / tokens in order to avoid replacement fees. Financial institutions should be discouraged from introducing / increasing these replacement charges if they wish to also rely on the 'unreasonable delay' provisions in the Code. The final paragraph of Clause 5.5 is relevant here, but there is no available data on its use.

Q35 – Should the circumstances when the account holder is liable on the basis of unreasonably delayed notification under cl 5.5(b) be extended to encompass unreasonable delay in notifying online security breaches of which the user becomes aware?

Unreasonable delay is an important test of liability in the Code and should be extended to cover all relevant circumstances. The test, however, should remain focussed on when the user becomes ***aware*** of a breach.

Clause 5.5 (b) could be improved by the addition of a third Sub-Clause to cover circumstances where another form of security breach has resulted in an unauthorised transaction, and the consumer has become aware of the resulting unauthorised transaction.

Care needs to be taken to ensure that the user does not have to report potential security breaches that have not lead to an unauthorised transaction outside the limited circumstances covered in Sub-Clause (a) and Sub-Clause (b). The example scenario provided in the ASIC Consultation paper is too broad because consumers will regularly provide basic identifier information (e.g. card number and expiry), but they cannot be expected to be aware of a security breach in such circumstances until an unauthorised transaction occurs.

Q36 – Should the standard of 'unreasonably delaying notification' under cl 5.5(b) be replaced by a specific time after which the account holder is liable? What would be an appropriate time, if such a change were introduced?

This issue appears to be adequately addressed in Guidelines issued by external dispute resolution providers, such as the Banking and Financial Services Ombudsman.[44] As it has been the subject of considerable debate and guidance at that level, it may be difficult to remove the current test and replace it with a specific timeline.

Q37 – To what extent do subscribing institutions currently use the other 'no fault' liability provision in cl 5.5(c)?

Consumer stakeholders do not have additional data available on this question.

Q38 – Is there a case for increasing the current 'no fault' amount of $150? If so, on what basis and what should the new amount be?

Consumer stakeholders oppose any further change to the no fault liability regime in this Review of the Code. The last Review resulted in an enormous increase in the amount of the no-fault payment from $50 to $150 despite the objections of consumer stakeholders. This increase occurred despite continued record profits for financial institutions and record growth in fee income.

[44] Banking and Financial Services Ombudsman, *Policies and Procedures Manual*, <http://www.bfso.org.au/abioweb/ABIOWebSite.nsf/Level2Docs/C260E55223CF6FFACA256C23001D15F1/$File/Policies&Procedures_Manual_061219.pdf?OpenElement>.

The fee should not be used as a negotiating instrument in each Review of the EFT Code. It is a regressive fee that has a disproportionate impact on low income and disadvantaged consumers. Financial institutions and their representatives can sometimes be disconnected with the financial position of low income consumers. It may be necessary to remind all stakeholders that $150 is more then the weekly payment for Youth Allowance, ABSTUDY and Rent Assistance and is close to the average weekly payment for most pensioners and job-seekers.

The other provisions in the EFT Code need to stand on their own merits and the current $150 no-fault payment should be maintained or reduced. It is already a significant payment in circumstances where the consumer may not be at fault, and it already acts as a strong incentive for improving consumer behaviour.

Q39 – Should subscribers prohibit in their merchant agreements the practice of taking customers' PINs or other access codes as part of a 'book up' arrangement? If so, should this be subject to any exceptions; and, if it should, what should those exceptions be?

Consumer stakeholders support amending the EFT Code in a way that will prohibit the use of book-up except in exceptional circumstances.

However, book-up is a complex issue and the exact drafting of such a provision would require detailed consultation with relevant stakeholders (indigenous representatives, disability advocate groups etc.). This issue may need to be considered by a sub-committee of the Working Group or other relevant experts.

Q40 – Should cl 6 be reformulated to clarify that the subscribing institution is liable for any failure resulting from equipment malfunction when they have agreed to accept instructions through that equipment?

Clause 6 already appears to clearly cover the situation where institutions are relying on equipment acting on their behalf. The clarification proposed in the ASIC Consultation paper appears unnecessary.

Q41 – To what extent, and how, should the Code address the issue of mistaken payments? Discuss the usefulness, practicality and cost of implementing some or all of the measures outlined, as well as any other measures you consider appropriate.

Consumer stakeholders are concerned at the ease with which mistaken payments can occur in Internet banking and the difficulties subsequently faced by consumers when they do occur. The onus is on financial institutions to ensure that their Internet banking systems are able to minimise opportunities for basic errors.

Other systems, such as BPay, Paypal, Direct Debits etc all have built in mechanisms to minimise mistakes and provide confirmation of the transaction to the consumer.

It appears that financial institutions are working on upgrading systems so that mistakes can be reduced. However, this may take some time. In the intervening period consumer should not be exposed to increased liability and /or difficulties in correcting mistakes.

Current terms and conditions are particularly harsh in relation to mistaken payments. For example, some banks will not even reverse mistaken transactions when both accounts are with the *same* bank. The Westpac terms state:

> Westpac cannot reverse transactions you make in error, either to Westpac or non-Westpac accounts. Should an amount sent by you in error not be returned automatically by the receiving financial institution, it may not be recoverable at all.

Consumer stakeholders support an eventual resolution of this issue to be based on a technical solution. This might involve the matching/checking of account names against account numbers, double entry of key data, and/or the widespread use of receipts and confirmation notices that include the name of the funds recipient.

In the interim, consumer stakeholders would be willing to consider the inclusion of the Banking and Financial Services Ombudsman approach to liability in the Code. This would require a Clause allocating liability to the account institution if funds are transferred to an account that does not match the account name entered by the consumer, irrespective of the account number entered. The position of the financial institutions might be assisted by the introduction of a chargeback regime for mistaken payments. Some improvements in dispute resolution in relation to mistaken payments may also be required.

In addition, the parties to this submission have read and endorse the recommendations on this issue contained in the *Consumer Caseworker Submission*. In particular their comments below:

> Mistaken payments occur due to the Internet banking interface. The means for providing a safe interface system entirely lies with the code member, and by not having the best practice methods in place consumers are at risk of transferring funds incorrectly. Currently, unless the institution makes the mistake themselves the consumer will not be reimbursed unless the member's hand is forced by the Banking and Financial Services Ombudsman. Clearly a more effective system is to discover any issues with the payment at the bank's level, before the transfer takes place.

8. EFT Code, Part B (Scope and interpretation)

Q42 – Should the scope of Part B of the EFT Code continue to be defined by reference to the concepts of 'stored value facilities' and 'stored value transactions' as at present; or should a different approach be taken? What issues are raised by possible alternative approaches?

This may be a good opportunity to try a completely new approach for stored value products. In the interest of shortening and simplifying the Code and its core consumer protections for EFT facilities, consumer stakeholders are willing to consider removing Part B from the Code and re-publishing it as separate better practice guidance, to be used by industry on a purely voluntary basis.

It appears that stored value product providers are unlikely to subscribe to the EFT Code. This may be because the Code is not sufficiently focused on stored value products and its core brand remains linked to EFT.

At some time in the future, if stored value products become widespread, Part B could be used as the basis for a more specific Code of Conduct for stored value products, not linked to the EFT Code.

There appears to be little risk in this approach. The benefits to the other parts of the Code will be significant.

Q43 – Assuming the scope of Part B of the EFT Code continues to be defined in terms of the concepts of 'stored value facilities' and 'stored value transactions', what changes, if any, should be made to the definitions and other provisions of cl 11?

Consumer stakeholders would prefer to see Part B removed from the Code.

9. EFT Code, Part B (Obligations)

Q44 – Should any changes or additions be made to cl 14?

Consumer stakeholders would prefer to see Part B removed from the Code.

Q45 – Should operators of facilities regulated under Part B be required to make a transaction history for the facility available on request for a specified period?

Consumer stakeholders would prefer to see Part B removed from the Code.

Q46 – Are any aspects of Part B of the EFT Code incompatible with the requirements of the Corporations Act? How should any incompatibility be addressed?

Consumer stakeholders would prefer to see Part B removed from the Code.

Q47 – Should the rights to exchange stored value under cl 15 be narrowed?

Consumer stakeholders would prefer to see Part B removed from the Code.

Q48 – Should the EFT Code include a requirement that all prepaid facilities regulated by Part B must have a minimum use time (i.e. the time before value expires) of at least 12 months?

Consumer stakeholders would prefer to see Part B removed from the Code.

Q49 – Should the EFT Code include a requirement that the use period or date be displayed on any physical device (such as a card) used to make payments in connection with a prepaid facility?

Consumer stakeholders would prefer to see Part B removed from the Code.

Q50 – Should the right to a refund of lost or stolen stored value under cl 16 only be mandated for facilities that allow more than a certain amount of value to be prepaid? If so, what should the minimum amount be?

Consumer stakeholders would prefer to see Part B removed from the Code.

Q51 – Should there be a requirement that regulated facilities over a certain value include a mechanism (such as PIN security) that allows users to control access to the available value on the facility?

Consumer stakeholders would prefer to see Part B removed from the Code.

Q52 – Should the use of unilateral variation clauses in the terms and conditions for facilities regulated under Part B be restricted?

Consumer stakeholders would prefer to see Part B removed from the Code.

Q53 – Should the complaint investigation and dispute resolution regime under cl 10 of the EFT Code apply without limitation to Part B facilities and transactions under cl 19?

Consumer stakeholders would prefer to see Part B removed from the Code.

Q54 – Should Part B of the EFT Code address the issue of payment finality?

Consumer stakeholders would prefer to see Part B removed from the Code.

10. EFT Code, Part C (Privacy and electronic communications)

Q55 – Should the provisions about privacy under cl 21 be modified and/or extended to cover other areas or issues?

Consumer stakeholders support the continued inclusion of privacy provisions in the EFT Code. Generic privacy legislation in Australia remains weak and subject to numerous exemptions. Privacy complaints mechanisms are also slower and more cumbersome than external dispute resolution options available in the financial services sector.

This Review presents an opportunity to strengthen, clarify and simplify the privacy provisions in the Code.

Q56 – Should the status of the cl 21.2 guidelines be changed to make these provisions contractually binding requirements?

Consumer stakeholders believe that some of the privacy guidelines in the current Code should be revised and implemented as contractually binding requirements. It is confusing and inconsistent for some provisions of the Code to be binding and for others to be mere guidance. This Review is an opportunity to clarify this situation.

The binding privacy clauses should be:

- **Clause 21.2 (a) Surveillance**
  This Clause ensures that where a person calls a customer care hotline they are warned before the call is recorded. Similarly, ATMs using video surveillance must carry a notice to that effect. It is unlikely the same level of certainty could be achieved by relying on the vague National Privacy Principles (NPPs) in the Privacy Act; and

- **Clause 21.2 (c) Transaction receipts**
  This Clause ensures that key personal information is not disclosed when receipts are misplaced. It is uncertain whether the NPPs could be relied upon to achieve this result as the information is initially disclosed to the consumer, and the NPPs are designed to cover third party disclosure. However, it is clear that receipts do represent a significant security risk as they are easily forgotten at the counter or misplaced.

The two other clauses (Clause 21.2 (b) Authorisation and Clause 21.2 (d) Privacy Policies) could be safely removed from the Code. These appear to be adequately covered by the NPPs and industry practice.

Q57 – Should the EFT Code require that transaction receipts include only a truncated version of the account number?

It may be easier in this case to relay on a negative test rather than a positive requirement. If the Clause is amended to become a binding contractual requirement that the receipt should not reveal the customer's full name or account number, this will allow financial institutions to meet the requirement in a number of flexible, innovative ways.

The positive requirement (truncation) suggested in the ASIC Consultation paper may be too technology specific. The current Clause should be retained (as a binding contractual requirement).

Q58 – Should the EFT Code require that transaction receipts not include the expiry date and/or other information that is not required for transaction confirmation purposes?

If the Clause is amended to become a binding contractual requirement that the receipt should not reveal the customer's full name or account number this will allow financial institutions to meet the requirement in a number of flexible, innovative ways. In the absence of a full name or account number, other information (e.g. expiry date) should not present any risk.

The specific requirement not to include an expiry date or other information 'not required' suggested in the ASIC Consultation paper may be too technology specific. The current Clause should be retained (as a binding contractual requirement).

Q59 – What would be the cost of implementing the suggested changes? Are there any implementation issues that should be considered? What would be an appropriate implementation timeframe?

This is a question for financial institutions to address.

Q60 – Should cl 22.1(b)(ii) be deleted or amended in some way?

In the interest of improved security, Clause 22.1(b) (ii) should be removed.

Q61 – Should cl 22.2(b)(ii) be deleted or amended in some way?

In the interest of simplifying the Code and providing certainty to subscribers, Clause 22.2(b)(ii) should be removed.

Q62 – Should changes be made to the EFT Code to address issues associated with products that only allow electronic communication of account information? If so, what changes should be made?

Many EFT products are entering the market which are based entirely on electronic communications. The EFT Code does not appear to present an impediment to such products – there is only one requirement for paper records to be supplied (Clause 22.3) and it will only apply in exceptional circumstances. All organisations already have the capacity to provide paper records in exceptional circumstances (e.g. litigation).

The ASIC Consultation paper asks whether the EFT Code should include further provisions on disclosure for products based solely on electronic communication. For example, it suggests increased disclosure on the implications of relying solely on electronic communication. However, in 2007 these implications are well understood and are likely to be accepted by customers selecting such products. For consumers switching from paper communication to electronic communication in existing products Clause 22 already provides sufficient disclosure.

This is not a high priority issue for the Code. In the interests of simplifying and shortening the Code no additional disclosure requirements should apply to products that rely solely on electronic communication.

Q63 – Should the EFT Code address the situation when an account institution receives a mail delivery failure message after sending a communication mandated under cl 22? If so, what approach should be adopted? How is this situation currently handled?

This is a question for financial institutions to address.

11. EFT Code, Part C (Administration and review)

Q64 – Should ASIC continue to be primarily responsible for administering the EFT Code? Are there other arrangements that should be considered?

ASIC should retain primary responsibility for the Code as it is important to retain industry independence. As the Code is a functional Code, ASIC remains the only suitable regulator for this role.

Q65 – Should the EFT Code allow its requirements to be modified in certain circumstances? If so, what modification powers should be included and how should they be administered?

A general modification power should be retained in order to manage any necessary changes during the long periods between reviews. The current modification powers are very specific and are unlikely to be useful. A carefully drafted general power that included requirements for stakeholder consultation and procedural fairness would be more appropriate. It is unlikely to be widely used.

Q66 – How should compliance be monitored? What alternatives to the current self-reporting survey should be considered?

Consumer stakeholders are sceptical about the usefulness of the self-reporting survey and annual report. This submission refers to, and agrees with the comments made in the *Consumer Caseworker Submission* in relation to the survey and report. However, there are other priorities for consumers in this review, and resources should be first be devoted to these issues. Hopefully the survey will be shorter and simpler following the proposed shortening and simplification of the Code in this Review.

The problems with current data collection are noted. This is chiefly an issue for financial institutions to resolve. However, consumer stakeholders note that improvements in data collection on complaints should be a higher priority than other areas of data collection.

Consumer stakeholders would be interested in discussing some form of independent monitoring, with perhaps reference to the experience with the Code Compliance Monitoring Committee of the Code of Banking Practice. In lieu of reviewing the compliance and monitoring provisions in detail at this time, a one-off independent evaluation of compliance (e.g. a one-off shadow shopping exercise) would be very helpful. This would provide invaluable information for the ongoing governance of the Code and for the next Code Review.

Q67 – How should the EFT Code be reviewed? What alternatives to the current approach should be considered?

There is support for the current Review process, but consumer resources and time are limited. The EFT Code is a complex piece of regulation in a sector that changes rapidly. Participating in the Code Review process requires technical and legal knowledge and is a challenge for consumer stakeholders.

An independent reviewer might be engaged for some technical parts of each Review (for example the proposed Technology Neutrality Review). However, ASIC should continue to coordinate the overall Review process, as ASIC has the greatest knowledge of the history of the Code.

12. Other issues from ASIC Consultation Paper

Q68 – In your view, why has membership of the EFT Code remained limited generally to providers of generic banking services?

The limited membership of the Code reflects the dominance of Part A of the Code. Part B was probably too ambitious and too early and it is not surprising that organisations in the early stages of developing stored value products see Code subscription as a low priority.

However, limited membership is of concern in relation to some new, dominant Internet based payment systems, such as PayPal and Checkout. It is essential that such systems are covered by the same consumer protection rules as traditional EFT Code subscribers.

Q69 – What steps could/should be taken to broaden EFT Code membership?

As the EFT Code is a functional Code there is no obvious industry association to take on a leadership role in encouraging membership. ASIC may have to engage with stakeholders in a campaign to encourage target organisations to subscribe.

Q70 – How much of the EFT Code's requirements do non-subscribing entities take into account even though they do not subscribe to it?

It is unlikely that non-subscribing entities take any notice of the EFT Code provisions. PayPal and Checkout both offer EFT services. Their terms and conditions do not reflect basic EFT Code consumer protections.

For example, Google Checkout makes the consumer liable for 'any and all transactions by persons that you give access to or that otherwise use such username or password'.

Q71 – What changes could/should be made to the way the EFT Code is written, designed and presented to make it a more user friendly and accessible document?

As suggested elsewhere in this submission, the EFT Code can be improved through shortening and simplifying the text. Some other minor improvements might also be considered:

- Once the text is shorter, it may be able to move the endnotes to short footnotes or notes within the main text so that they can be read together;
- Clauses 8 and 20 should be shortened and moved to the scope and definitions sections at the beginning of the Code, as this is a more appropriate location and it will be useful to have all scope and interpretation provisions in one location; and
- Part B should be deleted (discussed above). This may allow the remaining Part A and Part C to be combined so that there is no need for the constant references to 'Part X' in the text of the Code.

Q72 – Should the EFT Code include a statement of objectives? If so, what should the objectives of the EFT Code be?

It is unclear what could be achieved by a Statement of objectives and it may take some time to reach agreement amongst diverse stakeholders. This is a low priority issue and resources and effort should be allocated to other tasks.

13. Additional Consumer Issues

Q73 – Are there other issues not covered in this consultation paper that the review should address?

Consumer stakeholders wish to raise two additional issues:

Technology neutrality

Technology neutrality is a core concern in the EFT Code. Consumer stakeholders support a technology neutral approach in the Code to ensure that the Code is able to keep up with developments in EFT technology.

Unfortunately the text of the Code is struggling to address developments in the EFT sector. The key area of concern is the complex use of the following terms and their inter-relationship in the Code text:

- Electronic equipment;
- Device;
- Identifier; and
- Code.

At different points in the Code the use of each of these terms results in a specific liability outcome. However, there are now so many ways to provide instructions for an electronic funds transfer or to access and account that these terms may not adequately cover all circumstances. If they do cover all circumstances, the use of these terms may result in unexpected liability results.

These terms may need to be reviewed to ensure technology neutrality is maintained. One issue here is that modern access methods now include two factor authentication approaches resulting in a plethora of new devices – smart cards, one-time password generators, mobile phones, USB tokens – all of which might play a role in providing access.

As a result, some of the definitions (e.g. device and electronic equipment) may need to be reviewed for technology neutrality. Some initial observations show the complexity of these definitions in practice:

- A mobile phone is currently defined as both a device and electronic equipment.
- The definition of code means that it must be known to the user, but modern codes (e.g. one-time passwords) are generated by devices and only ‘known’ to the consumer for a short period if at all.

It may be useful to conduct a thorough Technology Neutrality Review of the definitions in the Code once other clauses are agreed in the Review process.

Financial hardship

In addition, the parties to this submission have read and endorse the recommendations on financial hardship contained in the *Consumer Caseworker Submission*. In particular their comments below:

> Members appear to need to be pushed to consider the financial and medical circumstances of consumers. Consumer law organisations would like to see a mirroring of the s 25(2) of the Code of Banking Practice which requires members to make allowances for financial difficulty. Such provisions need to be introduced in the EFT Code, as it covers a much greater member base than just banks.

14. Appendix 1 – Authentication Technologies

Attempts to Strengthen Two-factor Authentication

There have been attempts to improve the ability of two-factor authentication to combat online fraud. For example, rather than prompt the user to enter a passcode presented by their token at the time of login, The National Australia Bank has created a system in which the customer is prompted to enter the latest passcode displayed by their token (in this case, their mobile phone) whenever an outside-payment transaction is initiated on their account.[45] Arguably, it is hard for a fraudulent man-in-the-middle to obtain these subsequent passcodes even if they have obtained the customer's login credentials, since the customer is unlikely to supply further passcodes to authorise transactions that they did not initiate themselves.

However, a man-in-the-middle could circumvent this by creating a mechanism whereby the user is prompted (through a spoofed interface) to supply another passcode after they have logged in. The man-in-the-middle could then immediately use this passcode to initiate a transaction on the customer's account. The NAB's system deals with this problem to some extent by ensuring that customers only have access to passcodes once they have been sent to the customer's mobile phone – the customer does not have a token that is able to generate the passcodes independently of the bank's involvement.

Tricerion Strong Mutual Authentication

Tricerion's Strong Mutual Authentication (SMA) Server technology provides an example of how keypad technology can be used to achieve website authentication. SMA is a server-based solution in which organisations install an SMA server behind their firewall alongside their existing web application servers. The SMA server incorporates innovations that provide security against phishing attacks.[46]

One of these innovations is **keypad personalisation**. This works in the following fashion:

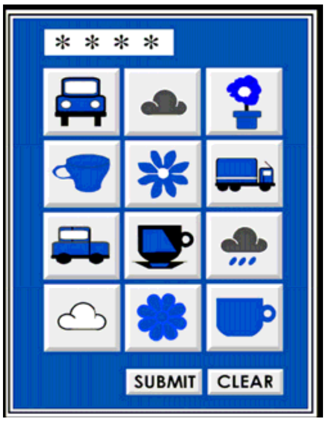
- The user is prompted to enter an account / user name; and
- The application server passes the account name to the Tricerion SMA server. The SMA server then generates an image map in the form of a personalised keypad for the specific user. The keypad is presented on the user's screen. The user enters their password by use of the keypad (they cannot enter their password directly using a keyboard – they must use the keypad – avoiding the danger of keystroke loggers being used to intercept the password). The positions of the various characters on the keypad are randomly varied each time the user attempts to log-in.

[45] National Australia Bank, *SMS Payment Security*, 2007, <http://www.nab.com.au/Personal_Finance/0,,82833,00.html>.

[46] Tricerion, *Account Hijacking Prevention with the Tricerion Strong Mutual Authentication (SMA) Server*, 2005, <http://www.tricerion.com/downloads/984_Tricerion_SMA_-_Account_Hijacking_Protection.pdf>.

Authentication of the website to the user is possible because the SMA server stores personalised keypad data for each user. This personalised data allows each user to specify display properties their keypad should exhibit, including background colour, border design, fonts and font size. A fraudulent party does not have access to this personalised data and so even if they try and emulate the keypad display, it is unlikely they will be able to create a keypad that adheres to each user's individual display preferences. If the keypad displayed to the user varies in appearance from the one they expect to see, they are immediately alerted to the possibility the website they are visiting is spoofed.

SMA supports the use of passwords consisting of either alphanumeric characters or pictures. Users can accordingly define an individual set of symbols (characters or pictures) that is to be displayed to them each time they attempt to log in. Only a subset of these symbols will actually form the user's password, and the positions of the various symbols will vary at each log in attempt. Thus, if a spoofed website uses a keypad to display symbols that the user does not expect to see, they are again alerted to the possibility that they are being subjected to a phishing attack. Additionally, it is quite likely that the subset of symbols displayed on a spoofed keypad to the user will not contain all the symbols that are part of the user's password, making it impossible for the user to disclose their password to a fraudulent party.



An example of a personalised keypad that may be presented to an end-user

Tricerion's implementation of keypad technology is based on another innovation known as triangulation. Triangulation describes a communication paradigm which provides additional resistance to man-in-the-middle attacks. Triangulation works by moving from traditional models of communication between the user and the online service to a trialogue in which communication occurs between the user, online service and a third party server. Communications are thus segmented into multiple, discrete channels so that even if a fraudulent party is able to intercept data transmitted along two of the three channels, they will not be able to make use of it unless they can also compromise the third channel.

Secure Remote Password Protocol

A typical implementation of SRP works by applying a function to a password chosen by the user to generate what is known as a 'verifier'. The verifier is sent once to the financial institution's server where it is stored.

Each time the user needs to log-in, they enter their username and password. However the password, unlike the username, is *not* sent to the financial institution's server. The password is instead used by the customer's computer to generate the verifier referred to earlier. The financial institution's server and the customer's computer then generate random values and exchange these. Using the combination of the verifier (which the customer's computer has generated and the financial institution's server should already have a copy of) and both sets of random values, each party is able to produce a congruent session key that can be used to encrypt communications. Each party then proves it has the same session key by producing a hash of that key and sending it to the other party along with the random values provided by that other party. Both the customer and financial institution have thus proven they hold the correct verifier without actually sharing it, facilitating a process of mutual authentication and significantly reducing the possibility of a fraudulent third party being able to use an end-user's password to initiate a replay attack.

Delayed Password Disclosure

One of the vulnerabilities of the Secure Remote Password protocol discussed previously is that in many cases the password-entry interfaces provided to end-users by SRP compatible software agents can be spoofed by fraudulent parties.[47]

Delayed Password Disclosure (DPD) technology works to overcome this key vulnerability. In DPD, user passwords are supplemented by a sequence of images specific to each user, web server, and password. At the establishment of a relationship between a user and web server, the server provides the user with a sequence of images that corresponds to their password. Then, whenever the user wishes to log-in, they enter the first character of their password into a DPD compatible software agent. The web server uses its knowledge of what image should be presented to the user to send back specific data (for example, a sequence of binary digits). The software agent on the user's machine uses that data in combination with a previously agreed upon method of manipulating it (for example, an algorithm known only to the web server and end-user) to determine what image should be displayed to the user for the particular password character that was entered. If the correct image is displayed to the end-user, they know that in all probability they are communicating with the correct server, and so enter the next character of their password. The process of displaying an image then repeats, until all characters are entered. If at any stage an incorrect image is displayed, the user can terminate the communications session before they have disclosed any sensitive data. If the correct sequence of images is displayed, the user knows they are communicating with the server they intend to.

A fraudulent party attempting to impersonate the web server will have great difficulty in determining what sequence of images should be displayed to the end-user, because the images are never transmitted across the network and hence cannot be intercepted. Rather, the end-user's machine simply uses data provided by the server to compute what image should be displayed to the user. Secondly, even if the fraudulent party is able to guess what image should be displayed, that does not mean they learn the user's password. It simply means that the user will enter the next character in their password, and the fraudulent party will then have to re-guess what image should be displayed to the user. Particularly if the pool of images which displayable to the user is large, it is unlikely that the fraudulent party will be able to successfully guess the image that is to be displayed for each password character.

[47] Jakobsson G M and Myers S, *Stealth Attacks and Delayed Password Disclosure*, AI3, 2006, <https://www.a-i3.org/content/view/69/104/>.

Federated Identity Management Systems

In a federated identity management system, authentication of a party X by one member of the community (or a trusted 3rd party identity broker) ensures that party X is authenticated to all members of the community.

In these situations, a client wishing to access a server could also request the server to authenticate itself to a particular identity broker. The broker then performs authentication as necessary and re directs the client to the appropriate server. The identity broker could also provide the server with a secret previously provided by the client, so that the server can display this to the client in order to authenticate itself.

One advantage of this model is that it can take advantage of situations where communities of trust have already been established. Additionally, if an identity broker performs the task of forwarding an end user to the correct website, this averts the possibility that the user may be exposed to a man in the middle attack.

Challenge/Response Mechanisms

An illustration of the application of challenge / response techniques to website authentication is provided by examining the work of the initiative for open authentication (OATH).[48] OATH is built around-the *Industry Roadmap for Open Strong Authentication.*

OATH has created a one-time password technology called HOTP to facilitate two-factor authentication. HOTP is based on the HMAC-SHA-1 cryptographic standard. A client can generate a one-time password using the HOTP algorithm when it is combined with a secret key (shared by both the server and client) and a counter value which increments every time a password is required. The server can verify the password is correct by applying the HOTP algorithm to its own copy of the key and counter value. One of the key advantages of this approach is that HOTP is not a proprietary model but an attempt to establish an industry standard for authentication. It also potentially avoids the expense of rollouts associated with hardware-based technology, although several vendors still employ OATH's HOTP algorithm in hardware tokens.

The *Mutual OATH: HOTP Extensions for mutual authentication*[49] discusses possible ways in which the HOTP algorithm can be adapted for mutual-authentication (see in particular section 4.3). One way the document suggests this could be achieved is by replacing the incrementing counter value with a challenge / response mechanism. For example, a financial institution's server could issue a challenge to the client. The client uses the challenge, in combination with the shared secret key, to generate a response via the HOTP algorithm. If the server is satisfied with the response, the client can then issue its own challenge to the server.

Another method which could be used to achieve mutual authentication would involve the creation of two keys, K1 and K2. K1 is used by Party A to check responses and K2 is used to produce responses to a challenge. Party B uses the keys for the reciprocal purpose. Party A can then issue a challenge to Party B, and B computes the response using K1 and the HOTP algorithm. Party A checks the validity of the response using K1 and then is issued its own challenge by Party B using K2.

[48] Open Authentication Initiative, *OATH Reference Architecture Release 1.0*, 2005, <http://openauthentication.org/OATHReferenceArchitecturev1.pdf>.

[49] Open Authentication Initiative, *Mutual OATH: HOTP Extensions for mutual authentication*, December 2005, <http://openauthentication.org/pdfs/draft-mraihi-mutual-oath-hotp-variants-00.pdf>.

OATH has been subjected to claims that the security of its HOTP technology is questionable because the SHA-1 algorithm upon which it is based has been compromised.[50] These claims are however debatable primarily because the computing resources required to mount an attack on SHA-1 are exorbitant.[51] HOTP could also be modified to use more complex algorithms which would be even more difficult to crack.

QUATRO

The *QUATRO approach to Transparency and Usability of Web Authentication*[52] specifically proposes trust marks as a form of website authentication.

QUATRO uses machine-processable labels expressed as Resource Description Framework (RDF) metadata. Essentially, website administrators link all the content on their site to an RDF content-label. The label makes assertions about the content on the website (for example, an absence of a specific type of objectionable content).

QUATRO employs two tools to assist web users to verify the legitimacy of the RDF trust mark.

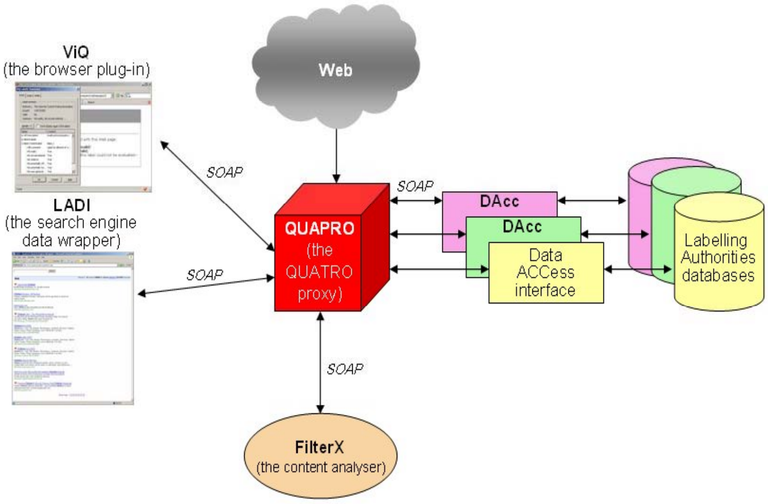
— **ViQ**
The first is a browser extension known as *ViQ.* When *ViQ* is installed, it forwards the URL of any websites visited by a user to a special proxy server known as QUAPRO (using SOAP XML messages). QUAPRO then visits the URL and looks for a link to an RDF content-label. If an appropriate content label is found, QUAPRO ascertains from the label the specific labelling authority from whom further information is available to support the claims made in the trust mark regarding the content on the website. QUAPRO then contacts the labelling authority's database to verify the legitimacy of the trust mark. This information is then forwarded to *ViQ,* which adds icons to the browser to indicate the level of trust that should be attributed to site's RDF content label; and

— **LADI**
Another tool to verify the legitimacy of trust marks is known as *LADI,* which is a search engine wrapper. When a user enters a search query, each URL returned by the search engine is forwarded by *LADI* to QUAPRO. As with *ViQ,* QUAPRO will then visit each URL and look for a link to a content-label, and determine the labelling authority that can verify the label's validity. This information is then forwarded back to the *LADI* client, which annotates the search results displayed in the user's web browser accordingly. If the user decides to visit a specific website contained in the search results, *LADI* then requests QUAPRO to consult the labelling authority to ascertain the label's validity.

[50] Merritt R, *Crack in SHA-1 code 'stuns' security gurus*, EETimes, February 2005, <http://eetimes.com/news/latest/showArticle.jhtml?articleID=60402150>.

[51] Bellare M, *Attacks on SHA-1*, OATH, March 2005, <http://www.openauthentication.org/pdfs/Attacks on SHA-1.pdf>.

[52] Archer P, *The QUATRO approach to Transparency and Usability of Web Authentication*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, <http://www.w3.org/2005/Security/usability-ws/papers/04-quatro-trust/>.



GeoTrust True Site

True Site is a technology owned by GeoTrust which facilitates the dynamic creation of seals to verify the authenticity of a particular website.

Websites wishing to display a True Site trust mark (known as 'smart icon') register for the use of the technology by providing a fee (payable annually) and completing an enrolment form outlining details about the company. The information provided is verified by an independent third party and is then stored in a database administered by GeoTrust. The website owner then places a special JavaScript tag in the HTML code of any web page that is to display the smart icon. This tag causes the web browser to contact GeoTrust. The browser also forwards the domain name of the website which referred it to GeoTrust. GeoTrust uses the provided domain name to perform a lookup in its database. If the domain name exists in the database, GeoTrust dynamically generates an image (the smart icon) which contains a time stamp and the official name of the company as listed in the database. This image is then passed back to the web browser which in turn displays the image on the web page. Users can click on the smart icon to obtain more information from GeoTrust as to the precise identity of the produces of the web page.[53]

Petname

Petname is a web browser user interface widget that sits in the browser's toolbar in clear view of the user at all times. The onus to provide parameters for proper authentication of a website is placed on the user by way of notes reminding the user of the relationship they have with a particular site.

The Petname widget displays this reminder note in every instance that the website is accessed by the user, allowing them to quickly determine the authenticity of a site they are visiting. The key advantage of such a solution is that the visited website has no way of determining the reminder note that the user has set using the widget. This differentiates the Petname widget from other tools which operate inside of the browser chrome. In this way, the user can be certain that the messages appearing in the Petname widget are created solely by the user and have not been altered by an external source.

[53] For more information see <http://www.geotrust.com/products/identity_verification/true_site.asp>.

This approach of detecting a spoofed website reveals shortcomings in current trends in web browser user interface design. In accessing a spoofed website, the information presented to the user is all provided by the attacker: the web page; the URL; the SSL certificate (if any).[54] Allowing the user to set reminder notes regarding their relationship with a website provides an opportunity to enhance the ability of a web browser's user interface to assist with the authentication of websites by incorporating an element into the interface that is user-derived.

SpoofGuard

SpoofGuard is an Internet Explorer browser plug-in developed to assist users in determining when they are visiting a spoofed website.[55] SpoofGuard works by examining web pages a user has visited and using a variety of criteria to calculate a score, known as a 'spoof index', for the website. If the index exceeds a threshold set by the user, SpoofGuard then warns the user that the site is likely to be spoofed. SpoofGuard uses the following techniques to calculate the index for a particular web page:

— **URL Checks**
If a URL for a web page contains suspicious elements (such as the use of IP addresses, '@' symbols and the like), this means it is more likely the site is spoofed. Similarly, if the URL closely resembles (but yet slightly varies from) a well-known domain name or a domain name previously visited by the user (e.g. paypaI.com may be used instead of paypal.com), this increases the spoof index.

— **Image Checks**
SpoofGuard maintains a database of well-known images (often these are corporate logos of well known organisations whose websites are likely to be the target of spoofing attempts) and their associated domains. So, for example, logos used by eBay are stored in SpoofGuard's database with the domain-name association 'www.ebay.com'. If a user visits a site that uses those images, but the domain name does not match the corresponding domain name in SpoofGuard's database, this increases the probability that the site is spoofed (spoofed sites will often use the same images used on the real site in order to create a convincing spoof). Although spoofers could easily overcome this by making very slight modifications to the image before putting it on the spoofed site, this can be combated through the use of a hash function. Specifically, a hash function would allow SpoofGuard to store the hashes of images rather than the images themselves. The hash function works in such a way that minor modifications to an image will not result in a different hash being produced. This allows SpoofGuard to perform an image check even if an attacker has slightly modified an image compared with one used on the real version of the website.

The image check could however be circumvented if a spoofer divided the image into 'slices' that were placed alongside each other on the spoofed website. Although the slices would appear as one contiguous image to an end-user, SpoofGuard would treat each slice as a separate image and would thus be unable to match any individual slice with an image hash stored in its database.

[54] Close T, *Petname Tool: Enabling website recognition using the existing SSL infrastructure*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, <http://www.w3.org/2005/Security/usability-ws/papers/02-hp-petname/>.

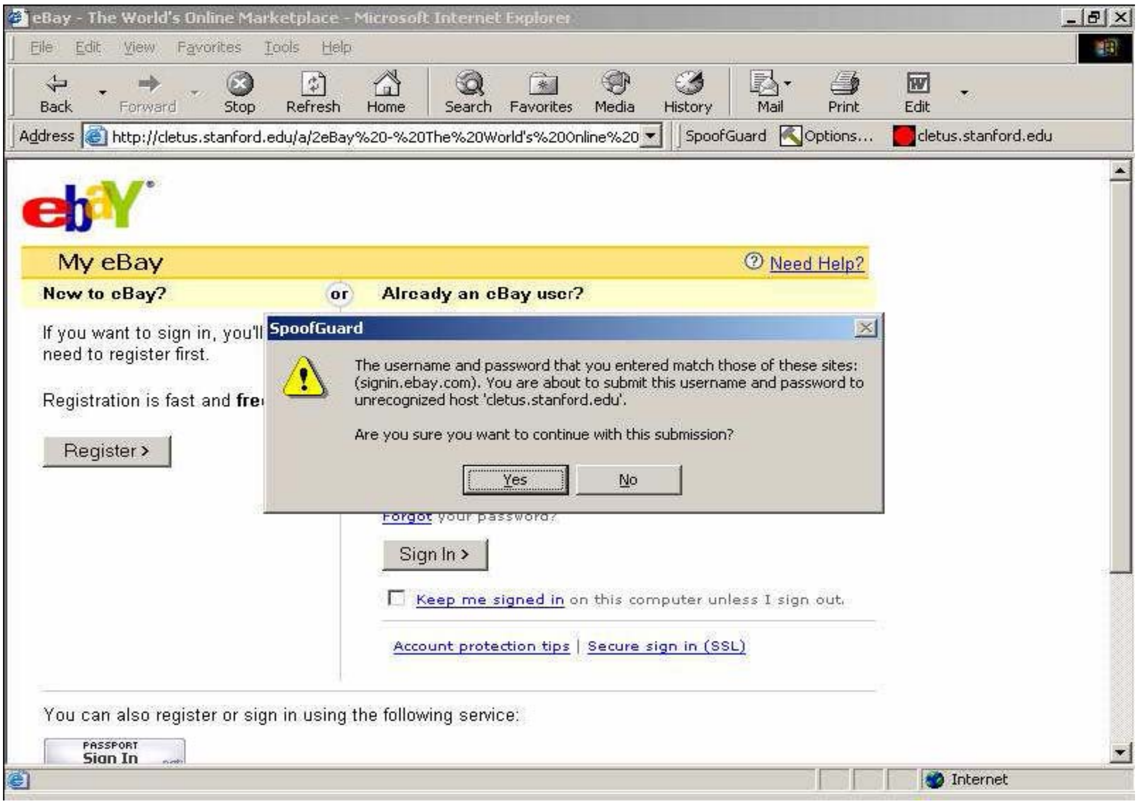
[55] Refer to Chou N, Ledesma R, Teraguchi Y, Boneh D and Mitchell J C, *Client-side defense against web-based identity theft,* Stanford University Computer Science Department, February 2004, <http://crypto.stanford.edu/SpoofGuard/webspoof.pdf>.

— **Link Checks**
SpoofGuard checks to see how many of the links on the web page actually work; if at least one-fourth of the links fail, the site is more likely to be spoofed.

— **Referral Checks**
If the user has followed a hyperlink to reach another web page, SpoofGuard increases the spoof index if the referring page was one where the user may have been reading email (for example, hotmail.com). This is because it is possible the user may have been lured to the site by use of a phishing email containing a hyperlink to the spoofed site.

— **Outgoing Password Checks**
SpoofGuard monitors the websites a user visits and maintains a database recording usernames and passwords, as well as the domain name where each username and password is typically used (for security purposes, the password is stored as a hash). If the user then visits a spoofed website and attempts to enter the same authentication credentials they have used at another website, SpoofGuard will detect this and warn the user that they are about to submit their password and username to a site that is different from the one they normally submit the credentials to.

This check could be defeated by an attacker breaking the password input field on the spoofed web page into multiple adjacent fields which appear as one single input field to the user. SpoofGuard would then be unable to perform a password comparison test.



eBay - The World's Online Marketplace - Microsoft Internet Explorer

Address: http://cletus.stanford.edu/a/2eBay%20-%20The%20World's%20Online%20

SpoofGuard

The username and password that you entered match those of these sites: (signin.ebay.com). You are about to submit this username and password to unrecognized host 'cletus.stanford.edu'.

Are you sure you want to continue with this submission?

If you want to sign in, you'll need to register first.

Registration is fast and fre

Keep me signed in on this computer unless I sign out.

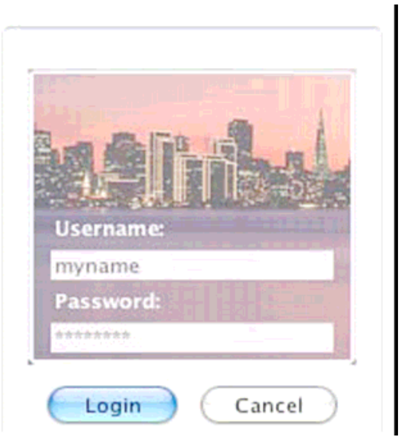
You can also register or sign in using the following service:

An example of SpoofGuard in operation

Trusted Password Windows and Dynamic Security Skins

In their paper entitled *The Battle Against Phishing: Dynamic Security Skins*,[56] the authors discuss the development of an extension for the Mozilla web browser which implements two techniques to prevent spoofing of websites.

The first technique involves presenting the end-user with a 'trusted' window which is dedicated to the function of username and password entry. The user shares a secret (an image) with the browser and each time the user visits a website where they are required to enter a username and password, they are presented with the trusted window which contains the image. This makes it far easier for the end-user to detect when they have been presented with a spoofed window prompting them to enter their authentication credentials, since a spoof is unlikely to be able to display the image the user expects to see. A further advantage is that the user shares their secret with the web-browser rather than a server. This means that the user need not remember a different shared secret for each website where they need to log-in: the one image can be used for all websites. This reduced burden on the end-user perhaps reduces the likelihood of users lacking motivation to adopt the technology. However this implementation does not protect against spoof servers, since any website can instruct the browser to open the window.



Username: myname
Password: ********

A trusted password window which displays a user's secret image as the background

The second technique involves applying the Secure Remote Password Protocol (SRP) (discussed at page 52) to generate a 'dynamic security skin' that is displayed to the user on any authenticated web pages..

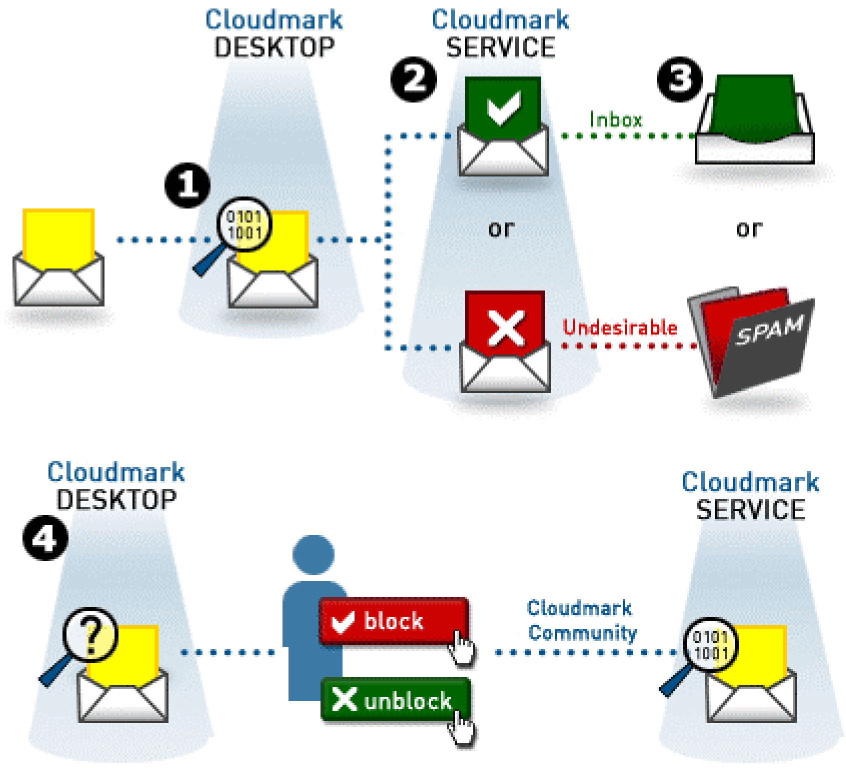
The authors' plug-in extends SRP by using the hash values exchanged in the last part of the authentication process to enable both the server and client to independently generate an 'abstract image' or 'skin' using a special algorithm. If both parties have been successfully authenticated, the skins should match. The skin the browser expects to receive can be displayed to the user in the trusted password window. The server will correspondingly display the skin it has generated in any web pages it presents to the user. The user then simply needs to ensure that the skins match in order to ensure they are not interacting with a spoofed version of the website.

[56] Dhamija R and Tygar J D, *The Battle Against Phishing: Dynamic Security Skins*, Symposium On Usable Privacy and Security, July 2005, <http://cups.cs.cmu.edu/soups/2005/2005proceedings/p77-dhamija.pdf>.

Cloudmark Network Feedback System

Since phishing emails that attempt to lure users to spoofed websites will often be sent out to multiple recipients, if one recipient recognises that the email is fraudulent in nature there have been suggestions that they should be able to effectively communicate that information to other Internet users.[57]

An example of a collaborative technology which gives effect to these suggestions is provided by the Cloudmark Network Feedback System (CNFS), which allows users from around the world to report when they have received what they perceive as a phishing email. Fingerprints for each of these emails is generated using specific algorithms. Once a certain number of users (the number may vary depending on the trust rating of the various users who have made a report to Cloudmark) have identified a specific fingerprint as belonging to a 'phishing' email, all messages with the same fingerprint are filtered in real-time from the inboxes of other users that are part of the network. The algorithms which generate email fingerprints are flexible enough to accommodate minor changes to the email that may be made by an attacker as part of an attempt to avoid the message being recognised as a phishing email.



[57] Fette I, Sadeh N and Cranor L, *Web Security Requirements: A Phishing Perspective*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, <http://www.w3.org/2005/Security/usability-ws/papers/13-cmu-requirements>, page 1.

15. Appendix 2 – Resources

General Resources

ABC, *Banking sector wants consumers to pay for online fraud*, 15 January 2007, <http://www.abc.net.au/pm/content/2007/s1827360.htm>.

Bajkowski J, *Police reject bank clients copping loss*, Australian Financial Review, 19 April 2007.

Bendigo Bank, *Bendigo e-Banking Security Tokens*, <http://www.bendigobank.com.au/public/personal/e-banking_security_tokens.asp>.

Carreker, *ANZ Recognised for Internet Banking Security*, 9 March 2007, <http://www.carreker.com/main/media/press_releases/releases2007/03-09-07-ANZ-IB-Award.htm>.

Espiner T, *Phishing attacks surge*, ZDNet UK, 7 November 2006, <http://news.zdnet.co.uk/security/0,1000000189,39284591,00.htm>.

HSBC, *HSBC launches second factor authentication for retail customers*, 25 October 2005, <http://www.hsbc.com.au/information/news/051025.html>.

Kotadia M, *Citibank helps phishers improve their bait?*, ZDNet Australia, 13 November 2006, <http://www.zdnet.com.au/blogs/securifythis/soa/Citibank_helps_phishers_improve_their_bait_/0,139033343,339272163,00.htm>.

National Australia Bank, *SMS payment security*, <http://www.nab.com.au/Personal_Finance/0,,82833,00.html>.

Nielsen J, *User Education Is Not the Answer to Security Problems*, October 2004, <http://www.useit.com/alertbox/20041025.html>.

Sneddon M, *Legal Liability and E-Transactions: A scoping study for the National Electronic Authentication Council*, August 2000, <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN014676.pdf>.

Tubin G, *The Sky Is Falling: The Need for Stronger Consumer Online Banking Authentication*, TowerGroup, April 2005, <http://www.bnet.com/>.

Woodhead B, *Stronger security for Commonwealth's retail users*, Australian IT, March 27, 2007, <http://australianit.news.com.au/articles/0,7204,21449009%5E15318%5E%5Enbv%5E,00.html>.

Wüest C, *'Phishing In The Middle Of The Stream': Today's Threats To Online Banking*, Symantec, 19 March 2006, <http://www.bnet.com/>.

Regulatory and Policy Resources

APACS, *Remote Card Authentication*, 2005, <http://www.apacs.org.uk/payments_industry/new_technology2.html>.

Banking and Financial Services Ombudsman, *Policies and Procedures Manual*, <http://www.bfso.org.au/abioweb/ABIOWebSite.nsf/Level2Docs/C260E55223CF6FFACA256C23001D15F1/$File/Policies&Procedures_Manual_061219.pdf?OpenElement>.

Federal Financial Institutions Examination Council, *Authentication in an Internet Banking Environment*, 2005, <http://www.ffiec.gov/pdf/authentication_guidance.pdf>.

Hong Kong Government, *Launch of Two-factor Authentication for Internet Banking*, 30 May 2005, <http://www.info.gov.hk/hkma/eng/press/2005/20050530e3.htm>.

Monetary Authority of Singapore, *Technology Risk Management Guidelines for Financial Institutions*, 11 November 2002, <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN011549.pdf>.

Yam J, *Two-factor Authentication*, Hong Kong Government, 2 June 2005, <http://www.info.gov.hk/hkma/eng/viewpt/20050602e.htm>.

Authentication Technologies Resources

Adelsbach A, Gajek S and Schwenk J, *Visual Spoofing of SSL Protected Web Sites and Effective Countermeasures*, Horst Gortz Institute for IT Security, 2005, <https://www.a-i3.org/content/category/7/51/130/>.

Alves-Foss J, *Provably Insecure Mutual Authentication Protocols: The Two-Party Symmetric-Encryption Case*, Centre for Secure and Dependable Software, University of Idaho, October 1999, <http://www.cs.uidaho.edu/~jimaf/docs/prov99.pdf>.

Amir Herzberg, *TrustBar: Protecting (even Naïve) Web Users from Spoofing and Phishing Attacks*, September 2004, <http://eprint.iacr.org/2004/155.pdf>.

Archer P, *The QUATRO approach to Transparency and Usability of Web Authentication*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, <http://www.w3.org/2005/Security/usability-ws/papers/04-quatro-trust/>.

Bakker B, *Mutual Authentication with Smart Cards*, USENIX, 1999, <http://www.usenix.org/events/smartcard99/full_papers/bakker/bakker.pdf>.

Bellare M, *Attacks on SHA-1*, OATH, March 2005, <http://www.openauthentication.org/pdfs/Attacks on SHA-1.pdf>.

Chou N, Ledesma R, Teraguchi Y, Boneh D and Mitchell J C, *Client-side defense against web-based identity theft,* Stanford University Computer Science Department, February 2004, <http://crypto.stanford.edu/SpoofGuard/webspoof.pdf>.

Close T, *Petname Tool: Enabling web site recognition using the existing SSL infrastructure*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, <http://www.w3.org/2005/Security/usability-ws/papers/02-hp-petname/>.

Cloudmark, *Cloudmark Anti-Phishing Services*, 2006, <http://www.cloudmark.com/releases/docs/ds_anti-phishing_10470406.pdf>.

Cloudmark, *Cloudmark Automated Feedback System Helps Service Providers & Customers Combat Messaging Threats*, May 2006, <http://www.cloudmark.com/press/releases/?release=2006-05-30-01>.

Consumer and Business Affairs Victoria, Department of Justice, *Web Seals Of Approval*, January 2002, <http://www.consumer.vic.gov.au/CA256902000FE154/Lookup/CAV_Publications_Computers_Internet_Discussion_Papers/$file/WebSealsFinalReport.pdf>.

Deare S, *Australia Post tests online identification service*, ZDNet Australia, 6 September 2006, <http://www.zdnet.com.au/news/security/soa/Australia_Post_tests_online_identification_service/0,130061744,339270865,00.htm>.

Dhamija R and Tygar JD, *The Battle Against Phishing: Dynamic Security Skins*, Symposium On Usable Privacy and Security, July 2005, <http://cups.cs.cmu.edu/soups/2005/2005proceedings/p77-dhamija.pdf>.

Digital Resolve, *Trusted Server™ Technology*, 2006, <http://www.digital-resolve.net/solutions/trusted_server.html>.

Dreymann DT, *CertifiedEmail™ – a New Trustworthy Messaging Class,* W3C Workshop on Transparency and Usability of Web Authentication, 2006, <http://www.w3.org/2005/Security/usability-ws/papers/38-goodmail>.

Entrust, *Securing What's at Risk: A Common Sense Approach to Strong Authentication*, 8 November 2005, <http://www.entrust.com/resources/download.cfm/22313/>.

Fette I, Sadeh N and Cranor L, *Web Security Requirements: A Phishing Perspective*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, <http://www.w3.org/2005/Security/usability-ws/papers/13-cmu-requirements>.

Financial Services Technology Consortium, *Financial Industry Recommendations and Requirements for Better Mutual Authentication*, June 12 2006, <http://fstc.org/projects/docs/Recommendations_and_Requirements_for_BMA_v1.0.pdf>.

Fraser N, *The Usability of Picture Passwords*, Tricerion, 2006, <http://www.tricerion.com/downloads/Usability-of-picture-passwords.pdf>.

Gabrilovich E and Gontmakher A, *The Homograph Attack*, February 2002, <http://www.cs.technion.ac.il/~gabr/papers/homograph_full.pdf>.

Gajek S and Schewnk J, *Reversed Responsibilities: Browser Authentication instead of Server Authentication,* W3C Workshop on Transparency and Usability of Web Authentication, March 2006, <http://www.w3.org/2005/Security/usability-ws/papers/09-dortmund-reverse/>.

GeoTrust, *Identity Verification: Verified Domain™*, 2005, <http://www.geotrust.com/products/identity_verification/verified_domain.asp>.

GeoTrust, *True Site™: Identity Assurance for Web Sites*, 2004, <http://www.geotrust.com/resources/product_pdfs/pdfs/TrueSite.pdf>.

Green Armor Solutions, *Identity Cues Two Factor™ & Two Way Authentication*, 2005, <http://www.greenarmor.com//DataSheets/Identity Cues Two Factor Data Sheet.pdf>.

Hall K, *Vulnerability of First-Generation Digital Certificates and Potential for Phishing Attacks and Consumer Fraud*, April 2005, <http://www.geotrust.com/resources/white_papers/pdfs/SSLVulnerabilityWPcds.pdf>.

Hardmeier S, *The Phishing Filter: Fighting the Modern Day Con Artist*, Microsoft, 10 November 2005, <http://www.microsoft.com/windows/ie/community/columns/phishing.mspx>.

Hirsch F and Le Van Gong H A, *Approaches to Simplify Server Authentication*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, <http://www.w3.org/2005/Security/usability-ws/papers/07-nokia-and-sun/>.

Howarth F, *Deploying psychology in the fight against phishing*, Bloor Research, 15 July 2005, <http://www.it-director.com/article.php?articleid=12808>.

IBM, *An overview of the SSL handshake*, 2005, <http://publib.boulder.ibm.com/infocenter/wmqv6/v6r0/topic/com.ibm.mq.csqzas.doc/csshandshake.htm>.

IBM, *How SSL provides authentication*, 2005, <http://publib.boulder.ibm.com/infocenter/wmqv6/v6r0/topic/com.ibm.mq.csqzas.doc/cssauthentication.htm#cssauthentication>.

Iconix, *How eMail ID Works*, 2005, <http://www.iconix.com/learnmore.php>.

IEEE Security and Privacy, *The TIPPI Point: Towards Trustworthy Interfaces*, July 2005, <http://www.cs.dartmouth.edu/~sws/pubs/ss05a.pdf>.

Jakobsson GM and Myers S, *Stealth Attacks and Delayed Password Disclosure*, AI3, 2006, <https://www.a-i3.org/content/view/69/104/>.

Jones MB, *The Identity Metasystem: A User-Centric, Inclusive Web Authentication Solution*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, <http://www.w3.org/2005/Security/usability-ws/papers/28-jones-id-metasystem/>.

Keizer G, *5 Tools To Bulletproof Firefox*, InformationWeek, 14 July 2006, <http://www.informationweek.com/shared/printableArticle.jhtml?articleID=190400479>.

Linn J, Kaliski B, Nyström M and Yung M, *Applying Context to Web Authentication*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, <http://www.w3.org/2005/Security/usability-ws/papers/03-rsa-context/>.

MacFarland A, *Iconix Truemark Authentication Service Add More Trust into E-Business*, The Clipper Group (Navigator), December 2005, <http://www.clipper.com/research/TCG2005078.pdf>.

Marchesini J and Smith S, *Virtual Hierarchies – An Architecture for Building and Maintaining Efficient and Resilient Trust Chains*, May 2002, <http://www.cs.dartmouth.edu/~sws/pubs/ms02.pdf>.

Merritt R, *Crack in SHA-1 code 'stuns' security gurus*, EETimes, February 2005, <http://eetimes.com/news/latest/showArticle.jhtml?articleID=60402150>.

Microsoft, *How CA Certificates Work*, 2003, <http://technet2.microsoft.com/WindowsServer/en/Library/0e4472ff-fe9b-4fa7-b5b1-9bb6c5a7f76e1033.mspx?mfr=true>.

Miller R, *SSL's Credibility as Phishing Defense Is Tested*, March 2004, <http://news.netcraft.com/archives/2004/03/08/ssls_credibility_as_phishing_defense_is_tested.html>.

Mysore SH, *Web Authentication Today and For Tomorrow*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, <http://www.w3.org/2005/Security/usability-ws/papers/25-mysore-webauth-today-tomorrow/>.

National Australia Bank, *SMS Payment Security*, 2007, <http://www.nab.com.au/Personal_Finance/0,,82833,00.html>.

National Consumers League, *A Call for Action: Report from the National Consumers League Anti-Phishing Retreat*, March 2006, <http://www.antiphishing.org/reports/200603_NCL_Phishing_Report.pdf>.

Nelson J and Jeske D, *Limits to Anti-Phishing*, W3C Workshop on Transparency and Usability of Web Authentication, 2006, <http://www.w3.org/2005/Security/usability-ws/papers/37-google>.

NetworkWorld Asia, *Australia Post approves online banking*, 21 February 2007.

Open Authentication Initiative, *Mutual OATH: HOTP Extensions for mutual authentication*, December 2005, <http://openauthentication.org/pdfs/draft-mraihi-mutual-oath-hotp-variants-00.pdf>.

Open Authentication Initiative, *OATH Reference Architecture Release 1.0*, 2005, <http://openauthentication.org/OATHReferenceArchitecturev1.pdf>.

Open Authentication Initiative, *OATH Roadmap*, November 2005, <http://openauthentication.org/pdfs/OATH Public Roadmap 2006.pdf>.

PCWorld, *VeriSign Redesigns Trust Mark Seal*, November 2003, <http://www.pcworld.com/news/article/0,aid,113264,00.asp>.

PhishCops, *How Does PhishCops™ Work?*, 2005, <http://www.phishcops.com/how.asp>.

Phoenix Technologies, *Phoenix SPEKE – Strong Authentication for Devices, Networks, and Data*, 2006, <http://www.phoenix.com/NR/rdonlyres/04BD87B1-F01A-449E-AE1E-743A7399A3C0/0/SPEKE_ds.pdf>.

Quatro, *How to make your trustmark machine-readable using the Quatro system*, May 2006, <http://www.quatro-project.org/howto/>.

Rivest LR, *Separable Identity-Based Ring Signatures: Theoretical Foundations For Fighting Phishing Attacks*, February 2005, <http://theory.lcs.mit.edu/~rivest/AdidaHohenbergerRivest-SeparableIdentityBasedRingSignatures.pdf>.

Rosenberg J, *True Site™: Helping on-line companies create trusted brands so their site visitors feel confident enough to stay and pay*, GeoTrust, November 2001, <http://www.geotrust.com/resources/white_papers/pdfs/TrueSiteWP.pdf>.

Rotondi D, *A Server Authentication Procedure Proposal*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, <http://www.w3.org/2005/Security/usability-ws/papers/06-rotondi-authentication/>.

RSA Security, *Protecting Against Phishing by Implementing Strong Two-Factor Authentication*, 2004, <http://www.indevis.de/dokumente/anti_phishing_rsa.pdf>.

Rubinoff S and Steinberg J, *Key Human Factors Issues Surrounding Consumer Two Factor Authentication and Mutual Authentication*, Green Armor Solutions, 11 July 2006.

Sestus Data Corporation, *PhishCops™ White Paper*, 2006, <http://www.phishcops.com/docs/pc51013-r.pdf>.

Staikos G, *Improving Internet Trust and Security,* W3C Workshop on Transparency and Usability of Web Authentication, March 2006, <http://www.w3.org/2005/Security/usability-ws/papers/33-staikos-improving-trust/>.

The Office of the Information and Privacy Commissioner/Ontario and The Office of the Federal Privacy Commissioner of Australia, *Web Seals: A Review of Online Privacy Programs*, September 2000, <http://www.privacy.gov.au/publications/seals.html>.

Transport Security Layer Working Group, *The SSL Protocol Version 3.0*, 1996, <http://wp.netscape.com/eng/ssl3/draft302.txt>.

Tricerion, *Account Hijacking Prevention with the Tricerion Strong Mutual Authentication (SMA) Server*, 2005, <http://www.tricerion.com/downloads/984_Tricerion_SMA__Account_Hijacking_Protection.pdf>.

Tricerion, *Tricerion SMA Product Description*, 2006, <http://www.tricerion.com/downloads/978_Tricerion_SMA_Product_Description.pdf>.

Tumbleweed Communications, *Digital Certificate Validation in Public Key Infrastructures (PKI), and the Online Certificate Validation Protocol (OCSP)*, 2003, <http://tumbleweed.com/pdfs/tmwd_certvalidation_in_pki_wp.pdf>.

VeriSign *VeriSign Unveils Newly Designed Security Trust Mark To Aid Consumers In Identifying Safe Web Sites To Shop This Holiday Season*, 2003, <http://www.VeriSign.com/VeriSign-inc/news-and-events/news-archive/us-news-2003/page_200312181046341.html>.

VeriSign, *The VeriSign Secured™ Seal Research Review*, 2006, <http://www.VeriSign.com/static/013506.pdf>.

VeriSign, *VeriSign Enhances Online Transaction Security With Mutual Authentication Solutions Leveraging Microsoft Internet Explorer 7 and 'InfoCard'*, February 2006, <http://www.verisign.com/verisign-inc/news-and-events/news-archive/us-news-2006/page_037034.html>.

Wade C, *Financial Industry Requirements for Better Mutual Authentication*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, <http://www.w3.org/2005/Security/usability-ws/papers/15-wade-financial>.

WiKID, *WikID Mutual Authentication*, 2006, <http://www.wikidsystems.com/product-info-downloads/technology/mutual_authentication/>.

WiKID, *WiKID releases HTTPS Mutual Authentication*, October 2005, <http://www.wikidsystems.com/WiKIDBlog/69>.

Willoughby M, *OATH Swears Authentication is the Next Big Thing*, Digital ID World, January 2005, <http://magazine.digitalidworld.com/Jan05/Page34.pdf>.

Wright K L, *W3C Workshop on Transparency and Usability of Web Authentication*, March 2006, <http://www.w3.org/2005/Security/usability-ws/papers/21-wright-position>.

Ye EZ, Yuan Y and Smith S, *Web Spoofing Revisited: SSL and Beyond*, Dartmouth College Department of Computer Science, February 2002, <http://www.cs.dartmouth.edu/~pkilab/papers/tr417.pdf>.

Zurko ME and Wilson D, *Using History, Collaboration, and Transparency to Provide Security*, W3C Workshop on Transparency and Usability of Web Authentication, March 2006, <http://www.w3.org/2005/Security/usability-ws/papers/19-zurko-history/>.

Zurko ME, *User-Centered Security: Stepping Up to the Grand Challenge*, IBM Software Group, 2005, <http://www.acsac.org/2005/papers/Zurko.pdf>.

Fraud and Identity Theft Resources

AusCERT, *Haxdoor: Anatomy of an ID Theft Attack Using Malware*, 12 December 2006, <http://www.auscert.org.au/render.html?it=7069>.

AusCERT, *Managing Risks Associated with Online ID Theft for Government and Providers of e-Government Services*, 24 November 2005, <http://www.auscert.org.au/render.html?it=5777>.

Evers J, *Phishers come calling on VoIP*, CNET, July 2006, <http://news.com.com/2100-7349_3-6092366.html>.

IBM developerWorks, *The cranky user: What you can do about phishing*, January 2006, <http://www-128.ibm.com/developerworks/web/library/wa-cranky60.html>.

Infidel Incorporated, *Phishing 2.0: Next Generation Attacks Makes Current One Time Password Technologies Obsolete*, 2005, <http://www.infidel.net/phishing.php>.

Out-Law.com, *Phishing attack evades ABN Amro's two-factor authentication*, 18 April 2007, <http://www.out-law.com//default.aspx?page=7967>.

Risk Management Magazine, *Reeling 'em in – tackling phishing*, 15 March 2005, <http://www.riskmanagementmagazine.com.au/articles/BC/0C02C8BC.asp?Type=124&Category=1240>

Internet Banking Terms and Conditions

Arab Bank, *Product Disclosure Statement*, 2003, <http://arabbank.com.au/docs/pds20060703.pdf>.

Bendigo Bank, *Bendigo Personal Accounts and Facilities: Terms and Conditions*, 1 November 2006, <http://www.bendigobank.com.au/public/fsra/pds/pdf/BBL_personal_PDS.pdf>.

Citibank, *Non-Cash Payment Facilities: Terms and Conditions*, 1 August 2006, <https://www.citibank.com.au/global_docs/pdf/cbol_termsandconditions.pdf>.

Commonwealth Bank of Australia, *Netbank: Electronic Banking General Information and Terms and Conditions*, 29 January 2007, <http://www.commbank.com.au/NetBank/disclosurestatement.asp>.

Westpac Banking Corporation, *Internet Banking and BPAY Product Disclosure Statement: Terms and Conditions for using the services*, 4 August 2006, <http://www.westpac.com.au/manage/pdf.nsf/BE09F15A5772D338CA2570D7007BF074/$File/IB_PDS_new.pdf>.