



**Project on Strengthening Technical Competency for  
Consumer Protection in ASEAN**

# **Phones Internet Services & E-commerce**

**Version 21 January 2016**



The overall objective of the project is to "enhance AMS with effective capacities to adopt and implement consumer protection laws at the national level". The project should build/strengthen capacity of government agency personnel through the design, development and delivery of training programs, modular components and materials, focusing on technical requirements provisionally involving consumer concerns and demands in 6 core areas, as identified in the AADCP II Project Report on "Road-mapping Capacity Building Needs in Consumer Protection in ASEAN" (AADCP report) in 2011. These areas are: 1) Product safety and labelling; 2) Phone and internet services, and e-commerce; 3) Consumer credit and banking; 4) Environment; 5) Healthcare services; and 6) Professional services. For further information about the project, please contact the ASEAN Secretariat, Ms Yap Lai Peng ([yap@asean.org](mailto:yap@asean.org)) or Ms Sarah Firdaus ([sarah.firdaus@asean.org](mailto:sarah.firdaus@asean.org)), and Mr. Pierre Horna ([pierre.horna@unctad.org](mailto:pierre.horna@unctad.org)), Manager of the Project on Strengthening Technical Competency for Consumer Protection in ASEAN.

This report has been drafted by UNCTAD Ad-hoc consultant Carl Buik. Our special thanks to the ASEAN Secretariat for an excellent partnership and the AADCP II for the trust given to UNCTAD in executing the present project



## Table of contents

<b>Executive summary.....</b>	<b>5</b>
<b>Glossary.....</b>	<b>7</b>
<b>I. Introduction.....</b>	<b>10</b>
1.1 The effective use of these technologies is central to economic growth and increased consumer welfare.....	10
1.2 Some requirements for effective use of the technologies.....	10
1.2.1 Access.....	11
1.2.2 Confidence.....	11
1.3 Consumers use of phones, the Internet and e-commerce.....	12
1.4 Consumer protection needed online as it is in traditional or 'bricks and mortar' markets.....	13
1.5 Consumer experiences in using these technologies can be made better.....	13
<b>II Online consumer protection: the market, behavioural and public intervention contexts.....</b>	<b>16</b>
2.1 Market conditions.....	16
2.2 Consumer behaviour features.....	17
2.3 The rationale, limits and scope of public intervention.....	18
2.4 Technology neutral and technology specific regulation.....	21
<b>III. Some broad observations about the technologies relevant to consumer protection.....</b>	<b>23</b>
3.1 Phones.....	23
3.2 The Internet.....	27
3.3 E-commerce.....	29
3.4 Some implications for consumers and governments.....	30
3.4.1 Regulatory responsibility.....	31
3.4.2 The benefits of interagency co-operation.....	32
<b>IV. The principal consumer protection issues in respect of consumers use of telecommunications technologies.....</b>	<b>34</b>
4.1 How do we know what problems consumers are encountering?.....	35
4.2 Consumer protection issues identified from international experience.....	37
4.2.1 Misleading conduct.....	37
4.2.2 Unfair contract terms.....	40
4.2.3 Scams using phones, the Internet and e-commerce.....	43
4.2.4 Cross border purchases.....	50
4.2.5 On-line security.....	51
4.2.6 Malware.....	51
4.2.7 Data protection and privacy.....	53
4.2.8 Secure payments.....	56



4.3	Some strategies for addressing the most frequently experienced consumer problems.....	59
4.3.1	Consumer education.....	59
4.3.2	Business education.....	67
4.3.3	Interagency co-operation.....	69
4.3.4	Effective investigations by consumer protection authorities.....	80
4.3.5	Capacity building to support more effective regulatory responses to the principal problems associated with consumer use of telecommunication technologies.....	91

<b>Appendixes.....</b>	<b>93</b>
------------------------	-----------

<b>Appendix 1:</b> Status of e-commerce law harmonization in ASEAN as of March 2013....	94
<b>Appendix 2:</b> Presentations delivered at the Training Workshop in Manila.....	95
<b>Appendix 3:</b> ACCC media releases.....	97
<b>Appendix 4:</b> Example emails of Scams.....	124
<b>Appendix 5:</b> Exercises and scenarios used at the Manila Workshop.....	140
<b>Appendix 6:</b> Questions to the design and delivery of training workshops on e-commerce..	153
<b>Appendix 7:</b> Further reading.....	158



## Executive summary

1. Efficient and effective use of phones and the Internet are essential building blocks in 21st century economies, whatever their stage of development. While the current contribution of these technologies may still be restricted by access, pricing and other regulatory issues, consumers and traders are 'voting with their feet' by constantly finding new and innovative ways to use the technologies to facilitate the buying and selling of an ever increasing range of goods and services.
2. In traditional 'bricks and mortar' markets consumers undertook pre-purchase research by talking with salesmen and friends, seeing advertisements in-store, in print and on TV and radio. Because the range of information sources was limited and largely local they could more easily form opinions about the reliability of these information sources. Of course this is no fool proof and consumers have always been subject to harms from the actions of careless or unscrupulous traders.
3. When consumers use their phones or computers to do pre-purchase research they lack many of the contextual indicators they are used to using, such as the appearance and location of the trader, its goods, staff and shop. Also the consumer is often alone as they access the net rather than walking with friends or family through a physical market.
4. In traditional transactions the goods and any relevant documentation (such as a contract, instructions, warranties etc.) are physically present when cash is handed over. Again, unscrupulous traders have always found away to deceive consumers, but the scope and scale of that deception was limited. In online transactions, not only are the goods and documents not physically present, cash has given way to various electronic means of payment.
5. Post purchase actions such as warranties claims and repairs may also be more difficult because the consumer and trader are physical distance from each other. All that means that when consumers go online, they are subject to the problems associated with traditional markets and some new risks. The very attributes that make online markets so attractive also magnify existing risks and generating new risks.
6. The good news is that consumer experiences in using these technologies can be made better. At the very least consumers reasonable expect that that regulatory protection they receive from legislation and regulators will be no less that the protection they currently enjoy in the 'bricks and mortar' world of traditional markets. At various levels this has been recognised within ASEAN and significant progress made and planned, particularly in respect of legislation.
7. Before discussing some of the strategies that might be used to improve consumer outcomes this paper briefly looks at the market, behavioural and regulatory contexts in which consumer use the technologies. It also explains some of the more commonly encountered consumer problems, including many of the scams that plague our online lives. Trainers must maintain an understanding of this content: the examples given in this paper are topical now. However, just as the technologies are evolving, so to are the particular problems confronting consumers.



8. The paper concludes that there is no one instant fix to providing effective on-line consumer protection, as there are a number of contributing elements including:

- Understanding the nature, cause and cost of the various problems consumer experience when using the technologies.
- Having in place legislation that defines relevant conduct and provides for appropriate standards setting and enforcement.
- Having the capacity and desire to enforce the existing laws, particularly by robust investigations.
- Having the capacity and desire to undertake comprehensive and sustained consumer and trader education activities.

9. It is the opinion of the author that consumer protection authorities should consider prioritising consumer/trader education and active enforcement that can be implemented immediately, rather than delaying action pending the arrival of the perfect legislative suit. Not all online consumer problems can be immediately resolved by legislation or enforcement action by regulators. Effective consumer and trader education can play a very significant role in helping consumer to help themselves online by understanding the risks and implementing preventative strategies and actions as they use their smart phones and computers to access the net. It follows that the paper recommends capacity building initiatives reflect that same priority.

10. It is expected that workshop participants will subsequently undertake capacity building training within their own and other agencies. This paper provides an introduction to the challenges facing consumers as they use the technologies, provides explanations of investigation process and suggestions for priority 'messages' to be included in consumer education.

11. This paper is accompanied by workshop exercises designed to encourage participants to think critically about this paper's content and its application to typical consumer protection agency functions. The principal learning outcome should be more than simply additional knowledge about consumer problems experienced when using the technologies. We need to understand how the technologies contribute to both the problems and to their solutions. We need leave the workshop with a confident appreciation of when and why particular compliance responses will be appropriate,

12. In this paper the short cut term 'consumer protection authority' is used to include any and all authorities that have responsibility for any aspect of consumer protection for consumers when they use phones and computers to access the Internet to purchase goods or services (e-commerce) or for any other purpose preparatory or subsequent to online purchases. Around the world, national regulatory responsibility for on-line consumer protection is shared by a number of ministries or authorities, and ASEAN member states are no exception to this observation.

13. The challenge for authorities with consumer protection responsibilities is to work co-operatively to deliver a consumer protection multiplier effect from their combined respective



efforts. The alternative of operating in regulatory silos will inevitably lead to diminished consumer protection outcomes. For individual consumers this may mean financial losses or other harms.

14. Collectively, consumers will have reduced confidence in on-line transactions. Reduced confidence means suboptimal use, with the result that economic development will be below the potential promised by effective use of these telecommunication technologies.

15. The bottom line is that enhanced protection for consumers when they use their phones and computers to access the Internet makes good sense, economically, socially, for individual consumers and traders, for national economies and for the ASEAN region.

16. Key principles in the development of the Training Module:

- Protection: Consumers should be protected from unfair practices.
- Responsibility: Transparent legislation in addition to effective consumer and business education programmes to enable consumers and traders to have sufficient information in order for them to exercise their respective responsibilities and protect their own interests.
- Enforcement: There should be prompt and efficient enforcement of legislation to deter breaches of the consumer protection laws by businesses.
- Change: new and emerging consumer issues are identified so that legislation is updated and consumers have access to relevant information on these issues in order to make informed choices
- Competition: Free and open competition is generally beneficial for consumers and Government regulations and legislation help to ensure a fair environment in the marketplace for consumers and businesses.
- Representation: Legitimacy for representation by non-governmental consumer organisations must be recognised including the right to association.





## Glossary

- Apps:** an application is software designed for a particular purpose. An 'app' is generally used to mean an application designed to run on a mobile device such as a smart phone or tablet.
- B2B:** Business to business transaction
- B2C:** Business to consumer transaction
- B2G:** Business to government transaction
- Bricks and mortar:** a term used to describe convention markets where traders have a physical presence to distinguish them from on-line (or virtual) markets
- Broadband:** A high speed connection to the Internet
- Browser:** A web browser (commonly referred to as a browser) is a software application for retrieving, presenting and traversing information resources on the World Wide Web (the Net). The major web browsers are Firefox, Internet Explorer, Google Chrome, Opera, and Safari.  
[http://en.wikipedia.org/wiki/Web\\_browser](http://en.wikipedia.org/wiki/Web_browser)
- e-commerce:** buying or selling online, that is over the Internet
- e-commerce platforms:** e-commerce platforms are services that allow traders to outsource [all or part of] their transactions processes to an outside firm. (ref DSTI/ICCP/IE/IIS(2012)1/FINAL). Well know examples are eBay and Amazon
- e-fulfilment:** delivery of goods ordered through e-commerce.
- e-payment:** methods of payment used in e-commerce, including online payments (made via the internet using credit and debit cards, online direct bank transfers, Bpay, electronic currency systems) and mobile payments (which can be on-line payments made via a mobile device, via SMS or payments charged to the consumers mobile account)  
(ref DSTI/ICCP/IE/IIS(2012)1/FINAL)
- EDI:** Electronic data interchange
- Elasticity of demand/supply:** Demand/supply elasticity is a measure of how much the quantity demanded/supplied will change if another factor changes. One example is the price elasticity of demand; this measures how the quantity demanded changes with price.  
Ref [www.investopedia.com/terms/d/demand-elasticity.asp](http://www.investopedia.com/terms/d/demand-elasticity.asp)
- ICPEN:** The International Consumer Protection and Enforcement Network is an international organisation whose members are national consumer protection authorities. See [www.icpen.org](http://www.icpen.org)
- Internet:** a worldwide computer network with standardised protocols providing an interconnectivity that allows for complex communications, information searching and transactions between people
- ISP:** Internet service provider (ISP)
- Malware:** Malware is short for "malicious software." Malware is any kind of unwanted software that is installed without the users adequate consent. Viruses, worms, and Trojan horses key loggers and other spyware are examples of malicious software that are often grouped together and referred to as malware.





Malware is mostly created for profit through forced advertising (adware), stealing sensitive information (spyware), spreading email spam or child pornography (zombie computers), or to extort money (ransomware).

<http://www.pctools.com/security-news/what-is-malware/>

**M-commerce:** Irrelevant or unsolicited messages sent over the Internet, typically to large numbers of users, for the purposes of advertising, phishing, spreading malware, etc.

**Mobile devices:**

a general term to include smart phones and tablets (such as the iPad) and smart watches to distinguish them from computers, including desk tops and laptops

**PCW:** Price comparison websites (PCW) are sites representing that users can compare prices between products or vendors.

**NFC:** Near field communications

**Search engine:**

A web search engine is a software system that is designed to search for information on the World Wide Web

**Popular search engines include:**

Google, Baidu, Bing, and Yahoo!

[http://en.wikipedia.org/wiki/Web\\_search\\_engine](http://en.wikipedia.org/wiki/Web_search_engine)

**Smart phone:** a mobile phone that can be used to run a number of applications (apps) and access the internet in addition to making calls as a conventional mobile phone to make calls. Smart phones typically have a touch screen as the user interface.

**Social networking:**

Social networking services [are on-line] platforms to build social networks or social relations among people who share interests, activities, backgrounds or real-life connections. The most popular social networking services are Facebook, Twitter, LinkedIn, Pinterest, Google Plus+, Tumblr and Instagram

[http://en.wikipedia.org/wiki/Social\\_networking\\_service](http://en.wikipedia.org/wiki/Social_networking_service)

**Spam:** Irrelevant or unsolicited messages sent over the Internet, typically to large numbers of users, for the purposes of advertising, phishing, spreading malware, etc.

[www.oxforddictionaries.com/definition/english/spam](http://www.oxforddictionaries.com/definition/english/spam)

**Virus:** A piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

[www.oxforddictionaries.com/definition/english/virus?q=computer+virus#virus\\_\\_7](http://www.oxforddictionaries.com/definition/english/virus?q=computer+virus#virus__7)



## I. Introduction

17. Mobile phone and Internet access services are telecommunications technologies that allow citizens to communicate with others at a distance, both in their capability as private individuals and as consumers. They are not the first technologies to allow long distance communications, but their particular attributes, costs and capabilities have combined to transform the lives of consumers. In particular these technologies have facilitated the development of e-commerce, the virtual market place where consumers and traders buy and sell using the technologies.

18. Throughout this paper two terms are used extensively:

- 'Online': this term is used as a short cut to refer to transaction involving mobile phones (including smart phones), the Internet and e-commerce.
- 'Bricks and mortar': this term is used as a contrast to 'online' and refers to traditional market places (shops) and older technologies

### 1.1 The effective use of these technologies is central to economic growth and increased consumer welfare

19. Effective use of these online technologies delivers benefits to both consumers and businesses:

- Consumers enjoy increased choice (in quality, price and other attributes) because they can now select from a larger range of products/services than traders to better match their needs.
- Consumers can benefit from increased competition as more traders compete for their custom (innovation, lower prices)
- Consumers can lower their search and transaction costs
- Traders can potentially make offers to a great number of potential customers. If those increased offers become increased sales, there may be economies of scale and scope to be realized, further boosting profits
- Traders can make significant saving in marketing and transaction costs

### 1.2 Some requirements for effective use of the technologies

20. Effective use of these technologies by consumers requires consumers to have:

- Access to and performance of the telecommunications technologies; and
- Confidence that their use of the technologies will be advantageous



### 1.2.1 Access

21. Access to and use of these technologies is well established and widespread in each ASEAN country, although variable as between countries. Publically available data indicates that in all ASEAN more than 50% of the population have access to and frequently use mobile phones. A significant and increasing proportion of these mobile phones are smart phones capable of accessing the net. Most consumers with access to smart phones have used it for one form of e-commerce or another, while an increasing percentage frequently use their smart phones for at least a component of their transactions, whether they eventually purchase on-line or from a traditional 'bricks and mortar' trader.

22. Publically available data indicates that access to the net is enjoyed by a significant and growing percentage of consumers across ASEAN, although of course that proportion varies between counties. Consumers access the net:

- From desktop and laptop computers and mobile devices such as smart phones and tablets
- From their own devices or devices at kiosks, libraries, places of work
- On variable bandwidths (affecting speed, reliability and what sites accessed and activities may undertaken)
- Under various arrangements (for example, free access, prepaid, fixed and variable cost contracts)
- Under various regulatory regimes, that can affect what sites may be accessed, privacy and protections available

### 1.2.2 Confidence

23. Consumer confidence is an important, although intangible requirement of their participation in any market. A general definition of 'confidence' is 'the feeling or belief that one can have faith in or rely on someone or something'. In this paper consumer confidence is thought of as:

'Consumers can be said to have confidence in a market (bricks and mortar or online) if they believe that the risks of doing business are small and manageable. If consumers lack confidence in any market (the goods/services, the trader or the process) they unconsciously or consciously convert their concerns into an additional cost of doing business (completing a transaction). When consumers are confident they are more willing to try new products and traders, and to buy more.'

24. The building blocks of consumer confidence include consumers:

- Being aware of the potential hazards and having the knowledge of strategies to avoid them and mitigate harms
- Having an ability to implement the strategies to avoid them and mitigate harms

- Knowing that there are laws and other regulations in place to prohibit harmful conduct, create liability of harm caused and facilitate remedies
- Knowing that they can do something practical if they have a problem. For example, lodging a complaint with an authority or NGO that has the capacity to:
  - Investigate
  - Obtain redress

25. protection whether they buy online or in bricks and mortar markets. That is consumer protection will be technology neutral. This is not an endorsement of the current levels of consumer protection, because:

- That clear varies as between ASEAN member states and
- There will always be a need to improve the efficacy and effectiveness of consumer protection, particularly in new or rapidly evolving markets or for vulnerable consumer groups
- Improving the effectiveness and efficiency of online consumer protection will do more than improving consumers' confidence about using telecommunications technologies. Improving online consumer protection will have positive flow on effects to consumer protection more generally because most of the problems and the strategies to address them are not unique to online transactions.

### **1.3 Consumer use of phones, the Internet and e-commerce**

26. Consumer use of phones, the Internet and e-commerce is increasing, however measured: in number (interactions and transactions), the range of activities and the complexity of activities. Broadly common uses include:

- Free entertainment and information
- For example surfing the net to view information sites without entering into a transaction with the content provider, for example to explore news and government sites
- Social interaction, for example emails to family and friends, social network sites to communicate with family and friends
- Transactions, including both bricks and mortar and e-commerce transactions. This may include:
  - pre-purchase research or shopping around
  - purchasing
  - post purchase interactions, including usage information (manuals, troubleshooting), delivery information, warranty issues, refunds etc.



27. Increasingly businesses are relying on consumers using the technologies. While this is obvious in respect of e-traders with no physical presence in consumers village/city/country, it is becoming increasingly true of bricks and mortar traders, many of whom:

- Maintain websites to advertise their businesses and products even if they have not yet expanded to online sales.
- Encourage consumer to go online as a means of reducing costs, for example for paying accounts or resolving problems encountered with the use of products.

#### **1.4 Consumer protection needed online as it is in bricks and mortar markets**

28. While the experience of most consumers using these technologies, most of the time, is beneficial and without problems, that is not always the case. As in any other area of consumer activity there are always those who will take the opportunity to exploit consumers for their own gain and against the interests of consumers. Additional harms are caused when otherwise legitimate traders do not manage their consumer protection compliance risks and consumers do not act in their own best interests.

#### **1.5 Consumer experiences in using these technologies can be made better**

29. The good news is that the consumer experiences in using these technologies can be made better. The incidence of problems can be reduced and the severity of harm caused lessened. The immediate payoff will be consumers who will be more confident in using their mobile devices and computers to access the net and to purchase online. The longer-term payoff will be an expansion in economic activity to the synergistic advantage of consumers and businesses in each ASEAN member state. In other words improved consumer outcomes is good news for business.

30. Improving consumer experiences requires a mix of strategies including:

- More effective enforcement of existing regulation
- The majority of ASEAN member states have existing consumer protection laws that are technology neutral in their application and laws addressing cybercrime and electronic transactions. Several jurisdictions have active enforcement regimes, while in others enforcement is developing. Active enforcement of existing laws need not be delayed pending other developments.
- Easier access to a range of low cost/no cost systems for quick and fair resolution of consumer complaints.

This issue was identified and addressed in ASEAN-Australia Development Cooperation Program Phase II: Supporting Research and Dialogue in Consumer Protection Consumer protection laws and regulations for online purchasing.

- Expanded consumer education by consumer protection authorities, sector regulators and infrastructure providers

- Expanded roles for business associations and individual traders, including the infrastructure providers to ensure comprehensive compliance with consumer protection laws
- More effective and efficient interagency co-operation at the national, regional and global levels
- Filling in legislative gaps by enacting new national laws as identified

This issue was identified and addressed in ASEAN-Australia Development Cooperation Program Phase II: Supporting Research and Dialogue in Consumer Protection Consumer protection laws and regulations for online purchasing.

- Harmonization of general consumer protection laws and technology specific consumer protection laws across ASEAN.

It is noted that the Chiang Rai Declaration on Consumer Protection in Telecommunications proposes that various stakeholder groups work together to propose a basic standard for consumer protection in telecommunications

31. Much work has already been done in respect of e-commerce within the ASEAN region at both the national and regional levels. Individual countries have enacted legislation and adopted policies that directly or indirectly address consumer issues in respect of these technologies (See attachment 1).

32. Brunei Darussalam, Indonesia, Malaysia, Philippines, Singapore, Thailand and Vietnam are members of APEC whose Electronic Commerce Steering Group (ECSG) promotes the development and use of electronic commerce 'by creating legal, regulatory and policy environments in the APEC region that are predictable, transparent and consistent'.

(see [www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx](http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx))

33. Additionally there have been reviews of the 'state of play' and recommendations for action. In particular this paper follows on from UNCTAD's Review of e-commerce legislation harmonization in the Association of Southeast Asian Nations 2014 and does not seek to go over issues of legislation.

34. This paper is also informed by recent work undertaken for ASEAN that looked in detail at complaint systems and redress models: Models for internal complaint systems and external consumer redress schemes in ASEAN & Development of Redress Mechanism Models in ASEAN: Output 8 & 9 Guidelines for the selection and implementation of complaint and redress models 2013. While this paper does refer to complaint handling and redress, it does not duplicate the detail of these documents.

35. How different are consumer protection issues identified in this paper from consumer issues elsewhere?





For the most part the problems encountered by consumers online are the same as they experience in the brick and mortar world. However the mix of problems, their incidence and severity of harm are often different.

36. The emphasis in this paper is on the issues that can be best addressed by capacity training. Issues relating to legislative and policy gaps have been comprehensively addressed by other recent projects as noted throughout this report.

37. Given the common theme of 'consumer protection' it is to be expected that there is some overlap between the various papers written for this project. Where possible topics that are covered in one or more of these papers are only referred to briefly in this paper.



## **II. Online consumer protection: the market, behavioural and public intervention contexts**

### **Learning objectives and outcomes of Section II**

38. This section of the train-the-trainer manual describes:
- the broad market conditions in which consumers use phones, the internet and e-commerce
  - some of the important behavioural characteristics that drive consumer use of these technologies
  - the rationale, limit and scope of public intervention
  - the significance of technology neutral and technology specific regulation
39. Following completion of the train-the-trainer sessions, participants should be able to:
- discuss the potential direct and indirect effects of regulation in respect of consumer protection outcomes
  - discuss the pros and cons of technology neutral v technologic specific regulation
  - give examples of where supply side policy objectives can enhance or hinder enhanced consumer protection outcomes

### **2.1 Market conditions**

40. Phone, Internet services and e-commerce are usually defined by their respective technologies and may be grouped together under the umbrella of 'telecommunications'. While they have many similarities in respect of their respective demand and supply conditions, there are some significant differences between the three services that are relevant to consumer issues.

41. Phone, Internet services and e-commerce are all driven by technological innovation and allow an immediacy of communication that was not possible by in-person shopping or even by post.

42. All three forms of telecommunication offer supplies significant economies of scale and scope and reduce the significance of physical distance between consumers and traders. Consequently worldwide connectivity is intrinsic to the value of these services and an essential attribute to most consumers.

43. As a generalization, continuing technical innovations in these telecommunication services is providing increasing numbers of consumers with access, cheaper prices and



increased utility. However, consumer access to and costs of using these technologies varies significantly between ASEAN member states.

44. In each member state, as in countries around the world, government regulates which entities (government owned and/or private sector businesses) are able to provide telecommunications services and under what conditions. In some countries, for example Singapore and Brunei) government (or state) owned enterprises (SOEs) are also major providers of telecommunications and other Internet related services such as ISPs.

45. Government policy and its application through regulation may impact directly on consumers in many ways:

- What services can be provided
- What content can be accessed
- The terms of service, including price, performance
- The available processes for resolution of consumer problems.

46. Very importantly government policy and regulation will affect the existence and intensity of competition between service providers. The forces of competition can be a powerful driver of consumer protection as competitors vie for customers, and customs exercise choices about which traders and which products or services they will purchase. While an effective competition policy and law are arguably the single most effective consumer protection policy and law, competition issues are beyond the coverage of this paper.

47. While the provision of mobile phone services and access to the internet is generally supplied on a national market basis and therefore amenable to national regulation, many consumer transactions undertaken using the technologies are cross border (international) with the implication that while national regulation is necessary, other market influencing strategies may be significant contributors to improving consumer experiences.

## **2.2 Consumer behavioural features**

48. Generally consumers are not the passive victims they are some times made out to be. Most consumers use a variety of strategies to prioritize their needs and wants, and to make purchases that will maximize their overall welfare and the utility from individual purchases. However, sometimes these collective and individual strategies do not maximize either aggregate consumer welfare or individual welfare. For example, individual consumers are more likely to make economically suboptimal decisions when non-economic objectives are more important. For example young consumers are more likely to choose a mobile phone and service provider if their friends have that product and service.

49. When using telecommunications consumers may miss out on many of the visual and contextual indicators (such as a physical appraisal of the goods on offer, the appearance and demeanour of traders and the location and appearance of their shop) that they are used to using when they contemplate purchases in traditional shops. If consumers are unaware of

some of the risks, or underestimate the risks associated with using telecommunication services they will not give risk avoidance strategies sufficient priority.

50. As noted above consumers may notionally underutilise these technologies if they lack confidence in respect of online transactions as compared with brick and mortar transactions. An important behavioural aspect of consumers in respect of telecommunications is the different level of product/service understanding and usage between different groups of consumers. For example teenagers and educated adults are generally more knowledgeable about and are greater users of these products and services than are older adults. Increasingly children are using some of these services unsupervised by adults, even though their ability to avoid consumer problems is often not sufficiently developed. There is also often a knowledge and usage divide according to education, income and location (for example between city v rural).

51. The implications of these observations are that:

- Various groups of consumers are likely to experience different problems and at differing degrees of severity
- Appropriate strategies for the most effective and efficient resolution of consumer problems may vary between groups.
- A continuous program of empowering consumers through education and the provision of clear accurate information about the products and services will need to be continuous and evolving, as new consumers enter the market and the market itself evolves.

52. Consumer protection agencies will need the ability to respond to problems with a range of enforcement responses. These should include:

- effective consumer and trader education
- encouragement of trader compliance programs
- industry codes of conduct, including trust mark schemes
- multiple dispute resolution mechanisms
- efficient and robust and well managed investigations
- a broader range of available sanctions and remedies
- routine and ad hoc interagency co-operation

## **2.3 The rationale, limit and scope of public intervention**

53. Conventional economic theory shows that market forces will maximize aggregate consumer welfare, but only when there are few significant impediments to competition. The market forces that protect consumer interests are driven by a combination of informal and formal processes of varying effectiveness:

- Consumers looking out for themselves. For example by shopping around to find out what products are available from different traders at different prices and quality. The significantly lower cost and greater convenience of online research is a significant and direct benefit to consumers, and ultimately to more efficient traders.
- Businesses responding to changes in consumer demand and the actions of their competitors, so as to maximize their individual profits. For example by changing prices, products, advertising, location, opening hours etc. Online technologies significantly increase the ability of traders to evaluate changing consumer demand, the activities of their competitors and to inform consumers about how they are responding.
- Social pressure on traders to treat consumers fairly. On one hand, online technologies greatly amplify and accelerate the processes of social pressure via social media, blogs, emails and customer feedback processes. On the other, the ability to remain anonymous can encourage irresponsible or ill-founded comment and criticism.
- Active media and consumer organizations exposing consumer problems, for example naming and shaming, trader and product/service evaluations and comparisons etc.
- Private enforcement of rights under consumer laws protection law(s) that provide the potential for remedies without public intervention.
- More effective investigations have been facilitated by these same technologies. For example, investigators can search online and observe trader conduct as it occurs and they can obtain evidence of representations, communications, documents and money transfers transmitted and stored electronically.

54. If market forces maximize consumer welfare, then why would there be a debate about the rationale, limits and scope of public intervention?

55. Some level of public intervention will be necessary because:

- Although many consumer detriments such as unsafe goods or fraudulent behaviours will eventually be rendered unprofitable in an efficient, competitive market, there will always be an adjustment period during which some consumers will suffer harm. In some cases the severity or incidence of such harms will be unacceptable to the community who will expect public intervention. In all cases these harms will affect individual and collective consumer confidence, as noted above.
- Unlike the impression given by simplistic supply and demand graphs typically used in introductory presentations, efficient, competitive markets usually result in a wide range of goods and services being traded at varying prices and qualities. It may sometimes be that the market equilibrium results in goods or services causing long-term harm to consumers survive in the market. There can be many reasons for this, for example because:
  - the problematic characteristics of the goods or services are not apparent to consumers at the time of purchase.

- consumers often put a higher value on short term benefits versus longer term effects
- the person buying the goods or service is not the person ultimately consumer them (for example in the case of gifts or components of bundled supply) and may place less emphasis on quality and safety than might the final consumer, or
- people on very low incomes have no practical alternative than to purchase the cheapest goods on offer despite the risks.
- Stakeholders including consumers, consumer organizations, businesses, business organizations and government have goals in addition to simply maximizing aggregate welfare that may not be achieved by market forces alone. For example goals such as, fairer income distribution, elevating poverty, regional development and sector development.

56. Some markets have significant impediments to competition with the result that market forces are weakened or distorted. These distortions may be the result of impeded availability of information relevant to consumers purchasing decisions, for example because problematic characteristics of goods or services are not apparent to consumers at the time of purchase.

57. There can be many reasons for the ineffectiveness of the forces of competition including:

- ineffective or non-existent consumer associations
- low levels of access to independent sources of information such as the media, including online media
- significant levels of ah hoc or non-sustained imports, for example when a batch of sub-standard goods are dumped on a market
- the misuse of significant market power by individual businesses
- anticompetitive arrangements between businesses in a market
- the intended consequence of government intervention, for example when government policies are directed improving the competitiveness of local manufacturers intentionally increases the cost of imports.
- the unintended consequence of government intervention. An example might be when a policy to prevent misleading advertisements unintentionally makes all advertising more difficult and costly by imposing high compliance costs
- structural characteristic of particular markets. For example natural or legislated monopolies.
- market forces are dynamic, resulting in an ever-changing market place that may reveal consumer detriments not previously foreseen.
- It is important to recognize that public interventions vary in the effectiveness and efficiency:

- They can be easier or harder to ignore, avoid or mitigate
- They can be narrower or wider in their application
- They can have more, or less, collateral (unintended) effects

58. Markets (and hence market problems) are dynamic: what may be an effective and/or efficient intervention today, may not be tomorrow. Interventions that facilitate more informed choice by consumer or business are more likely to be effective in the long run than prescriptive intervention that restricts choices. Interventions that affect essential elements of supply such as price setting or whether particular goods or services can be supplied at all, are more likely to directly and predictably affect consumers purchasing decisions.

59. All market intervention has a cost. These costs may be direct and easily identified or indirect and hard to identify and quantify. Who ultimately pays for interventions will depend on the elasticities of supply and demand. For example the costs of compliance will be readily passed on to consumers in the form of higher prices where demand is only weakly affected by price. This may be the case with many basic services such as mobile phone services. Furthermore, in response to limited resources it is imperative that government agencies be strategic about how, when and where they intervene, so that they and consumers get the best value for money.

60. Anticipating the ultimate effect of an intervention requires a thorough understanding of the market dynamics. For example before prescribing a set or maximum price for a particular product or service, it is important to understand how the current price came about. In a situation where the size of the market and economies of scale suggest that there will only ever be one supplier there may be an argument for prescribing a price that makes the products/services available to more consumers. However, in other market conditions the prescription of a set or maximum price may significantly reduce the availability of the relevant goods or services or deter new entrants who would bring competitive pressures to the market and ultimately drive process down.

## **2.4 Technology neutral and technology specific regulation**

61. Building on the comments about technology neutrality above, the premise underlying this paper is that consumers expect that they will have the same protections when they use electronic technologies and go online, as they do in the tradition bricks and mortar markets. That is, they expect that consumer protection is technology neutral.

62. Most consumer protection laws are technology neutral. This means that they apply generally to matters affecting consumers regardless of how the transaction takes place. For example prohibitions on misleading advertising generally apply to all forms of advertising, from roadside signs to pop-up ads on websites. This general application happens by default when the law is cast in general terms and does not refer to specific technologies. The advantages of technology neutral laws are that:





- They do not have to be amended to maintain consumers' protections as they and traders sell products and services involving new technology, or they adopt new technologies for making their transactions
- The protection provided to consumers and the compliance costs borne by traders (and ultimately shared by consumers through increased prices) does not have an anticompetitive effect by affecting relative costs between technologies.

63. Some consumer protection laws may be technology specific because the relevant protection:

- Must be expressed in technology specific terms to be effective; or
- Is only relevant with reference to a specific technology

64. In ASEAN countries, as elsewhere laws that address consumer protection issues are not all neatly labelled as 'consumer protection' and their enforcement often not even the responsibility of a designated 'consumer protection authority'. This is certainly the case in respect to mobile phones, the Internet and e-commerce as the table shown as Attachment 1 shows. While the UNCTAD Review of e-commerce legislation harmonization in ASEAN 2013 identified 'consumer protection' as a category of regulation it is readily apparent that other categories of Internet related laws all have consumer protection elements and effects. And it is also the case with product safety and labelling (see the session and paper 'Product Safety and Labelling' Session).

65. Realising the same legislative protections irrespective of the technologies used is, of course, only part of the story. If consumers are to have the same level of protection then the other elements of providing consumer protection (consumer education, enforcement, access to dispute resolution, appropriate remedies and sanctions etc.) must also have broadly uniform application.



### III. Some broad observations about the technologies

#### Learning objectives and outcomes of Section III

66. This section of the train-the-trainer manual describes:
- the range of uses to which consumers typically put their phones and other devices when accessing the internet and engaging in e-commerce., internet access
  - the major issues raised by consumers use of these technologies for consumer themselves and regulators
  - the complexity of regulation when in every jurisdiction there are multiply agencies involved, and the imperative of interagency cooperation
67. Following completion of the train-the-trainer sessions, participants should be able to: discuss the range of uses to which consumers put these technologies and how this both empowers consumers and makes them more vulnerable to both scams and deception. discuss the opportunities and challenges of interagency cooperation

#### 3.1 Phones

68. For consumers mobile phones were initially simply the access hardware to a telephone service that allowed calls to be initiated and received away from fixed termination points such as their homes and places of work. With two exceptions the benefits to consumers were similar to the traditional fixed landline phone services. These exceptions are important to consumers, as evidenced by the rapid consumer uptake of mobile phone services; the benefits of mobility and, in many developing countries with underdeveloped landline networks, a significant increase in access to phone networks. The usage costs are generally higher, but for many consumers the benefits were clearly worth the extra cost.

69. The advent of smart phones has brought increased benefits and costs to consumers. Smart phones offer significantly extra functionality such as connectivity to the Internet and so provide consumers with additional benefits. However, enjoyment of these benefits may incur additional monetary and non-monetary costs.

70. Information provide by government ministries and others during UNCTAD field visits and literature searches suggest that in respect to mobile phone consumer concerns can be summarised as follows:

- Technical issues  
Most of consumer concerns about quality of service involve technical issues: access, performance, interoperability, and billing. Generally these issues are well understood by the relevant telco (telecommunications) regulators.

While identifying any regulatory gaps or omissions relevant to technical issues is beyond the scope of this paper, it is noteworthy that the current regulation and significance of SOEs in the sector may restrict or impede the realisation of the benefits to consumers

that would be expected from stronger competitive forces. On the other hand the status quo may simplify and even facilitate cooperation between consumer protection authorities and key infrastructure service providers.

It is apparent that some regulators may not have access to comprehensive and timely data on relevant consumer concerns. These deficiencies might be addressed by more effective consumer complaints handling that will generate better market intelligence and more comprehensive, ubiquitous corporate compliance programs by the mobile phone service providers. Consequently it is recommended that appropriate staff participate in complaint handling training with staff from consumer protection authorities.

- Pricing issues

- The price is too high

Pricing of mobile phone services generally falls as networks increase in size, new technologies are introduced and competitive forces increase. Pricing is very much affected by government policies determining the number of service providers, community service obligations and the likelihood/viability of sharing infrastructure. No specific regulatory gaps or training needs were identified that would improve the ability of regulatory agencies to better respond to consumer concerns on scheduled or regulated prices. However, a great role for competitive forces within the sector might be expected to exert downward pressure on prices paid by consumers.

- the price is higher than the consumer expected

Price surprises in respect of mobile phone services are commonly reported in jurisdictions around the world. However, the interviewed agencies did not identify this as a significant area of consumer concern. It is unclear as to whether price surprises are in fact not an issue for ASEAN consumers or whether they are being systematically underreported.

Price surprises can occur because:

- consumers did not shop around sufficiently before signing up to a service
    - contracts are written in such a way that makes it difficult to understand what the final price will be.
    - contracts are written in such a way that it is difficult to make accurate comparisons between contracts (plans)
    - there are insufficient or inadequate warnings that a consumer is approaching or has exceeded agreed parameters (such as downloads or minutes connected) and the cost consequences or alternative responses (such as buying extra download allowances or time top ups extensions).
    - consumers are unaware of the cost of certain types of calls, for example premium number services, international calls and data roaming.

These uncertainties are likely to be resolved by improved and expanded complaint handling that would provide authorities with improved intelligence. This intelligence should then inform future product/service design and marketing.

More effective consumer complaints handling that will generate better market intelligence and more comprehensive, ubiquitous corporate compliance programs by the mobile phone service providers.

Interestingly pricing concerns are almost always in respect of mobile phone services rather than for fixed line phone services. This is largely because of the greater variability in mobile phone contracts and pricing structures compared with traditional fixed line services.

Again it is apparent that some regulators may not have access to comprehensive and timely data on relevant consumer concerns. These deficiencies might be addressed by more effective consumer complaints handling that will generate better market intelligence and more comprehensive, ubiquitous corporate compliance programs by the mobile phone service providers. Consequently it is recommended that telco businesses review and further develop complaint handling processes and that appropriate staff participate in complaint handling training.

- Usage issues

Problems using mobile phones including smart phones

Internationally there are a number of problems commonly experienced with the use of phones, whether landline, (non-smart) mobile phones or mobile smart phones. These include:

- hoax calls:
  - nuisance calls from individuals
  - organized scams where callers seek to convince consumers that they are representatives from software suppliers, financial institutions or charities when they are not. (see discussion of Internet issues below)
  - unsolicited sales presentations attempting to sell any number of goods or services
  - unsolicited calls from charities seeking donations

At the time of writing it was no know what, if any legislation has been enacted in each ASEAN member state to address the issues listed above. Internationally these problems are dealt with by a range of responses including consumer and business education, 'do not call registries', number blocking and prosecutions for non-compliance.

71. It is recommended that appropriate staff participate in training covering:

- issues awareness
- complaint handling
- investigations skills
- consumer education programs
- problems associated accessing the internet with smart phones:

- as citizens in their private capacities (i.e. when they are not acting as a consumer), for example when they send and receive emails to family and friends, or use social networking services to communicate with family and friends.

Common problems include:

- spam (unsolicited emails). Spam can be a concern because of the sheer volume received by some consumers. Dealing with high volumes of spam can significantly detract from the user experience because of the time taken to identify and delete unwanted emails and for some consumers, the deleterious effect on download speeds and quotas. Spam is often a vehicle for malware or scams.

It is noted that the ASEAN Telecommunications Regulator's; Council is working on this issue.

- malware (detailed below under 'The Internet'). While most malware is targeted at desk and lap tops there is some malware specifically written for mobile devices
- scams unrelated to e-commerce (detailed below under 'The Internet'). While most scams are not device specific there are some scams that target phone users generally, such a premium number and call back scams.

- as citizens in their private capacities (i.e. when they are not acting as a consumer), for example when they send and receive emails to family and friends, or use social networking services to communicate with family and friends.

Common problems include:

- as citizens in their private capacities (i.e. when they are not acting as a consumer), for example when they send and receive emails to family and friends, or use social networking services to communicate with family and friends.
- as consumers, i.e. when they are contemplating buying a product or service. This may entail:
  - presale misrepresentations by parties other than the intending seller, for example comparison web sites (detailed below under 'E-commerce')
  - presale misrepresentations by the intending seller. While often misrepresentations are not device specific, consumer protection authorities have detected that some sites display differently on mobile devices such as smart phones. In these problematic cases necessary information is omitted on the mobile display, misleading mobile device using consumers. (detailed further below under 'E-commerce')
  - post sale misrepresentations about the application of warranties (detailed below under 'E-commerce'), non



delivery or goods commerce (detailed below under 'E-commerce'), supply of unsafe goods (detailed in the Product Safety Paper), supply poor quality goods or otherwise not as ordered (detailed below under 'E-commerce')

72. Usage issues are often similar whether a citizen is accessing the net via mobile phones or another means. Consequently these issues are dealt with below under the subheading of 'The Internet'. Most consumer authorities do not particularly distinguish between consumer problems on whether or not they are encountered in a commercial or non-commercial context. Phone specific responses by regulators include education, 'do not call registries', number blocking and prosecutions.

73. It is recommended that appropriate staff participate in training covering:

- issues awareness
- complaint handling
- investigations skills
- consumer education programs

### **3.2 The Internet**

74. Initially the Internet offered consumers (as distinct from business and government) not much more than email. However, the development and roll out of broadband and significant and sustained decreases in hardware costs and increases in computing power (including the advent of smart phones) has facilitated the development of business to consumer (B to C or B2C) e-commerce (see a fuller outline under the subheading 'E-commerce' below), that is, trading between consumers and traders on-line. These on-line traders may or may not also have a physical 'bricks and mortar' or local, physical presence in the form of traditional business premises such as shops. Because of the global nature of the Internet, the trader and consumer may not ever meet and may be located in different cities or countries.

75. Citizens use the Internet for many and varied purposes. The Australian Government's Internet Basics website ([internetbasics.gov.au](http://internetbasics.gov.au)) provides a short list of some of the uses to which consumer put mobile phone and Internet services:

- Keeping in touch with friends and family
- Finding information on almost any topic and accessing all sorts of online content like news, sport, weather and entertainment
- Searching for jobs or using the internet to work from home
- Online shopping and banking and for planning holidays, and



- For finding the government information and services.

76. As with phones, sometimes the boundary between a citizen accessing the net in their person capacity, for example when emailing a family member, and when acting as a consumer, for example making an online transaction, is difficult to determine, or may change over time. For example an online romance may start off on a commercial fee for service dating agency but quickly move to personal email exchanges directly between the dating couple. Other times a consumer may appear to be enjoying a free personal service, but the cost of the service may be indirect or borne by intermediaries. Yet another variation is where a citizen's use of 'free information' available on an educational site may be simply the 'teaser' or inducement to persuade the consumer to acquire a paid product or service.

77. As noted above in respect to the use of mobile phones to access the net, the more common problems experienced by consumers include:

- Spam that causes a problems both because of its performance debilitating volumes and a vector for malware and scams.

At the time of writing it is not know which ASEAN countries have laws prohibiting or regulating spam. While the application of anti spam laws in the US and the EU have resulted to the closure of some notorious spammers, it does not seem the average 'background' level of spam has decreased. The management of spam requires a combination of consumer education (knowledge of what spam is and steps ordinary consumers can take to manage it), installation and use of spam filters at the consumer and ISP levels and concerted cooperation between consumer protection authorities and ISPs/domain hosts to identify spammers and close their access to the net (at least until they relocate).

- Malware

'Malware' is a generic term to cover a range of malicious code that installs on devices accessing the net without the informed consent of users, such as smart phones and more commonly, on desk and lap tops. The harms caused by malware include:

- stealing of financial and other personal information
- preventing a consumer's computer from using their computer until a 'ransom' is paid
- damaging files including system and data files that adversely affects or prevents use
- hijacking a computer and using it to disseminate spam, for example by creating a botnet

At the time of writing it is not know which ASEAN countries have laws prohibiting the creation and distribution of malware. However, in practice, the existence of such laws have a limited effect on the type and quantity of malware to which consumers are exposed because much of it originates outside of ASEAN jurisdictions. Consequently while malware laws have their place in the mix, they are not the first, nor most effective line of defence.

The key to preventing the installation of and mitigating the harm from malware lies in a combination of strategies including:

- educating consumers about the harms caused by malware and preventive strategies such as keeping operating systems, applications and antivirus and other applications up to date with the latest security fixes, identifying suspicious vectors (executable file attachments, emails and website links) and isolating and removing malware.
- encouraging ISPs and the creators of operating systems to improve security of their products and services and to engage with their users to amplify the education messages of consumer protection authorities.

78. It is recommended that appropriate staff participate in training covering:

- Consumer protection issues awareness
- Complaint handling
- Investigations skills
- Consumer education programs

### **3.3 E-commerce**

79. While B2C e-commerce is often thought of as simply the act of a consumer buying from an online trader, it is much more than a simple transaction. Just as in the real bricks and mortar world consumer contemplating buying online go through a multistep process both before, during and after a purchase.

80. For example many consumers will do at least some research before committing to a purchase. That could be as simple as following up on an unsolicited email to view the content of a site promoting a desired good or service. However, some obvious strategies as this may simply assist the spammer by verifying that the recipient email address is active and worth spamming again and again.

81. Pre purchase research may also entail visiting comparison web sites to compare prices and features of products, or blogs where other consumers have commented on the same or similar goods and services and/or traders. At this point, consumers may be exposed to misleading representations by 3<sup>rd</sup> parties (i.e. by someone other than the traders they are researching). For example while well run and comprehensive comparison websites and blogs can provide consumers with unbiased and insightful information, others may give poor or biased comparisons and comments that are overtly misleading, or misleading by omission. This may occur because the site is receiving undisclosed commissions or other payments, such as advertising revenues.

82. When the consumer decides to buy a product from a particular online trader they typically complete an order form that requires them to input personal and financial information. This process raises issues about the security of provided information and its future use by the trader.

83. Consumers will also be provided with information (representations) about the product and the trader. The consumer protection issues at this point include the adequacy of the



information provided (does it address all of the elements of the contract that are important in their purchase decision making) and whether the information is relevant and correct or false or misleading? Important information will not only include price, quantity and quality descriptors, but information that may not always be relevant when purchasing from a local bricks and mortar trader, such as delivery details, customs arrangements, insurance and warrantee arrangements.

84. Post sale communications between the consumer and trader may also be very important and the source of consumer problems. For example, liability for and arrangements for the return of goods and refunds when goods are not delivered, are delivered in unsatisfactory condition or are materially different from the goods ordered.

85. The general protections provided by existing consumer protection laws in ASEAN countries address many of the most commonly encountered problems, partially misrepresentations.

86. However e-commerce presents some particular problems not specifically addressed in general laws:

- Practical problems of how well a consumer can interact (negotiate) or not with online traders compared to face-to-face interactions
- The question of consumer rights when goods are subject to delayed delivery or do not meet local (national) standards or norms but have not been misrepresented.
- Access to timely, affordable justice when traders are not located within jurisdiction
- A wide range of available remedies so that consumer protection authorities can take effective action in the context of online transactions

### **3.4 Some implications for consumers and government**

87. The supply and demand conditions referred to above have significant implications both for consumers and governments. Issues facing consumers include:

- Challenges in understanding all of the implications of using the services is difficult because the technologies are evolving rapidly
- Challenges in distinguishing between suppliers and products/services and evaluating alternatives because of uncertainties about future usage, performance and pricing
- Avoiding new scams made possible, and old scams that have been given new potency, by the technologies.

88. Issues facing governments include:

- Identifying current and emerging issues that may require public intervention



- Designing and implementing interventions that effectively address priority consumer issues
- Minimizing the direct and indirect costs of public intervention without diminishing the utility or increasing the costs of the services

### 3.4.1 Regulatory responsibility

89. Regulatory responsibility for consumer issues related to using mobile phones, the Internet and e-commerce is diffuse in each of the ASEAN countries, as it is in jurisdictions worldwide. This arises because:

- Various elements of consumer protection have always been the spread across multiple agencies. For example police forces are generally responsible for addressing fraud, whether the victims are consumers or not, and whether the fraud was committed face to face, over the telephone or the net. However, police forces are generally not charged with regulating misleading advertising, or ensuring that traders comply with weights and measures or consumer product safety standards.
- Consumer problems in respect of specific technologies are often within the responsibility of sector regulators, for example those regulating utilities such as electricity and water, telecommunications. However, many consumer problems experienced using the technologies are not unique to using them. Authorities with a general consumer protection brief can prioritize particular consumer concerns quite differently to sector regulators and this will influence whether and how each agency response to similar problems.

90. Diffuse responsibilities may lead to the following results:

- Consumers may not report a problem, or report it to an inappropriate authority because they are:
  - unsure of how to categorize their problem and therefore which authority is responsible,
  - unsure which authority is responsible for which issues
  - not convinced that the appropriate authority will be able to achieve a useful remedy for them
- Effective consumer protection in respect of consumers use mobile phones, the Internet and e-commerce will often require a collegiate approach by multiple authorities because:
  - Intelligence about the problems being experienced by consumers may be poor or unevenly distributed among authorities.
  - Intelligence can be proved by consumer complaints, from stakeholder engagement and from market observations and investigations
  - An individual authority may have insufficient powers to obtain necessary evidence. Obtaining evidence may require the exercise of investigatory powers by more than one authority



- Achieving effective and efficient sanctions and remedies may require the exercise of powers by more than authority
- An additional challenge to effective consumer protection in e-commerce is that traders will often be located outside the jurisdiction. Cooperation between consumer protection authorities across borders (within and outside ASEAN) may be required for the same reasons as is interagency co-operation within countries.

91. Already most ASEAN member states have established international links in respect of consumer protection, although this is not consistent across the region. Brunei Darussalam, Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam are all members of the APEC and eligible to participate in the Electronic Commerce Steering Group (see [www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx](http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx)).

92. Both the Philippines and Vietnam are members of the International Consumer Protection and Enforcement Network (ICPEN) (see [www.icpen.org](http://www.icpen.org))  
One of the key ICPEN collaborative efforts is [econsumer.gov](http://econsumer.gov), a cross-border complaint portal for consumer protection agencies. The project consists of the multilingual public website, on which consumers lodge cross-border complaints, and the password-protected website, through which the incoming complaints are shared with the participating consumer protection authorities. This intelligence resource includes complaints in respect of consumer experiences with mobile phones, the Internet and e-commerce.

### **3.4.2 The benefits of interagency co-operation**

93. The benefits of interagency co-operation across borders are probably greater in respect telecommunications related consumer issues than in any other area of consumer protection because:

- The technologies are universal
- Many of the service providers, particularly mobile phones service providers and application providers (for example companies providing the major operating systems, browsers and search engines and payment systems) involved operate in many countries
- The business with whom consumers are dealing with using the technologies (for example E-commerce traders) operate in many countries
- Most of the problems encountered by consumers are similar across countries

94. Some of the areas of interagency co-operation that will deliver the biggest benefits include:

- Sharing market intelligence  
Often if a consumer problem is detected in one jurisdiction it is probably being experienced in others. Sharing information about complaints can speed up detection and agency responses. Also the response of traders to public intervention in one



country (for example by co-operating, being evasive or even hostile) may be a good indicator as to how it will respond to intervention in another country.

- **Sharing resources**  
Some resources can be readily shared between agencies (such as intelligence) because they are both relevant and inexpensive to share, while others can provide a guide to receiving agencies and even reduce their costs, for example the sharing of educational resources. Of course education programs and material produced in one country will often need modification (for example translation and adaption by substituting locally relevant references and examples).
- **Sharing experiences**  
Sharing intelligence and resources can only go so far in building a consumer protection agency's performance. At the end of the day the experience of 'doing' investigations and educational campaigns that builds hard skills and experience. Sharing experience accelerates this learning process. Staff exchanges and joint training may often be a cost effective way of building knowledge and skills.

95. The benefits of interagency co-operation with jurisdictions in respect telecommunications related consumer issues are probably more obvious, more cheaply and more easily gained. In all ASEAN countries (as in countries worldwide) responsibility for the supply and use of these technologies is shared by multiply agencies. Each relevant agency will receive a share of the consumer complaints, but it will only by combining the data that a comprehensive picture of consumer experiences will be recognised. Each agency will have better access to some consumer and trader groups than other, so it will only be by sharing these communication and engagement advantages that effective education programmes will be delivered. And finally each agency will have its own particular powers and abilities to influence trader behaviour, so it will only be by combining these that effective enforcement programmes will be implemented.

## **IV. The principal consumer protection issues in respect of consumers' use of telecommunication technologies**

### **Learning objectives and outcomes of Section IV.1 – IV.2**

96. This section of the train-the-trainer manual:
- asks the question: 'How do we know what problems consumers are encountering?' This seems like an easy question, but is it?
  - describes the various sources of market intelligence about real consumer experiences
  - explains the major problematic areas encountered as consumers use these technologies, including misleading conduct, scams, unfair contract terms. Many of the most commonly encountered scams are described.
  - also noted are the vexing issues of malware, online security, privacy and data security
97. Following completion of the train-the-trainer sessions, participants should be able to:
- discuss how, in the context of their own individual jurisdictions, comprehensive and timely market intelligence might be acquired.
  - understand the breath of consumer issues encountered in the on-line world and to be able to discuss the differences and similarities with consumer experiences in the tradition brick and mortar markets
  - identify the most common scams and discuss how and why they continue to claim victims
  - appreciate the potential multiple consumer threats posed by many scams
98. Efficient and effective resolution of the many and varied problems encountered by consumers as they use mobile phones, the Internet and e-commerce necessitates the identification and prioritisation of the problems. This process is not always as easy as it might seem because different consumers may have different experiences depending on:
- Their level of knowledge about and experience of using the technologies and platforms
  - How and why they were using the technologies and platforms
  - Experiences may change over time as consumer and businesses particularly telcos and e-traders) learn from previous experiences, technologies evolve.
99. The problems reported by consumers or the media may not always be reflective of broad consumer experience, for example:

- consumer may not always be aware that they have experienced problem
- the media are more likely to report experience that make for interesting reading or viewing by their audiences
- The regulatory and media environments can influence the number and types of complaints made to authorities, consumer organisations and media organisations. An environment that is more consumer-friendly may actually increase the apparent incidence of problems as consumers become more aware and confident of their rights.

#### **4.1 How do we know what problems consumers are encountering?**

100. There are many potential sources of information about the problems encountered by consumers as they use mobile phones, the Internet and e-commerce:

- Consumer complaints to government authorities  
The value of consumer complaints are that they the information is coming directly from consumers without the delay and potential biases associated with complaints received via intermediaries. Intuitively complaints data should provide qualitative and quantitative data. However, the quantity of complaints and their repetitiveness to problems experienced will in part be affected by the performance of authorities with consumer protection responsibilities and the inclination of consumers to complain when they experience problems. For example:
  - to what extent do authorities facilitate and encourage consumers to lodge complaints (see text on effective complaint handling)
  - whether consumers lodge complaints will depend in part on whether they know where and how they can lodge a complaint and how likely they think it is that their complaint will be resolved satisfactorily
  - do current cultural attitudes and practices encourage or discourage lodging making complaints with government authorities? Where cultural influences are not supportive, complaints data is likely to under report the true incidence of problems and to disproportionately reflect the experiences of those who do complaint.Even in communities where consumers have a long history of lodging complaints, complaints received may only represent a fraction of the real incidences of problems encountered. For example the Internet Crime Complaint Centre (ic3.org) suggests that complaints in the US may represent <15% of the problems actually experienced.  
Where it is likely that number and focus of complaints received may not reflect broader consumer experiences it is vital that efforts be made to:
  - improve consumer awareness of and access to complaint handling systems
  - improve the transfer of complaints and complaints data between authorities so that individual complaints are more efficiently dealt with and the intelligence gleaned from complaints is more quickly and fully available to authorities.
  - broaden the authority's sources of intelligence about consumer experiences and problems



- Consumer complaints to consumer organisations

Complaints to consumer organisations may supply alternative or additional sources of information. The contribution of consumer organisations will depend in part on:

- the existence of active consumer organisations within a country
- to what extent the organisations facilitate and encourage consumers to lodge complaints
- to what extent their complaints data (individual complaints and aggregated data) is available to externally, for example to consumer protection authorities (see text on engagement with consumer organisations)

Where consumer organisations are inactive or absent, consumer protection authorities miss out on not just market intelligence about consumer experiences, but also a potentially powerful ally in advocacy and education activities.

- Non-complaint local market intelligence from those operating in and around the market  
In jurisdictions where there are relatively few complaints lodged with government authorities, information sources other than complaints will be relatively more important. For example consumer concerns may also be assessed by:
  - market observations, such as in-store inspections, covert purchases (mystery shopping), monitoring published advertising etc.
  - surveys of consumers consumer organisations and other NGOs and traders
  - information provided by corporate entities providing telecommunications infrastructure services and facilities, such as telcos and ISPs who may often be asked for advice or assistance by consumers

Non-complaint market intelligence should always play a role in informing consumer protection authorities about consumers' experiences. It will be more important when complaints underreported or are unrepresentative of consumer adverse experiences. They can be used to crosscheck the intelligence being provided by complainants.

- Experience in other countries  
While some areas of consumer concern may be local in nature and incidence, others are more likely to be similar across jurisdictions. Problems experienced by consumers when using mobile phones, the Internet and e-commerce are likely to be similar between countries within and outside ASEAN because:
  - the facilitating technologies are universal
  - many of the same corporations are involved internationally in providing mobile phones services (including virtual network operators)
  - consumer are using these technologies for similar purposes, for example communications, general information gathering and pre-purchase research and purchases.
  - most of e-commerce transactions are cross boarder and the traders usually adopt the same practices and mode of operation regardless of the jurisdictions they are selling into

101. The field missions undertaken indicated that complaints been received by authorities with consumer protection responsibilities in respect of consumer usage of mobile phones, the Internet and e-commerce are more often about access and pricing issues than they are about:

- Presale representations, for example misleading and deceptive conduct





- Contractual issues, for example unfair contractual terms
- Post sale issues, including non delivery, poor quality and unsafe goods, warranties, repairs and refunds

102. Given the experience of consumer protection authorities in countries around the world and the expectation that ASEAN consumers are likely to be facing the same problems, this is somewhat surprising. There could be a number of reasons for this observation, including that consumers are:

- Not experiencing the same problems, or at least if they do the harm caused is not so serious
- Relatively less aware that they are experiencing problems
- Experiencing similar problems that are causing similar harms but are not lodging complaints

## **4.2 Consumer protection issues identified from international experience**

### **4.2.1 Misleading conduct**

103. To make satisfactory purchasing decisions consumers need relevant and accurate information about available goods and services, and about the traders supplying those goods and services. If consumers rely on misleading information they are likely to make poor choices about:

- Which trader to buy from
- Which products they buy, how many and the price paid
- What they will do if they have a problem with the goods or services, for example if the goods are found to be unsatisfactory, need repairs or cease to function.

This is the same whether the consumer buys from a bricks and mortar trader or online from an e-trader.

104. The importance of prohibiting false and misleading conduct was recognised in ASEAN-Australia Development Cooperation Program Phase II: Supporting Research and Dialogue in Consumer Protection Consumer protection laws and regulations for online purchasing.

#### *The mechanics of misleading consumers*

105. Consumer may be misled by traders and others at any phase of the transaction process, including:

- Presale, for example advertising and other information disclosure, for example:

- Misleading information on trader's web sites,
- Misleading information on nominally independent web sites, for example on comparison sites and blogs
- At point/time of sale
  - Confusing disclosure that makes it unlikely most consumer will understand the full import of the disclosure or at least not until they are psychologically committed to the purchase. In the context of online purchases a frequent strategy is 'drip disclosure' particularly of pricing information
  - Effective non-disclosure of relevant information by presenting with inordinately long 'terms and condition' which the trader knows few if any consumers will read through while providing a simple, quick and convenient click on 'I agree' option
- Post sale, for example representations about warranties, repairs and refunds and the effect of other contractual terms. This may include statements that are contrary to applicable local laws or statements they discourage consumer from pursuing grievances.

#### *The importance of context*

106. Misleading representations can include both false and true information. Generally 'false' refers to representations that are contrary to fact and are most likely to mislead. However a representation can be misleading even though it is factually correct. A factually correct representation may be misleading because of the context in which it is made, or because of what is not said (i.e. what is omitted)

107. Misleading conduct should be differentiated from conduct that is generalised and self evidence exaggeration. Most consumers are not misled by common advertising or sales presentations that exaggerate the attributes of particular goods or services. Context is often very relevant, for example when the representations are part of an advertising or sales pitch. It is important to note that continual clues may be weakened or absent when representations are viewed online. For example a consumer who has 'goggled' a product hoping to find an independent review may not realise that they have inadvertently clicked on content created by the trader. Consequently they may not recognise the usual clues available in the brick and mortar environments that might cause them to be sceptical, or alert them on the need to seek out further information.

#### *Intention to mislead*

108. Generally consumer protection laws do not require that the trader intended to mislead a consumer. Intention is generally not relevant because:

- The core of the mischief is the result, i.e. that a consumer was misled, rather than the intention of the trader

- It would often be impractical to prove intention in respect of many representations
- The irrelevance of 'intent' puts the onus on traders to think about what they chose to say about the goods and services they offer to consumers and encourages them to commit to consumer protection law compliance.

*Misrepresentations concerning real goods and services v scams*

109. It is useful to differentiate between misrepresentations concerning real goods and services and scams. Otherwise legitimate (non scam) traders may mislead consumers because:

- They are so focused on selling that they fail to recognize that they have moved from exaggeration to misrepresentation
- They have poor product knowledge (ignorance)
- They do not have in place an appropriate compliance program and are either unaware of their legal responsibilities or negligence about compliance
- They seek to gain a competitive advantage over other traders who offer better goods and services and/or lower prices

110. These factors do not lessen the significance of the harms to consumers that may be caused by non-scam misleading conduct or the need for consumer protection authorities to address them. However, they are very relevant to selection the appropriate mix of regulatory responses.

111. What might constitute an effective and appropriate regulatory response will differ:

- Non-scam misrepresentations may be stopped and discouraged by enforcement responses towards the bottom of the pyramid [see the pyramid of enforcement responses]
- Scams are rarely stopped or discourage by enforcement responses towards the bottom of the pyramid
- Standard form contracts, licensing and other administrative responses may appropriate in respect of non-scams misrepresentations but not in respect of scams

**Scams**

112. Scams are fraudulent schemes purposely designed to mislead consumers. Deception is central to their design, rather than incidental to selling a product or service.

113. The significance of this differentiation is that:

- In regulated sectors such as telecommunications, misleading and deception conduct by service providers does it occur, it is not common. On the other hand scams are a much

more common cause of consumer harm and have the potential to cause more serious consumer harm.

- The most appropriate public intervention strategies will be different. For example corporate compliance programs, regulatory directives and adverse publicity are likely to be effective strategies to combat misleading conduct by otherwise legitimate traders, whereas they are unlikely to be effective against scammers. On the other hand consumer education and cooperation between agencies is likely to be more effective in combating scams.
- Alternate Dispute Resolution (ADR) is may be appropriate in respect of non-scam misrepresentations, but inappropriate in respect of scams
- Scams may constitute contraventions of consumer protection laws including prohibitions on misleading representations and also various criminal offences, such as fraud, theft and blackmail.
- Scams may be connected or unconnected with consumer transactions.

(see the text below concerning online scams)

#### **4.2.2 Unfair contract terms**

*What are unfair contract terms?*

114. Unfair contract terms are terms that are either very one sided in their benefit or cost and which are not reasonably necessary for the protection of a party's legitimate rights. Unfair contract terms must be determined objectively and are not simply terms that one party objects to. Generally a market economy works best where there is minimal interference in the rights of parties to contract as they see fit. Public interference is generally restricted to situations where one party is unable to look after its own interest, or where be adverse costs of particular contractual terms is likely to be born by parties outside the contract.

115. ASEAN-Australia Development Cooperation Program Phase II: Supporting Research and Dialogue in Consumer Protection Consumer protection laws and regulations for online purchasing noted the relevance of unfair contractual terms in online transactions.

116. Legislation prohibiting 'unfair' contract terms may be:

- General and principle based (i.e. the law does not specifically prohibit particular words but rather provides a test for determining when a term is unfair), or
- Specific terms may be prohibited. When a term of a contract is 'unfair' may be determined by court or agency determinations or by legislation.
- For example the Australian Consumer Law provides for a three steps test to determine if a contract term is 'unfair':



- Does the term cause a significant imbalance in the parties' rights and obligations?
- Is the term reasonably necessary to protect the legitimate rights of the parties, and
- would reliance on the term cause significant detriment to one of the parties?

*When are unfair contract terms more common?*

117. Unfair contract terms are most often encountered when there is a significant power imbalance between the consumer and trader. The power imbalance is not only about how wealthy or powerful a person or company is. Power imbalances can also be caused by differences in knowledge, social position or cultural norms that affect a consumer's ability or willingness to negotiate and agree.

118. Unfair contract terms may be found in both standard form contracts and transaction specific contracts. They are more likely to be found in contracts where there is little or no negotiation on most of the terms. This situation is more commonly encountered when traders use standard form contracts because one of both parties will be discouraged from negotiating or clarifying terms.

119. Standard form contracts are not necessarily problematic. Indeed business associations often develop standard form contracts for use by their members because they offer an opportunity to ensure that contracts are comprehensive in their coverage of important elements of the contract and that terms that have been troublesome in the past (for example a court or agency determination that a term is 'unfair'). However, the drafting of standard form contract should be done with expert knowledge of the applicable laws and in consultation with stakeholder groups such as consumer organizations and relevant government organizations.

120. Worldwide standard form contracts are the norm in contracts for the provision of telecommunications services such as mobile phones services, Internet access services and B 2 C e-commerce contracts.

121. It is also important that standard form contracts are not used as a vehicle for collusion, for example by denying or discouraging businesses to negotiate on elements of the contract that are likely to go to the heart of competitive pressures such as price, quality and performance.

122. Some of the most commonly encountered unfair contract terms that:

- Allow unilateral changes to key terms of the contract. For example where the trader, but not the consumer, can cancel or renew a contract or vary terms without the need for mutual agreement.
- Make the consumer liable for things that would normally be outside their control
- Allow the trader to charge amounts against the consumer credit card without further consultation or notice

- Provide for disproportionate penalties. For example forfeiture of large security bonds for minor instances of non-compliance that have not had a significant adverse impact on the trader.
- Deny all liability for negligence by the trader, its staff and agents.
- Nominate the national law applicable to the contract where there is no common jurisdiction
- Explicitly state that representations made by the trader outside of the written contract (for example in advertising or sales presentations) cannot be relied upon in case of dispute.
- Nominate the national law applicable to the contract are quite common in international commercial contracts. However, these terms may be unfair when they effectively limit consumers' access justice. For example if a contract nominates the law of a non ASEAN country as the sole law in respect of determining disputes under the contract to the contract, consumers may have no effective access to justice.

123. The adverse effect of such terms may be reduced or nullified in respect of:

- Criminal law which will apply regardless of the contractual terms
- Where national civil law specifically provides for consumers' rights and traders obligations outside of, or in addition to, the terms of the contract. For example the Australian Consumer Law provides for consumer warranties in 'consumer transactions' that have application regardless of the express terms of the contract.
- In respect of telecommunications services, or with products and services purchases using telecommunications, a complicating factor is that the supplier may not be either physically present or have assets within an ASEAN jurisdiction. In some circumstances this can limit the viability of asserting local jurisdiction and the effective resolution of consumer disputes.
- Terms that grant the seller or their nominees irrevocable, perpetual and fee free rights to use information about the consumer or things provided or created by the consumer. For example the consumers personal details, photos and documents
- Terms that allow an ISP to unilaterally change the download limits or speeds or shift the consumer to a new, less favourable plan
- 'Manufactured confusion': complex and lengthy contracts that make it difficult for average consumer:
  - to understand exactly what they are agreeing to
  - to identify unfair or harsh terms
  - to make accurate comparisons between competition products and services





#### **4.2.3 Scams using phones, the Internet and e-commerce**

124. As noted above, scams are dishonest schemes purposefully designed to trick consumers into paying money to the scammer. Scams are not unique to telecommunications such as phones (premium number based schemes) and Internet applications (web sites, email, SMSs, social media). However, the very features that make mobile phones and the Internet so useful and attractive to consumers may also be attractive and useful to scammers. Telecommunications technologies give new life to old scams and create opportunities for new scams because it facilitates:

- The quicker dissemination, operation and shut down of scams
- Greater 'market penetration' because physical distance and social isolation are much less significant obstacles
- Greater internationalization of scams
- Enormous economies of scale and lower costs of operation to the scammers

Telecommunications technologies can also:

- Make it more difficult for a consumer to recognize a scam
- Cause consumers' traditional protections such as the presence of family or friends, or location within the home less effective
- Limit the availability of remedies and sanctions

On the other hand telecommunications can also facilitate the:

- Tracing and identification of scammers and their funds
- Collection of evidence
- The dissemination of educational content

Common scams that use either smart phones or the Internet:

- Advance fee fraud schemes: a generic terms for a range of schemes that solicit pay fees up-front as a precondition to realising a promised financial reward
- Fake inheritance scams
- Lottery, competition and unexpected prize scams
- Dating and romances
- Scams



- Dating and romance scams
- Computer and smart phone hacking
- On-line auction scams
- Online advertising (classifieds) scams
- Banking, credit card and on-line account scams
- Employment scams
- Study scams
- Get rich quick scams: investments, gambling and pyramid schemes
- Charity and health scams

A number of real examples are provided in the presentations accompanying this paper.

125. Advance fee fraud schemes: a generic terms for a range of schemes that solicit pay fees up-front as a precondition to realising a promised financial reward

- Money transfer schemes

126. These schemes typically involve a supposed plan to shift money from one jurisdiction to another. Typically the potential victim is approached by way of an unsolicited SMS or email. The scammer will explain that the recipient has been approached because of their reputation for honesty and integrity. The scammer then goes on to explain that in return for assisting with the transfer of funds, they will revive a significant proportion of the funds as a commission. Often the background story includes a deposed or deceased president or some other wealthy or powerful person in a foreign country.

127. If the recipient responds, the scammer engages the victim directly, usually by email. Follow-up may also be done by phone. Invariably a request is made for a relatively small sum of money as a fee 'for lawyers', to pay 'government fees' or to 'bribe an official'. If the victim pays the requested money the sequence then continues with the scammer making further requests for larger sums, all the time assuring the victim that the transfer and hence the commission are imminent.

- Inheritance scams

128. These schemes typically involve the promise of a sizable inheritance from a previously unknown family member or friend. Typical the potential victim is approached by way of an unsolicited SMS or email. The scammer will explain that they are a firm of lawyers acting on behalf of a deceased estate in a foreign country. The scammer then

goes on to explain that either the deceased died without leaving a will or that the victim is named in the will. If story line is that the deceased left no will, then it will be explained that a comprehensive research has revealed that the potential victim is the only or closest relative and therefore entitled to the estate.

129. If the recipient responds, the scammer engages the victim directly, usually by email. Invariably a request is made for a relatively small sum of money as a fee for lawyers, to pay government processing fees or to bribe an official. If the victim pays the requested money the scammer making further requests for larger sums, all the time assuring the victim that their inheritance is about to be paid.

- Lottery, competition and unexpected prize scams

130. These scams typically involve unsolicited SMSs or emails, but can sometimes be triggered by visiting fake lottery websites. The scammer informs the potential victim that they have won a substantial prize in a foreign lottery. All that is required to collect the prize, the scammer explains, is to pay some fees or taxes. Like many online scams the amount requested is usually small to begin with but escalates if the victim keeps paying.

131. Alternatively the scammer may tell the victim that they have to call or SMS a premium rate phone number to claim their prize. If the demand is for personal details, the scammer is probably intending to use those details to commit frauds at the expense of the victim.

132. In some scams the scammer 'drip feeds' the victim by providing small prizes or gifts. These are intended to excite the victim and win their confidence that winning the big prize really is possible. They may also try to lull the victim into a false sense of security by personalising correspondence with stories that the members of the 'lottery team' are thinking of them and hoping that the victim will finally received their deserved big win.

- Dating and romance scams

133. Dating and romance scams can cause significant financial and emotional harm to victims. Financial losses are often quite high, and victims also experience emotional distress when they finally realise what has happened. The most common dating and romance scams involve scammers creating fake profiles on legitimate dating websites. They use these profiles to build an online relationship with victims so they either ask for payments or obtain their personal details for later frauds.

134. The scammer will develop an apparently strong relationship with the victim and then ask for money to help cover costs associated with some made-up illness, injury, travel costs or family crisis. Scammers seek to exploit the victim's emotions by pretending love or by exploiting the victim's vulnerability in wanting to help others in distress. They may also promise to help the victim. Inducements may include the promise of money, visas, relocation, employment and family support.

135. Often victims keep the new romance secret from their families and so miss-out on the warnings that family members could give. In any case victims are often very

reluctant to accept that they have been scammed, even when told by family members, the police or consumer protection officers.

#### *Computer and smart phone hacking*

136. Some scams operate by stealing consumers' identities or authorities so that they can:

- Take money from the victim's bank accounts,
- Buy things using the victims' credit cards
- Use the victims' computers to distribute scam messages to other consumers
- Take over the victims' computers and hold them for ransom by denying access to the computers until money is paid to the scammer
- 'Phishing' emails

137. 'Phishing' emails are commonly used by scammers to trick consumers into giving the scammer access to their computers. They 'fish' for personal details by encouraging consumers to click on a link or attachment. If the consumer clicks, malicious software attempts to install. Once the malware is installed the hacker will have access to files and information stored on the victims' computer. A phishing email often appears to come from a well-known and trusted organization such as a government agency or bank.

- Social networking scams
  - Social networking scams can be initiated via a phishing emails that ask consumers to enter their account passwords on a fake copy of the networking site's login page. If the victim provides their account details, the scammer can access the accounts and take control of the victims' profiles. They may then pose as the victim in an attempt to gain money or personal details from the victims' family and friends,

139. Phone calls from scammers pretending to be from Microsoft or other well know companies are often used as an alternative to phishing emails. Scammers call consumers and explain that the consumers' computer is infected with a virus or other malware or has some other technical fault. Like phishing emails the objective of these phone calls are to gain direct access to the victims' computer or smart phone or to obtain their personal details.

#### *On-line shopping, products and services advertising and auction scams*

140. Whereas a personal shopper can inspect products before purchase or at least physically see the trader and his place of business, distance selling makes this difficult or impossible. When the consumer must pay before delivery, as is usually the case, they are vulnerable to the supply of inferior goods or non-supply.

141. Not all cases of alleged inferior or different goods are scams. Some times the problem may be one of mistake by the supplier, or the consumer. For example sometimes consumers do not read the description or adequately think about how well the product might fit their needs or wants.



142. As with many other scams, the intention of the scammer may be to either obtain money immediately in the form of a direct payment, or to obtain personal details so that later fraud can be committed.

#### *On-line auction scams*

- 143. On-line auction scams often take advantage of consumers trust in well-established, legitimate auctions sites. For example, the scammer may contract consumers with a story that prompts the consumer to complete a transaction away from the secure payment mechanism of the legitimate site. A common explanation given to the consumer by the scammer is that while the consumer was not the highest bidder, they now have a second chance because the highest bidder has now pulled out.

#### *Online advertising scams*

- 144. Advertising scams use legitimate sounding advertisements to lure unsuspecting consumers into paying money or providing personal information. They can be targeted at either intending buyers or sellers.

145. While the advertisements can be about any products or services, they are frequently feature commonly traded goods and services including rental properties, second hand consumer goods such as cars and cameras. Often the key feature is that the goods are cheaply priced.

146. Invariably the scammer will nominate an insecure method of payment such as money transfer rather than credit card or payment systems such as PayPal.

147. If the scammer is offering to buy, a common trick is to overpay by cheque or money order. He then asks the victim to refund the overpayment by immediate money transfer. After the victim has transferred the overpayment he will find that the original cheque is cannot be processed or the money order is not genuine.

#### *Banking, credit card and on-line account scams*

(These financial services scams are also referred to in the Manual on Consumer credit and Financial Services)

148. Phishing scams are a common method to fraudulently obtaining consumers' financial and other personal information. Most frequently the scammer contacts the consumer via emails or SMSs alerting the consumer to a problem with their account such as a 'security breach', the need to update a password or a suspect transaction.

149. Victims can be asked to go to a web site that looks like their bank's legitimate website where they are instructed to provide their financial and other personal information.

150. Often the web sites look very like the legitimate web site because the scammers have copied the look and feel of the bank's site. At first glance the web site address may even look like the bank's URL. However, hovering the cursor over the URL will usually reveal that the



site's actual URL is different to the displayed address, although it may include some of the same characters like the bank's name.

151. *Card Not Present* (CNP) scams are where scammers obtain and use consumers' names, addresses, credit card numbers and security codes to purchase good and services in transactions that do not require the trader actually seeing the card itself. Typically such transactions occur over the Internet or phone.

152. Most often the scammer obtains the information via a person working for a legitimate trader. This can be done when a consumer hands his card over to be swiped or when he provides the information as part of a legitimate net or phone transaction.

#### *Employment scams*

153. Employment scams may involve offers to work at home, in another town or city, or overseas. Usually they offer 'guaranteed' opportunities and attractive pay. Many require payment of fees up front. Often the required fees will be described as payments for training, travel, software, security clearances, visa fees, taxes and government charges.

154. These scams can be difficult to identify because they may appear to be indistinguishable from legitimate employment services.

155. Pyramid selling scams are sometimes disguised as employment services or offers of employment. The distinguishing feature is that in pyramid scams payment is dependent upon recruiting of other into the scheme.

#### *Study scams*

156. Study scams are similar to employment scams. In this case the lure is the offer of a place at an educational institution. Generally study scams require the student victim to pay fees up front. The victim then finds that:

- The course or the institution or course does not exist, or the courses are 'cancelled'
- The courses are substandard and/or the awarded qualification is unrecognized by industry or government.

157. Consumers are often misled as the site looks like the real thing because study scams sometimes copy the web sites of legitimate educational institutions. The offer is made more attractive because the stated entry requirements and fees are lower than other institutions. There may even be a scholarship or other inducements such as computers or mobile phones offered

#### *Get rich quick scams: investments, gambling and pyramid schemes*

158. Get rich quick schemes come in many different formats, the most common being offers of investment schemes or gambling opportunities and pyramid schemes. Invariably these schemes come with inducements that guarantee large, quick, risk free rewards.





159. These schemes are often made to sound all the more enticing because they involve specialized computer software applications and the advice of successful expert or a 'proven' process. Testimonials by successful participants are a common feature and can be quite persuasive.

160. These schemes usually require up front fees for membership, special calculators and applications and exaggerated promises of returns. Investment schemes may involve no actual investments (because the fees paid by the victim are taken by the scammer) or overpriced or poorly managed assets or portfolios.

161. Gambling schemes may involve non-existent gambling forums, fictitious participation in real competitions or, less commonly, actual betting on real races or casino games or other competitions.

162. Pyramid schemes are a variation where in return for joining (with an upfront fee) the rewards are linked the victim arranging for others to join. Inevitably pyramid schemes must collapse, with most participants losing all of their 'investment'.

#### *Charity and health scams*

163. Charity scams involve scammers pretending to be collecting for legitimate charities or even non-existent charities. They frequently become active after catastrophic events such as tsunamis or cyclones/typhoons, epidemics or conflicts.

164. Charity scammers rely on the good will of consumers. By coinciding with catastrophic events they are hoping to get an immediate 'yes' response and receive the donation before the victim can do any research or have second thoughts. Scams using emails or web sites can make use of graphic photos of sick or injured children to reinforce the urgency and seriousness of their cause, and to breakdown victim resistance.

165. Health scams often target vulnerable consumers who:

- are suffering (or have family who are suffering from) incurable or chronic diseases and injuries including cancer, HIV, arthritis, back pain.
- are desperate for quick and easy fixes to age and lifestyle related problems such as obesity, impotency or hair loss.

166. These scams often feature 'miracle cures' or wonder products that offer a solution not provided by conventional treatments and products. They may also seek to appeal to consumers' preferences for traditional medicines or 'natural' treatments.

The major harm from these scams is usually the money lost in purchasing products that will not be effective. Unfortunately in some cases the harm is worse because the products (if any are supplied) that are usually sold outside the normal protections of regulated medicines, may have adverse effects on the victim's health. The harm can be even worse where the victim declines or ceases conventional treatments.

#### 4.2.4 Cross-border purchases

167. When consumers purchase over the Internet the process of buying is no more complex whether the e-trader is located in the same city as the consumer or in another country. Consequently when buying over the net consumers can easily purchase from a trader located in another jurisdiction. However, the post purchase ramifications may be significant.

168. E- traders will almost certainly be selling to consumers in multiple countries and those countries may well have different regulation in respect of:

- Product safety  
The importance and relevance of product safety to consumer confidence in online transactions was noted in ASEAN-Australia Development Cooperation Program Phase II: Supporting Research and Dialogue in Consumer Protection Consumer protection laws and regulations for online purchasing. This topic is more fully address in the Product safety and labelling module<sup>1</sup>
- Product labelling  
This topic is more fully address in the Product safety and labelling Paper. <sup>2</sup>
- Product approval  
For example some products such as pharmaceuticals may require specific approval to be sold in the consumer's jurisdiction. This topic is more fully address in the Health Services Paper<sup>3</sup>
- Warranties, repairs and refunds  
The common issue is the practicality of applying local consumer protections (national laws) to transactions where the trader is off shore and has no locally located assets. Merely asserting the application of national laws is meaningless to consumers if there is no means of enforcing those laws.

169. This problem is not unique to ASEAN and is a challenge for jurisdictions around the world. The problem is exacerbated in smaller economies because international traders may either not adequately consider compliance with local laws or conclude that:

- The profits from local sales are insufficient to make a business case for the incurring the compliance costs
- The inability of local authorities to enforce national laws on cross border transactions and consumer apathy about non compliance mans that non compliance does not significantly affect sales or the business case for incurring compliance costs

---

<sup>1</sup> See Module on Product Safety and Labelling. Luke Nottage (Dec, 2015). UNCTAD and ASEAN Secretariats. Project on Strengthening Technical Competency for Consumer Protection in ASEAN.

<sup>2</sup> Loc. Cit.

<sup>3</sup> See Module on Health Care services. Allan Asher (Jan, 2016) with the support of Carlota Montes. UNCTAD and ASEAN Secretariats. Project on Strengthening Technical Competency for Consumer Protection in ASEAN



- Current international arrangements in respect of mutual recognition of laws, enforcement of foreign judgments etc. are insufficiently developed and robust to prompt conscientious compliance with the consumer protection laws in multiple jurisdictions

### 3.2.5 On-line security

170. Three broad types of security threats are commonly identified (ref <http://www.ijarcce.com/upload/2013/july/69-o-Niranjanamurthy%20-The%20study%20of%20E-Commerce%20Security%20Issues%20and%20Solutions.pdf>):

- Denial of service  
For most consumers denial of service attacks are nuisance rather than a serious security threat. The strategies for preventing unauthorised access, theft and fraud will also help minimise denial of service attacks.
- Unauthorized access to information  
While unauthorised access to information may be a precursor to theft and fraud, information may be misused for any number of purposes, including so called identity theft (impersonating another person online), spreading misinformation, social and business embarrassment
- Theft or fraud of information or money  
Money can be taken directly, for example through bank transfers, or indirectly through the purchase of goods and services using the victim's credit card details. Information can be sold to 3rd parties for any number of purposes. For example to create address lists for spam, for commercial intelligence etc.

171. Consumers are most often concerned about online security in respect of:

- Payments
- Data protection and privacy

172. Most frequently security breaches result from the unintended downloading and installation of malware (described below).

173. However, e-commerce like its traditional bricks and mortar counterparts are also vulnerable to unauthorised off-line access to consumers' information and theft or fraud by individuals, for example by:

- A person watching consumer type in passwords or be reading written down passwords
- Business employees misusing access and knowledge of consumer information such as credit card numbers and passwords

### 3.2.6 Malware



174. 'Malware' is a collective name for malicious software that interferes with the users' intended use of computer technologies by damaging or disrupting its functionality. The term includes:

- Viruses that disrupt e-commerce transactions through denial of service. Viruses are generally installed when users click on an executable file (for example a '.exe' or a '.zip' file) attached to an email.
- Worms are a self-replicating subclass of viruses. The replication process, often through sending copies of the malicious code to everyone on a user's contacts list may overwhelm bandwidth or servers resulting a denial of service. Installation of worms may not require the user to click on an executable file.
- Trojans (Trojan horses): applications down loaded to a consumer's computer that hijack the system and allow remote 3rd parties to initiate activities on the hijacked computer. For example a Trojan can be used to copy data (user names, passwords, email contact details, keystrokes etc.) from a computer or to allow a 3rd party to use the computer's resources and connections to send emails or to complete transactions such as placing orders or transferring funds.
- Blended threats that combine the characteristics and harms of viruses, worms and Trojans

(reference: <http://www.webopedia.com/DidYouKnow/Internet/virus.asp>)

175. Many guidelines for managing risks are available on-line from government authorities and businesses well established in e-commerce trader, or intermediaries.

Consumers can reduce the risk of a compromised (infected) system, more effectively respond to malware attacks and reduce the damage (financial and convenience) by:

- Keeping their operating systems and applications up to date most operating system developers update their operating systems to include fixes to recently discovered vulnerabilities and malware threats. Malware attacks are often more successful on out of date operating systems.
- Only installing applications and updates from the trusted sites, for example the original vendors' site.
- Malware can be installed under the guise of updates to popular applications. By only downloading from the original vendors site (or some other trusted download sites) consumers can use the security of those sites.
- Using the security features imbedded in the installed operating system Most operating systems have inbuilt security features such as firewalls or related free security applications. These features may not always be on by default or can be turned off.
- Installing and routinely running anti malware applications downloaded from well-established and reputable applications developers.



- There are many useful and reputable anti malware applications with various features and costs.
- Maintaining a regular backup routine so that the operating systems, applications and data can be restored if compromised by malware.
- When a computer has been compromised by malware it is sometimes advisable or necessary to reinstall the operating systems, applications or data files. However this option will only be available if the user has maintained a robust backup regime.
- Being aware of the warning signs indicating that an email or website presents a higher risk of malware, and taking appropriate actions. For example not opening the email, not downloading or opening suspect files and leaving (or not visiting) suspect websites.

Reference: <http://www.ijarcce.com/upload/2013/july/69-o-Niranjanamurthy%20-The%20study%20of%20E-Commerce%20Security%20Issues%20and%20Solutions.pdf>

### **3.2.7 Data protection and privacy**

176. Consumers principal concerns about data protection and privacy are that personal information about them may be:

- Used by the trader to whom they gave the information for unknown, unexpected or unwanted purposes
- Obtained by third parties, without the informed consent of the consumers, and then used for unknown, unexpected or unwanted purposes.

177. Before credit and debit cards and before the Internet, the vast bulk of consumer transactions were done with minimal collection and processing of data about the consumer. For example in most cash transactions involving non-ongoing contracts between a consumer and trader, the consumer was not required to provide the trader with any personal information. Even for larger purchases and the establishment of an ongoing relationship, the information required by the trader was often not much more than the consumer's name and address. However, the use of credit and debit cards and remote purchases (using phones and the internet) has led to a huge increase in the frequency with which the personal information about consumers is being collected by traders and intermediaries.

178. Traders and intermediaries collect information for a variety of purposes including:

- Identification of the consumer for security of payment or for delivery
- Collection of market intelligence to improve their own performance (for example better marketing, stocking, inventory management etc.)
- Building a marketable asset for sale or hire



179. Intermediaries already have significant information about cardholders from the card issuing process including:

- Name and address
- Account number and passwords
- Gender and age
- Contact details including telephone numbers and email addresses
- Income and assets
- Employer
- Other cards held

180. Traders sometimes collect this information. For example tradition traders may ask for name and address if goods are being delivered, or routinely ask for information such as suburb or postcode. Distance traders, including mail order traders, e-commerce traders will routinely require this information before a transaction can be concluded.

181. When consumers use their cards traders and intermediaries collect transactional records showing the goods or services bought, the price paid, the time and date of the transaction and the store location. Combining transactional information with information already held allows traders and intermediaries to analyse the data in respect of individuals and customers generally.

182. Person data is a valuable commodity to intermediaries, traders and others because it significantly adds to their market intelligence, both generally through aggregated data and specifically in respect of individual consumers. Personal a data can be sold between businesses and stolen.

183. The advantages of personal data collection to the consumer may include:

- Better targeted offers of additional goods and serves
- Analysis of personal data has the potential to facilitate better targeting of offers to match consumers' needs, wants and preferences
- Better fraud detection
- Card issuers can use the information about individual consumers and their card usage to identify likely fraudulent use and then alert the cardholder
- Offers of additional or different goods and services



- If analysis of data reduces traders operating risks they may offer goods and services that they otherwise would not have, or they may offer them to additional consumers who they previously would have rated as too risky.

184. The disadvantages of personal data collection to the consumer may include:

- Data may be used by traders and intermediaries unknown, unexpected or unwanted purposes. For example a consumer may happily provide a home address thinking that this information simply relates to identification and delivery, whereas it may be used to build a profile of the likely future value of transactions and the risks of non-payment.
- Data may be obtained by 3rd parties with the agreement of traders and intermediaries and used for unknown, unexpected or unwanted purposes.
- Data may be obtained by 3rd parties without the agreement of traders and intermediaries and used for unknown, unexpected or unwanted purposes. For example when trader and intermediary databases may be hacked. The hacker may use the data for market intelligence or for nefarious purposes including fraud and blackmail.

185. These risks are covered in more detail under 'Malware' above.

186. Managing data protection and privacy in the context of consumers using mobile phones, the Internet and e-commerce requires a range of strategies including:

- Consumer education  
While many consumers are generally concerned about data protection and privacy most probably do not understand the scale of data collection and its implications, or what they can do to protect their own personal information. While individual consumers cannot usually negotiate with e-traders or intermediaries about what information they must provide in order to complete transactions they can:
  - protect their data from unintended disclosure, particularly data theft and destruction via malware
  - monitor, at least to some extent, what personal data traders and intermediaries maintain and seek to correct inaccuracies
  - support consumer protection authorities and consumer organisations advocating for greater data protection and privacy protections

The key education messages are explained below.

- Trader education  
More informed and informative behaviour by traders is likely to significantly diminish consumer concerns in respect of data protection and privacy and increase consumer confidence in e-commerce. For example traders should be fully informed of their legal obligations in respect to the collection and dissemination of personal information from consumers and encouraged to develop and implement compliance programs to manage their risks effectively.

*Data protection and privacy legislation*



187. Many countries have enacted legislation to address data protection and privacy concerns, particularly in the EU. The UK's Data Protection Act provides an excellent illustrative model. Its scheme is based on 8 key principles:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act. The list rights address:
  - subject access request
  - damage or distress
  - prevention of direct marketing
  - automated decision taking
  - correcting inaccurate personal data
  - compensation

138. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

139. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Reference: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/>

188. Data protection and privacy regulation varies widely from country to country and is more fully addressed in the Consumer Credit and Financial Services Paper.

#### **4.2.8 Secure payments**

189. All methods of payments and money transfers have risks associated with them. For example carrying cash to a shop has always carried with it the risk of robbery. Non-cash payments, for example those by credit or debit card give rise to different risks, such as the fraudulent use of cards in unauthorised transactions (for example, a consumer misusing a card



given to them by their employer) card or transactions by unauthorised persons (for example where a store employee uses a consumer's card for their own purchases).

190. When consumers go online there are some additional and very significant risks:

- Their information will be accessible to multiple parties, many unknown to the consumer
- Their information, once accessed can be easily copied and distributed

191. The major security concerns are encountered across platforms, whether the Internet is accessed via computers or mobile devices (so called M-commerce), and no matter what operating system is used, although vulnerabilities do vary.

192. Security problems may be encountered at any step of the e-commerce processes. The basic steps in a secure e-commerce transaction are:

- Verification of the merchant
- Review of order information
- Verification of the customer
- Review of payment information
- Confirmation of order
- Authorize or deny payment

193. One of more payment systems (to provide verification of the parties and authorize or deny payment) will be involved in every e-commerce transaction, all of which must offer a high level of security, if consumers (and merchants) to feel secure:

- Credit cards  
Well know credit cards include Visa, MasterCard and American Express
- Bank accounts  
Customer may use bank issued debit cards or transfer money directly through online banking facilities
- Online buying:  
Payflow Pro, 1 ClickCharge are applications that allow customers to purchase securely from e-traders
- E-Bill payment: CheckFree (US), PayTrust (US) , BPAY (Australia)
- Electronic cash: applications that allow buyers to app sellers who don't have credit card merchant accounts, for example Paypal



194. The elements involved in any particular transaction will depend upon the nature of the transaction and the choices made by buyers and sellers.

195. While there are multiple security tools available to consumers and traders, there remain major weaknesses in online security of payments. Security tools include:

- Firewalls  
Most operating systems and add on security applications include an optional firewall that is design to detect potential malware and block its installation
- Public key infrastructure allowing encryption applications, digital certificates (for hardware) and digital signature for users
- Biometrics: for users, for example finger prints
- Passwords
- Locks and bars to prevent access to listed sites or at particular times

196. As with all technology centred consumer activity new problems are emerging as consumers and traders take advantage of advances in those technologies. A July 2014 ICPEN report International Consumer Protection and Enforcement Network Report on Mobile Payments examined the expanding use of mobile payments and the resultant challenges to consumers and consumer protection authorities. That report noted that ‘in the past, consumers used mobile payments mainly to purchase digital services that they consumed on their mobile devices. Recently, however, consumers’ use of mobile payments for purchases has expanded and now includes a wide range of goods and services. With consumers’ increasing use of mobile devices, which now includes smartphones and computer tablets, this expansion is ongoing.’

197. The topic of payments and money transfers has been addressed in ASEAN Australia Development Cooperation Program Phase II: Supporting Research and Dialogue in Consumer Protection Money transfer fraud, July 2014.



#### **4.3 Some strategies for addressing the most frequently experienced consumer problems**

Learning objectives and outcomes of Section 6.3

198. This section of the train-the-trainer manual:

- Provides a comprehensive list of recommendations about the key messages relevant to the most commonly encountered scams, that need to be included in consumer education activities
- Following completion of the train-the-trainer sessions, participants should be able to:
  - discuss the key consumer messages
  - appreciate the limitations of consumer education and the importance of intermediaries in maintaining the urgency of educational messages
  - discuss ideas for enhance the dissemination of key messages

199. Consumer protection authorities have a wide range of strategies to use when public intervention in the market is deemed necessary. In broad terms these tools involve:

- Market surveillance
- Consumer education
- Business education
- Investigations
- Dispute resolution
- Interagency co-operation

200. Each of these is likely to have a role in consumer protection in respect of telecommunication technologies, specifically the use of mobile phones and the Internet, including e-commerce.

##### **4.3.1 Consumer education**

201. Consumer education includes but must not be limited to knowledge of their rights and obligations under consumer protection and other legislation.

202. Prevention and avoidance strategies are the most cost effective response to scams generally, and particularly with respect to those scams using telecommunications. Effective education of consumers is the key element of these strategies.

*General advice*



203. General advice:

- If it is too good to be true, it probably isn't true
- Remember communications at a distance reduces your ability to evaluate the trader and their products/services by talking to them in person and examining their shop and products.
- Email and the net provide consumers with will an increased ability to make wide enquiry about the trader and the goods. Use them. For example many consumer protection agencies and provide organisations around the world provide free information on scams: [consumers.ftc.gov/scam-alerts](http://consumers.ftc.gov/scam-alerts), [scamwatch.gov.au](http://scamwatch.gov.au), [scambusters.org](http://scambusters.org)
- Always do you checking prior to providing financial or other personal information or paying any money
- Report any suspicious offers to your consumer protection agency or other appropriate government agency

*Conduct specific advice*

204. Specific advice in respect of consumer protection problems encountered when using smart phones, computers to access the Internet, including e-commerce.

205. *Advance fee fraud schemes*

- Avoid arrangements with strangers requesting upfront payment via money order, wire transfer or international funds transfer. Scammers will suggest these methods of payment because they are quick and it is usually difficultly to recover money sent this way.
- Do some checking: conduct a search online using the exact wording of the offer to check. If the scam or a similar scam, has been operating for a while it is likely to have been reported on-line
- Don't open suspicious or unsolicited emails from people that you don't know. At the very least you may be sending a message that your account is active and this will trigger more emails. If you computer security is not strong you may be exposing your computer to malware. Worse you may be tempted to click on attachments or links that are a common source of malware.

206. *Lottery, competition and unexpected prize scams*

- If you did not enter a lottery or other competition then you could not have won.
- Legitimate lotteries and other competitions do not require winners to pay fees up front before receiving their prize





- Official looking documents and brochures that appear to have government approval or to have come from a reputable company may not be what they seem. Scammers go to a lot of trouble to make they fraud look respectable.
- Only dial premium numbers if you are really sure that you want the service offered. Using these numbers to claim a prize is the same as paying up front fees, its part of the fraud.

207. *Dating and romance scams*

- Never send money or give your personal details to someone you
- Have only recently met online, even if they tell a convincing story and ask for your support
- Avoid any arrangement with a new contact who asks for upfront payment
- Be alert if the new contact asks to communicate outside the dating website after only a few conversations

208. *Computer hacking via phishing emails and social network scams*

- Keep your software, including the operating system and apps, up to date
- Consider installing and using anti malware software. Keep it up to date.
- When visiting site on which you will enter your financial and other personal information go to that site directly (by typing in the URL or clicking on it in your favourites list) rather than by clicking on a link provided in an email or on a site that you are not certain of.
- Avoid responding to software updates prompts that appear on your screen when visiting new sites. For example rather than clicking on 'download' when notified that the installed version of Flash Player us out of date and that a newer version is available for download, go to the Adobe website and download Flasher Player from there.
- Be suspicious of all 'cold calls' (calls that you have not requested). Do not simply accept the caller's assertion about who they are. The caller should be able to give you sufficient information so that you can check them out before providing personal information. For example you can visit the organizations official site or phone the organization on their publically listed phone number.
- Do not click on links or attachments from senders you don't know.
- Be suspicious of emails that appear to come from family or friends but are in a different style or format to their usual emails. Typical example includes different subject descriptions or attachments.

209. *On-line auctions and advertising scams*



- Before shopping on-line do some preparatory research. Check out the website to understand its terms and conditions of usage and any security protection or warnings. Research the opinions of previous users of the site.
- Before buying from or selling to a particular seller or buyer see if the website rates their transaction satisfaction score, number of previous transactions and history of transactions
- Wherever possible use established secure payment process, provided by reputable websites. Look for a web address that starts with 'https'. Hypertext Transfer Protocol Secure (https) allows you to communicate securely with the web server. The communication is encrypted, so that even if it is intercepted it will be unintelligible without the decryption key. <http://www.healthit.gov>
- Do not accept overpayments.
- If payment is made via a non secure method such as cheque or money order do not hand over the goods until the funds have been transferred into your account.

#### 210. *Banking, credit card and on-line account scams*

- Banks and other legitimate traders do not broadcast generic warnings that ask you to take specific action. If you receive such an email, contact your bank directly via their publically listed phone number or web address, or visit the bank in person. Do not use the links provided in unexpected phone calls or emails.
- Report suspicious or incorrect transactions immediately. In most cases the consumer will not be liable for transactions that they did not authorise or allow to be authorised, and reported quickly.
- Frequently check your card transactions record so that if your account has been accessed without authorization, this can be reported to the financial institution with a minimum of delay.
- Do not access your on-line bank accounts via clicks on links provided in unexpected emails or from other web sites. When visiting a site on which you will enter your financial and other personal information, go to that site directly (by typing in the URL or clicking on it in your favourites list).
- When banking online check that the web site address is correct before entering your financial or other personal details. Look to see that the address starts with 'https' and has a closed padlock symbol

#### 211. *Employment scams*

- Be wary of unsolicited offers of employment or employment services, they are more likely to be a scam.



- Be wary of offers of employment or employment services made by SMS, email or on-line. You will need to do some research to check if they are genuine.
- Be wary of offers that require you to commit immediately or without much time to do your research. Giving you a tight deadline may be simply a means of making it difficult for you to check things.
- If you are required to pay fees up front make sure that you know what they are for and reasonable in the circumstances. If possible pay by a secure means such as by credit card that will generate a transaction path and records, including receipts. Avoid sending money orders or making wire transfers. Legitimate operations should provide secure payments
- Independently verify everything that you are told in the offer. You can do this by:
  - checking with relevant business associations
  - checking with relevant government agencies
  - on-line searches of the company to find out more about it and to see if others have had experiences with it
  - even doing a search on the key phrases used in the SMS or email can be very revealing. Often scams use the same phrases over and over, and other victims have or scams sites have noted this.
  - always check using multiple sources as sometimes scammers will create their own secondary site praising their scam as a legitimate enterprise, or place many favourable entries on independent blogs. Remember a few posted comments may not be sufficient. Look for patterns in the postings and put less weight on those that appear overly enthusiastic.
- Many require payment of fees up front. Often the required fees will be described as payments for training, travel, software, security clearances, visa fees, taxes and government charges. These scams can be difficult to identify because they may appear to be indistinguishable from legitimate employment services.
- Pyramid selling scams are sometimes disguised as employments services or offers of employment. The disguising feature is that in pyramid scams payment is dependent upon recruiting of others into the scheme.

#### 212. *Study scams*

- Study scams are similar to employment scams. In this case the lure is the offer of a place at an educational institution.
- General study scams require the student victim to pay fees up front. The victim then finds that the courses:
  - the institution or course do not exist or course are cancelled
  - the courses are substandard and/or the awarded qualification is unrecognized by industry or government.
- Study scams sometimes copy the web sites of legitimate educational institutions



- The offer is made more attractive because the stated entry requirements and fees are lower than other institutions. There may even be a scholarship or other inducements such as computers or mobile phones offered.
- Beware of offers or schemes claiming to guarantee income or requiring payment upfront. Never agree to an offer over the phone: ask for it in writing.
- Do your research before agreeing to any offer: ask around, search online

213. *Get rich quick scams: investments, gambling and pyramid schemes*

- Remember that schemes that sound too good to be true usually are. Consumers should be encouraged to ask themselves: 'if this investment in a gambling system is so good, why would the scammer encourage others to join in? Wouldn't they make more money be keeping it to themselves?'
- Independently verify everything that you are told in the offer. Search for information about the type or investment or gambling, the name that the trader is using and for key phrases in their promotional material.
- Do your research before signing up or sending any money
- Check to see if the type of scheme being offered is legal in your country. For example many countries prohibit participation in pyramid schemes and regulate gambling and have controls on foreign transfers of money. Gambling schemes can sometimes be used to facilitate money laundering.
- Think before sending any money. Can you afford to lose the money you are being asked to send, if the scheme is a scam?

214. *Charity scams*

- Do your research; check out the charity before you donate. You can do this online or by contacting the relevant government authority.
- Give yourself some time to think about it. Do not let yourself be pushed into committing to a donation, particularly an ongoing donation like child sponsorship, immediately if that's not what you want to do.

*Businesses as providers of consumer education*

215. Unfortunately consumer education will never be the complete answer to scams because:

- Not all consumers will receive the education message
- Not all consumer who receive the message will act on the messages



- Consumers are constantly entering and leaving the market, so a messages need to be repeated periodically

216. Businesses providing facilitating services such as mobile phone services and Internet connection services, as well as e-commerce traders can all play an important role in consumer education because:

- They have an interest in consumers having a problem free experience using their services
- They have direct access to their customers
- They are likely to be one of the first recipients of consumer complaints
- They often have the means of responding effectively to consumer complaints, for example by denying scammers access to their services

*Note on consumer protection and social media*

217. According to [whatis.techtarget.com/definition/social-media](http://whatis.techtarget.com/definition/social-media) social media is 'the collective of online communications channels dedicated to community-based input, interaction, content sharing and collaboration. Websites and applications dedicated to forums, micro blogging, social networking, social bookmarking, social curation (collaborative sharing of web content), and wikis are among the different types of social media.'

218. Currently (Oct 2015) the most popular social media networking services, each with >100,000,000 'Estimated Unique Monthly Visitors' (ref <http://www.ebizmba.com/articles/social-networking-websites>), are:

- Facebook
- Twitter
- LinkedIn
- Pinterest
- Google+
- Tumblr
- Instagram

219. These social network applications/services may be accessed through any device accessing the Internet, including smart phones. They are enormously popular throughout the world.



*Consumers, traders and consumer protection agencies all use social media*

220. Consumers typically use social media to:

- 'shop around' to better understand the qualities, prices and sources of goods and services they may be interested in
- learn from the experience of other consumers, as reported on social media.

221. Consumers should be advised to use social media with caution as it is generally not regulated or mediated, with the result that the relevance, accuracy and fairness of content is highly variable.

222. Traders may use social media for a number of purposes including:

- Advertising or generally promoting their brand, goods or services
- Market intelligence
- Responding to particular or general complaints and enquiries about their goods, services or company
- Recruiting staff

223. Consumer protection authorities may use social media for a number of purposes including:

- Market intelligence gathering
- Receiving complaints
- Disseminating educational messages

224. Consumer protection authorities should be aware of both the benefits and challenges of using social media. Social media may offer significant advantages:

- Speed of message transmission. Many consumers, particularly young people check their favourite social media many times per day.
- Breath of coverage. The number of people who regular use social media is huge, in every country.
- The cost of using social media is minimal when compared to the costs associated with traditional communications such as advertising and publishing.

225. However, agencies need to be careful when using social media because social media:





- Is generally an open forum where an agency will not be able to restrict who may view its postings.
- Involves two-way communication that is very different from traditional advertising and dissemination of educational materials. Consumers, traders and anyone else accessing the particular social media may respond directly and publically to anything posted by an agency.
- Is largely unregulated and unmediated, so that there is no quality control over postings. Furthermore many posting are anonymous.

#### **4.3.2 Business education**

226. As with consumer education, business education is far more than merely providing knowledge about relevant consumer protection laws. Traders need to know:

- Their specific obligations:
  - positive obligations, for example things the must do, such as provide mandated warranties and
  - negative obligations, for example avoiding proscribed conduct such as false or misleading representations
- The activities and conduct that constitute the highest compliance risks for their type of business, for example:
  - the provision of telecommunications services such as mobile phone services, internet access etc.
  - the provision of on-line trading
- How they, like consumers, can become the victims of on-line scams
- How they can manage their consumer law compliance risks by developing and implementing a consumer protestation compliance program

#### *Codes of conduct*

227. The concept of 'codes of conduct' is a simple one: the specification of trader conduct that would avoid or mitigate harm to consumers. Codes of conduct can come in many shapes and sizes, from comprehensive schedules of required or prohibited conduct through to very specific prescriptions and proscriptions about particular terms of contracts or trader conduct. Codes of conduct can be developed and implemented by:

- Individually traders
- Traders or industry organizations
- Government authorities

228. In many countries codes of conduct developed and implemented by traders or trader associations have been discredited or diminished in status because they have been perceived as ineffectual or self-serving.

229. Common reasons for the failure of industry codes to deliver effective consumer protection outcomes may include:

- Failure of the code to address the major consumer protection issues
- Poor coverage of traders in the market place
- Inadequate performance appraisal, review and remedial action
- Inadequate or absent detection of contraventions or non-observance
- Inadequate remedial action following detection of contraventions or non-observance

230. It is inevitable that some traders will deliberately or inadvertently contravene or otherwise fail to observe at least some code requirements. Quick, effective remedial action is required if contraventions are to be stopped and further contraventions discouraged.

- Poor recognition by consumers  
If consumer do not know of the scheme or rate it as relevant and effective the operation of the code will not influence their purchasing decisions. If the code does not influence their purchasing decisions it will have poor uptake and implementation by businesses

#### *Standard contracts*

231. Standard contracts have an attraction to regulators and sometimes to consumers because they offer the promise of contracts that:

- Address all of the recognized elements of the transaction and
- Allow for easy comparison between competing suppliers and models
- Address particular problems that market forces or existing regulations have not resolved.

232. However, standard form contracts may not be appropriate or produce the expected benefits if:

- The relevant products are highly customizable as between customers
- The attributes of the products and/or their uses is variable because of changing technologies, supply conditions and consumer demand



- The standard form contract can easily be avoided and its protections lost. For example scammers are unlikely to be concerned with standard form contracts, or written contracts at all.

#### **4.3.3 Interagency co-operation**

233. In the context of the:

- Diversity of consumer protection regimes within ASEAN
  - Limited resources of government authorities
  - Strategic advantages of involving the non government players
- interagency co-operation should be wider than simply relations between government authorities with consumer protection responsibilities. Of course in most member states it is intergovernmental relations that will be prioritised.

234. Consequently in this paper the term 'stakeholder' is used and it is taken to mean external organisations and people who have a particular interest or concern in the activities of a consumer protection authority. These include:

- Consumers
- Consumer organisations
- Businesses
- Business associations
- Other government authorities

235. Interacting or engaging with these groups can offer a consumer protection authority significant benefits including:

- More informed decision making based on information and opinions provided by stakeholders
- A more effective complaints handling: more complaints, complaints from a wider cross section of the community, easier access for complainants organisations
- More effective educational activities
- More effective investigations
- More effective remedies and sanctions

236. That stakeholder engagement is a desirable aspiration for any government regulator is somewhat of a 'motherhood statement'. Who would argue against it? However, for many



regulators sustained actions do not follow the aspirations. Where stakeholder engagement does occur, it is often ad hoc or relying on the energy of one or two activists at particular points in time.

237. The good intentions of a consumer protection authority and stakeholders and individual activism are insufficient by themselves ensure that the benefits of engagement are sustained in the longer term. Adopting a considered, strategic approach to stakeholder engagement is likely to maximize the long term benefits to a consumer protection authority and coincidentally to the participating stakeholders.

238. This section has drawn upon the Stakeholder Engagement Standard 2011 (AA1000SES) – UK Institute of Social and Ethical Accountability (UK), Final Exposure Draft and publications by other regulators influenced by that Standard.

*Who are stakeholders and are some more important than others?*

239. In general parlance an agency's stakeholders are those individuals or groups who have a vested interest into the outcomes of the authority's activities and performance. However, not all stakeholders have the same level of interest or the same ability to benefit an authority. Key stakeholders include consumer organizations, business association and other government authorities because they have a tangible interest in an authority's consumer protection activities and performance because their respective rights and obligations and the consequential benefits and costs will be directly affected. Importantly they also have the potential to benefit the operations of the consumer protection authority. For the reasons noted below a consumer protection authority's ability to effectively and efficiently achieve its objectives will be significantly enhanced by successful engagement of key stakeholders.

240. The following discussion focuses on two significant stakeholder groups: 'other' government agencies and consumer organisations.

*Realizing the benefits of engaging with consumer organizations may not always be pain free*

241. It is easy to assume that the interests of a consumer protection authority and its stakeholders are and will remain the same. This may not necessarily be the case. Each stakeholder has:

- Different objectives and functions  
For example the objectives of a
  - a consumer organization may be much narrower than those of a consumer protection authority, and their functions more limited.
  - each government agency will have its own legislation and policies
- Different constituency,  
For example
  - a consumer organisation is responsible to its members rather than government (members, not government) unless, as in the situation of Singapore where the consumer association CASE has a unique arrangement with government.
  - another government authority may well report to a different Minister

- Different legal powers and constraints

For example:

- a consumer organisations may have no formal power to investigate or to impose sanctions, nor any legal obligation to investigate or to report to parliament
- another government agency have quite different powers (for example no power to prosecute, but the power to grant of revoke licences) and be constrained by other government polices, for example national or sector development, contractual obligations, international politics

- Different priorities

The differences in objectives, functions, resourcing, regulation affecting legal status, accountability and transparency will all affect priorities.

For example:

- a consumer organisation may prioritise issues most affecting its particular members or the special interest of its executive, whereas a consumer protection authority may prioritise issues that are causing the most serious and/or widespread harm and where it is most likely to achieve a worthwhile result.
- the regulator of telecommunications services may prioritise the long term commercial viability of service providers ahead of current consumer protection concerns.
- a police department, although interested in consumer problems such as fraud or unsafe goods may prioritise investigations into drug and violence offences

242. Consequently consumer protection authority/stakeholder engagement should:

- Identify, recognize and manage differences. Failure to do so may transform differences of opinions or operating environments into impediments to co-operation and give rise to a 'lose-lose' scenario.
- Recognize that the benefits of engagement will vary between issues, over time and between organizations. The fact that benefits may be enjoyed more by the authority or by a particular stakeholder in respect of any one issue is unlikely to be an impediment to engagement, so long as significant benefits accrue to each organization in the longer term.

#### *Distinguishing between strategic and operational elements*

243. Strategic principles include:

- Significance: identify and address those issues of greatest significance to the consumer protection authority and to consumer organizations.
- Completeness: develop and maintain a comprehensive appreciation of the selected issues from both the authority's and stakeholders' perspectives
- Responsiveness: 'actions speak louder than words.' Respond coherently, appropriately and without undue delay.



244. Operational principles include:

- Communication: open and effective communication
- Transparency: clear and agreed information and feedback processes
- Collaboration: work to seek mutually beneficial outcomes where feasible
- Inclusiveness: recognize, understand and involve stakeholders in the process
- Integrity: conduct engagement in a manner that fosters mutual respect and trust

245. Key elements:

- Identifying key stakeholders

The purpose of stakeholder engagement is the increased effectiveness and efficiency in attaining the authority's own goals. Not all organisations that identify as stakeholders will meet this criteria. Because stakeholder engagement requires resources it must be managed like any other activity. However, tolerating some 'coasters' who cannot significantly contribute to organisational objectives may be a small price to pay for being inclusive of significant interest groups.

In the context of consumer protection issues involving the use of telecommunication technologies the following government agencies are likely to be key stakeholders:

- telecommunications regulator(s) responsible for licencing and technical standards
  - the national standards authority
  - the police force
  - customs and excise
  - taxation
- Identifying significant stakeholder issues. This process involves two steps:
    1. Identifying the relevant consumer related issues that are important to the identified stakeholders and determining the co-incidence of interest
    2. determining the significance and appropriateness of mutual interest consumer related issues by asking questions such as:
      - is this an issue where the Authority/agency is bound by government policy?
      - is this an issue where the Authority/agency is bound by legal or financial constraints
      - is this an issue where the Authority/agency is restrained by corporate governance or other ethical considerations?
      - is this an issue that will have wider ramifications than just the immediate authority/stakeholder relationship?

The answers to these questions will help shape the authority's judgment as to what issues can be addressed through the engagement process and how they might be approached

246. *Preparing and engaging*



- Understanding senior management expectations  
It is likely senior management already have expectations and perhaps conceptual plans about engagement with consumer organizations. As with any purposeful journey, the intended destination is the starting point. Senior management needs to articulate:
  - what objectives they want the engagement to achieve
  - how they see the process working, at least in general terms
  - the budget
  - which Branches and officers are responsible for particular strategic and operational elements of the engagement program.
- Understanding expectations of each stakeholder to be engaged.  
Fully appreciating the stakeholders' perspective can be difficult and require some effort:
  - Consultations
  - Public statements

247. *The formal basis for engagement*

248. Some consumer protection and other regulatory laws may expressly provide for co-operation between specified agencies, including information sharing, joint investigations and other activities. If they do, then the requirements of the law(s) must be complied with.

249. More often they do not. Generally consumer protection authorities do not need a formal basis for engaging with stakeholders, but more successful engagement is likely when it is based on a formal stated basis. This can be as simple as an exchange of letters between the agencies or a more formal document such as a Memorandum of Understanding (MOU). MOUs are often the vehicle chosen when the relationship is expected to be ongoing and involve significant exchanges of information, or costs to either or both parties. MOUs establish the terms of engagement and formalise protocols, so minimising the need for ad hoc decision making and the potential for inadvertent, unauthorised disclosures or other actions.

250. A typical MOU includes the following elements:

- The objectives and purpose of the MOU
- Any guiding principles
- The respective roles and responsibilities of the parties
- The expected outputs and outcomes
- The operational dates (commencement and end of the MOU)
- Conflict resolution procedures  
In the event of a serious conflict between the parties the likely result will be the termination of the MOU. However, by specifying conflict reposition procedures is likely

that minor problems or problems resulting from inadvertence or misunderstanding can be quickly and effectively resolved.

- Confidentiality issues and processes  
Where a party to the MOU possesses confidential information, regulation or policy may prevent it from providing that information to other parties. An MOU may recognise this limitation to co-operation, or it may provide procedures that will manage the exchange of confidential information to the satisfaction of the parties. This could be as simple as the receiving party agreeing to the confidential status of the information and implementing procedures to safeguard that confidentiality.
- Resourcing  
Where there are likely to be non-trivial costs incurred, the MOU should specify the party responsible for various costs. This will be more important where the costs are otherwise borne disproportionately to the perceived benefits.
- The legal implications of the MOU  
Most MOUs specifically state that the MOU does not create any binding obligations on the parties and its operation is subject to relevant laws, regulations and policies of each party.

251. MOUs should generally be made public to ensure transparency and accountability.

252. Other means of approaching stakeholder engagement can include:

- An exchange of letters  
An exchange of letters between the parties is less formal and quicker to execute than the typical MOU and may be satisfactory where the level of interaction between the parties is low or temporary.
- A contract for services  
A contract for the provision of services may be appropriate where the services are:  
specific, for example product testing  
where the party providing the services routinely provides such services on a commercial basis
- where the party providing the services would not otherwise be willing to provide them

#### *Budgetary considerations*

253. All authority activities cost money and the engagement with stakeholders is no exception. Costs will be borne by both the consumer protection authority and stakeholders.

254. Likely costs include those:

- Associated with specific engagement activities arising from engagement
- Depending upon the activities these costs can be very significant. Activities such as market surveys, educational campaigns, investigations, product testing etc. cost money.

Where the amounts are small or ad hoc stakeholders may be willing to simply absorb them as part of their own budget. They are less likely to do so when costs are more significant or more frequent.

- Costs may entail more than simple cash expenditure, for example indirect costs and opportunity costs (that is the cost of not undertaking alternative actions). As a routine component of the engagement process it is important to explicitly agree on processes for:
  - estimating expected costs
  - approving the proposed budget and the responsibility for various costs
  - reviewing expenditure
  - undertaking any required remedial actions
- Associated with the engagement process:
  - secretariat expenses that may include costs such as a part-time coordinator, stationary, printing/copying etc. These are necessary overheads, so they should be accountable and allocated against the engagement budget rather than just being absorbed into other budgets.
  - attendees' costs
  - while other government agencies would normally carry their own costs associated with engagement process, this may not be a viable burden for consumer protection organisations.
  - meeting reasonable travel and other out-of-pocket expenses, or even paying a modest attendance/participation fee sends a strong and unambiguous message that the Authority values their input and does not simply take it for granted.

#### *Appropriate working arrangements*

255. Agreeing appropriate working arrangements will make the engagement process progress predictable. Important components of predicable arrangements will be:

- Nomination of contact officers  
One or more contact officers should be identified in the consumer protection authority and within each stakeholder participant. Failure to do so at the outset will result in lost or inappropriate communications requiring unnecessary duplications, delays or decision making without full knowledge of relevant information. Contact officers should have sufficient authority and time to take appropriate and timely actions.
- Branding  
Generally any authority undertaking activities to protect consumers will want to consumers and other stakeholders to be aware of its efforts, even if other agencies are also involved. This is achieved by 'branding' of activities that identifies and differentiates them from other agencies' activities. The effectiveness of branding can be less effective if the message is unclear or complicated.  
Misunderstandings about branding or 'who gets credit for what' should be agreed before joint activities commence. In particular a media strategy and individual announcements should be mutually agreed.

- Regular meetings

Agreed regular meetings with significant stakeholders will engender practical commitment and expectations. Regular meetings should not be postponed or cancelled without significant reason or due notice because that will be interpreted by stakeholders as an indication that the meetings are of secondary importance to the consumer protection authority's other activities.

Ad hoc meetings should only be called when there is a matter that cannot be held over to a regular meeting or dealt with by direct communication. Inappropriate ad hoc meetings will be disruptive to the organisations' planning and operations, and may be interpreted poor organisation and planning.
- Settling agendas prior to meetings

Setting agendas allows participants to plan ahead and prepare their own presentations or responses. Encouraging stakeholders to nominate agenda items will give them a sense of ownership and empowerment.
- Circulation of most documents prior to meetings

Often proper consideration of agenda items will require knowledge of relevant information, most often in documents. Circulation of most documents prior to meeting with sufficient time for them to be read and considered will facilitate informed discussion
- Proper meeting procedures including agreed agendas and a degree of formality agreed by participants.

Adoption of proper meeting procedures, agreed by participants, will facilitate ordered discussion and reduce the risk that some representatives feeling disenfranchised by stronger personalities and ensure that representatives are confident about what had been discussed and agreed to when they report back to their respective organisations.

A degree of formality will make it easier for the Chair to maintain control over the meeting without inhibiting full and frank discussion. This will be very helpful when emotions are running high, representatives 'pet' issues are in debate or the meeting is running over time. How formal procedures should be is a matter for the participants, with due consideration to any established norms.
- Taking, circulating and settling meeting minutes

Taking, circulating and settling minutes is a time honoured way for creating an agreed record of who attended particular meetings, what matters were discussed and what was agreed at meetings. As with all minutes, care must be exercised when deciding how detailed the minutes should be. If discussion or information is considered confidential that should be noted in the minutes.
- Action items

Designating and assigning 'action items' and including them as a standard agenda item can be a useful way of prompting participants to follow-up on meetings and prepare for future meetings.
- Appropriate direct communications

Direct communications with individual organizations or representatives outside of regular Committee meetings have an important role to play in:



- urgent matters that need to be actioned before the next meeting
  - matters relevant to only one or just a few participants
  - discussions involving a level of detail not appropriate for regular multi party meetings, for example the administrative arrangements for co-operative activities or the provisions of case specific information.
- Duration of meetings
- There is no optimal length of meetings, or start and finish times. What will be far more important to participants is whether a meeting is well run and that each of the agenda items is both relevant to the Committee (if not each participant) and deserving of their attention (i.e. a priority issue).
- Generally participants will appreciate a break after 2 hours with a chance for refreshments and use of washroom facilities. If participants can be encouraged to stay together at the venue over a lunch break the momentum of the meeting is less likely to be lost.
- Starting and concluding meetings at the agreed time will generally be greatly appreciated by participants unless, in the case of the finishing time, all agree that an extension is required. In that case it will be desirable to formally extend the meeting rather than simply let it run on.

#### Reviewing and reporting

256. A formalised and scheduled engagement evaluation process will maximize the likelihood that the benefits of engagement will be realised in the long run. Agreeing relevant performance evaluation criteria will help focus minds on whether the identified benefits are attainable and whether the proposed process is likely to facilitate their delivery.

The easy to obtain quantitative measures such as 'the number of complaints received/referred via the organizations' may sometimes be informative but more often are of limited value because they are the result of multiple causative factors. It will be the more difficult to measure subjective elements that are like to be a better measure of real performance.

257. Easily quantifiable measurements have their place because they help quantify the engagement experience. For example the:

- Number of meetings per year
- Number of organizations represented at each meeting
- Number of agenda items at each meeting
- Number of actions agreed
- Number of complaints received via the organizations
- Number of [name of authority] items published on organizational website or in their publications



- Estimated number of consumers influenced, informed or educated by co-operative [name of authority] /[name of stakeholder(s)] activities

258. More difficult to measure, more subjective to evaluate and usually more useful measures may include information such as the:

- Extent to which consumers changed their thinking or buying activities due to co-operative [name of authority] /[name of stakeholder(s)] activities
- Strength, credibility and influence of organizations' public and private support of [name of authority] and advocacy for the /[name of consumer protection law] the quality of organizations' contributions contributing towards eliminating or reducing consumer problems
- Influence of organizations' views and submissions on [name of authority] policies, practices and actions.

259. These subjective measurements may be achieved through surveys and interviews of consumers, consumer organizations members, [name of authority] staff etc. and analysis of publications, public statements and media reports. Once a methodology has been developed it should be undertaken regularly to facilitate identification of temporal patterns and regular reporting to [name of authority] and [name of stakeholder(s)] management.

#### *Confidentiality*

260. All government agencies may sometimes require information to remain out of the public area for a variety of reasons including that disclosure of certain information:

- Will jeopardise the future provision of information essential to the agency's operations
- Prior to certain enforcement actions can give people time to dispose of evidence
- Prior to the launch of educational and information campaigns can reduce the success of campaigns because the messages are no longer 'news'
- That might be detrimental to individuals or their businesses can leave the agency open to legal action or negative publicity such as allegations of 'trial by media' or 'guilt without proof'.
- Concerning enforcement or educational/information strategies prior to their launch can provide opponents of such strategies with advanced lead times for pre-emptive counter attacks such as influencing other stakeholders or by going public with self serving public statements that an agency may not be in a position to effectively respond to at that time.

261. Consumer organizations may sometimes require information to remain out of the public area for similar reasons. Additionally the office holders of such organizations will not have the same protections from legal suit, as do consumer protection authority and other government agency staff.





262. While most matters discussed between authorities and stakeholders will not involve confidential information that may not always be the case. Consequently an authority should consider how confidential matters might be best handled in the context of stakeholder engagement. It should be borne in minds that while government agencies and their staffs have strong incentives to maintain confidentiality (regulations, reputations, careers etc.) these same constraints may not exist or be perceived differently by NGOs and their members.

#### *Effective two-way communication*

263. The potential for misunderstanding or disagreements can be reduced or mitigated by effective two-way communication. Effective communication in exchanges between stakeholders requires:

- Respectfulness  
Close identification with one's agency can sometimes lead to a degree of professional arrogance that shows itself in disrespect for the status of other agencies, for example between policy and implementing departments, of between consumer protection investigators and police. It is important that agency representatives take a holistic view of government and appreciate that each agency has its own valuable role.  
For the most part the representatives of consumer organizations are giving their time freely and are likely to be passionate about their cause. As community based NGOs they will be well aware that there is a significant power imbalance in the government agency/NGO stakeholder relationship. Any disrespect, even if unintended or inadvertent is likely to be keenly felt. Honesty and full disclosure will demonstrate respectfulness.
- Relevance  
Government agencies are unlikely to engage effectively if they come to the view that their resources are being wasted on activities irrelevant to their mandate.  
Because consumer organizations usually have minimal resources to read and respond to correspondence and because they need to consult widely among members it is imperative that any communications concern priority matters of immediate interest and significance. Frank, unambiguous communication will allow easy recognition of what is relevant and what is not.
- Timeliness  
Keeping key stakeholders 'in the loop' on relevant matters will engender confidence, avoid organizations hearing things for the first time in the media, promote reciprocity and build a feeling of collective activism.

#### *Building the right team for engagement*

264. If the engagement process is to develop and maintain credibility it is vital that each participant assign the right mix of people to the engagement team. Team attributes should include:

- A person of sufficient seniority to send an unambiguous message '[name of authority] rates this engagement highly'. The senior officer needs to demonstrate that he/she is on

top of the agenda issues and is focused on the matters at hand. It will be counter productive if the senior officer is constantly checking unrelated SMSs and emails, or is coming in and out of meetings.

- A person of sufficient seniority to send an unambiguous message '[name of authority] rates this engagement highly'. The senior officer needs to demonstrate that he/she is on top of the agenda issues and is focused on the matters at hand. It will be counter productive if the senior officer is constantly checking unrelated SMSs and emails, or is coming in and out of meetings.
- An energetic officer with an eye for detail to provide secretariat support to the engagement process. This would include the vital roles of ensuring that:
  - adequate notice of meetings and reminders are communicated
  - accurate minutes are taken and distributed to attendees
  - required documents are distributed to the nominated representatives in a timely way
  - action items are implemented and reported on as appropriate

#### **4.3.4 Effective investigations by consumer protection authorities**

Learning objectives and outcomes of Section 6.3.4

265. This section of the train-the-trainer manual:

Provides an introductory guide to effective investigations, including a description of the investigative processes and the basics of evidence. Following completion of the train-the-trainer sessions, participants should be able to:

- discuss the life cycle of typical consumer protection investigations
- understand that the success of an investigative process is not measured by whether a conviction was obtained, but whether the process was efficient and effective.
- Understand the need for rigour and process in the collection, storage and presentation of evidence
- Understand that investigation are only one component (albeit important) of the regulatory response

266. Whatever the argued shortcomings of currently enacted laws within each ASEAN member state, it seems certain that the quickest boost to consumer confidence in using telecommunications technologies to access products and services online will be more comprehensive and systematic enforcement of existing laws. A priority element of effective enforcement is effective and efficient investigations.

267. An investigation is 'the action of investigating something or someone; formal or systematic examination or research' ref: [www.oxforddictionaries.com](http://www.oxforddictionaries.com)

### *The objectives of investigations*

268. In the context of consumer protection the objectives of an investigation are to determine whether or not:

- Is it likely that an offence under the relevant consumer protection law has occurred?
- Is it likely that the relevant consumer protection authority obtain sufficient evidence to prove the offence?
- Is it likely that the relevant authority can achieve an effective outcome from its investigation?
- Where does this problem/issue lie in respect of the authority's enforcement priorities and currently available resources.

### *The power to investigate*

269. While all activities undertaken by consumer protection agencies should be based on appropriate authority and powers, this is even more important in respect of investigations because:

- They are often intrusive into the affairs of those being investigated and those providing evidence
- The fact that a person or company is being investigated is likely to adversely affect them even if the investigation does not prove a contravention
- The result of the investigation may be very adverse to the parties involved. This may include direct and indirect financial and reputational harm.
- Courts and administrative reviewers of fact, process and outcome of the investigations will place great importance on the legal status of the agency and each of its actions
- The authority to investigate may be very general and listed in the under the 'functions' of the agency's enabling laws or regulations. Where the authority to investigate is limited to particular areas of the agency's functions, the authority to investigate may be provided for in one or more locations within the enabling laws or regulations.
- Enabling laws or regulation are sometimes be worded such that an agency is empowered to investigate consumer 'complaints' rather than suspected contraventions, however detected. Restrictive words may sometimes limit an agency's ability to undertake investigations on its own initiative.

270. Sometimes the expected or assumed authority to investigate is absent or unclear. While correction of these types of anomalies or omissions will be a priority for an agency prior to undertaking investigations, this may not always be practical. Sometimes a successful challenge



of the agency's power to investigate will provide the proof that the enabling law or regulation does in fact need amending.

*Key concepts: evidence and information*

271 In our every day lives we use information about traders, goods and services, other consumers experiences to help us decide what to buy and from who. We know from common sense and past experience that the information we have is of variable quality. We put more weight on some information because we trust its source and/or because we have other corroborating or consistent information that leads us to a similar conclusion. How we evaluate particular information is likely to vary between people and over time as we learn from our experiences or study.

272 If courts and tribunals are to deliver consistent, predictable and well-reasoned justice, they cannot afford to accept and evaluate information in the same informal and variable way that we do as individual consumers. Courts and most administrative tribunals have developed rules and procedures to ensure that the information they consider is most likely to be reliable

***\*\* Important note concerning the topic of evidence \*\****

273. There are significant and important differences in the laws and procedures in respect of evidence each jurisdiction. Furthermore, evidence is a complex topic that cannot be comprehensively addressed in this paper. The following are generalised comments and observations and may not reflect the rules and procedures of evidence in your country.

*Types of evidence*

274. There are many types of evidence: the detail of how evidence is classified and described varies between jurisdictions. Evidence most commonly relevant to consumer protection cases include:

- Testimony including: personal appearance, affidavits, statements
- Documentary including: reports, letters, invoices, receipts, advertisements, official records (such as record of incorporation, registration of business name), customs declaration, leases, certification of compliance with standards
- Physical including: products such as handsets
- Expert evidence is evidence provided by an expert on issues requiring detailed scientific or technical knowledge. Expert evidence is opinion evidence. An expert must have knowledge or expertise in a relevant subject area, as demonstrated by his/her qualifications, experience and peer recognition Expert evidence may include:
  - hearsay evidence of a specialist nature, e.g. as to the consensus of medical opinion on the causation of particular symptoms or conditions
  - Opinions based on facts adduced in the case.
  - Circumstantial evidence, i.e. evidence that relies on inferences to connect it to a conclusion of fact. Circumstantial evidence can be relevant as corroborating evidence or to challenge the probative value of other evidence

### *Managing evidence during an investigation*

275. Managing the identification of required evidence, where and how to obtain it, its preservation and presentation are all basic to successful law enforcement. As noted earlier one of the objectives of an investigation is to obtain evidence to prove each element of the relevant offences. An 'Evidence Matrix' is a practical technique for setting out the evidence required in a systematic way.

- Sources of evidence

Evidence may be obtained from any number of sources. In consumer protection investigations evidence is often sourced from:

- complainants
- traders complained about
- individual consumers and consumer organizations
- individual businesses including competitors of the trader complained about including traditional (bricks and mortar) and online traders (e-traders)
- business associations
- information providers including publishers, media
- service facilitators including Internet Service providers (ISPs) and Mobile phone service providers
- Retailers and manufacturers of mobile phones, modems/routers, computers
- Regulatory agencies responsible for landline, mobile phone, and internet related services and standard setting
- experts
- investigators
- foreign consumer protection authorities: they may be able to provide:
  - evidence relating to the trader, for example incorporation, registration, location, banking, assets, share ownership, previous convictions
  - evidence relating to the trader's activities in or originating from their jurisdiction
  - advice on obtaining evidence, for example forensic examination

- Obtaining evidence

A lot of evidence is obtained voluntarily. However most evidence provided voluntarily is not provided at the instigation of those with the evidence. Identifying sources and persuading them to voluntarily provide the evidence is the job of the investigator.

Often essential evidence is uniquely in the possession of those with a strong interest in not providing the evidence to investigators. In many jurisdictions around the world consumer protection authorities have been given powers to coerce individuals and companies to provide information and evidence. Sometimes these powers include the power to:

- require nominated people to attend the relevant authority to answer questions; and
- enter nominated premises and seize evidence.

Where these powers exist there will also be procedures that the Authority must follow. Typically these procedures will set out:

- the prohibitions in respect of which the powers may be used



- the trigger for the use of the powers, for example when the Authority 'believes' or 'suspects' that the person may have information relevant to a nominated offence.
- the procedure for notifying the party, including the specification of the evidence required
- the penalties for non-compliance.  
Failure to comply with specified procedures may result in sanctions against the officers in contravention and the inadmissibility of evidence acquired invalidly.
- Securing the evidence  
Evidence is only really useful if it is admissible. One critical aspect of admissibility is being able to show the 'chain of evidence', that is the record of the seizure, custody, control, transfer, analysis and presentation of evidence from the time it was seized until it is presented in court. By securing the chain of evidence investigators maximize the likelihood that the relevant Authority, Tribunal or Court will admit (consider) the evidence, and be able to make an accurate assessment of its probative value. Typically the integrity of the chain of evidence is proved by documentation created by investigators. Generally it will be important to secure evidence as quickly as possible. If this is not done then the evidence may be:
  - deliberately tampered with or destroyed
  - accidentally lost or destroyed
  - diminished in evidential value by the effect of time or weatherThe chain of evidence can be broken by:
  - failing to record how and when the evidence was obtained
  - failing to attach a unique identifier to the evidence (or its container)
  - failing to maintain custody and a record of that custody, evidence during transport, storage or testing
  - failing to secure the evidence while in custody against theft, substitution, tampering or spoilageMethods for maintaining the chain of evidence include the routine use of:
  - case officers (investigator's) note book
  - transportable secure storage and identification tags
  - evidence custody records
  - appropriate secure storage
  - appropriate explanations to, agreements with and supervision of external parties handling evidence
- Storage and transport facilities for evidence  
Facilities need not be expensive or extensive, for example:
  - several lockable filing cabinets
  - a lockable storage room
  - zip lock plastic bags
  - adhesive tape that can be written over
  - a lockable plastic storage container that can be placed inside the boot of a car
  - a designated 'Evidence Officer' with responsibility for managing storage and transport facilities





### *Rules of evidence*

276. As explained above, it is important to note that the rules of evidence vary between jurisdictions, although the basic intent of the rules is universal: to ensure the quality, integrity and relevance of evidence.

277. While case officers (investigators) are not generally not required to become experts in the rules of evidence, it is important that they develop a general understanding of the more important and commonly encountered rules.

278. The rules of evidence are complex and investigators will need to obtain (internal or external) legal advice before a matter goes for decision.

279. The rules of evidence that may often be relevant in consumer protection cases are that:

- Opinion evidence is generally not admissible
- Hearsay evidence is generally not admissible
- Secondary evidence is generally not admissible

280. However, there are often exceptions to these general rules, in particular circumstances:

- Opinion evidence

Opinion evidence refers to evidence of what the witness thinks, believes, or infers in regard to facts, as distinguished from personal knowledge of the facts themselves. Opinion evidence is generally not admissible. Two common exceptions to this rule are:

- Common exceptions

Particular matters of every day life where a person may be expected to give opinions and which opinions may be safely acted upon by others, for example the time of day, or the weather conditions. The matters coming within this exemption may be determined by precedent or regulation. In many jurisdictions the following matters are ones which non-expert opinion has been admitted:

- identification of handwriting
- eye witness identification
- identification of physical objects
- the general condition of objects
- the approximate value of objects
- time
- the ability to speak and understand a language

### *Hearsay evidence*

281. Hearsay evidence is a statement made by a person about facts in respect of which they do not have first hand or direct knowledge and is generally not admissible. In every day life we



often rely upon hearsay to form opinions and decide actions. The rules of evidence generally exclude hearsay evidence (with some important exceptions).

282. For example, if an investigator needed to prove who authorized a particular advertisement for a mobile phone or ISP service the following situation might occur:

- John provides a statement saying that ‘Tom told me that Susan authorised the advertisement’. In respect of proving that Susan authorised the advertisement, this is hearsay evidence and is generally inadmissible. It is direct evidence of what Tom told John. However, that fact is irrelevant to proving who authorised the advertisement.

*Avoiding the hearsay rule trap:*

- Be alert and recognise hearsay
- Identify and pursue original sources of evidence
- When a potential witness tells you something always ask them ‘How do you know that?’, so as to establish if they know 1st hand or if not and to identify the source of that knowledge or believe. In the previous example we recognised that John’s statement about what Tom told him was not the evidence required. It would be better to obtain a statement from Susan, for example, *and* to obtain the document signed by Susan authorizing the advertisement.
- Draft statements in the ‘He said, I said’ form
- Exceptions to the hearsay rule:
  - there are many, sometime complex exceptions to the hearsay rule
  - an important exception and one that is often relevant to consumer protection cases is Expert Evidence
- Even if evidence is admitted as an exception to the hearsay rule, there is still the question of its probative value.

*The best evidence rule:*

- General secondary evidence, such as a copy, will be not admissible if an original document exists, and is not unavailable due to destruction or other circumstances indicating unavailability.

*What is an effective investigation outcome?*

283. Too often we leap to the seemingly obvious conclusion that a successful investigation is one that proves a person or company guilty of contravention a provision of a relevant law. Proving someone or something guilty is one possible outcome of an investigation, but it is by no means either the only one or, perhaps surprisingly, always the best outcome.

- Stopping the conduct



- Empowering consumers to recognise, avoid and report similar conduct in the future
- Undoing the harm to affected consumers
- Compensating those who have been harmed
- Encouraging future compliance by the particular trader
- Encouraging future compliance by the traders generally
- Punishment

or

- Showing that no contravention occurred

284. The critical point to understand is that achieving one of these outcomes should be the objective of each investigation.

*The generalized life cycle of an investigation:*

- A trigger, such as a complaint or a market observation by the consumer protection agency
- A preliminary or initial investigation
- A substantive investigation
- The end game: NFA (no further action), administrative settlements, court proceedings

*Most complaints are not investigated*

285. Most complaints will not trigger investigations because:

- The available information suggests that no significant contravention has occurred
- It is apparent that investigation is unlikely achieve an outcome justifying the costs of the investigative process.

286. As an illustrative example the Australian Competition and Consumer Commission (ACCC) has recently reported that it receives about 200,000 enquiries and complaints a year, of which it investigates about 500; that's .25% of complaints. It takes between 30 to 40 cases to court each year; that's .02% of complaints and only 6% to 8 % of investigations.

*Initial investigations*

287. The objectives of an initial consumer protection investigation are to obtain sufficient information about alleged or suspected conduct to determine the:

- Likelihood that a contravention of [name of relevant law] has or is occurring
- Likelihood that sufficient evidence will be obtainable to prove a case
- Likely incidence of the conduct the likely amount of individual and collective harm caused or being caused by the conduct
- The likely options for responding to the conduct
- An assessment of how likely it is that we will be able to achieve a timely, cost effective and useful outcome

288. An initial investigation is a quick investigation taking no more than a nominated number of days\* that may include:

- Follow-up contacts with the complainant by phone, other electronic methods or personal interview, to obtain further information or evidence
- Contact with the party complained about (the trader) by letter, phone or personal interview to obtain further information or evidence, including their response to the alleged contravention
- Net research to obtain relevant information and evidence
- Contact with obvious potential sources of further information and evidence, such as broadcasters, suppliers and consumer organizations
- Obtaining and examining documents and physical objects by officers.

(\* the number of days would be specified by the agency's management taking into account the complexity of the matter they typically investigate and the available resources]

289. Generally initial investigations would not include:

- Formal interviews
- Analysis of evidence by third parties (for examples by expert or testing laboratories)
- Obtaining external legal advice
- Contacts with multiple potential witnesses

290. In all but the simplest of cases, an initial investigation will not obtain sufficient evidence to prove all of the elements on an offence. However, it will often obtain sufficient evidence and information to justify discontinuing the investigation.



### *Substantive investigations*

291. The objectives of a substantive consumer protection investigation are to obtain sufficient evidence to:

- Prove:
  - a contravention
  - the incidence of the contraventions
  - the person harmed by the contraventions
  - the nature and level of harm suffered
  - the nature and quantity of ill-gotten gains
- Determine that:
  - information and evidence obtained is inconsistent, or at least not consistent, with a contravention having occurred, and
  - that it is unlikely that further investigation will obtain evidence sufficient to alter that conclusion
  - the information and evidence obtained is consistent with a contravention, but that the circumstance of the case are such that further action is unlikely to achieve a timely, cost effective and useful outcome.

292. Substantive investigations may include the whole range of evidence gathering techniques, including:

- Informal interviews multiple potential witnesses
- Formal interviews multiple potential witnesses
- Surveillance, photographs, recordings
- Obtaining physical evidence
- Obtaining documentary evidence
- Testing physical evidence by third parties
- Recording conversations
- Obtaining external legal advice

### *Planning investigations*

293. Developing and maintaining an investigation plan is critical to the management of an effective and efficient investigation:

- The elements of the offence(s): by identifying the components of an offence the investigator identifies each of the evidentiary requirements.



- Where and how are you likely to obtain the evidence?
- Sequencing of activities and events, and of obtaining evidence
- Authority requirements: powers of investigation, notices, conferences
- Other peoples/agencies requirements and agendas, other laws, regulations, processes that must be complied with
- Resourcing; people, money, vehicles, photocopies etc.
- Other agencies: some investigation include cooperation with other agencies such as Standards Authorities, Telecommunications regulators, police, Department of Public Prosecutions etc.
- Media relations
- Periodic review of the plan and appropriate modification to it
  - investigations should be reviewed at agreed points, for example after the evidence in respect of the most problematic elements has been obtained or a nominated number of complainants have been interviewed, or the response of a regulator has been received
  - periodically, for example after a nominated time such as every month
  - at the end of the investigation. Each investigation should inform future investigations so that mistakes will not be repeated and successful innovative strategies adopted and applied
- Do not set unrealistic timetables. While it is imperative to develop timetables and set deadlines for particular actions, it is important to be realistic about how much time may be required for some activities. This is particular the case when progress is dependent on factors outside the authority's control. For example response from other agencies and regulators
- Document everything. It is easy to neglect documentation during the excitement of an investigation because interviewing, seizing goods etc. will often seem to be both more urgent and more important than 'paper work'. However, documentation brings order and systematic process to investigation, reduce the risk of duplication of effort and later challenges from aggrieved parties.
  - case officers should maintain a casebook (physical or virtual) for each investigation in which they record important information. For example the names of witnesses interviewed, dates of interviews, goods bought etc.
  - all directions given by case managers should be in writing
  - evidence related documentation (see notes under 'Evidence')
- When things go wrong

Despite training, sound procedures and planning is inevitable that from time to time something will go wrong during an investigation. For example:

  - obtained evidence may be lost or damaged



- witnesses may change their story
- complainants may seek to withdraw their complaint
- an officer may act inappropriately. For example by acting outside his authority, threatening a person or by accepting a gift.

All problems should be reported upwards immediately to the appropriate senior officer. The senior officer can then take responsibility for managing the problems and take remediate action as appropriate. Delay in reporting invariably makes matters worse because:

- it may limit the remedial options available to the senior officer
- the problem may become more serious
- those that are responsible for the delay may be suspected of complicity in the original problem

#### **4.3.5 Capacity building to support more effective regulatory responses to the principal problems associated with consumer use of telecommunication technologies**

294. Sustained and rapid technological advances in telecommunications continue to provide consumers with increasing choices of goods and services. The increased choices may be reflected in a wider range in the quality and price of goods and services already available, and in the availability of new goods or services.

295. For the purposes of this paper we have considered 3 particular telecommunications technologies: mobile phones, the Internet and e-commerce. These technologies provide consumer with a number of advantages over traditional consumer communications:

- Speeding up communications
- Enabling communications with distant parties
- A wider range of traders and goods to be compared
- More comprehensive comparisons to be undertaken

296. By facilitating increased consumer choices the uptake of telecommunications by consumer and businesses is a key driver in economic growth and increasing consumer welfare. However, like other drivers of economic growth the impact on consumer welfare can be enhanced by policies and regulations that:

- Facilitate business and consumer use of telecommunications
- Encourage pro-consumer behaviour of businesses
- Empower and protect consumers.

297. For most consumers, most of the time, transactions do not involve significant concerns before, during or after purchase. However some transactions do cause concerns.

298. Most often consumers are concerned about the basics of transactions: quality, quantity and price. In market economies these essential elements of a consumer transaction are largely determined by the interaction of supply and demand.

299. The use of telecommunications technologies does not change the basic paradigm described above. The use of telecommunications may provide consumers with increased ability to look after their own interests.

300. With respect to consumer protection regulation, ASEAN is very similar to other regional groupings:

- The nature of basic consumer concerns is broadly similar across the region. The nature of consumer concerns linked to telecommunications is also similar. However, the extent and prioritization of concerns differs. They appear to reflect:
  - the take up of telecommunications
  - consumers knowledge of potential threats and their
  - the current effectiveness of consumer protection regulation
- Consumer protection regulation varies significantly between member states. Some member states have well established and well functioning consumer protection regulation. The specification and application of consumer protection regulation is variable in other states.
- In all AMSs responsibility for consumer protection is shared across multiple agencies and Ministries
- The take up of telecommunication technologies by consumers varies significantly between AMSs.

301. At the outset two broad requirements for the effective use of these technologies by consumers were identified:

- Access to and performance of the telecommunications technologies and
- Confidence that their use of the technologies will be advantageous

302. Key capacity building recommendations are that:

- Enforcement of existing laws and other regulation be prioritized  
This will require development of
  - Online issue awareness
  - complaint handling skills and
  - investigations skills
- Consumer empowerment be prioritized  
This will require development of:
  - Consumer education skills
  - Business compliance education skills



# Appendixes



## APPENDIX 1: Status of e-commerce law harmonization in ASEAN as of March 2013

Member Country	Electronic Transactions	Privacy	Cybercrime	Consumer Protection	Content Regulation	Domain Names
Brunei Darussalam	Enacted	None	Enacted	Partial	Enacted	Enacted
Cambodia	Draft	None	Draft	None	Draft	Enacted
Indonesia	Enacted	Partial	Enacted	Partial	Enacted	Enacted
Lao People's Democratic Republic	Enacted	None	None	Draft	Enacted	Partial
Malaysia	Enacted	Enacted	Enacted	Enacted	Enacted	Enacted
Myanmar	Enacted	None	Enacted	Enacted	Enacted	Enacted
Philippines	Enacted	Enacted	Enacted	Enacted	None	Enacted
Singapore	Enacted	Enacted	Enacted	Enacted	Enacted	Enacted
Thailand	Enacted	Partial	Enacted	Enacted	Partial	Partial
Viet Nam	Enacted	Partial	Enacted	Enacted	Enacted	Enacted

UNCTAD Review of e-commerce legislation harmonization in ASEAN 2013



## APPENDIX 2

Four presentations were prepared to accompany this paper. They are:

Presentation 1: an introduction or general overview of the topic.

Presentation 2: an introduction to the most commonly scams encountered by consumers as they use their mobile phones and other mobile devices, laptops or desktops to communicate, access the net and buy or sell online.

PowerPoint Presentation: this presentation is provided as a PDF attachment to this document.

Handout for discussion: participants were provided with copies of 14 emails collected by the presenter and asked:

- to identify which emails they thought might be scams,
- which they thought might be genuine
- the basis for that assessment, and
- what action(s) would they advise the recipient of the emails to take

Presentation 3:

Presentation 4: an introduction to consumer protection investigations.

This presentation was in the form of a scenario exercise. Participants sat in self-designated groups of 3 – 5 members to facilitate group discussion. Each group were presented with the same sample complaints and asked to provide a

The handout is provided as APPENDIX 5

*Expectations about participants that influenced the format and content of the presentations and exercises*

Key presenter expectations on which the design of the presentations were based:

- That most or all participants would have at least several years professional exposure to consumer protection issues generally
- That most or all participants would be planning to take their learning experience back to their home organisations with the intention of passing it onto colleagues, either through formal or informal training.
- Mixed personal experience, knowledge and expertise in using mobile and other devices to access the net.
- Mixed personal experiences in buying or selling online.



- Most, but not all, participants would have experience with consumer education activities
- Few participants with prior experience of consumer protection investigations
- There would be < 20 participants, facilitating close interaction between the presenter and participants, for example informal two way questions and discussion
- Reasonable to good oral and written English language skills
- Having available 4 half day sessions (with breaks midsession and for lunch) over 3 days
- Access to a projector for *PowerPoints* presentations and a printer for handouts.

#### *Responding to participant feedback*

ASEAN Secretariat sought and obtained feedback from the participants after each presentation/exercise. Participants' comments were passed to the trainer who adapted subsequent presentations to better match with participants' needs and expectations.

#### *Post training report*

Before Presentation 1 the presenter asked for a participant volunteer to take brief notes during the presentations and to present a report (brief written report and a brief *PowerPoint* presentation) to the plenary session detailing:

- The major topics discussed
- A summary of the country reports
- A summary of each presentation/exercise
- The learning outcomes achieved

#### *Use of these materials*

Trainers using this paper should feel free to develop other presentations or to modify the original four. This will be necessary where original presenter expectations are not valid in your training situation or where you wish to put your own personal stamp on the preparations.





### **APPENDIX 3: ACCC media release concerning consumer issues relating to their use of phones, the Internet and e-commerce**

The following ACCC media releases were provided to participants as examples of the consumer protection issues investigated by a well established consumer protection agency in respect of consumers' use of phone, the Internet and e-commerce.

Media releases such as these add interest and authenticity to a discussion because they are 'real' examples' and can be discussed with reference to the different topics covered in the presentations, for example:

- Is this a problem or issue relevant in your jurisdiction?
- How did the agency (in the example you will provide) come to know about this problem? or issue?
- Why was this matter investigated? Or Would you prioritise this matter for attention and why?
- Was the outcome worthwhile?

Source: <http://www.accc.gov.au/media/media-releases>

### **Court finds Bet365 engaged in misleading and deceptive conduct following ACCC action** *11 September 2015*

The Federal Court has found that Bet365's Australian and UK companies engaged in misleading and deceptive conduct when offering free bets to new customers, in proceedings brought by the Australian Competition and Consumer Commission. Bet365 is one of the worlds' largest online betting providers.

His Honour Justice Beach stated "the ACCC has made out its case against Hillside Australia and Hillside UK in relation to the promotion and advertising during the period 18 March 2013 to 13 January 2014 of the "\$200 FREE BETS FOR NEW CUSTOMERS" offer. Their relevant conduct was misleading or deceptive or likely to mislead or deceive and also involved the making of false representations. For the reasons already given, new customers who had not previously used such types of services were drawn into this web of deception. But other customers who had used such types of services before may have been similarly enticed."

The Federal Court found against both the Australian Bet365 company, Hillside (Australia New Media) and its UK sister company Hillside (Shared Services).

"This judgment makes it clear that companies cannot use the word 'free' in offers to consumers where any conditions that seek to neutralise the 'free' nature of the offer are not clearly identified. Inducements like free bets run the risk of signing up new and inexperienced gamblers based on a deceptive claim," ACCC Chairman Rod Sims said.

"The free bet offer was directed at new customers, which included inexperienced gamblers and young people. The ACCC will take action where it thinks consumers are being misled,



especially in emerging markets where there are potentially vulnerable consumers.”

Some of the conditions the ACCC was concerned about included a condition where customers had to gamble their deposit and bonus three times before being able to withdraw any winnings. As a result, a customer who makes an initial deposit of \$200 and receives \$200 must then gamble \$1200 before being able to withdraw any money.

“Compliance with the Australian Consumer Law is essential for all companies that sell to Australian consumers, regardless of geographic location. Bet365 in the UK provided essential support to the Australian company including finance, customer service, and the Bet365 website,” Mr Sims said.

The ACCC did not succeed in its allegations that representations made by the companies offering Deposit Bonus with qualifications were misleading or in relation to Free Bet representations made for a short period of time in January 2014 where the terms and conditions applying to the offer were displayed in full on the opening page. The ACCC also did not succeed in its allegations of involvement of Bet365 Group Limited, the ultimate holding company of Hillside (Australia New Media) and Hillside (Shared Services) Limited.

The free bet claims came to the attention of the ACCC as part of a coordinated sweep of ‘free’ representations on websites targeting Australian consumers. This initiative was part of a larger global effort through the International Consumer Protection and Enforcement Network.

There will be a further trial in relation to penalty.

Release number:

MR 175/15

## **ACCC successfully completes pilot broadband performance monitoring and reporting program**

*11 September 2015*

A report released by the Australian Competition and Consumer Commission has found that a program to monitor and report to consumers on the quality of broadband services could be readily established in Australia.

“The ACCC believes a broadband performance monitoring and reporting program would promote competition and consumer outcomes by providing transparency over the quality of broadband services,” ACCC Chairman Rod Sims said.

“As the NBN rollout progresses, providing transparency over the performance of the monopoly network provider will be particularly important as retail service providers (RSPs) will be dependent on NBN Co for the underlying network capability. In this regard, visibility over any network-based performance issues would help identify whether any bottleneck issues in the network are attributable to RSPs or the network provider.”

“In addition, it is also important for consumers to have information about how different broadband products perform when choosing the option that’s best for them,” Mr Sims said.

“A broadband performance monitoring and reporting program can be designed to increase the available information about service performance, and thereby encourage RSPs to compete on the basis of service quality, not simply price.”

The ACCC’s Pilot Broadband Performance Monitoring and Reporting Program involved testing approximately 90 Melbourne-based volunteers’ home fixed-line broadband connections on various technologies over a three-month period. The Pilot Program was carried out by SamKnows, who operate similar broadband performance monitoring programs internationally, and Comdate.



Volunteers installed a hardware probe on their home connection and the probe ran a series of network performance tests. The metrics selected for testing included download/upload speeds, web browsing time, latency, packet loss, video streaming, jitter and DNS resolution. A range of results were observed against these metrics, with a noticeable trend in deteriorating performance during peak use periods, particularly in relation to download speeds.

"The ACCC is greatly encouraged by the results of the Pilot Program; however a decision to proceed with a future program has not been made and any finalised program would involve further stakeholder consultation," Mr Sims said.

"Similar broadband monitoring programs have been established in the United Kingdom (2008), United States of America (2010), Singapore (2011), and more recently, Canada. Such programs have led to improved transparency of information and increased performance-based competition for broadband services."

See: [The ACCC's report on the findings of the Pilot Program](#).

Release number:

MR 173/15

## **Chairman discusses affordable communications and calls for transparency around broadband performance**

*1 September 2015*

Chairman Rod Sims today outlined aspects of the Australian Competition and Consumer Commission's work which contributes to affordable communications services.

As part of a wide-ranging speech, Mr Sims discussed the ACCC's focus on pursuing the long-term interests of end-users in regulating communications markets. He mentioned that, for broadband customers, the effective price per gigabyte (GB) had fallen from approximately \$30 /GB in 2007 to less than \$1/GB today.

Speaking at the Australian Communications Consumer Action Network Conference in Sydney, Mr Sims also argued the case for a broadband performance and monitoring program.

"A broadband performance and monitoring program would promote competition and consumer outcomes by providing transparency over the quality of broadband services that are on offer to consumers.

"Consumers need this information to help them select the most appropriate service for their needs and to confirm they are likely to be getting the service for which they are paying."

Mr Sims said the US, UK and other countries have adopted broadband monitoring models which aim to improve transparency and encourage performance-based competition for broadband services.

"Since late 2013, the ACCC has consulted on the possible introduction of a fixed broadband performance monitoring and reporting program in Australia. We have looked at the technical and commercial aspects of such a program and anticipate publishing our work in the near future."

In discussing competition in the communications sector, Mr Sims said the ACCC's role in assessing mergers is important for affordability due to the potential long-term impacts on market structures.

"In the TPG acquisition, the ACCC concluded that the removal of iiNet as an independent competitor would lessen competition in the relevant markets, but not substantially, which is the test to breach the competition law," Mr Sims said.

"We took comfort that TPG would continue to face three major competitors after the acquisition. Clearly, we would have no such comfort in the case of any subsequent proposed acquisition



involving any two of Telstra, Optus, TPG or M2, as things stand.”

Mr Sims said the ACCC is also considering the likely competition impacts of the proposed suite of acquisitions between Foxtel, Ten and Foxtel’s digital advertising agency MCN.

“We are conducting extensive market inquiries to hear a range of views on the proposed acquisitions, given their scope and the potential inter-relationships between them.”

Mr Sims said the ACCC is focusing on three main questions.

“First, will Foxtel’s tie-up with Ten substantially lessen competition for sporting rights?”

“Second, will Foxtel’s tie-up with Ten substantially lessen competition for other, non-sport content and result in popular TV shows and movies being available on first release on Foxtel rather than on free-to-air TV?”

“Third, will Ten’s acquisition of a stake in MCN substantially lessen competition in the supply of advertising opportunities?”

Mr Sims also outlined compliance and enforcement activities including the ACCC’s input into the review of the Telecommunications Consumer Protections (TCP) Code.

The Chairman’s speech is available at <https://www.accc.gov.au/speech/communications-affordability-and-the-role-of-efficient-markets>

Release number:

MR 162/15

## **ACCC releases final decision on mobile call and SMS terminating charges and non-price terms report**

24 August 2015

*Note that this is a competition rather than a consumer protection matter*

The Australian Competition and Consumer Commission has released its final decision on the price that mobile network operators should charge each other and fixed-line network operators for receiving calls on their mobile network. For the first time, the ACCC has also decided on a price for mobile network operators to charge to receive SMS messages.

“The ACCC does not regulate retail charges, either for mobile calls or SMS, but expects these savings from these two decisions will be passed onto consumers either by way of lower charges or through improved call and SMS inclusions in retail plans,” ACCC Commissioner Cristina Cifuentes said.

Mobile network operators have exclusive control of access to subscribers on their networks. The ACCC regulates the terms of access and the prices that they can charge to terminate calls and SMS messages on their networks to promote competition and benefit end-users of mobile and fixed-line voice services.

“The final regulated rates reflect the costs of terminating calls and SMS messages on Australian networks and is based on benchmarking the costs of these services against those in other countries,” Ms Cifuentes said.

The ACCC has decided that the wholesale price of terminating calls on an Australian mobile network should be 1.7 cents per minute, reduced from the current rate of 3.6 cents per minute.

“In Australia, the majority of mobile calls and SMS are carried on 3G networks, which are more efficient than the 2G networks which are used to a larger extent overseas. The mobile networks in Australia also carry a much larger amount of data traffic than overseas networks. These features reduce the cost of terminating calls on Australian networks and have been taken into account in the decision,” Ms Cifuentes said.

Voice over 4G technology (voice over long term evolution (VoLTE)) is also expected to reduce the costs of terminating mobile calls and SMS messages. Voice over 4G has not yet been





commercially rolled out in Australia and its actual impact on the costs of terminating calls and SMS is uncertain.

"The ACCC will monitor the planned roll out of voice over 4G technology, which could be as soon as later this year. If there is evidence of voice over 4G take-up which affects the costs of terminating calls on Australian networks, the ACCC may review the regulated rates," Ms Cifuentes said.

For the first time, the ACCC has decided to set the price mobile network operators charge to receive SMS messages at 0.03 cents per SMS.

"This price maintains the rate proposed in the ACCC's draft decision. It is based on the network capacity and equipment used to carry SMS messages on Australian networks and is well below current commercial rates for SMS termination," Ms Cifuentes said.

The regulated prices for mobile voice and SMS termination will apply from 1 January 2016 to 30 June 2019.

The ACCC has released a revised report from WIK-Consult detailing the international benchmarking study undertaken to inform the regulated prices.

The mobile termination access determination also includes non-price terms and conditions of access which are relevant to mobile termination services.

Further information on the Mobile Terminating Access Service Final Access Determination (MTAS FAD) public inquiry, including a copy of the ACCC's final decision and the WIK-Consult revised report, is available at [MTAS FAD Inquiry page](#).

### **Non-price terms**

The ACCC has also released a report on non-price terms for a number of regulated services. The report includes the ACCC's final decision on the non-price terms of access for terminating access services provided by mobile network operators.

The non-price terms focus on aspects of access where commercial agreements are less likely to ensue and where specific competition concerns are likely to arise. They cover commercial and operational matters such as billing and notification, general dispute resolution processes, use of confidential information, and new terms which address a lack of recourse to regulated terms after parties enter in to access agreements.

The non-price terms final report and the non-price schedules are available at the [non-price terms and conditions webpage](#).

Release number:

MR 155/15

### **ACCC releases comparator website guidance**

*3 August 2015*

The Australian Competition and Consumer Commission has released consumer and industry guidance on the operation and use of comparator websites.

"The consumer guidance offers tips to help consumers get the best outcomes when using comparator websites. The industry guidance sets out the standards that the ACCC expects comparator websites to meet," ACCC Deputy Chair Delia Rickard said.

"Comparator websites can drive competition and assist consumers to make informed purchasing decisions when comparing what are often quite complex products. However, the ACCC is concerned that poor conduct by some industry participants can mislead consumers," Ms Rickard said.



The consumer guidance sets out tips that can assist consumers to understand and benefit from comparator websites, including:

- Making sure they know what is being compared
- Understanding commercial relationships
- Know what their needs are.

The industry guidance is targeted at the operators of comparator websites and businesses whose products are listed on them. This guidance sets out how industry can comply with competition and consumer protection laws, including setting out three guiding principles of:

- Facilitating honest, like for like comparisons
- Being transparent about commercial relationships
- Clearly disclosing who and what is being compared.

“Operators should carefully read this guidance as there will be no excuse for non-compliance with the Australian Consumer Law, and the ACCC will continue to take action where necessary,” Ms Rickard said.

The ACCC’s recent review of comparator websites was prompted by consumer and business complaints of misleading information being provided to consumers. The ACCC found that a number of websites, in particular those comparing energy plans, included information that may mislead consumers as to the extent of the comparison service, the amount of savings that could be achieved and the impartiality of the comparisons.

Following contact by the ACCC, website operators quickly implemented appropriate changes to remove or amend the potentially misleading information.

In November 2014, the ACCC released a report *The Comparator Website Industry in Australia*. The report set out the ACCC’s concerns over a lack of transparency in regards to the:

- extent of the comparison service, including market coverage
- savings achieved by using the comparison service
- comparison services being unbiased, impartial or independent
- value rankings
- undisclosed commercial relationships affecting recommendations to consumers
- content and quality assurance of product information.





The guidance is available at:

- [Industry guide for comparator website operators and suppliers](#)
- [Consumer guide to comparator websites](#)

#### **Background:**

The ACCC had previously secured over \$2 million in penalties against comparator website [EnergyWatch](#) for misleading advertising related to representations about the nature of the Energy Watch service and the savings consumers would make by switching energy retailers through the Energy Watch service.

[Compare The Market Pty Ltd](#) paid a penalty of \$10,200 following the issue of an infringement notice by the ACCC in relation to claims made in recent advertising promoting Compare the Market's health insurance comparison service.

Release number:

MR 141/15

#### **Australians lose \$45 million to scams in 2015**

*13 July 2015*

The Australian Competition and Consumer Commission is urging the community not to send money or personal details to strangers after \$45 million was reported lost to scams already this year and 45,000 complaints made.

"Scammers are becoming increasingly sophisticated in their attempts to get your money or personal details. Scams succeed because they look like the real thing and catch you off guard when you're not expecting it," ACCC Acting Chair Delia Rickard said.

"Our new Scamwatch website, which is being launched today, has all the latest news and tips to help you identify and avoid scams. By following the advice on this site, you can help to protect yourself against scammers."

"For the first time, the ACCC has published data on common scams that are causing the most harm in Australia, which will be updated every month on Scamwatch. This tool will help you keep one step ahead of the scammers," Ms Rickard said.

"Scams target people of all backgrounds, ages and income levels across Australia. There's no one group of people who are more likely to become a victim of a scam and all of us may be vulnerable to a scam at some time."



Australian  
Competition &  
Consumer  
Commission



**SCAMWATCH**

## Scam statistics

January - June 2015

### Amount lost

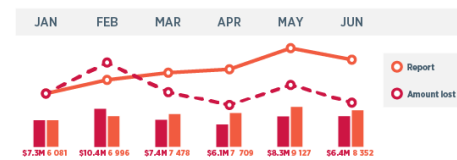
**\$45 902 666**

### Scams reported






**45 743**

10.3% reported losing money

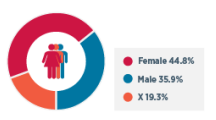
### Year to date



### Top 5 scams by losses

	Amount lost	Reports
 Dating & romance	<b>\$10 099 323</b>	<b>1 088</b>
 Investment schemes	<b>\$9 185 984</b>	<b>521</b>
 Inheritance scams	<b>\$3 599 558</b>	<b>1 727</b>
 Nigerian scams	<b>\$2 383 064</b>	<b>345</b>
 Betting & sports investment schemes	<b>\$1 307 916</b>	<b>167</b>

### Gender



### Delivery method



### Age



Visit [scamwatch.gov.au](http://scamwatch.gov.au) to find out how to recognise, avoid, and report scams.



- **Be alert to the fact that scams exist:** When dealing with uninvited contacts from people or businesses, whether it's over the phone, by mail, email, in person or on a social networking site, always consider the possibility that the approach may be a scam. Remember, if it looks too good to be true, it probably is.
- **Know who you're dealing with:** If you've only ever met someone online or are unsure of the legitimacy of a business, take some time to do a bit more research. Do a Google image search on photos or search the internet for others who may have had dealings with them.
- **Do not open suspicious texts, pop-up windows or emails – delete them:** If unsure, verify the identity of the contact through an independent source such as a phone book or online search. Don't use the contact details provided in the message sent to you.
- **Keep your personal details secure:** Put a lock on your mailbox and shred your bills and other important documents before throwing them out. Keep your passwords and pin numbers in a safe place. Be very careful about how much personal information you share on social media sites. Scammers can use your information and pictures to create a fake identity or to target you with a scam.
- **Keep your mobile devices and computers secure:** Always use password protection, don't share access with others (including remotely), update security software and back up content. Protect your WiFi network with a password and avoid using public computers or WiFi hotspots to access online banking or provide personal information.
- **Choose your passwords carefully:** Choose passwords that would be difficult for others to guess and update them regularly. A strong password should include a mix of upper and lower case letters, numbers and symbols. Don't use the same password for every account/profile, and don't share your passwords with anyone.
- **Beware of any requests for your details or money:** Never send money or give credit card details, online account details or copies of personal documents to anyone you don't know or trust. Don't agree to transfer money or goods for someone else: money laundering is a criminal offence.
- **Be careful when shopping online:** Beware of offers that seem too good to be true, and always use an online shopping service that you know and trust.

Key features of the new Scamwatch website

- **Types of scams** ([link is external](#)) - The ACCC provides information on the most common types of scams in circulation in Australia, and collects and publishes data on these scam types.
- **Report a scam** ([link is external](#)) - If you think you've been scammed or know someone who has, report it to the ACCC using our report a scam page.
- **Get help** ([link is external](#)) - If you've been scammed there are steps you can take straight away to reduce the damage and prevent further loss. Find out what you can do to protect yourself, your business or your loved ones from scams.

We also encourage you to sign up for our [Scamwatch radar alerts](#) ([link is external](#))

to stay informed about the latest scams. You can also follow us on [Scamwatch Twitter](#) ([link is external](#))

**Release number:**

MR 119/15



## **Indigenous consumers lost \$740,000 to scams last year**

21 May 2015

This Fraud Week, the Australian Competition and Consumer Commission is urging Indigenous consumers to be wary of requests over the internet for personal information. The ACCC's [2014 Targeting Scams Report](#) revealed that Indigenous consumers lost over \$740,000 to scammers last year.

"Sadly, almost one third of Indigenous Australians who came into contact with a scammer last year lost money. This is more than double the figure for non-Indigenous consumers," ACCC NT Regional Director Derek Farrell said.

In fact, scams accounted for almost 90 per cent of complaints by Indigenous consumers to the ACCC in 2014.

"Internet scams caused the highest losses for Indigenous Australians, totalling \$655,000, so we're urging the community to be wary of all internet approaches asking for personal details or money," Mr Farrell said.

"Scammers today are not just after your money – your personal information is valuable too. In 2014, identity theft scams were the top reported scam for Indigenous consumers."



## Targeting scams

Snapshot 2014 - Indigenous consumers

### Scams reported

**584** reports from  
Indigenous consumers

### Loss amount

**\$742 478**

### Reported losses

**28%** reported losing money

Over twice the  
national figure  
of **12.1%**



### Delivery method

#### Reports



#### Amount lost

Online **\$655 474**

Phone **\$79 952**

Others **\$7 052**

### Top 10 scams by reports



### Dating & romance scams

#### Reports

**33 ↑**  
5.7% of total reports

#### Amount lost

**\$159 680**  
21.5% of total losses

### More information



**Targeting scams**  
Report of the ACCC on scams activity 2014  
» [accc.gov.au/publications](http://accc.gov.au/publications)





“When scammers steal your details, they can use them for all sorts of crime such as making unauthorised purchases from your bank accounts, taking out loans or carrying out other illegal business under your name,” Mr Farrell warned.

Today we are launching a scams campaign on our [‘Your Rights Mob’ Facebook page](#) [\(link is external\)](#)

to spread the message to Indigenous consumers about how to spot a scam and how they can protect themselves from scammers.

SCAMwatch tips

**Keep your personal details secure** - never just throw out bills or important documents that have your personal details on it like your address, bank account details or date of birth. Be careful sharing private information about yourself online, including Facebook and Divas Chat.

**Keep your mobile devices and computers secure** - always use password protection, update security software and don’t share access to your phone or computer with others.

**Choose your passwords carefully** - use strong passwords (a mix of upper and lower case letters, numbers and symbols), and change them regularly.

**Beware of any request for your details or money** - Use the phone book or an internet search to check the organisation’s contact details to make sure they’re not gammon. NEVER use the contact details provided in the original request.

**Get a copy of your credit report** – to find out if somebody is pretending to be you. Visit ASIC’s [MoneySmart](#)

[\(link is external\)](#)

website to find out how you can get a free copy of your credit report every year to make sure no-one is using your name to borrow money or run up debts.

Scams target everyone. Watch our video to find out what to look out for and outsmart the scammers.

## Scams

You can report scams to the ACCC via the [SCAMwatch report a scam page](#) [\(link is external\)](#)

or by calling 1300 795 995

Stay up to date with the latest news, by liking [ACCC's Indigenous Facebook page](#) [\(link is external\)](#)

Release number:

MR 88/15





## **Small business warned to watch out for ransom ware**

*19 May 2015*

This Fraud Week, the Australian Competition and Consumer Commission is warning small business operators to think twice before opening email files that could contain ransomware after the latest [Targeting Scams Report](#) revealed that almost \$1 million was lost to these scams last year.


Ransomware is a type of malware that infects a computer system by restricting access unless a ransom is paid to a scammer for the restriction to be removed.

"The ACCC received over 2,500 ransomware and malware complaints last year with over \$970,000 reported lost by small businesses and consumers. Several people reported losing over \$10,000 to these scams, which can have a devastating effect on a small business," ACCC Deputy Chair Dr Michael Schaper said.



CryptoLocker
Buy Decryption
Decrypt Single File
FAQ
Support

## Buy decryption and get all your files back



Buy decryption for 640 AUD before 2015-03-08 11:47:42 am  
**OR** buy it later with the price of 1280 AUD  
Time left before price increase: **71:42:14**  
Your total files encrypted: **9275**  
Current price: 1.792 BTC (around 640 AUD)  
Paid until now: 0 BTC (around 0 AUD)  
Remaining amount: 1.792 BTC (around 640 AUD)

### Buy Decryption with bitcoin

What is Bitcoin?  
Bitcoin is the virtual currency used in Internet.

- #### Buy Bitcoins

You can buy Bitcoins from Exchangers **OR** Marketplaces.

  - ##### Buying from Exchangers

Use one of the following exchange services to buy Bitcoins with cash over the counter via bank-teller at one of the partner banks.

Use  in "Your Bitcoin wallet address" field when placing your order.

    - [forepost.net](#) - Buy Bitcoins with Westpac, Commbank and NAB.
    - [www.hardlock.net](#) - Buy Bitcoins with Westpac and Commbank.
  - ##### Buying from Marketplaces

Sign up on one of the following websites. Enter your name and address details then get your account verified with GreenIDB. You will need to provide some basic forms of identification such as a drivers license number, passport number, or electoral roll details.

    - [btcmart.net](#) - You can use direct bank transfer from any Australian bank account. Deposits are automatically processed at 6am following a business day and any deposits made over the weekend do not clear until Tuesday morning. Also, you can deposit directly at any Westpac branch in Australia. Branch deposits will clear same day, within an hour.
    - [www.coinat.com](#) - You can use BPAY from any Australian bank account. Only make BPAY transfers from a transaction account with available funds. BPAY transfers typically reach CoinJar within 1-3 business days and will be added to your Cash Account. For best results, be sure to make your BPAY transfer within regular business hours, Melbourne local time.

"Ransom ware can also see your business losing all of its business and financial records, which may be catastrophic."

Victims reported receiving an email purportedly from a reputable sender such as Australia Post or FedEx, with a file attached that will install ransom ware on your computer once opened.

"Many small businesses and consumers have reported that their computer has been frozen, with a pop-up alert that claims to be from the Australian Federal Police stating the computer has been locked because they have visited an illegal website or breached various laws," Dr Schaper said.

"Scammers claim that they will unlock the computer if a fee is paid. However, even if you pay the ransom, there is no guarantee your computer will be unlocked and you're likely to be up for expensive repairs to your computer and the loss of your invaluable data."

"Scams like this often succeed because they look like messages from a government agency or reliable large corporation. It's important that small businesses are aware that government agencies will not send these demands and they're dealing with a scammer," Dr Schaper said.

SCAMwatch tips

Ensure your computer has a firewall and up-to-date anti-virus and anti-spyware software.



Do not click on links or download files in emails you receive out of the blue; especially if they are executable (.exe) files or zip files. These files are likely to contain malware.

Use a pop-up blocker as a lot of ransom ware is delivered after following links in pop-up alerts.

If there is any doubt about the legitimacy of an email supposedly from a legitimate business, do not rely on contact details or links provided or open any attachments - contact the organisation using the number in the telephone directory or on their official website to verify.

Regularly back-up your computer's data on a separate hard drive so this can be easily re-installed if your computer is infected by malware or ransom ware.

You can report scams to the ACCC via the SCAMwatch [report a scam](#)

([link is external](#))

page or by calling 1300 795 995.

For the latest small business news and events you can follow us on [LinkedIn](#)

([link is external](#))

or sign up to the [Small Business Info Network email updates](#).

Release number:

MR 87/15

### **Electronic Bazaar operator to pay penalties of \$100,000 for misleading consumers**

*13 May 2015*

The Federal Court of Australia has ordered Mr Dhruv Chopra, the sole operator of the online electronics store Electronic Bazaar, to pay penalties totalling \$100,000 for contravening the Australian Consumer Law (ACL), in proceedings brought by the Australian Competition and Consumer Commission.

Electronic Bazaar sold camcorders, digital cameras, mobile phones, laptops, projectors, and other electronic goods through its website [www.electronicbazaar.com.au](http://www.electronicbazaar.com.au). The Court declared that since at least 21 May 2014, Mr Chopra had made false or misleading representations to consumers about the availability of refunds and the extent of Electronic Bazaar's liability for faulty goods.

These representations included that consumers were not entitled to a refund, repair, or replacement for goods in various circumstances, such as where the goods were no longer under an express warranty, where the goods had been used or were not in their original packaging, or unless a claim was made within a specified time period.

Mr Chopra was also found to have made false or misleading representations that consumers' refund rights were against a company called "Unreal Technologies Private Limited" or "Unreal Technology Private Limited", when neither of those companies existed.

The Court also declared that on four separate occasions between June 2012 and July 2014, Mr Chopra accepted payment for goods but failed to supply those goods to consumers within a specified, or reasonable, timeframe.

"The Court's decision to impose a significant penalty on Mr Chopra, a sole trader, for misrepresenting consumers' refund and warranty rights makes it clear that this conduct is a serious breach of the Australian Consumer Law. A consumer's right to a refund, repair, or replacement in certain circumstances under the ACL consumer guarantees cannot be excluded or modified by terms or conditions published on a website," ACCC Chairman Rod Sims said.

"The penalty imposed in respect of failure to supply goods within a specified or reasonable timeframe also highlights the need for online traders to ensure that when accepting payments for goods, they must be able to supply those goods within the stated timeframe, or otherwise within a reasonable period," Mr Sims said.



The Court also ordered that Mr Chopra be restrained from engaging in similar conduct for a period of 5 years, undertake training on his obligations under the ACL and pay the ACCC's costs of the proceeding.

Release number:

MR 83/15

### **Electronic Arts undertakes to provide refunds to consumers**

*28 April 2015*

The world's third largest publisher and developer of video games, Electronic Arts Inc and related companies, EA Swiss Sàrl and Electronic Arts Proprietary Limited (together, EA), who run the Origin video game distribution service have provided a court enforceable undertaking to the Australian Competition and Consumer Commission. In the undertaking, EA acknowledged that representations it made to consumers about their rights to refunds and the application of the Australian Consumer Law (ACL) consumer guarantees were likely to have breached the ACL.

"Businesses such as EA selling digitally downloadable goods cannot avoid their responsibilities under the Australian Consumer Law just because they are located outside of Australia," ACCC Chairman Rod Sims said.

"If you sell to consumers in Australia, then the Australian Consumer Law applies to all goods or services you supply. This includes all of the ACL consumer guarantees, which cannot be excluded, restricted or modified."

"It is a breach of the Australian Consumer Law for businesses to state that customers are not entitled to refunds under any circumstances. Where a product has a major failure, consumers can insist on a refund or replacement at their choice. Representations that this right has or can be excluded, restricted or modified are false or misleading," Mr Sims said.

Under the terms of the undertaking, EA has agreed to implement a consumer redress program. Any consumer who purchased a faulty video game through Origin after 1 January 2012 and wishes to seek redress should contact EA to have their claim assessed or, where they have already been denied a refund or remedy by EA, have their claim reassessed in accordance with their statutory consumer rights under the ACL.

EA will set up a 1800 complaints number, an email address and a post office box to handle customer complaints and enquiries. For further information, please visit the front pages of the

[Origin website](#)  
(link is external)

or your Origin gaming service. EA is an entertainment software and technology company located in the United States of America and Switzerland. Origin, has over 50 million users worldwide and sells downloadable video games to Australian consumers.

In the 2014 financial year, the American based Electronic Arts Inc earned over US\$3.5 billion in net revenue, with over US\$1.8 billion coming from digital revenue. There was about a 27% increase of EA's digital revenue from the previous financial year.

The ACCC was concerned that from at least 1 January 2012, EA made statements through the terms and conditions on Origin and through its customer support representatives that were likely to have conveyed false or misleading representations to the effect that:

- Australian consumers were not entitled to any refunds for digitally downloaded video games purchased through Origin;
- EA had modified or restricted consumer guarantees in relation to games purchased by Australian consumers through Origin.





Complaints from a variety of sources, received from early 2012, brought this matter to the ACCC's attention. The ACCC then raised concerns with EA, which cooperated with the ACCC's investigation and gave a court enforceable undertaking to the ACCC.

Additionally, EA has undertaken for a period of three years that it will not make any representation to an Australian consumer that:

- EA has a 'no refunds' policy for games purchased through Origin that excludes any right to a refund under the Australian Consumer Law; and/or
- Australian consumers are not entitled, under any circumstances, to a refund for games purchased from Origin.

EA will also:

- amend their terms and conditions to comply with the Australian Consumer Law; and
- implement and maintain an Australian Consumer Law Compliance Program, with particular measures for risk assessment, complaints handling and staff training.

The undertaking is available in full on the ACCC's [public register](#).

For more information about your consumer guarantee rights, please see [Consumer rights & guarantees](#).

Release number:

MR 68/15

### **Spreets to pay penalties of \$600,000 for misleading consumers**

*24 April 2015*

The Federal Court has ordered Spreets Pty Ltd (Spreets) to pay total penalties of \$600,000 for making false or misleading representations to consumers about deals offered on its online group buying website in contravention of the Australian Consumer Law (ACL), in proceedings brought by the Australian Competition and Consumer Commission.

The Court declared that between June 2011 and April 2012 when operating one of Australia's largest online group buying websites, Spreets contravened the ACL by engaging in misleading and deceptive conduct and making false or misleading representations about the price of certain deals, consumers' ability to redeem vouchers, and consumers' refund rights.

"Online consumer issues remain an enforcement priority for the ACCC. The Court's decision is a further reminder for online traders that the Australian Consumer Law applies to them, including consumer guarantees" ACCC Commissioner Sarah Court said.

"All online businesses, including those offering daily deals, must ensure that representations made on their websites are clear and accurate, particularly in relation to price and any restrictions on a deal being offered, including availability and redemption conditions."

Spreets agreed to joint submissions on penalties and a statement of agreed facts to be filed with the Court, and consented to the other orders made by the Court.

Following the ACCC's investigation, Spreets also took steps to update and improve its compliance program.

It is noted that Spreets no longer offers deals directly to consumers. It now gathers and publishes deals offered by a range of third party online group buying sites.

#### *Background*

The ACCC has received a significant number of complaints since the online group buying industry emerged in Australia in 2010 and has worked with other ACL regulators to improve practices in the industry.

These websites, also referred to as 'daily deals' or 'deal of the day' sites, sell vouchers for

discounted goods or services. Online group buying sites typically negotiate these deals with businesses and then market the deals to their members and the public by promotional emails, social media promotions and on their websites.

In December 2013, the Federal Court ordered Scoopon to pay total pecuniary penalties of \$1million for making false or misleading representations to both businesses and consumers.

In December 2014, the ACCC accepted a court-enforceable undertaking from LivingSocial as a result of the ACCC's concerns about a term in LivingSocial's consumer contracts, and representations made on LivingSocial's website.

Release number:

MR 67/15

### **Hang up on an immigration scam**

*23 April 2015*

The Australian Competition and Consumer Commission is urging visa holders and Australian citizens to hang up on fraudulent phone calls from scammers.

The ACCC has received reports of scammers impersonating government officials who threaten visa holders and citizens with deportation because they claim these people have not filled out immigration forms correctly.

Scammers are targeting people by demanding up-front fees of around \$1,000 to resubmit forms. A high proportion of those targeted have been people from India and Pakistan.



ACCC Deputy Chair Delia Rickard said they have received 150 reports of this scam since February with more than \$35,000 reported lost.

"Anyone who receives this type of call seeking payment should ignore the demands for payment and hang up. Scammers may try to pressure you by repeatedly calling and harassing you – but if you give your money to a scammer you will never see it again," Ms Rickard said.

"Don't be fooled because someone has your personal information such as address, birth date, visa status or nationality because these details can be collected online through websites and social networking forums."

"Never send money or give your account details to a stranger. Alarm bells should go off if you are asked for international wire transfers as these transactions are almost impossible to trace.





Scammers may not only steal what's in your account but use what you have provided to steal your identity," Ms Rickard said.

The Department of Immigration and Border Protection (DIBP) has confirmed that they never request payments over the phone or through international money transfer providers.

When more information regarding a visa application is required, DIBP will either contact the applicant or sponsor directly, or through their migration agent if they are using one.

To report a scam, contact the ACCC via [Report a Scam](#)

(link is external)

Further information is available on the [SCAMwatch website](#)

(link is external)

and the [Department of Immigration and Border Protection website](#)

(link is external)

Release number: MR 64/15

## **Consumers continue to benefit from falling prices for telecommunications services**

*6 March 2015*

The Australian Competition and Consumer Commission's annual telecommunications reports for 2013-14 show that the prices paid by consumers for telecommunications services fell by 2.7 per cent in real terms in 2013-14.

The reports, tabled in Parliament yesterday, reveal that the average real prices of landline and mobile voice calls have now fallen by around 50 per cent since 1997-98. Broadband customers are also benefiting from larger data allowances, faster speeds and lower prices.

"Competition is driving substantive reductions in the price of telecommunications services, significant infrastructure investment to improve the quality and coverage of services, and technological innovation," ACCC Chairman Rod Sims said.

"Consumers are seeing lower prices and improved services as a result of the vigorous competition that began in the 1990s."

The report also notes that the structure of the telecommunications industry and the role of the NBN will have a fundamental influence on the delivery of telecommunications services for many years to come.

"The Australian Government's review of the structure and regulation of the telecommunications industry in 2014 was an important opportunity to re-examine the competitive safeguards and policy settings in the sector," Mr Sims said.

"The ACCC supports the review's focus on the benefits of infrastructure-based competition."

NBN Co made significant investment in fibre infrastructure during the year while investment in legacy networks declined. As the NBN is progressively rolled out, consumers will be disconnected from the copper network as the NBN becomes available to them. Mr Sims noted that the NBN migration is not automatic and it is important consumers understand what they need to do to switch over to the NBN.

"Once the NBN is available in your area, we encourage you to contact your preferred retail service provider to discuss the migration process and to ensure you continue to have access to landline phone and internet services," Mr Sims said.

"If consumers don't switch over to the NBN on time, they face the risk of losing their telephone or Internet service at the cut-off date and a delay before they can be connected to the NBN."

The ACCC has further information about [migrating to the NBN on its website](#).



Investment in mobile networks was also strong as mobile network operators responded to consumer demand for high quality mobile and wireless data services. The reports showed that Telstra continued to strengthen its market share in mobile handsets and wireless broadband markets in 2013-14.

Consumers used their mobile phones more intensively during the year, particularly for data services. However, mobile handset and wireless broadband subscriptions started to reach saturation levels after strong growth in recent years.

Consumers downloaded more data across all platforms, but continued to favour a fixed line connection for data-intensive activities, such as downloading movies and gaming. Fixed line connections accounted for 93 per cent of all downloads in 2013-14.

The reports also provide further detail on key developments in telecommunications markets and outline the ACCC's regulatory activities during the year.

The ACCC Telecommunications Reports for 2013-14 are available on the ACCC website.

[ACCC telecommunications report 2013-14](#)

Release number:

MR 27/15

### **Australians lose \$75,000 every day to romance scams**

*13 February 2015*

This Valentine's Day, the Australian Competition and Consumer Commission is warning the online dating community to beware of any love interest who asks for money.

"Sadly, \$28 million was reported lost to romance scams in Australia last year by 1,032 people. Of this, 81 people reported losing over \$100,000, showing just how financially devastating these scams can be. We know these figures are only the tip of the iceberg as many victims are reluctant to admit to friends, family or authorities that they fell for a scam," ACCC Deputy Chair Delia Rickard said.

"Signing up to dating websites has proven successful for many singles seeking a match. Unfortunately it has also proven popular among scammers who prey on people's vulnerabilities to steal their money, particularly around sentimental times of the year."

"Scammers are experts at preying on people's weaknesses and will spend months and even years grooming victims and lowering their defences. Inevitably, the fraudster will spin a tall tale about why they suddenly need your financial help, ranging from medical emergencies to failed business ventures to needing to rebook flights to visit you," Ms Rickard said.

"Once victims realise that their admirer is actually a criminal, the emotional consequences can be devastating. This is why disrupting relationship scams continues to be a priority for the ACCC."

Through the Scam Disruption Project, the ACCC is working to identify victims, contact them and let them know they may be the victim of a scam. We are also working with intermediaries that enable victims and scammers to connect or transfer money.

"These scams can also pose a risk to your personal safety as scammers are often part of international criminal networks. Scammers have lured unwitting Australian victims overseas, putting people in dangerous situations that can have tragic consequences," Ms Rickard said.

acc data: 1 january - 31 december 2014

Scam Category Level	Amount Reported Lost	Contacts	Contacts Reporting Loss	Less Than \$10k Lost	\$10k or Greater Lost	\$100K or Greater Lost	\$500k or Greater Lost
ACT	\$1 182 520	68	31	19	12	5	0
NSW	\$8 911 557	656	263	162	101	23	5
NT	\$101 485	23	10	7	3	0	0
Overseas	\$1 624 309	219	91	71	20	5	0
QLD	\$5 780 010	544	234	147	87	16	2
SA	\$801 848	142	50	39	11	1	0
TAS	\$328 425	68	23	17	6	1	0
VIC	\$6 811 791	496	228	134	94	22	0
WA	\$2 241 817	266	96	59	37	7	0
Not Supplied	\$120 800	15	6	4	2	1	0
<b>Total</b>	<b>\$27 904 562</b>	<b>2 497</b>	<b>1 032</b>	<b>659</b>	<b>373</b>	<b>81</b>	<b>7</b>

#### SCAMwatch tips:

- Never provide your financial details or send funds to someone you've met online. Scammers particularly seek money orders, wire transfers or international funds transfer as it's rare to recover money sent this way.
- Run a Google Image search to check the authenticity of any photos provided as scammers often use fake photos they've found online.
- Be very wary if you are moved off a dating website as scammers prefer to correspond through private emails or the phone to avoid detection.
- Don't share photos or webcam of a private nature. The ACCC has received reports of scammers using this material to blackmail victims.
- If you think you have fallen victim to a fraudster, contact your bank or financial institution immediately and report it to [www.scamwatch.gov.au](http://www.scamwatch.gov.au) (link is external)

The results from the ACCC's sweep of dating sites have been released today in a short report. Last year, staff joined an international initiative to protect vulnerable consumers by sweeping dating websites for misleading offers, unclear pricing policies or consumer contracts with unfair terms.

See: [Online dating industry report](#)

#### Key areas for improvement include:

- better upfront disclosure of fees, especially by those sites that advertise themselves as free;
- contracts should be easier to cancel – if you can sign up online you should be able to cancel online too, and
- better practice is for dating site operators not to re-use customer information without express consent.



## Dating websites report card



**65** dating  
websites  
analysed in Sept 2014

### Handling complaints

- ✓ Easy to complain about dating site service quality **86%**
- ✗ Easy to report would-be scammers or suspicious activity **23%**

### Scam warning messages

- Displays scam warning messages **61%**
- Scam warning messages are prominent **54%**
- ✗ Scam warning messages meet industry best practice<sup>1</sup> **23%**

### Personal info & privacy

- ✓ Discloses how personal information is used in a privacy policy **91%**
- Provides an easy 'opt-out' method from direct marketing **57%**
- ✗ Permits reuse of profile information for other means, including on partner sites **46%**

### Subscriptions

- ✓ Allows users to cancel subscriptions online **89%**
- ✗ Provides up-front service costs before users join **2%**

#### LEGEND

- ✓ Good
- Could do better
- ✗ Not so good

The ACCC analysed 65 dating websites as a part of the International Consumer Protection Enforcement Network global sweep in September 2014.

#### 1 Best practice guidelines for dating websites

▶ Helping you to achieve better results  
[accc.gov.au/publications](http://accc.gov.au/publications)



Release number:  
MR 8/15

**Telstra pays \$102,000 penalty following ACCC infringement notice for iPhone 6 advertisement**  
*16 December 2014*

Telstra Corporation Limited (Telstra) has paid a penalty of \$102,000 following the issue of an infringement notice by the Australian Competition and Consumer Commission in relation to a recent iPhone 6 advertisement.

Telstra's A3 advertisement appeared in *The Age* newspaper on 27 September 2014 and featured a large photo of the Apple iPhone 6. The advertisement for Telstra's iPhone 6 and phone plan bundle prominently displayed the plan cost of \$70 per month when, in fact, consumers were also required to pay an additional \$11 per month for the iPhone 6. The advertisement only disclosed the additional payment of \$11 and the total monthly cost of \$81 in fine print.

The ACCC considered that Telstra's advertisement misrepresented the price of the phone and phone plan bundle to consumers.

The infringement notice was issued because the ACCC had reasonable grounds to believe that Telstra had made a false or misleading representation about the price of goods or services, in contravention of section 29(1)(i) of the Australian Consumer Law.

"Consumers should be able to understand the true cost of an advertised product so they can make informed purchasing decisions," ACCC Chairman Rod Sims said.

"Businesses must be careful about using attention grabbing headline prices to ensure that their advertisements do not mislead consumers about the actual price they will have to pay. This is especially the case for bundled goods and services like phones and plans," Mr Sims said.

"Advertising that is clear allows consumers to make informed purchasing decisions and improves competition as it gives other businesses the opportunity to compete fairly."

Consumer protection in the telecommunications sector remains an ACCC enforcement priority.

In 2013, the High Court upheld a decision ordering TPG to pay a \$2M penalty to the ACCC in relation to misleading advertisements. The advertisements gave the impression that consumers could acquire TPG's Unlimited ADSL2+ broadband internet service for \$29.99 per month when in fact it could only be acquired with a bundled home telephone line for an additional \$30 per month plus start-up costs.

The payment of a penalty specified in an infringement notice is not an admission of a contravention of the Australian Consumer Law. The ACCC can issue an infringement notice where it has reasonable grounds to believe a person has contravened certain consumer protection laws.

As Telstra is a publicly listed company, the infringement notice penalty amount is \$102,000.

Telstra's A3 advertisement – *The Age* – 27 September 2014





**iPhone 6. EXPERIENCE THE BEST ON AUSTRALIA'S BEST MOBILE NETWORK**

plus \$11/mth handset payment

**\$81/mth**

iPhone 6. \$550  
\$70/mth

15GB Data  
\$700 Calls & SMS  
Unlimited Text

FREE TELSTRA NEW PHONE FEELING\*  
Ask us to find out more

FREE 1GB EXTRA DATA UPGRADE  
= 2.5GB TOTAL  
\*includes opt-in required

visit a telstra store or partner telstra.com/iphone

IT'S HOW WE CONNECT 

Release number:  
MR 309/14

## ACCC updates on scam disruption project 9 December 2014

In August 2014, the ACCC commenced its Scam Disruption Project which aims to stop potential scam victims from sending more money to scammers. The project involves utilising financial intelligence to identify Australians sending funds to West African nations and advising them they may have been targeted by a scam.

The project commenced because losses reported for relationship scams continues to be a significant concern with total losses for dating and romance scams this year just over \$23 million.

In the three months to the end of October 2014, almost 1500 letters have been sent to potential scam victims in New South Wales and the Australian Capital Territory.

"It is still early days and difficult to draw firm conclusions from the data collected but





approximately 60% of those receiving the ACCC's warning letters stopped sending money overseas for at least a 6 week period," ACCC Deputy Chair Delia Rickard said.

"While there is no guarantee that all of the people sent a letter will be a scam victim, there are very real questions about why people should be sending funds to these high risk jurisdictions. Funds transfers from the people we wrote to total over \$9 million and this does not include funds sent prior to the commencement of the project."

"The ACCC strongly urges anyone who receives such a letter stop sending money or if they are in doubt about whether they are being scammed to contact us and discuss their situation on a confidential basis. The information provided has enabled us to confirm that almost three quarters of the people who have contacted us were scam victims and hopefully we saved them from further losses. Collectively, these people have lost \$1.7 million at an average of \$34,000 each."



Australian  
Competition &  
Consumer  
Commission

## Scams disruption project

UPDATE AUG - OCT 2014

**1500** potential victims  
contacted via post



**60%** stopped  
sending money



**50** confirmed victims  
so far, with

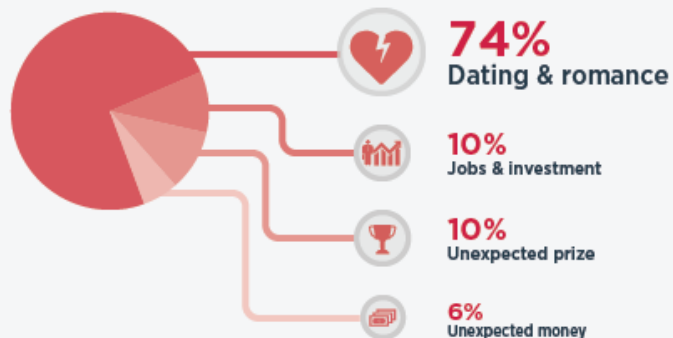


**\$1.7 million** lost

**\$34 000** avg. loss



### Scam types





“Interestingly, just over one third of these people were contacted by the scammer through social media channels. Scammers also target dating websites, email and regular mail, but this year is the first time we have collected data that clearly identifies social media is being used to facilitate fraudulent activity.”

“So far we see dating and romance scams being the chief culprit with 75% of victims reporting they had started an online relationship which led them to send money overseas. The scams are equally targeting men and women,” Ms Rickard said.

Most dating and romance scams start with the victim meeting someone online. The scammers say they come from a western country and claim to be posted overseas overseeing an infrastructure project, working for an oil company or deployed as a soldier or peacekeeping force. The scammer quickly declares his or her love for the victim and the requests for money soon follow.

Excuses for why the victim needs to send money are elaborate and varied but there is always some barrier or event that stops the scammer being able to come to Australia to be with the victim. Victims believe they are helping pay for airline tickets, military leave passes, visa applications, medical expenses or government fees. The requests are endless, promises are never kept and there is always another excuse for why more money is needed.

“What we often hear from victims is that the scammers introduce a story that they have a lot of money that they got from an inheritance, gemstone dealings, gold bullion or other unexplained wealth but there is always an excuse why they cannot get access to these funds. They promise to share the money with the victim once they get it out of the bank, through customs or pay associated government fees. A common ruse is to say this is a fee for anti-money laundering and terrorist financing regulations. These excuses and stories are designed to extract the maximum funds and commit the victim both financially and emotionally. Unfortunately, the scam can drag on for years,” Ms Rickard said.

Whatever the story, once the victim pays a scammer the money is gone and the chance of ever recovering the loss is almost nil.

The ACCC’s Scam Disruption Project is a joint initiative with the Australasian Consumer Fraud Taskforce (ACFT), including state and territory police and consumer affairs agencies to alert at-risk individuals to the possibility of being a victim of fraud.

More information can be found at [Scam disruption project](#).

Release number:

MR 302/14



## APPENDIX 4

The emails have been kept in the font used for the handout so as to retail, so far as was practical, the appearance of the original.

### Example 1

**From:** [unknown sender]  
**To:** [my name]  
**Subject:** INVITATION LETTER

Dear ,

**2<sup>nd</sup> ASEAN-European Union High Level Dialogue on Maritime Security Cooperation, Educational and Economic System**

The 2<sup>nd</sup> ASEAN-EU High Level Dialogue on Maritime Security Cooperation, themed “Developing Inter-Agency Cooperation and Regional Cooperation to Enhance Maritime Security” will take place in Kuala Lumpur from 27-28 July 2015.

The dialogue is hosted by the Maritime Institute of Malaysia (MIMA), in collaboration with the Ministry of Foreign Affairs and the European Union External Action Service.

A public forum on “Towards an Integrated Maritime Cooperation: An Exchange of Lessons and Experiences between ASEAN and the EU” will be held at the end of the dialogue. You are cordially invited to attend

Further details of the High Level Dialogue are attached. Please Kindly open the attachment for more details. Your presence will be highly appreciated  
Thank you

[INVITATION LETTER .zip attached]



## Example 2

**From:** HCF Health insurance  
**To:** [My name]  
**Reply to:** HCF  
**Subject:** Important Tax information from HCF for the 2014/15 year

Can't view this email? [View online](#)  
View online SECTION: Header

Membership Number: 30210XXX

Dear Carl,

Please find your Australian Taxation Office Statement and supporting documentation from HCF to assist you in completing your 2014/15 tax return.

For added security and privacy reasons, the pdf has been password protected. To view your documents simply enter the date of birth of Carl (the policy holder) where requested in the format **DDMMYYYY**.

To retrieve your documents, click on the secure link to download your pdf.

<https://memcomm.hcf.com.au/ATO.statements?res=20309851&exp=02012016&key=c3ec35b8b19286e89486f25d751d3e3d>

Alternatively you can copy and paste the link into a browser.

For security reasons your documents will be available to download until 31 December 2015. To view your documents after this date please go to the HCF members section at [hcf.com.au/members](http://hcf.com.au/members).

Thank you for your membership with HCF, Australia's largest not-for-profit health fund.

Yours sincerely,

Jim Dertouzos  
Chief Customer Officer



### Example 3

**From:** Mike  
**To:** [My name]  
**Subject:** So simple ANYONE can do it

Hey,

Check out what this lazy guy came up with  
to get rich...

[CLICK HERE... http://s8m2.goldbar.net/l/qbe0ofaq3otrgh769nsp/3d49b01](http://s8m2.goldbar.net/l/qbe0ofaq3otrgh769nsp/3d49b01)

Best,  
Mike

"The winners in life think  
constantly in terms of I can, I  
will, and I am. Losers, on the  
other hand, concentrate their  
waking thoughts on what they  
should have or would have done,  
or what they can't do."  
- Dennis Waitley

"There is no royal, flower-  
strewn path to success. And if  
there is, I have not found it.  
For if I have accomplished  
anything in life, it is because  
I have been willing to work  
hard." - C.J. Walker

"Whatever the mind of man can  
conceive and believe, it can  
achieve. Thoughts are things!  
And powerful things at that,  
when mixed with definiteness of  
purpose, and burning desire,  
can be translated into riches."  
- Napoleon Hill

Unless otherwise agreed to in writing, any message or content sent to this address may  
be subject to reproduction, publication and review by others without notice. Nothing





contained herein shall constitute professional advice. You are not entitled to rely on any statement, opinion or information contained herein or attached hereto. You are solely responsible for your use of any such products, goods, services or content. You should conduct your own independent research before taking action, or hire a third party to advise you with regard to same. The sender does not represent or endorse any person, product, good or service referenced directly or indirectly herein, and you agree to hold harmless and indemnify sender regarding any damage or loss associated with same. In many cases the sender of this email receives a financial benefit when you take action or make a purchasing decision respecting any information or content referenced in this communication.

-----

You have signed up to receive these free gift updates.  
If you no longer wish to receive notifications, please use  
the link at the bottom of this email to remove yourself  
from this free newsletter.

However, this is NOT recommended. By staying a member  
you will keep receiving daily reminders about net's  
hottest money-making systems, blueprints and  
shortcuts - you will MISS OUT if you leave!

If you have any particular concerns, questions or  
suggestions, feel free to reply to this email and  
a staff member will get back to you within 2 business  
days.

-----

#### DISCLAIMER

You subscribed to my newsletter to receive offers and advice on internet marketing,  
by entering your email address on one of my websites. You have the right to  
unsubscribe  
at any time by clicking the link at the bottom of the page to remove yourself from the list.



#### Example 4

**From:** Mr Santos Michael  
**To:** [undisclosed recipients]  
**Subject:** Link Investment Offer ...

Attn: Branch Manager

Dear Sir,

Irresistible Investment offer. Thank you for your email. Haven obtained your contact details from a reliable source as a potential partner. We are happy to introduce to you a woman with a Capital of 59.9 Million USD from Saudi Arabia searching for a good person to investment within your country. We are of the investment-brokering agent in your country and we offer irresistible service investment in your country. We are by this letter offering you an irresistible (Partnership), so as to allow us have you as our representative and manager of investment funds partnership in your country within the time frame of the investment relationship. Since, we cannot determine if this email is functional or valid and also your willingness, we have kept this proposal brief. We are in hope to share this irresistible offer with you based on a partnership investment program within your country. If you are interested in this partnership, please respond with your direct telephone and give us your full contact details plu

Thank you.

Santos Michael  
EMAIL: [linkinvestmentlink@outlook.com](mailto:linkinvestmentlink@outlook.com)  
[santosmichaellink@live.com](mailto:santosmichaellink@live.com)



## Example 5

**From:** Mrs Ruth Benson  
**To:** undisclosed recipients  
**Reply to:** Mrs Ruth Benson  
**Subject:** Charity Work From Madam Ruth Benson

Dearest One,

With due Respect and Humanity I write to donate and hand over some fund to you for charity work for community development, schools, farmers, less privileges and building of church. I am Madam Ruth Benson; I am 58yrs old, from Kuwait based in Ivory Coast with my late husband. I am married to Late Mr. Jean Benson who was until his death worked with Oil Company (PETROCI) Cote d'Ivoire; we were married for many years without a child. I am now very sick, after going through some medical checkup my doctor told me I would not last the next eight months due to Colon Cancer that I should pray hard.

When my husband was alive, He deposited the sum of (US\$2.8M) Two million eight hundred thousand dollars deposited in a Finance Security firm here in Abidjan, Ivory Coast capital. Presently this money is still in the Vault of the firm. Having known my condition I decided to donate this money to any God fearing person, Individual, NGOs, Government Organizations, and Farmers that will use this fund for the charity purpose I mentioned above. I took this decision because I have no offspring and seeing the sufferings of people around i decided to donate it for charity work.

Though I don't know you or met you before but I believe that God will work through you in accomplishing his will. I want you to always remember me in your daily prayers because of my upcoming Cancer Surgery.

As soon as I receive your message in acceptance of working with this charities mention above, I will give you more details and the contact of the Finance Security firm here in Abidjan Ivory Coast. Please assure me that you will act accordingly as I have Stated herein. Expecting to receive your reassuring reply,

Remain blessed in the Lord.

Yours

**Madam Ruth Benson.**

Sister,



## Example 6

**From:** Account Support  
**To:** [My name]  
**Reply to:** Mrs Ruth Benson  
**Subject:** Charity Work From Madam Ruth Benson

Hello,

You currently have an incoming message regarding a recent funds transaction. This message is urgent so please respond now.

[Message # 345](#)

For security reasons this message can only be accessed by confirming your account.

[Confirm](#) [Account](#) [Here](#)  
[.. http://s8m2.goldbar.net/l/w3b596m3lpxu6pd9eg2w/3d49b01](http://s8m2.goldbar.net/l/w3b596m3lpxu6pd9eg2w/3d49b01)

Alternatively you can verify your email address with our secure servers.

[Verify Email Address](#)

The pending message is urgent so please at now.

Automated Message.

1710 E INDIAN SCHOOL RD  
85026 Phoenix ARIZONA UNITED STATES

To unsubscribe or change your subscriber profile please click here:  
<http://s8m2.goldbar.net/uns/kbitc36pm4b0dikzar5n-1b4d>



## Example 7

**From: Members Support**

**To: [my name]**

**Subject: \$800 Bonus Collection**

Hi,

You are one of most loyal customers. As a thank you we are giving you a one off bonus of \$800!

This bonus is only available to claim for the 24 hours, then it will need to be passed on to the next customer for security reasons.

[Claim Bonus Here](http://smallfun.net/ssr0) [smallfun.net/ssr0](http://smallfun.net/ssr0)

You don't have to sign into your account, just make sure your email is verified to our servers and the funds will be passed along.

We hope for more custom with you in the future!

Thanks again,  
Richard



## Example 8

**From:** Accounts Receivable Dept.  
**To:** [my name]  
**Subject:** Payment Funds Unclaimed

Hello,

We have been trying to get into contact with you for a while now, but have not got any response.

There is [\\$23,570 of unclaimed cash](#), ready to access now.

If this cash is not claimed in the next 48 hours, it will be sent back to the sender.

[Click Here To Claim http://s8m2.goldbar.net/l/n1y1gs31pwpb8i8yu6fw/3d49b01](http://s8m2.goldbar.net/l/n1y1gs31pwpb8i8yu6fw/3d49b01)

Thanks,  
Paypal customer service team.





## Example 9

### 1<sup>st</sup> email received

**From:** [a friend's name]  
**To:** [my name]  
**Subject:** URGENT

hello im very sorry to bother you Im in istanbul turkey currently and during my stay my bag was stolen containing my international passport and my credit card.

The Embassy is willing to help me allowing me to take the return flight without a passport so I gave a short-lived; only that I have to pay the ticket and expenses related to the stay in the hotel. To my great regret I find I cannot log into my account to withdraw the monetary requirements of which I need because I do not have credit card; to work around this problem, my bank needs time to process all the data that I need to reset the whole thing. In everything I thought I'd resort to your help so that I can at least return home: I ask a modest loan that i obviously will pay you as soon as I get back. I must be on board the next flight. If you can send me money via Western Union would be great because it is the fastest way I have to receive the sum. I need the sum of 1500 Euros to cover my expenses.

Please, if you could send me the money through Western Union site in the resort closest to you, it would be much more convenient for me. I believe that in 20 minutes will be sent and received by me. I'm sorry for any inconvenience this mistake can create. I can send you the details on how to transfer the sum. Hope to receive your reply soon.

Best regards

### 2<sup>nd</sup> email received

**From:** [a friend's name]  
**To:** [my name]  
**Subject:** Traveling overseas Re: spam email

I am travelling overseas until July 6 2012 and will have limited access to phone and email. For urgent matter a text message to 0408 37nnnnwill work.

[friend's real name] [friend's real phone number]  
[friend's real address] [friend's real email address]Example 10



## Example 10

**From:** Incoming Fax  
**To:** [my name]  
**Subject:** Internal ONLY

\*\*\*\*\*Important - Internal ONLY\*\*\*\*\*

File Validity: 2015/06/29  
Company : <http://carlbui.com>  
File Format: Adobe Reader  
Legal Copyright: Adobe Corporation.  
Original Filename: Internal\_report\_2015\_06\_29\_2751359.pdf

\*\*\*\*\* Confidentiality Notice \*\*\*\*\*.

This e-mail and any file(s) transmitted with it, is intended for the exclusive use by the person(s) mentioned above as recipient(s).

This e-mail may contain confidential information and/or information protected by intellectual property rights or other rights. If you

are not the intended recipient of this e-mail, you are hereby notified that any dissemination, distribution, copying, or action taken

in relation to the contents of and attachments to this e-mail is strictly prohibited and may be unlawful. If you have received this

e-mail in error, please notify the sender and delete the original and any copies of this e-mail and any printouts immediately from

your system and destroy all copies of it.

[Internal Report .zip attached]



## Example 11

**From:** Deborah Paul  
**To:** [undisclosed recipients]  
**Subject:** I.C.V WORLD CONGRESS INVITATION!

Dear Madam/Sir,

You are cordially invited to participate in the forth - coming World Congress on Center for violence (ICV) against Women, Youth, Control of Ebola Outbreak & HIV/AIDS.

The International Center for violence (ICV) against Women, Youth, Control of Ebola Outbreak & HIV/AIDS, to be held in Wellington, August 17th-21st, United States and from August 24th-28th 2015 in Dakar-Senegal. We are inviting people from various countries around the world.

Note that all interested delegates that requires entry visa to enter the United States to attend this meeting will be assisted by the organization, in obtaining visa in their passport. Free air round trip tickets to attend this meeting will be provided to all participants. The Workshop welcomes paper presentation from any interested participants willing to present papers during the meeting.

For registration information you are to contact the Congress Secretariat: {[icv.2015@yandex.ru](mailto:icv.2015@yandex.ru)}.

Please share the information with your colleagues.

Sincerely,  
Miss Deborah Paul



## Example 12

**From:** Google UK  
**To:** [undisclosed recipients]  
**Reply to:** [gmail address provided]  
**Subject:** OFFICAL NOTIFICATION LETTER

Google UK Ltd  
Belgrave House

76 Buckingham Palace Road London SW1W 9TQ United Kingdom.

Ref No: GAAP/ 5653/657/2015 Batch: GAAP/ 563/GAPRO/UK

OFFICIAL NOTIFICATION LETTER.

This notification is coming to you following the official publication of results of the E-mail Electronic Online Sweepstakes Organized by Google Incorporation, in conjunction with the Google Foundation and foundation for the Promotion of Software Products, (F.P.S.) held in London UK.

Due to your active use of Google services, you have been selected as one of the Twelve (12) winners in the ongoing E- mail Electronic Online Sweepstakes. A Bank Draft of ?950,000.00 GBP {Nine Hundred and Fifty Thousand Great British Pounds} have been processed by our Foreign Payment Bureau and also a certificate of prize claim have been processed alongside your Bank Draft.

You are advised to fill the foreign payment form below and send to us with the following details below for the Processing of your Claims:

### FOREIGN PAYMENT RELEASE FORM.

- (1) Your Contact Address:
- (2) Your Contact Telephone/Mobile Number:
- (3) Your Nationality/Country:
- (4) Your Full Names:
- (5) Occupation:
- (6) Age/Gender:
- (7) Marital Status:
- (8) Private Email Address:
- (9) Ever Won An Online Lottery?
- (10) How Do You Feel As A Winner?

Kindly let us know how you would want your prize to be remitted to you:

1. Bank Transfer: (Bank Transfer of your official winning prize to your bank account).
2. Courier Delivery Of your Certified Winning Cheque/Bank Draft in your Name and other Winning Documents safely to you.

NB: You are advised to contact our CEO Mr. Larry Page with the details below for further instructions regarding the processing of your payment.

.....  
Mr. Patrick Pichette,  
Claims Administrator,  
Email: [patrickpichette@gawrdprouk.com](mailto:patrickpichette@gawrdprouk.com)  
[patrick.pichete@gmail.com](mailto:patrick.pichete@gmail.com)

.....  
Congratulations from the Staffs & Members of Google Board Commission.  
©2015 Google Incorporation.



### Example 13

**From:** Katty  
**To:** [my name]  
**Subject:** Hello

Hello, My Dear Friend! How is your day going? 我知 Katherine, but you can call me Kat if you like. What 痴 your name by the way? I know you 致 e been visiting this website quite often. And I was going to chat with you the other day but you suddenly went offline. What do you think about us spending some time here talking to each other? I would be glad to hear from you. My email [tinaqus750@yahoo.com](mailto:tinaqus750@yahoo.com)

Best wishes,  
Katty



## Example 14

### 1<sup>st</sup> email received

**From: Mr.Khayaletu Matrose**  
**To: [undisclosed recipients]**  
**Subject: READ THIS JOINT VENTURE PROPOA**

Hello,

Kindly Study attached document for a better understanding to my proposal.

Thanks for taking the time to read my e-mail message.

Regards,  
Mr.Khayaletu Matrose





**LETTER FROM THE DESK OF: Mr. Khayaletu Matrose**

**Tel: +27- 780-55-7504**

**Fax: +27-86-44-333-80**

**E-Mail: [khayaletumatrose@pisem.net](mailto:khayaletumatrose@pisem.net)**

**Request for Confidential Business Relationship**

I know that this will come to you as a surprise since we do not know each other before. For the purpose of introduction, I was a silent business partner to The Former Presidency Director-General, in South Africa. After due deliberation, I decided to contact you for your assistance in standing as benefactor to the sum of US\$46.5 Million (Forty Six Million, Five Hundred Thousand United States Dollars) equivalent because, I and two other colleagues are currently in need of a silent foreign partner whose identity we can use to transfer the said sum. This fund accrued legitimately to us as commission from foreign contracts we executed with Department of Mining & Energy through our private connections.

The fund is presently waiting to be remitted from Johannesburg here in South Africa to any overseas beneficiary confirmed by me as associate/receiver. By virtue of my political/religious position in my country, I cannot acquire this money with my name. For this reason I took it upon myself to look for an overseas silent partner who could work with me to facilitate transfer of this fund for our mutual benefit, hence the reason for this email. What I am requesting from you is:

(1) To be my silent partner and receive the funds as the sole benefactor to the contract amount which I shall secure all legal documentation here in South Africa to authenticate our claim. (2) Provide a private telephone number for easy communication under your control.

(3) Receive the funds as the beneficiary, take out your commission after tax and keep the rest of the money until I arrive there to meet you after the transfer is completed.

My proposal is that after you receive the funds, it would be shared as follows: (1) 20% to you as commission for your co-operation and assistance in facilitating the transfer to any of your nominated account, while the remaining 80% belongs to me. You will be free to take out your commission immediately after the money hits your country. Since my objective is to invest the money in a foreign country, it would be appreciated if you could also help me with advices and direction on investing into profitable/lucrative ventures in your country for an additional 5%.

However, this is optional, and if it is not convenient for you to further assist us with investing the money, we can end our cooperation after you make available to us our part of the money.

The transaction, although discrete, is legitimate and the money will be transferred successfully with all necessary back-up official documents showing legitimate source/origin of fund. The transfer will be affected within a period not longer than two weeks as soon as we reach an agreement and you furnish me with a suitable response indicating your interest for processing the transfer. I plead with you on one issue, whether you are interested or not, kindly do not expose this information to anyone else. I confirm that the transaction is legitimate and without any risks either to us or yourself. Please, give me your response immediately by return mail through my alternate email: [khayaletumatrose@pisem.net](mailto:khayaletumatrose@pisem.net)

Yours Faithfully,  
Mr. Khayaletu Matrose



## **APPENDIX 5**

This document is retained in its original font, for quick and easy reading by participants.

### **Training workshop for strengthening technical competency for consumer protection in ASEAN**

**Manila, Philippines 5 – 6 October 2015**  
**Presented by Carl Buik**

#### **Phones, the Internet and E-commerce**

#### **Investigation scenario exercise**

#### **Purpose of this exercise**

The purpose of this scenario exercise is to explore various elements of an investigation.

#### ***How the exercise will be conducted***

You are an investigations team leader working for a national consumer protection authority with general jurisdiction to investigate consumer problems in any sector of the economy. There are also sector regulators that also have an interest in consumer issues.

1. You will be given a brief scenario. You should then consider:
  - Is this a complaint that is worth investigating? Why?
  - What is the real problem here? Would this conduct constitute a contravention(s) of consumer protection law in your own home country?
  - What evidence might you need?
  - What are the limitations of the evidence you have so far?
  - Where do you think you would obtain that evidence and how would you go about obtaining it?
2. We will discuss your thoughts on the above questions
3. You will be given a sequence of other documents with additional information. What are the implications of the evidence that you now have?



4. We will discuss your thoughts on the above questions

*Expected outcomes:*

- (i) Practice in assessing the facts against the elements of an offence.
- (ii) Practice in analytical thinking:
  - assessing the value of information and evidence
  - identifying additional evidential requirements and potential sources for that evidence
- (iii) Have some fun



## Scenario 1

Your authority has received two complaints via email concerning the *Mobile Booster* brand of mobile signal enhancer.

### ***Scenario 1: the 1<sup>st</sup> complaint***

The first complaint reads:

'I wish to report a clear and blatant contravention of s[xx] & [xy] of the [*name of relevant consumer protection law*]. The contraventions are harming:

- (i) consumers because they are being misled into purchasing an inferior and poor value product
- (ii) established reputable traders because they are losing business sales when consumers are unfairly tricked into buying an inferior and poor value product.

On 18 January I went to the *Mobile Boosters (Philippines)* store in the Greenhills Shopping Mall. I approached sales representative Angel and asked her questions about the *Mobile Booster* for the purpose of seeing if she would be truthful or lie. She was deliberately false and misleading in her answers.

The conduct of *Mobile Boosters (Philippines)* is clearly contrary to [*name of relevant consumer protection authority*]'s '*Treating consumers fairly*' guideline for retailers and clearly comes within the authority's enforcement priorities as set out in the publication '*Consumer Enforcement Priorities*'.

I ask that [the Authority] take immediate action to:

- (i) prevent *Mobile Boosters (Philippines)* from publishing further false and misleading advertisements
- (ii) prevent *Mobile Boosters (Philippines)* sales representatives from making further false and misleading representations to customers
- (ii) Fine *Mobile Boosters (Philippines)* for its false and misleading conduct.



### ***Scenario 1: the 2<sup>nd</sup> complaint***

The second complaint reads:

‘Last week I bought a Mobile Booster and it doesn’t work. I can’t take it back because of health reasons. It cost me a lot of money. Can [the Authority] please get me my money back? Thank you. Joshua’



**Scenario 1: an advertisement in *the Philippine Daily Inquirer*  
1 October 2015**

(unofficial translation from the original Tagalog text)

Do you have *poor mobile reception* in your car?

Need to make calls, *no hassle?*

Missing *important calls?*

Tired of mobile phone carriers that *promise long but deliver short?*

You need ***Mobile Booster*** the latest hi tech scientific mobile reception booster that can increase the strength of your ***outgoing digital signals and sensitivity to incoming digital signals*** by a quantum leap.

Hurry, stocks are *limited* and *selling fast*. **Buy now or miss out!**

Technical details and full contract detailing other legal stuff concerning your obligations and our rights including but not limited to performance guarantees, refunds policy, coverage limitations, mandatory maintenance plan etc. etc. are available in store on application after purchase.





## Scenario 1: the text of John Paul's blog

(Blog available in multiple language versions: Tagalog, English Thai, and Vietnamese)

Search term used: mobile phone signal enhancement Indonesia

1<sup>st</sup> listed result: smart phones and cell phones  
[www.bestbuycomparisons.com/blog/mobilereception](http://www.bestbuycomparisons.com/blog/mobilereception)

Screen dump from [www.bestbuycomparisons.com/blogenglish/mobilereception](http://www.bestbuycomparisons.com/blogenglish/mobilereception):

Best Buy Comparisons                      blog

John Paul proves you with a daily independent commentary on the latest, best and cheapest gadgets to boost poor mobile reception: iOS, Android and Windows

11:20 am 30 June 2015

I'm often asked to recommend mobile phone signal enhancers suitable for in-car use. You know the story, poor mobile reception in your car, hassles calling out and missing important incoming calls. I should be recommending that you go back to your service provider. But I'm not. I'm tired of mobile phone carriers that promise long but deliver short.

Despair not, for help is at hand: the Internet and international ordering to the rescue. Mobile Booster is the latest hi-tech scientific mobile reception booster that can increase the strength of your outgoing signals and sensitivity to incoming digital signals by a quantum leap.

My recommendation? I've tried the lot. Well I may be exaggerating a little, but you see where I'm coming from?

My insiders tip No. 1: Hurry, there is a rumour from the usual 'well connected sources' that stocks are limited and being sold fast. I'm putting my money on this one: buy now or miss out.

My insiders tip No.2: You can order on-line at [www.mobileboosters.com](http://www.mobileboosters.com) or if you have the energy and don't mind the crowds you can buy the old fashioned way at any *Mobile Boosters* retail outlet at selected shopping malls throughout the ASEAN region.



## **Scenario 1: transcript from [www.mobileboosters.com](http://www.mobileboosters.com)**

[www.mobileboosters.com/products/mobilebooster](http://www.mobileboosters.com/products/mobilebooster)

Mobile phone signal enhancer

Mobile Booster [[jpeg](#)], [[video](#)]

There can be many reasons for poor reception of mobile phone signals including the location and technical specification of signaling infrastructure (towers), the location of mobile phones (for example in shielded environments such as basements), intervening factors (for example mountains) and the current volume of communications using particular infrastructure.

Mobile Phone Booster may contribute to fewer dropped or missed calls where the reception problems are caused by a low rated reception chip.

For user testimonials [[click here](#)]

For demo video [[click here](#)]

For other products [[click here](#)]

**To purchase** [[click here](#)]

For technical details including the appropriate use of and limitations of Mobile Booster [[click here](#)]



## **Scenario 1: the sales representative's recollection**

I recall both customs really well. The first was a man who seemed like a 'know it all'. He wasn't interested in anything I said. He seemed like he already had all of the answers to the questions he asked. The second was a different sort of guy. He didn't seem sure about anything.

I said more or less the same to both customers because that's what I was taught to say during training. I recall saying:

'In my opinion Mobile Booster is the best. I've read about it myself, so I know. I've heard that Mobile Boosters are very popular with PLDT employees. It works in most areas. Of course, I can't guarantee that it will work in your area because I 've not tested it there. But there is no risk because if you bring it back unopened within 7 days we will give you a credit to buy another model or brand.

And the price? I doubt that you will find a fully comparable competing product at a cheaper price anywhere. But don't take my word for it, shop around and then come back here. Or save you time and buy it now!'



## Scenario 1: the 1<sup>st</sup> complainant's recollection

I recall the representations of the salesgirl perfectly. She was young and seemed to be repeating all of the misleading claims parrot fashion as though she had been coached. She wasn't interested in anything I said. I recall what she said word for word:

*'Mobile Booster* is the very best phone booster, I can assure you. I've used it myself, so I know. *Mobile Booster* is endorsed by PLDT, all their employees are issued with one. It works in all areas. I can guarantee that it will work in your area. There is no risk because if you bring it back within 7 days we will give you a refund.

And the price? I can guarantee that you that you will not find another phone booster at a cheaper price anywhere. It's a bargain. Why don't you it now and save!'



## Scenario 1: the 2<sup>nd</sup> complainant's recollection:

I recall that the sales representative was a woman. She was really helpful and really wanted me to be happy with the Mobile Booster. I think that she liked me because we both read John Paul's blog to find out the latest.

I think that she said something like:

"If you are having problems with your mobile phone coverage you need *Mobile Booster*. *Mobile Booster* is PLDT, all their employees have one. And you've seen the videos and read what the independent guru says, haven't you? It works in all areas. I can guarantee that it will work in your area. There is no risk because if you bring it back within 7 days we will give you a refund.'

I also when to that other shop around the corner. I didn't like that sales person as much. Their booster was a *Premium*. It was more expensive but they said that it was much better than the *Booster*. But its not one that John Paul has even mentioned.

She said 'You must buy this phone now. You will not find another phone booster at a cheaper price anywhere. It's a bargain. You must buy this phone now.' Or it could have been the guy at *Premium*. They both said the same. Anyway if I buy now I will beat the price rise because he said that to make it fairer for everyone and improve quality they were going to be charging the same from now on which I guess will help.



## **Scenarios 1: Technical report by an independent *Mobile Phones Technologies* (MPT) expert Ms Ima Wizz:**

The *Mobile Booster* is a mobile signal enhancer sold by *Mobile Boosters (Philippines)*. It does boost outgoing signals and increase the sensitivity of reception, but only marginally and not in all areas. It does work in the complainants' areas.

It is similar in specification and performance to several other brands of mobile signal enhancers, some of which sell for a cheaper price than *Mobile Booster*.

The *Mobile Booster* is housed in an inert plastic casing and does not come into contact with consumers in the normal course of usage. Reuse by other persons does not carry any health implications whatsoever.





## Scenario 1: Contract:

### *Terms of this contract:*

By buying this product on-line the purchaser has agreed that:

101. The terms set out in this contract are the complete terms of the contract. The purchaser agrees that he/she has not relied upon any representations expressed or implied in any advertising, website content, by any sales representative or any other person whatsoever in respect to the suitability, applicability, absolute or relative value, performance or operation or any other characteristics of the *Mobile Booster*.

102. This contract is governed by the laws of California, USA

103. The terms of this contract supersede and override any and all regulations.

### *Refunds and returns policy:*

104. Due to Health Regulations *Mobile Boost (Philippines)* is unable to accept returns of *Mobile Booster* products once they have been taken from the store.

### *Free operating system and apps updates:*

105. the manufacturer reserves the right to issue software changes and updates as and when it deems necessary. Failure to install updates may render the unit inoperable. *Free Updates* Minor updates may be downloaded from [www.mobileboosters.com/products/mobilebooster/updatesdownload](http://www.mobileboosters.com/products/mobilebooster/updatesdownload) without charge. The manufacturer reserves the right to specify charges of major updates at its sole discretion and without prior notice.



### **Scenario 1: Information about the 1<sup>st</sup> complainant**

The complainant is a 40 year old transmissions technician for *Premium Mobile Accessories*, the leading and longest established seller of mobile signal enhancers in the Philippines.

### **Scenario 1: Information about the 2<sup>nd</sup> complainant**

The complainant is a 30 year old unemployed man with who has some mental health problems.

### **Scenario 1: Information about the sales representative**

The sales representative is a 16 year old woman in her first job after leaving school. She has no technical training and has learned how to talk to customers by following what she has heard other sales representative saying.



## **Qualifications of independent *Mobile Phones Technologies* (MPT) expert Ms Ima Wizz:**

Ms Ima Wizz

**Qualifications:** Bachelor of Communications Technologies University of South Manila  
1980 - 1982

Master of Applied Science (Telecommunications Networks)  
University of Mindanao  
1983 - 1984

**Employment:**

2012 - current: freelance writer of the *Consumers' Advice* column of the popular magazine ***Mobile Phones Technologies*** (Philippines Edition)

2000 - 2012: Manager, Consumer Mobile Phone Packages at *Mobile Boost Philippines*

1995 – 2000: Senior Technician, Mobile Phone Networks at *Premium Mobile Accessories*

1985 – 1995: Senior Advisor Mobile Phone Operations at the Communications Authority Philippines (CAP)

### **Certified extract from Court Case No. 123/2012**

**Applicant:** Ms Ima Wizz

**Respondent:** Mobile Boost (Philippines)

**Application:** That the respondent wrongfully dismissed the application and defamed her by stating that the reason for dismissal was professional incompetence, neglect of duty and falsification of records

**Finding:** The Court finds that respondent wrongfully dismissed the application and defamed her by stating that the reason for dismissal was professional incompetence, neglect of duty and falsification of records



## **APPENDIX 6 : The Design and Delivery of a Training Module on Phones Internet Services & E-commerce**

In designing a training module on Phones, Internet Services and E-commerce, a number of issues are to be considered:

1. Who would use this training material? And why?
  - a. Policy makers – looking to improve laws and regulations?
  - b. Enforcement officers?
  - c. Dispute resolution schemes?
  - d. Others?

2. Who is this module for?

The module is designed for people who have a role in protecting consumers' interests, including government officers, NGOs, consumer disputes settlement bodies, consumer associations, enterprises, financial institutions, consumers.

The training module might apply to

- (i) policy offices in consumer and other government agencies who seek to better understand the operation of their own laws and regulatory practices, and to seek further knowledge about laws and practices in other AMSs and world's best practice;
- (ii) regulatory and enforcement officers who seek to better understand existing laws and how to best implement and enforce those laws;
- (iii) other bodies and agencies that seek to better understand how to advise and assist consumers, how to improve their business practices, and how to advise, assist and respond to government moves to improve the law and industry and regulatory practices.

What resources/material do trainers need in order to conduct the training?

It is first necessary to have the trainer get the trainees to identify and fully understand the nature of the problems they are seeking to deal with. The training program would need to be designed to respond to the consumer related problems they are facing.

Options to deal with the issues, e.g. legislative, private sector participation, NGOs, international bodies and the roles of each institution, ASEAN cooperation and assistance, government coordination.

A training module may seek to use a case study or role-play to illustrate present consumer complaints and industry and regulatory practices, and how these complaints can be best resolved.

***A common trap! We often come to a solution before we fully understand the problem.***



## Design of Pilot Training Program, Materials and Tools

### A. Who is your target audience?

In designing your training program it is necessary to have an understanding of who the participants are? This better enables you to tailor your program to fit the needs of participants. In many cases they may be officials from consumer protection agencies selected for training will not necessarily be at the same level in terms resources, institutional framework and technical competencies.

The application of adult learning principles allows for each person to enter and engage with the program where their particular point of need is determined. The program needs to be designed for multiple exit and entry points depending on individual needs.

Individual learning needs will be determined by some or all of the following–

- a. Surveys of current practice and understanding
- b. The provision of 3rd party reports outlining levels of knowledge and practice
- c. Job roles and descriptions
- d. Job analysis
- e. Annual reports
- f. Legislation
- g. Consumer complaints/feedback

A well designed training program would usually have the following elements:

Assess training need

Determine detailed content

Design instruction

Conduct pilot training course

Evaluate, then modify training as necessary

### B. Applying the Adult Learning Approach

Part of being an effective educator involves understanding how adults learn best.

Andragogy (adult learning) is a theory that holds a set of assumptions about how adults learn. Andragogy emphasizes the value of the process of learning. It uses approaches to learning that are problem-based and collaborative rather than didactic, and also emphasizes more equality between the teacher and learner.

There are six principles of adult learning which can be applied. They are:

- a. Adults are internally motivated and self-directed
- b. Adults bring life experiences and knowledge to learning experiences
- c. Adults are goal oriented
- d. Adults are relevancy oriented
- e. Adults are practical
- f. Adult learners like to be respected

Cultural awareness can be demonstrated by the following:

- a. Clear simple use of language in all training materials
- b. Use of non-sexist language
- c. Brief and concise instructions for trainers as well as participants
- d. Use of colour and spacing as well as graphics to enhance understanding
- e. Respect for people's values, beliefs and behaviours
- f. Reducing judgements or generalisations about cultural practices



g. Encouraging students to share their own experiences and perceptions

Strengthening technical capacity and training strategy for consumer protection activities (education, investigations etc) in respect of consumers' use of phones, the Internet and e-commerce.

The process of strengthening technical capacity for consumer protection agencies should be based on a series of strategic documents, such as a government training policy, multi-annual strategy, short-term plans, and programs for training and development in respective AMS.

In these strategic documents, key opinions of the agencies should be taken into consideration. The training policy will be in coherence with key training system parameters, including:

- a. The objectives of consumer protection agencies (in accordance with strategic priorities and the short-term, mid-term, and long-term goals of the respective agency;
- b. The legal framework and legal provisions that need to be put into place;
- c. The type of training system/model to be created;
- d. The principal stakeholders and roles for policy and strategy development and training provision;

A formal commitment to training is a key pre-requisite for better service delivery at the national level, along with a shared understanding on the part of stakeholders of what training entails. This means quality assurance mechanisms and resource mobilisation arrangements.

In addition to the policy, a training strategy will be suggested in the follow on material from the validation workshop consisting of the following components, among others:

- a. The principles of training;
- b. Training and development objectives, sub-objectives, and activities (with timeframe and indicators);
- c. Priority training programs, as well as priority target groups;
- d. Role allocation between partners and cooperation mechanisms;
- e. Financing sources for strategy implementation;
- f. A quality assurance mechanism;
- g. A monitoring and evaluation mechanism.

The training strategy includes an implementation action plan as the assessment results and the priority training areas identified have a certain bearing on the overall training system, as they should inform entity strategy development as well as training curricula.

**Design and Methodology:**

The major increase in training provided by international donor organisations post-1996 has meant that conventional class-room-type training formats are increasingly supplemented by more progressive methodologies that include workshops, on-the-job training, and case studies. Practical and interactive training methods will be used to strengthen the capacity and furthermore, on-line learning opportunities will be explored, as they represent a cost-effective and accessible learning format.

This includes virtual on-site and classroom learning, as well as self-paced programs.

- a. Target Groups: This will take into account the job descriptions of individual staff (by organisational unit/occupation) in the consumer protection agency, as well as timeliness, relevance, sequencing of training, and the available financial resources.
- b. Quality Assurance: If quality of training and training materials is to be ensured in the long run, there is a need for standardisation. An assessment and certification process can be used which recognises quality training programs and training providers is envisaged. This will ensure the





value for time and resources spent that will also introduce a uniform standard of training quality across the board.

c. Certificates for completion of courses:

It is useful to signify successful completion of courses with an appropriate certificate. If this is desired it might be discussed at a regular project meeting to determine under what auspices such a certificate would be properly be given.

d. Conduct and Evaluation of Pilot Training

Participants could be asked for written and oral feedback outlining their experiences in the learning process and their view of the effectiveness of the training.

They will also be asked about the methods and modes of training and how these suited their needs. Particular attention will be given to the online accessibility and also the relevance of activities in the training to meet their own needs.

e. Supervisors could be asked for comment on changes of behaviour and attitude of the people in the workplace context. This could be done via a simple survey questionnaire.

f. This information will be used to make recommendations for any necessary modification to the subsequent training program to suit the needs of the workplace and the learners.

g. The training report will be prepared based on the feedback from the learners and the workplace supervisors.



## APPENDIX 7

### Further reading

For those participants who would like to further or more detailed information of the topics covered in this paper and the accompanying presentations, handouts and exercises I make the following suggestions:

- Because the topics cover here are all related to technologies the issues and the detail are evolving. Consequently:
  - it is necessary to continue building your knowledge and experience because otherwise it will soon be out-dated.
  - Providing a long list of books or articles for reading is of limited use because they have a limited 'shelf life' of relevant. Better is to suggest some useful sources for up to date content.
- While the theme of this paper is the consumer protection issues raised by consumers' use of the technologies, the basic issues are not restricted to using those technologies. Consequently general consumer protection laws and other regulation) need to be understood and references relating to general consumer protection issues need to be consulted
- For maintaining a good working knowledge in the area, you cant beat the relevant and convenience of web sites of the more active consumer protection agencies and international organisations.

- The Federal Trade Commission (FTC), US

[www.ftc.gov](http://www.ftc.gov)

Possibly one of the most comprehensive consumer agency sites both generally and in respect of consumer online lives. There is specific content aimed at consumers and at businesses. Topics include *Scam Alerts*, *Privacy and Identity*, *Your online life after death*

- The Australian Competition and Consumer Commission

[www.accc.gov.au](http://www.accc.gov.au)

The ACCC maintains a comprehensive range of documents on relevant issues, aimed at consumers and businesses. Of particular interest is the *SCAMWATCH* site at [www.scamwatch.gov.au/types-of-scams](http://www.scamwatch.gov.au/types-of-scams). The ACCC's ever-growing list of Media Releases at [www.accc.gov.au/media/media-releases](http://www.accc.gov.au/media/media-releases) is also worth revisiting periodically to monitor the latest developments affecting consumers online lives.



- The Competition and Market Authority (CMA), UK

[www.gov.uk/topic/competition/consumer-protection](http://www.gov.uk/topic/competition/consumer-protection)

[www.gov.uk/government/organisations/competition-and-markets-authority](http://www.gov.uk/government/organisations/competition-and-markets-authority)

The CMA provides a range of relevant documents within their *Guidance Collection*, *Popular Guidance* and *Latest New* tabs.

- UNCTAD

INFORMATION ECONOMY REPORT 2015: unlocking the potential for e-commerce in developing countries (see [http://unctad.org/en/PublicationsLibrary/ier2015\\_en.pdf](http://unctad.org/en/PublicationsLibrary/ier2015_en.pdf))

Online Consumer Protection Legislation Worldwide (see [http://unctad.org/en/Pages/DTL/STI\\_and\\_ICTs/ICT4D-Legislation/eCom-Consumer-Protection-Laws.aspx](http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Consumer-Protection-Laws.aspx))

- International Consumer Protection and Enforcement Network (ICPEN)

<https://icpen.org> ICPEN is an international organization made up of member agencies who have responsibility for consumer protection at the national level in their respective countries. The stated aims of ICPEN are to:

- Protect consumers' economic interests around the world,
- Share information about cross-border commercial activities that may affect consumer welfare
- Encourage global cooperation among law enforcement agencies

While the ICPEN site does provide some useful content to non members (under the tabs *for consumers* and *for consumer experts*, the principal content and functionality is only available to member agencies. Topics addressed include:

- Cross-border disputes
- Shopping online
- Scams
- ICPEN activities related to online consumer protection such as their annual *International Internet Sweep* and the online complaint filing process *e-consumer.gov* (see [www.econsumer.gov/](http://www.econsumer.gov/) - [crnt](http://www.econsumer.gov/crnt)) and *Fraud Prevention Month*.
- Activities that are regionally relevant such as the APEC Electronic Commerce Steering Group (see <http://icpen.org/for-consumer-experts/consumer-protection-around-the-world/apec-electronic-commerce-steering-group-1>)

- OECD (The Organisation for Economic and Cultural Development)

This site provides a wealth of relevant content. In respect of consumer protection generally see [www.oecd.org/sti/consumer](http://www.oecd.org/sti/consumer), while in respect of online



issues see [www.oecd.org/sti/consumer/consumersinthedigitaleconomy.htm](http://www.oecd.org/sti/consumer/consumersinthedigitaleconomy.htm), particularly the various guidelines and information on recent trends

- Although digital (or computer) forensic investigations are beyond the scope of this paper some participants may like to explore this topic. Two excellent introductions are:
  - *The Basics of Digital forensics: The Primer for Getting Started in Digital Forensics*, e-pub, ISBN 978-1-59749-661-2, [www.syngress.com](http://www.syngress.com)  
Sammons, John  
and
  - *A Practical Guide to Computer Forensics Investigations*  
e-pub ISBN 13: 978-0-7897-4115-8, Person Education Inc  
Hayes, Darren J.
- A best practice model for e-consumer protection  
Dan Svantesson a, Roger Clarke  
computer law & security review 26 (2010) 31 – 37 available at  
[www.sciencedirect.com](http://www.sciencedirect.com)  
[www.compseconline.com/publications/prodclaw.htm](http://www.compseconline.com/publications/prodclaw.htm)



### About the consultant



Carl Buik worked for the Australian Competition and Consumer Commission (ACCC) for 28 years, until 2008. Mr Buik managed investigations, consumer and business education programs and training for ACCC staff and external audiences. He also represented the ACCC at domestic and international fora including the International Consumer Protection and Enforcement Network (ICPEN).

Since leaving the ACCC Mr Buik has undertaken a range of consultancies involving both consumer protection and competition law issues for national governments, international organisations and the private sector in more than 30 countries, including the Common Market for Eastern & Southern Africa (COMESA), UNCTAD and the Competition Authority Kenya (CAK). The consultancies for CAK in 2014 and 2015 involved building operation capacity for the agency's expanding consumer protection role.

Mr Buik has qualifications in both law (LLB, ANU Australia) and economics (B.Ec UNE, Australia & Grad Dip Economic for Competition Law, KCL UK).