

Michael Funston
EFT Code of Conduct Review
Australian Securities and Investments Commission
eftreview@asic.gov.au

April 2007

**Re: Reviewing the Electronic Funds Transfer Code of Conduct (EFT Code)
ASIC consultation paper**

Thank you for the invitation to provide comment on the Australian Securities and Investments Commission consultation paper concerning the review of the Electronic Funds Transfer Code of Conduct (EFT Code).

The Consumers' Telecommunications Network (CTN) is a national peak body of consumer and community organisations, and of individuals representing community interests, who participate in developing national telecommunications policy. We advocate policies for better access, quality of service and affordability of telecommunications facilities for all residential consumers. CTN's members are national and state organisations representing consumers from non-English speaking backgrounds, deaf consumers, Indigenous people, low income consumers, people with disabilities, young people, pensioners and superannuants, rural and remote consumers, women and consumers in general.

Our submission to the consultation paper will focus on Section 3 (Growth in online fraud) and Section 7 (EFT Code, Part A (Liability)).

In November of 2006, CTN released a research report titled *Surfing on Thin Ice: Consumers and Malware, Adware, Spam & Phishing*. The report, funded by a grant from the Telstra Consumer Consultative Council, was inspired by growing concern among our members on the issue of e-security. In 2006 our Board identified e-security as one of CTN's top issues. The research, therefore, aimed to investigate residential consumers' experiences with e-security and to identify areas of concern and their implications on telecommunications policy and regulation in Australia.

The research included a literature review of existing research and media coverage of e-security (specifically residential consumers and e-security), paired with an

online survey of consumers. The survey consisted of 42 multiple choice and free-answer questions, was conducted online through our website, and was promoted to our members and other consumers through our extensive network. The survey ran from 29 June to 31 July 2006. The total sample size was 254. We will use results from this research to directly address some of the questions and issues raised in the consultation paper, but we also attach the full report for your consideration (see CTN APPENDIX - Surfing_On_Thin_Ice_NOV_06).

<p>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?</p>

There are many challenges and concerns that consumers face in relation to online fraud and the continuous development of e-security threats. E-security has become a major concern for residential telecommunications consumersⁱ. The most popular computer programs are vulnerable to attackⁱⁱ, as are new types of online services and technologiesⁱⁱⁱ.

The strong majority of consumers we surveyed had experienced many e-security threats despite using a range of security products and despite current legislative and commercial consumer protections. More than 4 out of every 5 consumers we surveyed had experienced Spam. Approximately 2 in every 3 consumers we surveyed had experienced computer viruses or spyware. More than 1 in every 3 consumers we surveyed had experienced adware, trojan horses, phishing or worms. 2 in every 3 consumers we surveyed had used anti-virus software, firewall software, software updates, or anti-spyware software.

Even security products themselves, designed to protect consumers from threats, are not always effective and are vulnerable to attacks^{iv}. Many of these products come at a significant monetary cost to consumers. What's more, e-security threats are constantly evolving^v, and form only part of a wider set of concerns around the use of the Internet, including privacy, child protection and online transactions^{vi}.

The accessibility and reliability of information available to consumers about e-security is questionable. There are no universally accepted definitions of security threats, and the terminology and concepts used to describe them can be confusing^{vii}. With the size of the Internet security market reaching billions of dollars^{viii}, there is room for commercial agendas to impact the way information is presented. Sources of information that may be considered 'independent', such as government agencies and community groups, may face challenges reaching the wider public with campaigns or face challenges to fund such work.

Among consumers we surveyed, the use of independent sources of information on e-security was low, and many questioned the reliability and accessibility of information they had used. Less than 1 in every 4 consumers we surveyed had used Government information on e-security, while most used security software companies and the media. More than half of the consumers we surveyed did not fully trust the sources of information they used, and many raised concerns over the availability and complexity of the information they used.

E-security specific consumer safeguards, investigation processes, reporting mechanisms, public education, and in-depth research are all still in their early days, and as we recommend in our report, need to be developed further. They need to encompass a number of related technology issues, for instance, how the accessibility or performance of broadband can impact e-security, or the total costs of protecting a PC against e-security threats, both monetary and intangible.

If consumers are encouraged, and even expected to complete important transactions or access important information online, basic consumer rights^{ix} must be met to ensure the accessibility, affordability and quality of online services. Currently, we believe that these rights are not being adequately fulfilled.

Q6 Is the growth in, and growing publicity given to, fraud issues having an impact on online transacting in Australia at present? (Again, you may wish to provide information on a confidential basis.)

We believe so. Our research found that a small but significant proportion of consumers suffered financially from e-security attacks, that many more suffered from a loss of productivity, and that many had changed how they used the Internet because of security problems and concerns. More than 1 in every 10 consumers we surveyed had experienced unexpectedly high bills or financial loss as a result of online security problems. Many consumers we surveyed commented on the loss of time and frustration they experienced when dealing with e-security problems. More than 1 in every 3 consumers we surveyed had stopped or changed the way they made online purchases, paid bills online, or used online banking because of online security concerns.

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

Our research found that, though consumer awareness of security threats was reasonable, their understanding and confidence to identify and guard against security threats was questionable.

Almost 9 out of every 10 consumers we surveyed answered that they were aware of and understood Spam and computer viruses, and more than 2 out of every 3 answered that they were aware of and understood spyware and adware. However, more than 1 in every 4 consumers we surveyed had either never heard of phishing, adware, worms, trojan horses or diallers, did not fully understand how they worked, or did not fully understand how they might get them.

More than half of the consumers we surveyed were less than confident they could successfully identify malware, adware, Spam or phishing. Almost 1 in every 3 consumers we surveyed rated their understanding of how security products protected them as less than good. Approximately 1 in every 3 consumers we surveyed had used security products installed by someone else, and many indicated that they relied on products or other people to manage their e-security.

Despite many using security products, and many being aware of security threats, a small but significant proportion of consumers were mishandling Spam and phishing attacks. The majority of consumers we surveyed had recognised and ignored phishing e-mails, but more than 1 in every 20 had been confused by a phishing e-mail, or had visited the websites they were asked to by a phishing e-mail. The majority of consumers we surveyed had deleted Spam without investigating it further, but more than 1 in every 4 had read or tried to unsubscribe from Spam, and 1 in every 20 had replied to it.

- | | |
|------------|--|
| 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? |
| 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 <i>phishing</i> attack? |
| 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 <i>phishing</i> attack? Do the benefits and costs of extending account holder liability justify such an extension? What implementation issues would have to be addressed? |

Simply, consumers are not well enough protected or resourced to bear such responsibility, and the whole area of e-security and electronic transactions is not well enough understood or researched, especially considering its ever-changing nature, to make such radical changes to the EFT Code.

Most consumers we surveyed thought Internet Service Providers and Government should take more responsibility to improve e-security (see also recent overseas research^x). More than 4 out of every 5 consumers we surveyed thought Internet Service Providers should take more responsibility to provide better security online for consumers. 2 out of every 3 consumers we surveyed thought Government should take more responsibility to provide better security online.

It is also important to note that we support the reasons listed in Table 9 of the consultation paper describing other serious implications of extending account holder liability for equipment.

This is not to say that consumers themselves do not have a role to play. 2 out of every 3 consumers we surveyed thought consumers themselves should take more responsibility to provide better security online, and indeed, as consumer protections, education resources and research improves, it may be reasonable for consumers to be held more accountable for the e-security measures they take.

At the present time, we think it holding consumers liable for their e-security is not appropriate. Our research recommends action on a number of fronts to prevent consumers from being unacceptably vulnerable to electronic security threats, including online fraud, as listed below:

R1. Development of consumer protections:

- a. A central, user-friendly, and well-promoted system for consumers to report e-security threats, and for subsequent investigation.
- b. Test cases, case studies and audits of existing consumer protection legislation to ensure adequate protection from current and emerging e-security threats.
- c. Informed consumer consent to the use of adware should be a central principle of Australian Adware guidelines, currently under development by the Internet Industry Association and the Australian Direct Marketing Association.
- d. Internet Service providers and software producers should be required to address e-security issues of the products they offer, including providing

warnings and consumer education, making software patches available, and providing e-security tools.

- e. Action on an international front, possibly forming international information sharing and enforcement arrangements with other governments and agencies, as has been done in the case of Spam.

R2. Development of consumer education resources:

- a. Up-to-date lists of confirmed e-security threats, especially phishing scams, for consumers to refer to.
- b. Using animated demonstrations, real-life examples and plain language to explain how e-security threats work, how to identify them, and how to best deal with them.
- c. Using animated demonstrations, real-life examples and plain language, explanations of how e-security products and other e-security measures work, especially in the context of online transactions.
- d. Addressing the challenges consumers face maintaining security measures across multiple computers, including work computers.
- e. Education resources should be delivered through an independent, central organisation and website – potentially encompassing or extending the NetAlert website or the Stay Safe Online website.
- f. Education resources should be widely promoted across all sectors of society, especially to young people, seniors and new computer users.
- g. Consumers should be encouraged to take more responsibility for their own e-security by actively accessing information from a reliable source, including www.staysafeonline.gov.au and www.netalert.net.au.

R3. Further research into consumers and e-security:

- a. The extent of financial loss, emotional distress and productivity loss on consumers as a result of e-security issues – the Productivity Commission may be well-placed to conduct such research.
- b. The financial capacity of consumers, especially low-income consumers, to effectively protect themselves online, and the viability of subsidised or free e-security products such as e-mail filters.
- c. A focus on e-security for consumers under the age of 30.

- d. A focus on e-security for consumers who are not regularly online.
- e. The most user-friendly ways to present information about online security to beginners, intermediate and advanced computer users of diverse backgrounds.
- f. The best distribution channels to reach beginners, intermediate and advanced computer users of diverse backgrounds with information about e-security, including point-of-sale information, and computer user and community groups.
- g. How the speed of an Internet connection, data download limits, or choice of operating systems may impact a consumer's ability to protect against e-security attacks.

Thank you once again for the opportunity to comment and to have our comments taken into account. Should you wish to discuss this response in more detail please contact myself or Ryan Sengara at the Consumers' Telecommunications Network on 02 9572 6007 or at ctn@ctn.org.au.

Yours sincerely,



Teresa Corbin
CTN Executive Director

This submission was prepared by Ryan Sengara, CTN Project Officer, and Teresa Corbin, CTN Executive Director. It was approved out of session by the CTN Board.

ⁱ **Consumer concern over online security**

Security issues relating to Spam, Phishing, and viruses were the main topic of interest of a sample of over 500 Australian Seniors Computer Clubs' members surveyed in 2006.

–Australian Seniors Computer Clubs Association – Bosler, N, *Seniors' Telecommunications Issues: Their Interests and Concerns*, Australian Seniors Computer Clubs Association, 2006. See www.seniorcomputing.org.

“Only two percent of home Internet users believe the Net is safe, according to a new survey commissioned by security vendor Symantec. The survey, querying 518 people, also found that close to half of all respondents believed their banking and personal details are not safe either.”

–iNews.com.au, “Aussie consumers fearful of Net security”, *iNews.com.au*, viewed 15 March 2006, <<http://www.itnews.com.au/newsstory.aspx?ClaNID=30863&r=hstory>>.

ii Popular platforms, programs and services vulnerable to security threats

“A new study has revealed that a staggering 83% of adults who visit social networking sites expose themselves to malicious hackers and identity thieves... The study revealed that extraordinarily high percentages of visitors to social networking sites, such as MySpace and FaceBook, are engaging in high risk security practices, which expose them to identity theft, fraud, spyware and viruses.”

–Beer, S. , “Social networking sites an open door to hackers”, *ITWire*, viewed 5 October 2006, <<http://www.itwire.com.au/content/view/6064/53/>>.

“On 8 August Microsoft released a bumper collection of security patches for 23 separate flaws in Windows and programs in the Office software suite. One of the problems identified in the August update was deemed so serious that the US Department of Homeland Security (DHS) issued a warning urging users to download the patch and apply it as soon as possible. The DHS has a role in securing America’s critical infrastructure which includes the internet.”

–BBC News, “Hackers target latest Windows fix”, *BBC News*, viewed 17 August 2006, <<http://news.bbc.co.uk/2/hi/technology/4797949.stm>>.

“Microsoft has patched almost as many critical vulnerabilities in the first 8 months of 2006 as it did in 2004 and 2005 combined, security researchers said Wednesday... Thus far this year, there have been 51 security bulletins and 98 patches, 64 of which were deemed critical.”

–iNews.com.au, “Microsoft breaks patch records”, *iNews.com.au*, viewed 14 August 2006, <<http://www.itnews.com.au/newsstory.aspx?ClaNID=35778&eid=1&edate=20060811>>.

“One in 600 profile pages on social networks host some form of malware, a new study has found... Traffic to social networking sites – such as MySpace and Bebo – thought to be popular with teens, accounted for one per cent of all Web use in the workplace...”

–iNews.com.au, “Social networks riddled with malware”, *iNews.com.au*, viewed 14 August 2006, <<http://www.itnews.com.au/newsstory.aspx?ClaNID=35799&eid=3&edate=20060811>>.

“Malware writers have developed worms capable of attacking all major instant messaging (IM) networks across both PC and Mac platforms, security experts warned today.”

–iNews.com.au, “‘Evolved’ worms target all IM networks”, *iNews.com.au*, viewed 14 August 2006, <<http://www.itnews.com.au/newsstory.aspx?ClaNID=35798&eid=3&edate=20060811>>.

“Apple Computer issued on Tuesday updates for its Mac OS X operating system to fix 26 security flaws.”

–ZDNet, “Apple fixes 26 Mac OS flaws”, *ZDNet*, viewed 3 August 2006, <http://www.zdnet.com.au/news/security/soa/Apple_fixes_26_Mac_OS_flaws/0,2000061744,39265286,00.htm>.

“Scammers are using bots to create bogus Ebay accounts that boast trustworthy profiles in a new scheme to rip off buyers, a security company said Monday.”

–iNews.com.au, “New bot-powered Ebay scam uncovered”, *iNews.com.au*, viewed 1 August 2006, <<http://www.itnews.com.au/newsstory.aspx?ClaNID=35456&eid=1&edate=20060801>>.

“Newly disclosed, unpatched flaws in three browsers could make the Web a more dangerous place to surf, security experts have warned. Security researchers published details on the bugs in Microsoft’s Internet Explorer, Apple Computer’s Safari and Mozilla’s Firefox to security mailing lists over the weekend.”

–ZDNet, “Bugs bite into popular browsers”, *ZDNet*, viewed 26 April 2006, <http://www.zdnet.com.au/news/security/soa/Bugs_bite_into_popular_browsers/0,2000061744,39252931,00.htm>.

“A hole in Microsoft Excel has been identified that could allow attackers to take control of a computer, a security group said on Thursday.”

–ZDNet, “Excel hit by another security hole”, *ZDNet*, viewed 10 July 2006, <http://www.zdnet.com.au/news/security/soa/Excel_hit_by_another_security_hole/0,2000061744,39262848,00.htm>.

“...SurfControl has discovered a new blended email/internet security threat, with a fake Google banner. The email claims to be from 'Team Google' launching a new 'Google Pharmacy' service. It directs users to a pharmaceutical site for purchasing medicines. However the website harbours two malicious trojans.”

–iNews.com.au, “Cyber crims fake Google pharmacy”, *iNews.com.au*, viewed 8 June 2006, <<http://www.itnews.com.au/newsstory.aspx?ClaNID=33481&eid=3&edate=20060608>>.

“British website bbc.co.uk has this week become the bait for a new phishing campaign aimed at stealing sensitive security data from computer users by exploiting an Internet Explorer flaw.”

–Sydney Morning Herald, “BBC News delivers security threats”, *Sydney Morning Herald*, viewed April 3 2006, <<http://www.smh.com.au/articles/2006/04/03/1143916454970.html>>.

iii New services and technologies affected by security threats

“In a third and final report on Windows Vista, Symantec examined the security of the operating system core and found some vulnerabilities.”

–ZDNet Australia, “Symantec picks away at Vista's core”, *ZDNet Australia*, viewed 10 August 2006, <http://www.zdnet.com.au/news/security/soa/Symantec_picks_away_at_Vista_s_core/0,2000061744,39266028,00.htm>.

“Some computers with wireless internet capabilities are vulnerable to attacks that could expose passwords, bank account details and other sensitive information even if the machines aren't actually online...”

–Sydney Morning Herald, “Hacker exposes security flaw in wireless computers”, *Sydney Morning Herald*, viewed 3 August 2006, <<http://www.smh.com.au/news/wireless--broadband/hacker-exposes-security-flaw-in-wireless-computers/2006/08/03/1154198254214.html>>.

“The Australian Tax Office confirmed yesterday that 178 taxpayers had unwittingly revealed their tax file numbers while lodging tax returns online...”

–Sydney Morning Herald, “Identity theft virus infects 10,000 computers”, *Sydney Morning Herald*, viewed 3 August 2006, <<http://www.smh.com.au/news/security/identity-theft-virus-infects-10000-computers/2006/08/03/1154198244503.html>>.

“Online scammers have found a new way of tricking computer users into handing over their secure banking details, this time by using internet telephone networks.”

–Sydney Morning Herald, “VoIP new target for financial fraudsters”, *Sydney Morning Herald*, viewed 19 July 2006. <<http://www.smh.com.au/news/security/voip-new-target-for-financial-fraudsters/2006/07/19/1153166440371.html>>.

“The first real mobile phone virus, which was found in the wild and could replicate on its own, was discovered almost two years ago... At AusCERT, Hyppönen [Finnish anti-virus firm F-Secure]...explained that malware aimed at mobile phones is close to evolving into something that could make cybercriminals lots of money.”

–Zdnet, “First mobile phone virus nears 2nd birthday”, *ZDNet Australia*, viewed 30 May 2006, <http://www.zdnet.com.au/news/security/soa/First_mobile_phone_virus_nears_2nd_birthday/0,2000061744,39257470,00.htm>.

“VoIP provider Skype rolled out an update on Friday to quash a bug that can let attackers send a file to a recipient without his or her consent, and potentially obtain access to the computer and its data.”

–iNews.com.au, “Skype sick with bad bug, must be patched”, *iNews.com.au*, viewed 22 May 2006, <<http://www.itnews.com.au/newsstory.aspx?ClaNID=32816&eid=1&edate=20060522>>.

“Over-hyped security threats have made companies unnecessarily hesitant to roll out new technologies, such as Internet telephony and wireless networks, a research firm said this week.”

–iNews.com.au, “Gartner IDs 'over-hyped' security threats”, *iNews.com.au*, viewed 9 August 2005, <<http://www.itnews.com.au/newsstory.aspx?ClaNID=19068>>.

iv Security products affected by security threats or ineffective against them

“Consumer versions of McAfee Inc.'s leading software for securing PCs are susceptible to a flaw that can expose passwords and other sensitive information stored on personal computers, researchers have said. The vulnerability affects many of McAfee's most popular consumer products...”

–Sydney Morning Herald, “McAfee security programs may expose data, researchers say”, *Sydney Morning Herald*, viewed 1 August 2006, <<http://www.smh.com.au/news/breaking-news/mcafee-security-programs-may-expose-data-researchers-say/2006/08/01/1154198118746.html>>.

“The most popular antivirus applications on the market are rendered useless by around 80 percent of new malware, according to AusCERT...the general manager of the Australian Computer Emergency Response Team (AusCERT)...told the audience that popular desktop antivirus applications “don't work”...“So if you are running these pieces of software, eight out of 10 pieces of malicious code are going to get in,” said Ingram.”

–ZDNet, “Eighty percent of new malware defeats antivirus”, *ZDNet*, viewed 19 July 2006, <http://www.zdnet.com.au/news/security/soa/Eighty_percent_of_new_malware_defeats_antiviruses/0,2000061744,39263949,00.htm>.

“Symantec Corp.'s leading antivirus software, which protects some of the world's largest corporations and U.S. government agencies, suffers from a flaw that lets hackers seize control of computers to steal sensitive data, delete files or implant malicious programs, researchers said on Thursday.”

–Sydney Morning Herald, “Flaw found in anti-virus program”, *Sydney Morning Herald*, viewed 26 May 2006, <<http://www.smh.com.au/news/security/flaw-found-in-antivirus-program/2006/05/26/1148524847847.html>>.

“According to the results of the AusCERT 2006 computer crime survey, even though 98 percent of companies used an antivirus product, almost half of them experienced a virus infection over the past year.”

–Zdnet, “Antivirus software 'is being defeated””, *ZDNet*, viewed 23 May 2006, <http://www.zdnet.com.au/news/security/soa/Antivirus_software_is_being_defeated_/0,2000061744,39257227,00.htm>.

“In the ultimate slap in the face, the world's largest anti-virus vendor Symantec has had its identity spoofed by a virus purveyor. A high risk malicious email, which appears to be a Symantec virus advisory, but actually is an e-mail that contains a payload that disables anti-virus updates, was discovered by another internet security services provider.”

–iWire, “Symantec gets spoofed by virus purveyor”, *iWire*, viewed 19 April 2006, <<http://www.itwire.com.au/content/view/3955/53/>>.

▼ Constantly evolving security threats

“Educating users to recognise potential phishing scams may no longer be an effective tool because recent attacks are so sophisticated that fraudulent sites were virtually indistinguishable from the original, according to MessageLabs.”

–Kotadia, M., “Education no longer enough to combat phishing?”, *ZDNet Australia*, viewed 20 September 2006, <http://www.zdnet.com.au/news/security/soa/Education_no_longer_enough_to_combat_phishing_/0,130061744,339271203,00.htm>.

“As security technologies have matured to address the types of flaws typically exploited by traditional attacks, attackers have shifted their focus to new attack vectors. Further, as technological solutions are proving increasingly more effective, attackers are reverting to older, non-technical means of compromise, such as social engineering, in order to launch successful attacks. Attackers are thus shifting attack activity away from network infrastructures and operating system services toward attacks that focus on the end user as the weakest link in the security chain.”

–Symantec, “Symantec Internet Security Threat Report – Trends January 06 – June 06”, Volume X, September 2006. See: <http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf>.

“In three years phishing has transformed from an unknown threat into a multi-million dollar industry; in the next stage of their evolution, phishers will be able to avoid sending spam and bypass anti-phishing tools by hijacking small parts of 'trusted' Web sites.”

–ZDNet Australia, “Web 2.0 makes phishing spam obsolete”, *ZDNet Australia*, viewed 12 September 2006, <http://www.zdnet.com.au/blogs/securifythis/soa/Web_2_0_makes_phishing_spam_obsolete/0,139033343,339270982,00.htm>.

"In the never-ending cat-and-mouse game between hackers and those charged with stopping them, it's pretty clear who's winning--and it's not the cat. Speaking at the Black Hat conference in Las Vegas last week, Kevin Mandia, president of Mandiant...[a] security consultancy, said attackers are using increasingly sophisticated methods to evade detection and make life difficult for security incident response teams."

–iWire.com.au, "Hacker sophistication outpacing forensics", *iWire.com.au*, viewed 10 August 2006, <<http://www.itnews.com.au/newsstory.aspx?ClaNID=35748&eid=3&edate=20060810>>.

vi Consumer research on Internet auctions

See: Moustakas, N 2006, "Online auctions: user protection and liability issues", *Communications Law Centre*, Melbourne. Available at: <http://www.comslaw.org.au/auction/>

vii Confusing security terminology

"Anti virus vendors historically pick a name for each piece of malware that they detect. As different vendors assign different names, end users can get confused when malware outbreaks are covered in the media."

–ITnews.com.au, "Security sector rethinks common virus names", *ITnews.com.au*, viewed 21 July 2006, <<http://www.itnews.com.au/newsstory.aspx?ClaNID=35099&eid=1&edate=20060721>>.

viii Size of the Internet security market

"The global Internet security market is estimated to be about \$27.7 billion in 2005 and is expected to rise at an average annual growth rate (AAGR) of 16.0%, reaching \$58 billion by 2010."

–BCC Research, "SAS012 Internet Security", *BCC Research*, viewed 20 September 2006, <<http://www.bccresearch.com/sas/SAS012A.asp>>.

ix 8 Basic Consumer Rights

As adopted by the United Nations Assembly on 9 April 1985: The right to safety, The right to be informed, The right to choose, The right to be heard, The right to satisfaction of basic needs, The right to redress, The right to consumer education, and The right to a healthy environment.

See: <<http://www.fairtrading.qld.gov.au/oft/oftweb.nsf/web+pages/ABDDDD88B517CA84A256B410081D4C2?OpenDocument>> and <<http://www.un.org/documents/ga/res/39/a39r248.htm>>.

x "Fewer than half of the UK's 29m adult internet users believe they are responsible for protecting personal information online, a survey suggests."

–BBC News "Many net users 'not safety-aware'", BBC News, Accessed April 13, 2007 from: <http://news.bbc.co.uk/2/hi/technology/6472723.stm>.