PHONES, INTERNET SERVICE, AND E-COMMERCE

Training Manual

Strengthening Technical Competency for Consumer Protection in ASEAN

With the Support of:

This publication is part of the wider-scale project entitled “Addressing Gaps in the Establishment of an ASEAN Consumer Protection Framework Phase I”, which is implemented by the ASEAN Committee on Consumer Protection (ACCP) and supported by the government of Australia through the ASEAN-Australia Development Cooperation Program Phase II (AADCP II).

FOREWORD

The commercialization of products and services in response to the needs and demands of the consumers in the global market presupposes that the producers make their products or services safe, and protect the customers from injury, harm, or any other negative consequence in using such products/services. On the other hand, the government, as a regulatory institution, sees to it that consumers are protected, by ensuring that laws and other regulations pertaining to consumer safety and protection are properly communicated and implemented.

As a growing and dynamic single market and production base, the Association of South East Asian Nations (ASEAN) is faced with the same issues on consumer protection and safety. In a proactive move, the ASEAN developed the AEC Blueprint 2025, which contains strategic measures to ensure comprehensive and well-functioning national and regional consumer protection systems by 2025, enforced through effective legislation, redress mechanisms, and public awareness.

The strategic measures were then elaborated under the ASEAN Strategic Action Plan for Consumer Protection (ASAPCP) 2025. The ASEAN Committee on Consumer Protection (ACCP) is the responsible body to coordinate and undertake regional work on consumer protection.

The project "Development of Teaching Tools to Apply Good Consumer Protection Practices in 6 Priority Sectors" is among the consumer protection initiatives supported by the ASEAN-Australian Development Cooperation Program Phase II (AADCP II). It is an offshoot of an earlier project, "Strengthening Technical Competency for Consumer Protection in ASEAN," which produced technical modules on 6 Priority Sectors, namely: (1) Consumer Credit and Banking; (2) Product Safety and Labeling; (3) Environment; (4) Phones, Internet Services, and E-commerce; (5) Health Care Services; and (6) Professional Services, with the assistance of UNCTAD.

This Training Manual will facilitate qualified AMS to be trainers, who can then train other personnel involved in consumer safety and protection efforts. This Manual provides detailed step-by-step procedures on how to conduct the training. Each session uses various training methods such as video clips, cases, structured learning exercises, info-search, role-playing, group discussions, and lectures with accompanying PowerPoint slides to aid in the presentation of the Learning Inputs. The **Trainer's Tips Box** cites additional reading materials and video clips that can deepen the Trainer's knowledge of the issues that are discussed in a session. Assessment methods such as meta-reflections and instrumentation are also included at the end of each module session to get feedback on the learning of the participants.

ACKNOWLEDGMENT

We would like to thank the team of consultants from the Center for Business Research and Development of De La Salle University (DLSU-CBRD) for preparing the six training manuals corresponding to the earlier six technical modules. The team is composed: Prof. Dr. Divina M. Edralin, Project Team Leader/Head; Dr. Jaime T. Cempron, Dr. Emiliano T. Hudtohan, and Dr. Ronald M. Pastrana as Research Associates; Dr. Ana Liza Q. Asis-Castro and Ms. Jennelyn J. Gannaban as Research Assistants; Ms. Ma. C. P. Assumpta C. Marasigan as Case Writer and Copy Editor of Training Materials; and Dr. Nelson J. Celis as Consultant.

The corresponding technical module for Phones, Internet Service, and E-Commerce was drafted by Carl Buik under the guidance of the United Nations Conference on Trade and Development (UNCTAD) and validated by the ASEAN Committee on Consumer Protection (ACCP). Our special thanks to the ASEAN Secretariat for an excellent partnership and the Australian Government for the support given in executing the present project.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

AADCP	ASEAN-Australian Development Cooperation Programme
ACCC	Australian Competition and Consumer Protection Commission
ACCP	ASEAN Committee on Consumer Protection
AMS	ASEAN Member States
APEC	Asia-Pacific Economic Cooperation
APPS	Application software
ASAPCP	ASEAN Strategic Action Plan for Consumer Protection
ASEAN	Association of Southeast Asian Nations
ATM	Automated Teller Machine
BSP/CB	Bangko Sentral ng Pilipinas (Central Bank)
B2B	Business to Business
B2C	Business to Customer
CNP	Card Not Present
CPA	Consumer Protection Authority (Agency)
DOJ	Department of Justice
DTI	Department of Trade and Industry
ECSG	Electronic Commerce Steering Group
EDI	Electronic Data Interchange
ICPEN	International Consumer Protection and Enforcement Network
ISMS	Information Security Management System
ISP	Internet Service Provider
MOU/MOA	Memorandum of Understanding/Agreement
NFA	No future action
NBI	National Bureau of Investigation
PDR	People's Democratic Republic
SEC	Securities and Exchange Commission
SMS	Short Text Messages

SOE	State-Owned Enterprises
UNCTAD	United Nations Conference on Trade and Development
URL	Universal Resource Locator

INTRODUCTION

MODULE DESCRIPTION

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.

The very attributes that make online markets so attractive also magnify existing risks and generating new risks. In online transactions, not only are the goods and documents not physically present, cash has given the way to various electronic means of payment.

The efficient and effective use of phones and the Internet is an essential building block in 21st century economies, whatever their stage of development. While the contribution of these technologies may still be restricted by access, pricing and other regulatory issues, consumers and traders are 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. However, consumers experience various safety and protection concerns in availing themselves of these e-commerce services.

In this regard, this module focuses on phones, internet services, and e-commerce in the ASEAN Member States. It aims to provide trainees, who are officials and heads of agencies, with additional competencies in terms of technical knowledge, better understanding of industry policies and practices, and skills in enhancing consumer protection in this sub-sector.

This training module provides a resource for trainers seeking to train participants on how to deal with systematic problems that arise in the telecommunications and e-commerce marketplace within the ASEAN region.

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.

Session topics will be discussed with their respective objectives, appropriate methodology for adult learning, time allocation, references, as well supplemented by online resources.

GENERAL LEARNING OBJECTIVES

At the end of the module, the participants will be able to:

Session 1	Explain the overview of phones, internet services, and e-commerce in the ASEAN context
Session 2	Identify consumer protection issues
Session 3	Examine pre-market interventions
Session 4	Assess post-market interventions
Session 5	Apply redress mechanisms for conflict resolution

SESSION 1: INTRODUCTION TO PHONES, INTERNET SERVICES, AND E-COMMERCE IN THE ASEAN CONTEXT

SESSION DESCRIPTION

This session introduces the broad policy context for consumer protection in phones, internet services and e-commerce. It describes the international and ASEAN policy measures for delivery of mobile and internet services as telecommunication technologies that allow citizens to communicate with others at a distance, both in their capacity as individuals and as consumers. It covers the effective use of online technologies and their impact on economic growth and consumer welfare, requirements for effective use of online technologies, consumer use of phones, the internet, and e-commerce; ensure that consumers enjoy the same regulatory protection as in the brick-and-mortar markets, and the way in which consumer experiences in using these technologies can be improved.

LEARNING OBJECTIVES

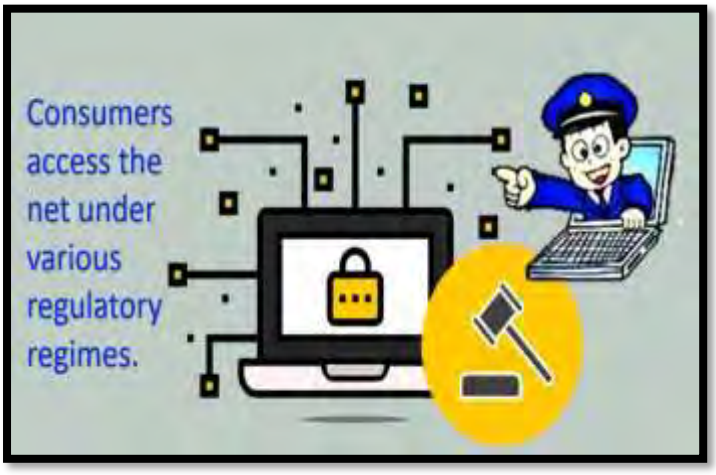
By the end of the session, the participants will be able to:

- Identify the effective use of online technologies and their impact on economic growth and increased consumer welfare;
- State the requirements for effective use of online technologies;
- Explain the use by consumers of phones, the Internet, and E-commerce;
- Recognize the need to accord consumer protection for online transactions in the same way that is provided in brick-and-mortar markets; and
- Translate the effective use and benefits of online technologies on consumer experiences.

SESSION TOPICS

In this session, the following topics will be covered:

- Effective use of online technologies and their impact on economic growth and consumer welfare.
- Requirements for effective use of online technologies.
- Consumer use of phones, the internet, and e-commerce.
- Consumer protection needed online in the same way that it is needed in brick-and-mortar markets.
- How consumer experiences in using these technologies can be made better.



DEFINITION OF TERMS

access
refers to consumers access to the Internet through the use of devices, bandwidth, arrangements, and under regulatory regimes

'brick and mortar'
refers to conventional or traditional market (shop) where traders have a physical presence to distinguish them from online (or virtual) markets

consumer protection
refers to rules/ laws/ legislations designed to ensure consumer rights, fair trade, fair competition, and accurate information in the marketplace

online transactions
refer to transactions involving mobile phones (smartphones), the internet, and e-commerce

e-commerce
refers to the use of the Internet and the Web to transact business. More formally, digitally enabled commercial transactions between and among organizations and individuals

TRAINING METHODS

Duration in Hours / Minutes:	**2 hours / 120 mins** Session Introduction and Video Showing: 30 mins Lecture: 60 mins Open Forum with Inquiry-Oriented Discussion: 15 mins Session Assessment: 15 mins
Materials / Visuals	▪ Video clips ▪ PowerPoint Presentation slides ▪ Laptop with LCD projector ▪ Flip chart ▪ Markers, pens, and notepads

Instructions/Procedures

1. Introduce the topics to be covered for Session 1.
2. Show the following video clips related to “Online Technologies in AMS”

ABS-CBN News. (2018 July 11). Business Nightly: DTI, ‘Verify online sellers before buying’ (Video). Available from https://www.youtube.com/watch?v=KeHjVdO0btc

Video length: 2 minutes and 32 seconds

7a9rian2. (Producer). (2014, April 2). Use of Phone: Impact of mobile phones on us! (Video). Available from https://www.youtube.com/watch?v=SKXhnnzLNH4

Video length: 2 minutes and 22 seconds

World Bank. (Producer). (2016, February 17). The Economics of the Internet (Video). Available from https://www.youtube.com/watch?v=EWkkt3tY2zw

Video length: 3 minutes and 23 seconds.

Trevor Tillotson. (Producer). (2015, March 14). Advantages and Disadvantages Of e.commerce – What Are They? (Video). Available from https://www.youtube.com/watch?v=LAxs8BsJPDE

Video length: 1 minute and 56 seconds

3. Lecture Session 1 using the lecture inputs (shown in the Box 1) with PowerPoint slides (See PowerPoint Slides Presentation Handout) for Session 1. Link the video message and the PowerPoint slides on the following topics.
4. Allow the participants to ask questions or seek clarification regarding the lecture inputs, as well as ask them questions in order to draw out ideas from them. Then, summarize the session in relation to the learning objectives.

TRAINER'S NOTES

- Refer to PowerPoint Presentation slides in another set of handout.
- Read the Technical Manual on Chapter 1 – Introduction, pp. 10-15
- Refer to PowerPoint Slides Presentation Handout.
- Access these online resources: www.apec.org for the Committee on Trade and Commerce on the development and use of e-commerce.
- Review these references for further reading:
  - ASEAN Secretariat 2016
  - Phones, Internet Services & E-commerce. In AADCPII, Project on strengthening technical competency for consumer protection in ASEAN (Version 21 January 2016. Retrieved from ASEAN website:http://asean.org/storage/2012/05/E-Commerce-Module-Final-21Jan16.pdf

BOX 1. LECTURE INPUTS

1. **Introduction to phones, internet service, and e-Commerce**
   - Background and context of the sector and the issues confronting the consumers with regards to the protection and safety.
   - Mobile phone and Internet access services are telecommunication 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 in every AMS and in various stages.

2. **Effective use of online technologies**
   - Consumers enjoy increased choice in quality, price, and other attributes.
   - Consumers can benefit from increased competition as more traders compete for their business.
   - Consumers can lower their search and transaction costs. At the same time, traders can make significant saving in marketing and transaction costs.
   - Traders can offer their products and services to more potential customers.

3. **Some requirements for effective use of online technologies**

   a. Access

   Consumers <u>access</u> to the internet:

   - Access to the internet is enjoyed by a significant and growing percentage of consumers across ASEAN.
   - Consumers access the internet through various ways (from desktop/laptop computers and mobile devices, on variable bandwidths and under various arrangements.

b. Confidence

Consumer confidence includes consumers':

- Being aware of potential hazards and knowing how to avoid them and mitigate harm
- Having the ability to implement strategies to avoid them and mitigate harm
- Knowing the laws and regulations that prohibit harmful conduct, create liability of harm caused, and facilitate remedies
- Knowing what they can do if they have a problem

When consumers are confident they are more willing to try new products and traders, and to buy more.

4. **Consumers' use of online technologies: phones, the internet, and e-commerce**

Consumer use of phones, the Internet and e-commerce is increasing for the following purposes:

- Free entertainment and information
- Social interaction
- Transactions

Because more consumers are using online technologies, brick and mortar traders:

- Maintain websites to advertise
- Encourage consumers to go online to reduce operating costs

5. **Consumer protection needed online in the same way that it is needed in brick-and-mortar markets**

Harm is caused when legitimate traders do not manage their consumer protection compliance risks and when consumers do not act in their own best interests.

6. **Consumer experiences in using these technologies can be improved using a mix of strategies**:

A. More effective enforcement of existing regulations

B. Easier access to a range of free or low-cost systems for quick and fair resolution of consumer complaints

C. Increased consumer education by consumer protection authorities, sector regulators, and infrastructure providers

D. Expanded roles for business associations and individual traders, including infrastructure providers, to ensure comprehensive compliance with consumer protection laws

E. More effective and efficient interagency cooperation at the national, regional, and global levels

F. Filling in legislative gaps by enacting national laws

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

Overall, progress towards harmonization has been the strongest in the area of electronic transactions laws, with 9 out of 10 member countries now having relevant legislation in place. Cambodia has not yet passed electronic transaction legislation, although a draft law has been completed in 2017 and awaiting for enactment this 2018.

Progress to date on appropriate consumer protection legislation for online transactions in the region is mixed. Six out of ten countries have legislation in place. Two countries have partial laws in place (Brunei Darussalam and Indonesia). One country has draft laws (the Lao People's Democratic Republic) and Cambodia has yet to commence work in this area. Cambodia has also no general consumer protection law that applies to e-commerce. However, the proposed omnibus e-commerce law will include a section on online consumer protection.

ASSESSMENT AND EVALUATION OF PARTICIPANT'S LEARNING

Method of Assessment: Reflection/Meta Learning Ask the participants to share in plenary their answer to the following questions:

- What have you learned from the topics discussed?
- How can you apply these learnings in your work related to consumer protection?

SESSION 2: SUBSTANTIVE CONSUMER PROTECTION ISSUES

SESSION DESCRIPTION

This session discusses the problems that consumers experience. It identifies consumer protection issues within and outside national borders, and the various sources of market intelligence about consumer experiences. It explains the major problems, including misleading conduct, scams, and unfair contract terms, that consumers encounter as they use these technologies. The most common scams are described, including the issues of malware, online security, and privacy and data security. It concludes with an examination of the multiple consumer threats posed by these scams.

LEARNING OBJECTIVES

By the end of the session, the participants will be able to:

- Discuss how, in the context of their own jurisdictions, comprehensive and timely market intelligence might be acquired.
- Describe the consumer experiences and consumer protection issues in terms of access (online vs traditional market) and in terms of jurisdiction (inside vs. outside national borders).
- Determine how and why the most common scams continue to claim victims.
- Assess the potential consumer threats posed by many scams.

SESSION TOPICS

In this session, the following topics will be covered:

- Problems consumers encounter in online transactions.
- Consumer protection issues identified from international experience.
- Most common scams and how and why they continue to claim victims.
- Potential consumer threats posed by many scams.

DEFINITION OF TERMS

malware
refers to malicious software that interferes with the users' intended use of computer technologies; includes viruses, worms, and Trojans.

phishing
refers to commonly used scheme by scammers via e-mail or SMS to trick consumers into giving access to their computers to "fish" for personal data (financial and other personal information) for fraudulent acts.

pyramid scheme
refers to participants attempt to make money soley by recruiting new participants, with the belief in the success of a non-existent enterprise, fostered by the payment of quick and high returns to the first investors from money invested by later.

substantive consumer issues
refer to concerns experienced by consumers and

TRAINING METHODS

Duration in Hour / Minutes:	**4 hours / 240 mins** Session Introduction and Video Showing: 30 mins Case Analysis: 60 mins Lecture: 120 mins Open Forum with Inquiry-Oriented Discussion: 15 mins Session Assessment: 15 mins
Materials / Visuals	• Video clips • Case study materials • PowerPoint Presentation slides • Laptop with LCD projector • Flip chart • Markers, pens, and notepads

Instructions/Procedure

1. Introduce the topics to be covered in Session 2.
2. Show the following video clips.

   oracle mind. (Producer). (2016, May 1). This is how hackers hack you using a simple social engineering (Video). Available from https://www.youtube.com/watch?v=lc7scxvKQOo

   Video Length: 2 minutes and 29 seconds

   Prosper Parabu. (Producer). (2016, April 13). News: LinkedIn & Indeed new job check scam (Video). Available from https://www.youtube.com/watch?v=HvwFguNfDCs

   Video length: 2 minutes and 42 seconds

   WCP.com I 9 On Your Side. (Producer). (2015, August 12). Beware offers of money to wrap your car (Video). Available from https://www.youtube.com/watch?v=_UVNG2NbojU&t=1s
   Video length: 2 minutes and 09 seconds

3. Lecture Session 2 using the lecture inputs (shown in the Box 2) with PowerPoint slides (See PowerPoint Slides Presentation Handout) for Session 2. Link the video message and the PowerPoint slides on the following topics.
4. Divide the participants into small groups of four for the case analysis on Ransomware.

5. Give the participants the following case guide questions.
   a. Who are the stakeholders in this consumer protection issue?
   b. What are the scam operations or deceptive acts were employed? How did the scams work?
   c. How did the Court or Consumer Protection Agency (CPA) decide on the dispute or issue? State the legislation, regulation, violation, or contravention, and the decision including the penalty and the rationale, if applicable.
   d. What potential consumer threats do these scams pose, and why do they continue to claim victims?
   e. How can consumers use online technologies better?
6. Remind each group to assign a facilitator and a note-taker of their answers.
7. Convene the participants in plenary for the presentation of the groups' answers to the case guide questions.
8. Allow the participants to ask questions or seek clarification about the lecture inputs. Then, summarize the session in relation to the learning objectives.

TRAINER'S NOTES

- Refer to PowerPoint Presentation slides in another set of handout.
- Read the Technical Manual on Chapter IV - The principal consumer protection issues with respect to consumers' use of telecommunications technologies, pp. 34-58
- Refer to PowerPoint Slides Presentation Handout.
- Access these online resources:
  - http://www.ijarcce.com
  - https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/
  - http://www.webopedia.com
- Review these references for further reading:
  - ASEAN Secretariat (2015). Product safety and labeling. In AADCP II, *Project on strengthening technical competency for consumer protection in ASEAN* (Final Version 21 December 2015). Retrieved from ASEAN website: http://asean.org/storage/2012/05/Product-Safety-Labeling-Module-Final-21Dec15.pdf
  - _____. (2016). Health care services. In AADCP II, *Project on strengthening technical competency for consumer protection in ASEAN* (Version 21 January 2016). Retrieved from ASEAN website: http://asean.org/storage/2012/05/Health-Care-Module-Final-22Jan16.pdf
- View these video clips

Banking, credit card, and online account scams

Spacebound. (Producer). (2016, February 8). 10 Internet scams you didn't know existed (Video). Available from https://www.youtube.com/watch?v=9kdky6vDD5o

Video length: 4 minutes and 28 seconds

ABC Action News. (Producer). (2018, February 5). Scam wipes out woman's bank accounts (Video). Available from https://www.youtube.com/watch?v=agO7RiX0KL8

Video length: 2 minutes and 12 seconds

TRAINER'S NOTES

Charity scams

CBS News. (Producer). (2010, January 14). Beware of Charity Scams (Video). Available from https://www.youtube.com/watch?v=FyzfdTVvV5k

Video length: 2 minutes and 19 seconds

ABC Actions News. (Producer). (2017, May 1). Scammers busted for fake veterans charity (Video). https://www.youtube.com/watch?v=g-1lkX8HJgI

Video length: 2 minutes and 16 seconds

Employment scams

ENGINEERED TRUTH. (Producer). (2014, June 22). 4 Signs that a Job is a Pyramid Scheme/Scam (Video). https://www.youtube.com/watch?v=aIsFHdK2o4I

Video length: 3 minutes, 33 seconds

Health scams

USFoodandDrugAdmin. (Producer). (2011, March 14). Health Fraud Scams – Be Smart, Be Aware, Be Careful Video (Video). https://www.youtube.com/watch?v=KsPlwKbGxE8

Video length: 3 minutes and 39 seconds

USFoodandDrugAdmin. (Producer). (2011, March 14). Health Fraud Scams - Don't let this Happen to You (Video). https://www.youtube.com/watch?v=eTGM0sRtk4o

Video length: 1 minute and 36 seconds

Online auction scams

rellau1. (Producer). (2009, April 9). News: The Real Deal: Online Auction Scam (Video). Available from https://www.youtube.com/watch?v=PrlWvIM4MrM

Video length: 2 minutes and 18 seconds

TRAINER'S NOTES

Phishing scams

te4chnology. (Producer). (2013, March 13). Phishing example (Video). Available from https://www.youtube.com/watch?v=fyfAKQM3qTY

Video length: 2 minutes and 53 seconds

TODAY, (Producer). (2017, May 4). Massive Google Hack Leaves Millions of Users at Risk In Phishing Scam I TODAY (Video). Available from https://www.youtube.com/watch?v=xs0vd-QKYyM

Video length: 2 minutes and 26 seconds

Pyramid scams

KRQE. (Producer). (2011, March 24). Get rich quick? Seminar scams hit NM (Video). Available from https://www.youtube.com/watch?v=p9jUDqEFi9g

Video length: 2 minutes and 35 seconds

Rushertv. (Producer). (2015, April 22). Beware of Real Estate Get Rich Seminars (Video). Available from https://www.youtube.com/watch?v=D57eztDbrfw

Video length: 3 minutes and 14 seconds

BOX 2. LECTURE INPUTS

1. **Indicators showing the problems consumers are encountering**:
   a. When using telecommunications, consumers may miss out on many of the visual and cotextual indicators that they are used to using when they are used when they contemplate purchases in traditional shops.

   b. Misleading conduct, scams, and unfair contract terms, that consumers encounter as they use online technologies and e-commerce,includes issues of malware, online security, and privacy and data security.

   c. Potential sources of information:
      - Consumer complaints to government authorities
      - Consumer complaints to consumer organizations
      - Local market intelligence on non-complaints from those operating in the market and from other stakeholders
      - Experience in other countries: problems experienced by consumers when using mobile phones, the Internet and e-commerce are likely to be similar between countries within and outside ASEAN.

   d. Access and pricing complaints often received by authorities on consumer protection responsibilities related to:
      - Pre-sale representations : misleading and deceptive conduct
      - Contractual issues :unfair contractual terms
      - Post-sale issues : non-delivery, poor-quality and unsafe goods, warranties, repairs, and refunds

2. **Consumer protection issues identified from international experience**:
   - *Misleading conduct*:

     Consumers are likely to make poor choices about:

     - which trader to buy from
     - which products to buy, how many, and at what price
     - what to do if they have problems with the goods or services during:
       - Pre-sale – misleading information on trader's websites
       - Point of sale – representations about warranties, repairs and refunds, and the effect of other contract terms

- *Unfair contract terms*:
  - The contract terms are very one-sided in their benefits or costs.
  - Legislation prohibiting unfair contract terms may be:
    - General and principle-based
    - Specific contract terms may be prohibited by the court, by an agency, or by law. E.g., the Australian Consumer Law provides a three-step test to determine if a contract term is unfair.
  - Unfair contract terms are more common when:
    - significant power imbalance exists between the consumer and the trader
    - traders use standard form contracts that discourage the consumer from negotiating or clarifying terms
  - Most commonly encountered unfair contract terms:
    - Allowing unilateral changes to key terms of the contract
    - Making the consumer liable for things that would normally be outside his or her control
    - Allowing the trader to charge amounts against a consumer's credit card without consultation or notice
    - Providing for disproportionate penalties
    - Denying all liability for negligence on the part of the trader and his or her staff and agents
    - Invoking the national law on the contract when there is no common jurisdiction
    - Explicitly stating that representations made by the trader outside of the written contract cannot be relied on in case of dispute
    - Invoking the national law on the contract is quite common in international commercial contracts
  - The adverse effect of unfair contract terms may be reduced or nullified with respect to:
    - Criminal law, which will apply regardless of the contract terms
    - National civil law that specifically provides for consumers' rights and traders' obligations outside of, or in addition to, the terms of the contract
    - Terms that grant the seller or his or her nominees irrevocable, perpetual, and fee-free rights to use information provided by the consumer
    - Terms that allow an internet service provider to unilaterally shift the consumer to a new, less favorable plan

- ❖ "Manufactured confusion": complex and lengthy contracts that will make it difficult for the average consumer to:
  - understand exactly what he or she is agreeing to
  - identify unfair or harsh terms
  - accurately compare competitors' products and services
- A complicating factor is that the supplier may not be physically present or may not have assets within an ASEAN jurisdiction

- *Scams*
  - Advance fee fraud schemes:
    - ❖ Money transfer schemes
    - ❖ Case: Hang up on an immigration scam, *23 April 2015*
    - ❖ Fake inheritance scams
    - ❖ Inheritance scam – example letter

      (https://www.scamwatch.gov.au/system/files/Inheritance%20scam%20-%20example%20letter.pdf)

    - ❖ Lottery, competition, and unexpected price scams triggered by visiting fake lottery websites
    - ❖ Example 12 (official notification letter from Google UK)
  - Dating and romance scams:
    - ❖ Scammers create fake profiles on legitimate dating websites to build online relationships and exploit the victims' emotions
    - ❖ They either ask victims for payments or obtain their personal details for later frauds
    - ❖ They ask for money to help cover costs associated with some made-up illness, injury, travel cost, or family crisis.
    - ❖ News: Australians lose $75,000 every day to romance scams, *13 February 2015*
  - Computer and smartphone hacking:
    - ❖ Stealing consumers' identities or authorities to:
      - take money from the victim's bank accounts
      - buy things using the victim's credit cards
      - use the victim's computer to distribute scam messages to other consumers
      - take over the victim's computer and hold him or her for ransom by denying across to the computer until money is paid to the scammer
      - 'Phishing' e-mail
        - Phishing e-mail is commonly used to trick consumers into giving their personal details

- Alternative to phishing e-mail – vishing (social engineering). It refers to psychological manipulation by scammers using phone calls and pretending to be from known companies

- Online auction scams:
  - Online auction scams often take advantage of consumers' trust in well-established, legitimate auction sites
- Online advertising scams:
  - Advertising scams use legitimate-sounding advertisements to lure unsuspecting consumers into paying money or providing personal information.
- Bank, credit card, and online account scams:
  - Phishing scams
  - Scammers obtain information:
    - When consumers hand their cards over to be swiped
    - When they provide the information as part of legitimate internet or phone transactions
- Employment scams:
  - May involve offers to work at home, in another town or city, or overseas
  - May require payment of fees up front for training, travel, software, security clearances, visa fees, taxes, and government charges
- Study scams:
  - The lure is the offer of a place at an educational institution and requires 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.
  - Consumers are often misled when:
    - The site looks like those of legitimate educational institutions
    - The stated entry requirements and fees are lower than normal
    - Scholarships or other inducements are offered.
- Get-rich-quick scams:
  - Investments
  - Gambling
  - Pyramids
  - The schemes are made more enticing due to:

- specialized software applications
- advice of an expert or a "proven" process
- testimonials by successful participants

- Investment Scheme:
  - No actual investments (because the fees paid by the victims are taken by the scammer)
- Gambling Scheme:
  - Non-existent gambling forums, fictitious participation in real competitions, or less commonly, actually betting on real races, casino games, or other competitions
- Pyramid Scheme:
  - The victim supposedly will receive a return for joining in exchange for an upfront fee; the rewards are linked with the victim's arranging for others to join.
  - Inevitably, a pyramid scheme will collapse, with most participants losing all of their "investments."
- Charity scams:
  - The scammer pretends to collect for legitimate charities or even non-existent charities.
  - By timing them with catastrophic events, the scammer hopes to get immediate positive responses and receive donations before the scam victims can do any research
- Health scams:
  - These feature "miracle cures" or wonder products that offer solutions not provided by conventional treatments and products
  - The victim loses money by purchasing ineffective products, and may suffer adverse effects to his or her health

- *Cross-Border Purchases*
  - Post-purchase ramifications may be significant.
  - Different countries may have different regulations on:
    - Product safety
    - Product labeling
    - Product approval
    - Warranties, repairs, and refunds
  - International traders may either not adequately consider compliance with local laws or conclude that:
    - Profits from local sales are insufficient to make a business case for incurring the compliance cost
    - Local authorities are unable to enforce national laws on cross-border transactions
    - Consumers do not care about compliance

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

- *Online Security*
  - Three broad types of security threats
    - Denial of service
    - Unauthorized access to information
    - Theft of information or money
  - Consumers' concerns about online security with respect to:
    - Payments
    - Data protection and privacy
  - Most frequently security breaches result from the unintended downloading and installation of malware.
  - E-Commerce are also vulnerable to unauthorized offline access to consumers' information and theft of fraud by:
    - A person's watching a consumer type in a password or reading a written down password
    - Business employees' misusing access to and knowledge of consumer information such as credit card numbers and passwords
- *Malware*
  - It is malicious software that damages or disrupts the functionality of computer technologies. It includes:
    - Viruses
    - Worms
    - Trojans
  - How to reduce damage (financial and convenience) and the risk of having compromised (infected) systems:
    - Update operating systems (OS) and applications (apps)
    - Install applications and updates only from trusted sites
    - Download only from original vendors sites
    - Use the security features imbedded in the installed OS
    - Install and routinely run anti-malware applications
    - Maintain a regular back-up routine of OS, apps, and data
    - Reinstall the OS, apps, and data files when they have been compromised
    - Be aware of the warning signs indicating that an e-mail or website presents a high risk of malware, and take appropriate actions

- Data protection and privacy
  Consumers' principal concerns about their personal information:
  - 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.
  - Collected by traders and intermediaries for various purposes including:
    - Identification of the consumer for security of payment or for delivery
    - Collection of market intelligence to improve their own performance
    - Building a marketable asset for sale or hire
- Intermediaries already have significant information about cardholders including names, addresses, account numbers, and passwords
- Advantages of personal data collection
  - Better targeted offers of additional goods and services
  - Better targeting of offers to match consumers' needs, wants, and preferences
  - Easier fraud detection
  - Reduction of traders' operating risks
- Data protection and privacy management
  - Consumer education
  - Trader education
- Data protection and privacy legislation
  - UK's Data Protection Act
- Example of pertinent provision of the Data Protection Act
  - After a long period in which no ASEAN member country had privacy legislation in place, there is now a great deal of progress and activity in ASEAN. Malaysia started the ball rolling by passing privacy legislation in 2010, followed by the Philippines and Singapore in 2012. Indonesia and Vietnam both have partial privacy legislation in place (contained in their omnibus e-commerce laws), but it does not provide the same level of detail and coverage as full privacy legislation. Thailand has been discussing the draft of the general data protection legislation which will provide the data .

        - The Data Privacy Act (DPA), or Republic Act No. 10173 was passed by the Philippines Congress in 2012 and finally implemented in 2016. RA 10173 assures the "free flow of information to promote innovation and growth"(Republic Act. No. 10173, Ch. 1, Sec. 2) while protecting the users' fundamental rights to privacy.
- *Secure payments*

  Online payment risks faced by consumers:
  - Their information will be accessible to multiple parties, many of whom are unknown to them
  - Their information, once accessed, can be easily copied and distributed.

  Security problems may be encountered at any step of the following e-commerce process:
  - Verification of the merchant
  - Review of order information
  - Verification of the customer
  - Review of payment information
  - Confirmation of order
  - Authorization or denial of payment
  - Payment systems
    - Credit cards
    - Debit cards
    - Online-buying apps (e.g., Payflow Pro)
    - E-bill payment
    - Electronic cash
  - Security tools
    - Firewalls
    - Public key infrastructure
    - Biometrics
    - Passwords
    - Locks and bars
- *Information Security Management Systems*
  - To ensure online security, data privacy, and protection and to secure payments, it is recommended that ASEAN traders and intermediaries adopt an internationally recognized information security management system (ISMS) such as ISO 27002.
  - In the Philippines, the National Privacy Commission recommends the use of the ISO/IEC 27002 control set as the minimum standard to assess gaps in the exercise of protecting privacy of personal information.

- Adoption of ISO 27002 by traders and intermediaries will secure their internal operations and e-commerce transactions.
- ISO 27002 provides hundreds of potential controls and control mechanisms that are designed to be implemented with guidance provided within ISO 27001. The suggested controls listed in the standard are intended to address specific issues identified during a formal risk assessment. The standard is also intended to provide a guide for the development of security standards and effective security management practices.

ASSESSMENT AND EVALUATION OF **PARTICIPANT'S LEARNING**

Method of Assessment: Ask the participants to share in plenary their answer to the following questions:

1. How do most common scams work and why they continue to claim victims?
2. What consumer threats do scams pose and how can they be addressed?

SESSION 3:	PRE-MARKET INTERVENTION AND CONSUMER PROTECTION REGULATIONS FOR PHONES, INTERNET SERVICES, AND E-COMMERCE

SESSION DESCRIPTION

This session describes pre-market intervention and consumer protection regulations concerning the use of online technologies. It also includes broad market conditions in which consumers use phones, the internet, and e-commerce; some of the important behavioral characteristics that drive consumer use of these technologies; the rationale, limit, and scope of public intervention; and the significance of technology-neutral and technology-specific regulations.

LEARNING OBJECTIVES

By the end of the session, the participants will be able to:

- Discuss the market conditions under which consumers use phones, the Internet, and E-commerce;
- Explain the consumer behavioral features and characteristics that drive consumer use of these technologies;
- Assess the rationale, limits, and scope of public intervention; and
- Explain the significance of technology-neutral vs. technology-specific regulations.

SESSION TOPICS

In this session, the following topics will be covered:

- the market conditions under which consumers use phones, the internet, and e-commerce;
- consumer behavioral features and characteristics that drive consumer use of these technologies;
- the rationale, limits, and scope of public interventions; and
- the significance of technology-neutral and technology-specific regulations.

DEFINITION OF TERMS

economic theory
refers to general principles that describe how the economy works. This includes the idea that increasing consumption of goods is economically beneficial, the role of market forces (supply and demand) competition, prices and aggregate economic forces (e.g., public welfare/consumption, and government intervention through legislation and executive acts and policies).

pre-market interventions
refer to schemes to prevent complaints of consumers through government policies and regulations to enhance consumer welfare in this sector.

***public** intervention*
refers to acts by the government and its agencies known as consumer protection authorities (CPA) to intervene in behalf of the general public for protection, through laws, policies, investigations, and adjudications.

TRAINING METHODS

Duration in Hours / Minutes:	**4 hours / 240 mins** Session Introduction and Video Showing: 30 mins Lecture: 90 mins Structured Learning Activity: 50 mins Case Analysis: 40 mins Open Forum with Inquiry-Oriented Discussion: 15 mins Session Assessment: 15 mins
Materials / Visuals	• Video clips • Case study materials • PowerPoint Presentation slides • Laptop with LCD projector • Flip charts • Markers, pens, and notepads

Instructions/Procedure

1. Introduce the topics to be covered for Session 3.
2. Show the video clips to illustrate the market conditions under which consumers use phones, the Internet, and E-commerce. Link this with the introduction.

   Amy Hebert. (Producer). (2016, June 15). How to avoid imposters: 4 videos you need to see (Video). Available from https://staysafeonline.org/blog/how-to-avoid-imposters/

   Video length: 49 seconds

3. Lecture Session 3 using the lecture inputs (shown in the Box 3) with PowerPoint slides (See PowerPoint Slides Presentation Handout) for Session 3. Link the video message and the PowerPoint slides on the following topics.
4. Give instructions for Structured Learning Activity in the form of drawing exercise entiled "**Doodles".**
   - Tell the participants to form groups of four to five members.
   - Ask each member to draw a picture with the following instructions:
     - Draw a picture that demonstrates consumer behavioral features and characteristics that drive consumer use of online technologies (e.g., phone, the internet, and e-commerce).

- Show your drawing to your group members and check whether they can figure out what your picture represents without your having to tell them. Let them know whether they got it right.

- Tips and variations:
  - When you tell the participants to draw a doodle, model what you want them to do by drawing a sample doodle on a flip chart. Some participants will draw what you draw; others will make up their own doodles. You can also make a point of asking them to copy your doodle especially if you have specific images you want them to associate with the concepts.
  - Have participants create doodles only for the facts that you want them to remember.
  - Create a note-taking page for participants before the training begins. Include blank spaces for doodling.

5. Convene the participants in plenary to process the Structured Learning Activity.
   a. Asking the group representing the professionals their reactions and observations.
   b. Asking the group representing the consumers about their reactions and observations of the exercise.
   c. Asking the neutral persons as representing the consumer protection agency about their reactions to the exercise.
6. Conduct a Case Analysis based on the following cases (See Appendix A.3).
   Case: The State of E-Commerce in Thailand
   For the above case, ask the participants to:
   - Form groups of four to five members
   - Assign a note-taker
   - Reflect on the following guide questions:
     a. What consumer protection issues are involved in this case?
     b. What violations have been committed with regard to the consumer protection law of the AMS jurisdiction in the case?
     c. What government interventions are applicable and available?
     d. Is this problem relevant in your jurisdiction/country (consumer protection agency or authority)?
7. Ask the participants to present their answers to the case guide questions.
8. Allow the participants to ask questions or seek clarification about the Lecture Inputs, as well as ask them questions in order to draw out ideas from them. Then, summarize the session in relation to the Learning Objectives.

TRAINER'S NOTES

- Refer to PowerPoint Presentation slides in another set of handout.
- Read the Technical Manual on Chapter II - Online Consumer protection: the market, behavioral, and public intervention contexts, pp. 16-22
- Refer to PowerPoint Slides Presentation Handout
- Access these online resources:
  - www.investopedia.com/terms/demand-elasticity.asp,
  - www.icpen.org
- Review these references for further reading:
  - ASEAN Secretariat (2015). Product safety and labeling. In AAADCP II, *Project on strengthening technical competency for consumer protection in ASEAN* (Final Version 21 December 2015). Retrieved from ASEAN website: http://asean.org/storage/2012/05/Product-Safety-Labeling-Module-Final-21Dec15.pdf
  - _____. (2016). Health care services. In AADCP II, *Project on strengthening technical competency for consumer protection in ASEAN* (Version 21 January 2016). Retrieved from ASEAN website: http://asean.org/storage/2012/05/Health-Care-Module-Final-22Jan16.pdf
  - Beal, V. (2015, December 14). The difference between a computer virus, worm and Trojan horse [White paper]. Retrieved from Webopedia Did you know?:

BOX 3. LECTURE INPUTS

1. **Online consumer protection: the market conditions under which consumers use phones, the internet and e-commerce- the market, behavioral, and public intervention contexts.**
   - **Market conditions**
     - Phones, internet services, and e-commerce are usually defined by their respective technologies and may be grouped together under the umbrella of telecommunications.
     - Phones, internet services, and e-commerce are all driven by technological innovation.
     - All three forms of telecommunication offer significant economies of scale and scope and reduce the distance between consumers and traders.
     - Continuing technical innovations are providing increasing numbers of consumers with access, cheaper prices, and increased utility.
     - Consumer access to and costs of using these technologies varies significantly among ASEAN member states.
     - Government regulates which entities are able to provide telecommunications services and under what conditions. Singapore and Brunei government- (or state-) owned enterprises (SOEs) are also major providers of telecommunications and other internet services.
     - Government policy through regulation may impact directly consumers in terms of services to be provided, content to be accessed, service terms including price, performance, and available processes for resolution of consumer problems.
     - Government policy and regulation affect the existence and intensity of competition among service providers.
     - Consumer transactions using these technologies cross borders.
     - Market-influencing strategies may contribute significantly to improving consumer experiences.

2. **Consumer behavioral features**
   - Consumers use a variety of strategies to prioritize their needs and wants.
   - Individual consumers are more likely to make economically suboptimal decisions when non-economic objectives are more important.

- Consumers may miss out on many of the visual and contextual indicators (physical appraisal of the goods on offer, appearance and demeanor of traders, and the location and appearance of the traders' shops). If consumers are unaware of some of the risks or underestimate the risks associated with using telecommunication services, they will not prioritize risk-avoidance strategies.
- Consumers will keep on using brick and mortar or the traditional way of shopping if they do not trust technologies to buy. Teenagers and educated adults are generally more knowledgeable about using these products and services.
- Implications:
  - Various groups of consumers are likely to experience different problems and at differing degrees of severity.
  - Resolution of consumer problems may vary across groups.
  - Empowering consumers through education will need to continue and evolve.
- Consumer protection agencies need to respond to problems with a range of enforcement responses.
  - Consumer and trader education
  - Trader compliance programs
  - Industry codes of conduct
  - Dispute resolution mechanisms
  - Well-managed investigations
  - Sanctions and remedies
  - Interagency cooperation

3. Pre-Market Interventions

- General consumer protection laws and regulations.
- Specific government policies and regulations:
  - Government policy directing at improving competitiveness in the sector.
  - Policy to prevent misleading advertisements (internet and e-Commerce).
  - Prescribing a set or maximum price for a particular product or service (telecommunciations).
  - Industry Code of Conduct.
- E-commerce legislation (IT and e-commerce Law).
- Legislated monopolies (telecommunications).
- Interventions that facilitate more informed choice by consumer or business.
- Other market influencing strategies to improve consumer experience.
- E-commerce legislation harmonization in ASEAN 2013.

4. The rationale, limit, and scope of public intervention

- In economic theory, market forces will maximize aggregate consumer welfare, but only when there are few significant impediments to competition. These forces include:
  - Consumers' looking out for themselves
  - Businesses' maximizing their profits
  - Traders' experiencing social pressure to treat consumers fairly
  - Active media and consumer organizations' exposing consumer problems
  - Private enforcement of rights under consumer protection laws
  - More effective investigations are facilitated by these same technologies.
- Public intervention will be necessary because:
  - Although unsafe goods and fraudulent behavior will eventually become unprofitable in an efficient, competitive market, some consumers will suffer harm during the adjustment period.
  - Market equilibrium results in goods or services causing long-term harm to consumers.
    - The flaws of goods or services are not apparent to consumers at the time of purchase.
    - Consumers often put a higher value on short-term benefits.
    - The buyers of the goods or services are not the ultimate consumers.
    - People with very low incomes have no practical choice but to buy the cheapest goods.
    - Stakeholders have goals in addition to simply maximizing aggregate welfare.
  - Some markets have significant impediments to competition with the result that market forces are weakened or distorted.
  - Reasons for the ineffectiveness of the forces of competition:
    - Ineffective or non-existent consumer associations
    - Poor access to independent sources of information
    - Ad hoc or non-sustained imports
    - Misuse of significant market power by individual businesses
    - Anti-competitive arrangements between businesses in a market
    - Intended and unintended consequences of government intervention
    - Structural characteristics of particular markets
    - Dynamic market forces

- Effective and/or efficient interventions today may not be effective and/or efficient tomorrow. Interventions that facilitate more informed choices by consumers or businesses are more likely to be effective in the long run than prescriptive interventions that restrict 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 affect consumers' purchasing decisions.
- All market interventions have costs. For example, costs of compliance will be passed on to consumers in the form of higher prices when demand is only weakly affected by price, which may be the case of many basic services (e.g., mobile phone services).
- Anticipating the ultimate effect of an intervention requires a thorough understanding of the market dynamics.

5. **The significance of technology-neutral and technology-specific regulations**
   - Most consumer protection laws are technology-neutral; i.e., they apply generally to matters affecting consumers regardless of how the transactions take place (i.e., online or brick-and-mortar).
   - Advantages:
     - they do not have to be amended to maintain consumer protection
     - they do not have anti-competitive effects
   - Some consumer protection laws may be technology-specific.
   - Not all consumer protection issues are neatly labeled. Enforcement is often not even the responsibility of a designated consumer protection authority.
   - Other elements of providing consumer protection must also have broadly uniform applications.

ASSESSMENT AND EVALUATION OF PARTICIPANT'S LEARNING

Method of Assessment: Reflection / Meta Learning. Ask the participants the following questions:

- What are the three most important learnings you have gained as a result of this Session.
- How can you use these learnings in your work in consumer protection?

SESSION 4: POST-MARKET INTERVENTIONS

SESSION DESCRIPTION

This session describes the range of uses to which consumers typically put their phones and other devices when accessing the internet and engaging in e-commerce; the major issues raised by consumers' use of these technologies for consumers themselves and regulators; the complexity of regulation wherein every jurisdiction multiple agencies are involved; and the imperative of inter-agency cooperation (in terms of providing consumer protection: post-sales misrepresentations, unfair pricing/competition; market intelligence, field investigations, information sharing, and enforcement of contracts and warranties).

LEARNING OBJECTIVES

By the end of the session, the participants will be able to:

- Identify the forms of post-market (post-sales) interventions:
- Explain the implications for consumer and government/public interventions
- Examine the regulatory responsibility (ASEAN and worldwide jurisdictions)
- Evaluate the benefits of inter-agency cooperation (ASEAN and international) enforcement, collaboration, and cross-border sharing of market intelligence.

SESSION TOPICS

In this session, the following topics will be covered:

- Post-market (post sales) issues on:
  - Phones
  - The internet
  - E-commerce
- Some implications for consumer and government/public interventions
- Regulatory responsibility (ASEAN and worldwide jurisdictions)
- Benefits of inter-agency cooperation (ASEAN and international) enforcement, collaboration, and cross-border sharing of market intelligence

DEFINITION OF TERMS

B2C
refers to business- to consumer e-commerce transactions

evidence
refers to testimonies, documentary records, physical products, and expert evidence supporting the complaints of consumers against the sellers used during civil and criminal investigations

hoax
refers to calls nuisance calls from individuals and charities, organized crimes and unsolicited sales presentations

post-market intervention
refers to schemes to address consumer complaints / availing of the products and/or services to protect the interest of consumers.

post-sales
refers the information exchange between the consumer and trader which may be an important source of consumer problems

remedy
refers to action by the consumer brought directly to the seller or through government intervention

TRAINING METHODS

Duration in Hours / Minutes:	4 hours / 240 mins Session Introduction and Video Showing: 30 mins Lecture: 90 mins Case Analysis: 90 mins Open Forum with Inquiry-Oriented Discussion: 15 mins Session Assessment: 15 mins
Materials / Visuals	• Video clips • Case study materials • PowerPoint Presentation Slides • Laptop with LCD projector • Flip charts • Markers, pens, and notepads

Instructions/Procedure

1. Introduce the topics to be covered for Session 4.
2. Show the following video clips.

   Facts About Herbalife. (Producer). (12 January 2015). How to Spot a Pyramid Scheme (video). Available at https://www.youtube.com/watch?v=VVUUbEw_Pm8

   Video length: 6 minutes and 21 seconds

   NowThis World. (Producer). (1 November 2016). Ponzi vs. Pyramid Scheme: What's The Difference? (video). Available at https://www.youtube.com/watch?v=y9rJZX72oIw

   Video length: 3 minutes and 19 seconds

3. Lecture Session 4 using the lecture inputs (shown in Box 4) with PowerPoint slides (See PowerPoint Slides Presentation Handout) for Session 4. Link the video message and the PowerPoint slides on the following topics.

4. Give the participants the case together with the discussion guide questions:
   a. How do consumers use these online technologies?
   b. How do the online technologies empower consumers yet make them more vulnerable to scams and deception?
   c. What post-market interventions (e.g., field investigations, enforcement of contracts and warranties, amended or new legislation, policies, and programs) were made by the government or consumer protection authorities?
   d. What are the opportunities and challenges of inter-agency cooperation?
5. Ask the participants to read the following case (See Appendix A.4)
   Case : Illegal Investment Schemes in Malaysia
6. Ask the participants to form groups of four to five members for reflection and sharing based on the guide questions in number 4 above.
7. Remind each group to assign a facilitator and a note-taker of their answers.
8. Convene the participants in plenary for the presentation of the groups' answers to the case guide questions.
9. Allow the participants to ask questions or seek clarification about the lecture inputs, as well as ask them questions in order to draw out ideas from them. Then, summarize the session in relation to the learning objectives.

TRAINER'S NOTES

- Refer to PowerPoint Presentation slides in another set of handout.
- Read the Technical Manual on Chapter III - Some broad observations about the technologies, regulatory responsibility, and interagency cooperation, pp. 23-33
- Refer to PowerPoint Slides Presentation Handout
- Access these online resources: www.icpen.org
- Review these references for further reading:

  Competition: consumer protection (n.d.) Retrieved from Gov.UK website: https://www.gov.uk/topic/competition/consumer-protection

  Competition & Markets Authority page (n.d.) Retrieved from Gov.UK website: https://www.gov.uk/government/organisations/competition-and-markets-authority

- International Consumer Protection and Enforcement Network website (n.d.). Retrieved from ICPEN website: https://www.icpen.org/
- UNCTAD (2015). *Information economy report 2015: Unlocking the potential of e-commerce for developing countries*. Retrieved from UNCTAD website: http://unctad.org/en/PublicationsLibrary/ier2015_en.pdf

BOX 4. LECTURE INPUTS

1. **Post-Market (Post-Sales) Intervention**
   - Complexity of regulation wherein every jurisdiction multiple agency is involved; and the imperative of inter-agency cooperation (in terms of providing consumer protection: post-sales misrepresentations, unfair pricing/competition; market intelligence, field investigations, information sharing, and enforcement of contracts and warrants).

2. **Some observations about the technologies, performance, and compliance by service providers and implications for consumer and government regulations in a post-market environment**
   - *Phones*
     - Smartphones have brought increased benefits and costs to consumers.
     - Mobile phone consumer concerns:
       - Technical Issues - access, performance, inoperability, and billing
       - Some regulators may not have access to comprehensive and timely data on consumer concerns.
       - More effective consumer complaints handling will generate better market intelligence and more comprehensive corporate compliance programs by the mobile phone service providers.
       - Pricing issues
         - The price is too high
         - The price is higher than the consumer expected
         - Price surprises can occur because:
           - consumers did not shop around
           - contracts are difficult to understand so that consumers do not understand what the final price will be
           - consumers have difficulty in accurately comparing contracts
           - there are insufficient or inadequate warnings that a consumer is approaching or has exceeded agree parameters
           - consumers are unaware of the cost of certain types of calls.
       - Usage issues

- Hoax calls: nuisance calls from individuals, organized scams, unsolicited sales presentations, and unsolicited calls from charities

❖ Common problems include: spam, malware, scams unrelated to e-commerce, pre-sale misrepresentations by parties other than the intending seller, and post-sale misrepresentations.

❖ At the time of writing, it is not known if any legislation has been enacted in ASEAN member states (AMS) to address the issues.

- *The Internet*
  - Some uses: keeping in touch with friends and family, finding information on almost any topic, searching for jobs, working from home, shopping and banking online, planning holidays, and finding government services.
  - Common problems:
    - ❖ Spam – at the time of writing, it is not known which ASEAN countries laws have prohibiting or regulating spam
    - ❖ Malware – harm caused: stealing of financial and other personal information, preventing consumers from using their computers, damaging files, hijacking computers. At the time of writing, it is not known which ASEAN countries laws have prohibiting the creation and distribution of malware.
    - ❖ Consumers' lack of awareness about the harm caused
    - ❖ Inadequate security of ISPs and creators of operating systems for their products and services
    - ❖ Lack of staff training on consumer protection issues awareness, complaint handling, investigation skills, and consumer education programs.
- *E-commerce*
  - Many consumers will do at least some research before purchasing.
  - Pre-purchase research may also entail visiting other websites to compare prices and features of products.
  - When consumers decide to buy products from online traders, they typically complete order forms that require them to input personal and financial information.
  - Consumers will also be provided with information (representations) about the products and the traders.
  - Post-sale communications between consumers and traders may be very important and be the source of consumer problems.

- Existing consumer protection laws in ASEAN countries address many common problems.
- Some problems:
  - How well a consumer can interact (negotiate) or not with online traders
  - 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 the consumers' jurisdiction
  - Available remedies so that consumer protection authorities can effectively act on online transactions
  - Some implications for consumers and government
    - Rapidly evolving technologies
    - Uncertainties about future use
    - Avoiding new scams as well as old scams that have been given new potency.
- Issues facing governments:
  - Identifying current and emerging issues
  - Designing and implementing interventions
  - Minimizing direct and indirect costs of public intervention

3. Regulatory responsibility (ASEAN and cross-border jurisdictions)

- This may be distributed over several government agencies in each of the ASEAN countries
- Consumers may not report a problem, may be unsure which authority is responsible, or may not be convinced that the authority can remedy the problem
- Effective consumer protection will often require a collaborative approach by multiple authorities because intelligence about the problems may be poor; an authority may have insufficient power to obtain evidence; sanctions and remedies may require the exercise of powers by more than one authority; or traders may be located outside the jurisdiction of an authority. Cooperation among consumer protection authorities across borders may be required for the same reasons.
- Most ASEAN Member States (AMS) have established international links with respect to consumer protection.
- The Philippines and Vietnam are members of ICPEN. A cross-border complaint portal for consumer protection agencies is econsumer.gov.

4. Benefits of interagency cooperation

- Universal technologies
  - Source providers operate in many countries
  - Problems encountered by consumers are similar across countries.
- Areas of interagency cooperation:
  - Sharing of market intelligence on complaints about and responses of traders
  - Sharing of intelligence, educational, and other resources
  - Sharing of experiences, which accelerates the learning process, staff exchange, and joint training
  - Combining data for a comprehensive picture of consumer experiences

ASSESSMENT AND EVALUATION OF PARTICIPANT'S LEARNING

Method of Assessment: Reflection / Meta Learning. Ask the participants the following questions:

- What are the three most important learnings you have gained as a result of this Session?
- How can you use these learnings in your work in consumer protection?

SESSION 5: REDRESS MECHANISMS

SESSION DESCRIPTION

Redress mechanism for phones, Internet services, and e-Commerce are the different approaches to the citizens' rights to petition the government to address a particular grievance for services of telecommunication that result in fraud and loss; this is to right to ask for governmental body to solve a problem without fear or reprisal from those who commit misleading conduct, scams, and unfair contract terms, that consumers encounter as they use online technologies and e-commerce. This includes issues of malware, online security, and privacy and data security. This session on redress mechanisms introduces redress claims available to the consumers drawing upon previous studies and cases developed by the ASEAN. It aims to help the trainees come up with guidelines for redress mechanisms in their respective countries. The session will cover redress models with their corresponding approaches / techniques and management and communication tools of the Consumer Protection Agency.

LEARNING OBJECTIVES

By the end of the session, the participants will be able to:

- Describe the redress models with their corresponding approaches / techniques; and
- Explain the management and communication tools of the Consumer Protection Agency.

SESSION TOPICS

In this session, the following topics will be covered:

- Redress Models with their corresponding approaches / techniques
- Management and communication tools of the Consumer Protection Agency

DEFINITION OF TERMS

capacity-building
refers to consumer empowerment through consumer education, business, compliance skills development, online issue awareness, and complaint and investigative handling skills development

conflict resolution procedures
refer to the process of resolving problems resulting from misunderstanding and inadvertence

redress mechanism
refers to approaches to the citizens' rights to petition the government to address a particular grievance; this is the right to ask for governmental body to solve a problem without fear or reprisal.

stakeholder
refers to an external organization and anyone who have particular interest or concern in the activities of a CPA (e.g., consumer, consumer organization, business, and government authority)

TRAINING METHODS

Duration in Hours / Minutes:	**4 hours / 240 mins** Session Introduction and Video Showing: 30 mins Lecture: 90 mins Role Play with given case scenario: 90 mins Inquiry-Oriented Discussion: 15 mins Session Assessment: 15 mins
Materials/ Visuals	• Video clips • PowerPoint Presentation slides • Case study materials • Laptop with LCD projector • Flip charts • Markers, pens, and notepads

Instructions/Procedures

1. Introduce the topics to be covered for Session 5.
2. Show video on consumer business education and consumer protection.

   FTCvideos. (Producer). (2 March 2011). Operation Empty Promises: Job and Business Opportunity Scams I Federal Trade Commission (video). Available from https://www.youtube.com/watch?v=rI5Ur9e-FxA

   Video length: 2 minutes and 42 seconds

3. Lecture Session 5 using the lecture inputs (shown in the box below) with PowerPoint slides (See PowerPoint Slides Presentation Handout) for Session 5. Link the video message and the PowerPoint slides on the following topics.
4. Ask the participants to form groups of 4 to 5 members and ask them to read the case “Sextortion in the Philippines”. Reflect on the case based on the following guide questions.
   - Who are the major players or stakeholders in the case?
   - What are the consumer protection issues (e.g., conflicts, complaints, and contraventions)?
   - How did the Court/Consumer Protection Authorities (CPAs) and/or other government agencies mediate and resolve the case?
   - What competencies (mediation, conflict resolution, arbitration, etc.) were observed or learned on the part of the CPA?
5. Orient the participants on the role-play activity based on the case on “Sextortion in

the Philippines"

GUIDELINES ON THE ROLE-PLAYING ACTIVITY

- Identify the relevant parties involved (major players – actors):
  - Consumer / Victim
  - Scammer / Mastermind / Blackmailer
  - Consumer Protection Authority (CPA)
  - Police
  - Judge
- Assign each participant to play one of the following roles:
  - Consumer: provide evidence of scam; file a complaint
  - Scammer: demonstrate how the scam was committed
  - CPA: collect evidence from sources and analyze the information; collect key documents including contracts
  - Police: Serve the warrant of arrest
  - Judge: Determine if there is probable cause; issue a warrant of arrest; determine whether the law has been breached; state the consequence/penalty
- Explain the scenario to the participants (refer to case in Appendix A.5).
- Divide the participants into four groups. Tell them to identify the problem in the case.
- Process the role play.
  - How was the complaint lodged to the CPA?
  - Was the CPA able to empathize and understand the complainant?
  - How did the CPA resolve the complaint?
  - If you were the CPA how would you have handled the case

6. Convene the participants in plenary and ask the group to prese its answers to the guide questions and its reactions to the role play.
7. Allow the participants to ask questions or seek clarification regarding the lecture inputs, as well as ask them questions in order to draw out ideas from them. Then, summarize the session in relation to the learning objectives.

TRAINER'S NOTES

- Refer to PowerPoint Presentation slides in another set of handout.
- Read the Technical Manual on Chapter IV Subsection 4.3.- Some strategies for addressing the most common consumer problems, pp. 59-99
- Refer to PowerPoint Slides Presentation Handout
- Access these online resources: www.healthit.gov,www.oxforddictionaries.com
- Review these references for further reading:
  - ASEAN Secretariat (2015). Product safety and labeling. In AAADCP II, *Project on strengthening technical competency for consumer protection in ASEAN* (Final Version 21 December 2015). Retrieved from ASEAN website: http://asean.org/storage/2012/05/Product-Safety-Labeling-Module-Final-21Dec15.pdf
  - ASEAN. (2016). Health care services. In AAADCP II, *Project on strengthening technical competency for consumer protection in ASEAN* (Version 21 January 2016). Retrieved from ASEAN website: http://asean.org/storage/2012/05/Health-Care-Module-Final-22Jan16.pdf
  - Beal, V. (2015, December 14). The difference between a computer virus, worm and Trojan horse [White paper]. Retrieved from Webopedia Did you know?: Competition: consumer protection (n.d.) Retrieved from Gov.UK website: https://www.gov.uk/topic/competition/consumer-protection

Read the supplementary case on "Australian lose $75,000 every day to Romance Scams". Refer to Appendix A.5.

BOX 5. LECTURE INPUTS

1. **Complaint and Redress Pyramid: Internal Complaints-Handling Systems and External Consumer Redress Schemes**

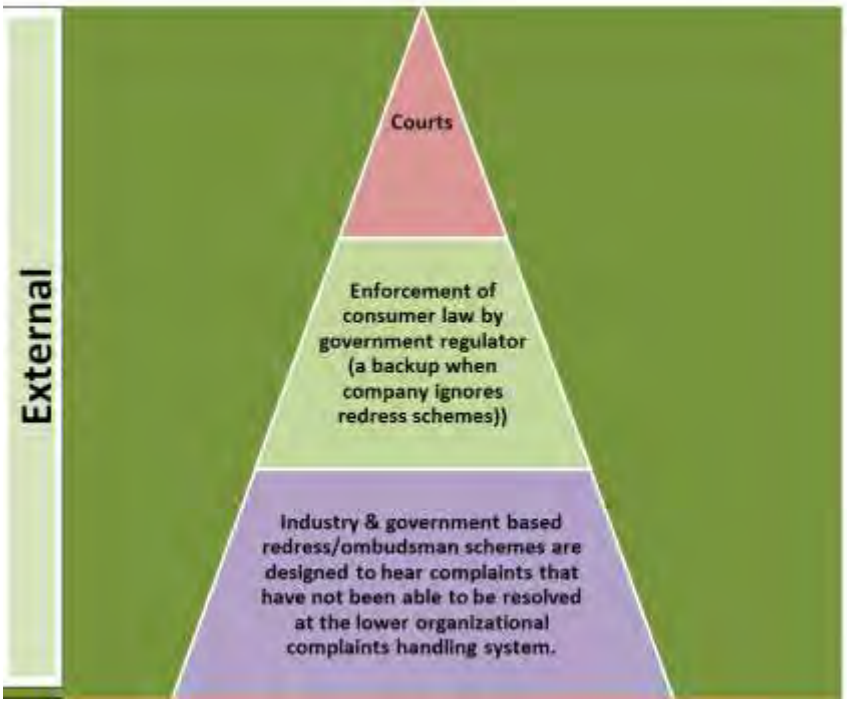


Figure 1. Complaint and redress pyramid: Internal complaint handling systems and external consumer redress schemes

2. **Redress Models with their corresponding approaches / techniques**
   - Redress mechanism for the phones, Internet services, and e-Commerce are the different approaches to the citizens' rights to petition the government to address a particular grievance for services of online technologies and e-Commerce providers that result in fraud and loss.
   - **Model 1: Internal complaint handling system** – this model has the following key features:
     - Implemented by businesses and government agencies providing services to resolve consumer complaints
     - Embody the principles and features of complaint handling systems
     - May be voluntary or required by law or regulations
     - Appropriate for organizations of all sizes

- Guidance in implementation can be found in international Standard ISO10002

Figure 2. Internal Complaint Handling System

- As the figure above indicates, this model has five cyclical steps:
  - Step 1: Survey IT professionals and e-traders (i.e. engaged in e-Commerce, online technologies e.g. the internet, phones).and see if there is a need for an internal conflict-handling system
  - Step 2: Develop a policy for conflict-handling and get regulatory approval to discuss with IT professionals and e-traders
  - Step 3: Design an internal complaint system with IT professionals and e-traders
  - Step 4: With professional and consumer groups and agencies, implement the complaint-handling system
  - Step 5: Encourage professional and consumer groups to review the system at least every two years with continuous improvements
- **Model 2: Self-Regulatory External Redress Schemes** – this model has the following features:
  - Set up with little formality
  - Usually used in the early stages of consumer policy and law implementation

- Tend to have relatively low standards of performance
- Unless they are based on contractual arrangements between industry members, such schemes are usually not enforceable
- There is no stakeholder engagement particularly with consumers and governments
- Generally held in low regard by consumers and some governments
- Considered to be just an interim step in development of consumer redress scheme

- **Model 3: Statutory Complaint Bodies** – this model has the following key features:
  - Broad jurisdiction, usually covering most economic activities
  - Some are established to deal with a specific industry or type of practice
  - They are generally part of a larger government agency responsible for policy and law enforcement
  - May be linked to industry regulators and small claims courts
- **Model 4: Public Sector Redress Body** (also known as Ombudsman) – this model has the following key features:
  - involves contractors working in behalf of government though having no power of enforcement
  - may include anti-corruption and human rights functions
  - can deal with systemic issues of poor administration
- **Model 5: Small Claims Courts or Tribunals** (also known as Consumer Claims Tribunals or Civil or Administration Tribunals) – this model has the following key features:
  - Designed for swift and inexpensive redress for consumers
  - Most do not permit legal representation
  - Suggests or require mediation prior to adjudication
  - Employ ADR techniques
  - Judgements are usually enforceable in the courts
- **Model 6: Private Organization to Improve Consumer Complaint System** - this model has the following key features:
  - Made up of representatives from businesses and government agencies who deal with consumer complaints
  - Provide best practice training on consumer support functions (e.g. complaints handling)
  - Requires senior management support to be successful
  - Highly effective in those countries in which they operate strong domestic and international networks
  - Consistent with building a responsible and responsive business sector

- **Model 7: Cross Border Redress: ASEAN Regional facility for Cross Border Complaints** – this model has the following key features:
  - Employs strategic approach towards consumer protection and has been adopted by the ACCP
  - Contains policy measures and detailed priority actions with specific timeframes for implementation, including the development of:
    - Notification and information exchange mechanism by 2010;
    - Cross border consumer redress mechanism by 2015; and
    - Strategic roadmap for capacity building by 2010.
  - Cross-border access to justice
    - To date, no single model suits all AMS. Guidelines therefore, should be taken to assess the current consumer protection framework of an ASEAN member state.
    - Initial steps to assess such framework include information-gathering regarding:
      - Basic professional admission/striking-off provisions for gross negligence or dishonesty
      - The need to respond to consumer complaints against phones, Internet services, and e-Commerce providers and merchants
      - Consumer pressure with the establishment of complaint and redress schemes
      - Professional associations' involvement in complaint-handling systems and redress schemes
      - Government intervention or threats to establish consumer redress schemes
      - Creation of industry ombudsman or other industry-based schemes
      - Best-practice complaint systems and redress schemes
- The above seven models incorporate the approaches of
  - Alternative Dispute Resolution (ADR)
  - Ombudsman
  - Arbitration
  - Mediation
  - Group actions / Class suit
  - Cross-border access to justice

2. Management and Communication Tools of the Consumer Protection Agency

- Consumer Awareness and Education:
  - A key role and responsibility of the CPA and other sector regulators is to help consumers become aware of their rights, including with respect to product safety.
  - Consumers should be informed of:
    - their right to safety;
    - available remedies if they encounter unsafe products;
    - how to access remedies; and
    - where to go for further advice.
  - Information dissemination targeting specific groups, including among others:
    - The general public
    - women and homemakers
    - students
    - rural communities.
  - Tools for information dissemination
    - websites and social media
    - media campaigns and public events
    - printed materials (e.g., leaflets and booklets)
    - partnership programs with civil society organizations such as consumer associations and schools
    - Toll-free consumer hotlines
    - Annual reports
  - An IT-based consumer complaints registration system should have:
    - basic information on common consumer complaint areas for easy retrieval;
      - categorized consumer complaints according to area with reference number for easy identification and retrieval;
      - standard letters with blanks to fill in information for different types of complaints; and
      - inter-agency contact information to enable easy referral.

- Inter-agency collaboration among related agencies:
  - Coordination among central and local CPA authorities is a major challenge in countries with:
    - new consumer protection law regimes (e.g., Myanmar since 2014);
    - limited financial resources (e.g., Laos); and
    - permitted high levels of decentralization (e.g., Indonesia)
  - Collaboration with related agencies, courts, and hospitals
  - Collaboration with regional and international bodies
- Converting Consumer Complaints to Consumer Policy
  - Retrieve data from the registration system
  - Analyse data and write report
  - Propose policy action from data analysis

ASSESSMENT AND EVALUATION OF PARTICIPANT'S LEARNING

Method of Assessment: Reflection / Meta Learning. Ask the participants the following:

- Share three most important learnings you have gained as a result of this Session.
- How can you apply these learnings in your work related to consumer protection?

OVERALL ASSESSMENT AND EVALUATION OF THE TRAINING MODULE

Method of Assessment: Instrumentation.

- Ask the participants to individually answer the evaluation form. Refer to Appendix B. This overall Assessment will provide feedback about the contents, process, and facilitator.

APPENDICES

Appendix A.2: Cases – Session 2

Case 1: **Small Businesses warned to watch out for Ransomware, *19 May 2015***

This Fraud Week, the Australian Competition and Consumer Commission is warning small business operators to think twice before opening e-mail 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.

Source: Phones, Internet, and E-Commerce Technical Module (p. 109)

Case 2: Singapore SMEs troubled by Ransomware

Singapore being advanced in terms of economic and technological development, nonetheless falls prey to ransomware attacks.

According to Kaspersky (2018), a multinational cybersecurity and anti-virus provider headquartered in Moscow, Russia, and operated by a holding company in the United Kingdom, ransomware, refers to "Trojans…designed to extort money from a victim." It also defines a Trojan virus as malicious ware or "malware that is often disguised as legitimate software" (Kaspersky (n.d.). Often, cyber hackers demand ransom to undo changes that the ransomware has made to a victim's computer.

According to tech firm IDC and security service provider Quann, 75% of medium to large city-state organizations in Singapore do not have stable planning processes or security budgets for IT (Alger, 2017).

Jeff Hurmuses, APA area vice president and managing director of Malwarebytes (2018) states that Singapore was relatively unharmed during the global "WannaCry and "Petya" ransomware outbreaks in 2017. But he cites the findings of Cyber Security Agency, which says that reported ransomware incidences increased by almost ten times in 2016 as compared to 2015 (Hurmuses, 2018).

SMEs make up 99% of Singaporean enterprises and contribute to about half of the country's GDP (Ministry of Communications and Information, 2017). In 2017, more than one-third of them experienced ransomware attacks, according to Malwarebytes' 2017 State of Ransomware report (Hurmuses, 2018). The report also stated that ransomware was the most cited concern for SMEs, with 72% of Singapore-based respondents pointing to ransomware as an issue.

The same report highlighted the following findings (Hurmuses, 2018):

- While such attacks cause financial loss through ransomware payments, downtime caused by ransomware could have a bigger effect on one's business.

- More than 61% of companies in Singapore hit by ransomware experienced downtime of more than nine hours from a single incident of ransomware.

- About 33% of Singapore organizations that did not pay the ransom lost their files, and 11% of SMEs reported revenue loss.

Cyber hackers prefer to target SMEs than MNCs as SMEs tend to lack planning and human resources to strengthen their cyber defenses (Hurmuses, 2018). Based on Malwarebytes' research, only 9% of organizations surveyed felt "very confident" in their ability to thwart ransomware. Hurmuses (2018) believes this lack of confidence stems from the following reasons:

- Because of the lack of budget and expertise, SMEs often do not have cybersecurity insurance, dedicated IT departments, and well-established cybersecurity infrastructure. If they have not yet been victimized by cyber hackers, they will usually just maintain their current cybersecurity measures.

- SMEs tend not to train their staff regularly on cybersecurity. Based on Malwarebytes' finding, 18% of organizations in Singapore do not conduct training specifically about ransomware. Among the 81% of Singapore organizations that do hold some training, half did so only when the staff joined the company, or only once a year. Thus, organizations are not equipped to tackle attack vectors, which evolve and grow more sophisticated quickly. (Attack vectors are the means by which hackers access computers or network servers (TechTarget, 2012)).

- Current technology solutions cannot solve the problem.

Malwarebytes' research revealed that organizations have various solutions to address ransomware concerns (Hermuses, 2018). However, while a quarter of SMEs in Singapore claim to be running anti-ransomware technologies, 35% of businesses surveyed still experienced ransomware attacks.

References:

Alger, L. (July 10, 2017). *Singapore firms vulnerable to cyberattacks.* Retrieved on April 24, 2018, from http://www.softwaretestingnews.co.uk/singapore-firms-vulnerable-cyberattacks/

Hurmuses, J. (January 5, 2018). *Ransomware a big problem for Singapore SMEs – how to make it go away?* Retrieved on April 24, 2018, from https://www.enterpriseinnovation.net/ article/ransomware-big-problem-singapore-smes-how-make-it-go-away-1740357791

Kaspersky (2018). *Ransomware & cyber blackmail.* Retrieved on April 24, 2018, from https://usa.kaspersky.com/resource-center/threats/ransomware

Kaspersky (n.d.). *What is a Trojan virus?* Retrieved on April 24, 2018, from https://www.kaspersky.com/resource-center/threats/trojans

Ministry of Communications and Information (SG) (February 20, 2017). *SMEs are at the heart of our economy.* Retrieved on April 24, 2018, from https://www.gov.sg/microsites/budget2017/ press-room/news/content/smes-are-at-the-heart-of-our-economy

TechTarget (May 2012). *Attack Vector.* Retrieved on April 24, 2018, from https://searchsecurity.techtarget.com/ definition/attack-vector

Appendix A.3: Cases – Session 3

Case: The State of E-Commerce in Thailand

According to various industry experts in Thailand, the e-commerce market in Southeast Asia will amount to $11.1 Billion by 2025, with Thailand's growth expected in 2017 to reach 20 per cent (Boonnoon, 2017). Although only about 3 per cent of Thai consumers shopped online in 2016, increased internet and mobile phone use, better logistics and e-payment systems, and more online shopping services would boost consumer confidence, convenience, and acceptance to shop online (Boonnoon, 2017).

These developments could only mean good news to Thai consumers, who distrust online commerce. A recent survey by ACI Worldwide, a payment systems company, of 266 technology workers in Thailand revealed the following:

> Fraud is pervasive: Thirty-two percent of respondents have experienced personal payments fraud within the last 12 months. ATMs, eCommerce and mCommerce were the three primary sources of fraud.
>
> Lack of trust in online commerce: While 50% of all respondents strongly agree that banks will keep their transactions and data safe, only 17% and 12% believe their payment credentials are protected from fraud when using mCommerce and eCommerce, respectively (Ecommerce is appealing, 2017).

The same study identified both old (phishing and card skimming) and new (card-not-present fraud and social engineering) fraud methods (Ecommerce is appealing, 2017).

The ACI article (Ecommerce is appealing, 2017) quoted a 2016 study of Aite Group, stating that

> 31% of those who experienced fraud were unhappy with the response they received from their financial institution. Forty-eight percent of those who experienced fraud in Thailand changed banks following the event. The news is not good for merchants either, as only 13% of all those surveyed strongly agreed that merchants would keep their payment details safe.

Allan (2018) cites other reasons for the low volume of online sales transactions:

1. Customers still pay in cash upon delivery of the products, perhaps because many Thais still do not have bank accounts, let alone debit and credit cards;

2. Businesses have limited expertise or resources to sell online, or believe that online sales will eat into their brick-and-mortar sales;

3. Cross-border regulations in Southeast Asia are complex, and product delivery by Thailand Post is unreliable; and

4. Dial-up internet connections are still the norm especially outside major cities.

The Thai government is acting on these concerns. According to Ong (2018), some of its initiatives are as follows:

1. Electronic Transactions Development Agency (ETDA) has partnered with Omise, an open payment platform, to initiate the National Digital ID project.

2. The Ministry of Commerce of Thailand has asked e-commerce giant Alibaba to share its experience and expertise to help build Thailand's National E-Commerce Platform; train around 10,000 individuals in digital technology; develop Thailand's supply chain and logistics systems; and help establish Thailand as a hub of digital technology and regional data center in Southeast Asia.

3. The government aims to complete by 2021 the Eastern Economic Corridor (EEC), which includes the provinces of Chonburi, Rayong, and Chachoengsao and spans 13,285 square kilometers. The government hopes make the EEC a hub for technological manufacturing and services, with strong connectivity to Cambodia, Laos, Myanmar, and Vietnam by land, sea, and air.

4. Through the Eastern Economic Corridor Bill, which was approved in principle in April 2017, the government will also loosen restrictions on foreign investments made in the EEC, cut personal and corporate income taxes for EEC-based investors and corporations, lease land in the EEC up to 50 years, and allow the free flow of foreign currencies in the area.

References

Allan, S. The changing face of ecommerce in Thailand (2018, 16 May). Retrieved from https://www.aware.co.th/ecommerce-thailand-changing/

Boonnoon, J. Thai e-commerce sector expected to expand by 20 per cent this year (2017, 27 January). *The Nation.* Retrieved from http://www.nationmultimedia.com/news/business/

EconomyAndTourism/30305036?__hstc=25127141.91ab1bb454f98e1f85668c029bd45458.1525156229482.1525156229482.1525156229482.1&__hssc=25127141.1.1525156229485&__hsfp=1762750006

Ecommerce is appealing to Thai tech workers, but merchants must overcome security concerns (2017). Retrieved from https://www.aciworldwide.com/-/media/files/collateral/trends/ecommerce-is-appealing-to-thai-tech-workers-tl-us.pdf

Ong, J. Ecommerce in Thailand (2018, 13 March). Retrieved from https://thelowdown.momentum.asia/1892-2/

Case: (Supplementary Case) ACCC final decision on Mobile Call and SMS terminating charges and non-price terms report

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

Source: Phones, Internet, and E-Commerce Technical Module (pp. 100 – 101)

Appendix A.4: Cases – Session 4

Case 1: Illegal Investment Schemes in Malaysia – The "Swisscash" saga: *modus operandi* and ensuing litigation

The "Swisscash" saga: *modus operandi* and ensuing litigation

Armed with "convincing" claims via the Internet of numerous investments in equities, commodities as well as foreign exchange, among others, and of an average investment return of up to 300 per cent returns within 15 months of investment, the so-called "Swisscash-fund" was able to induce an investment amount of, reportedly, RM585.5 million from Malaysian investors (Jayasankaran, 2007).

The Swisscash saga actually began in 2006, when the Securities and Futures Commission of Hong Kong placed Swisscash on a list of scam Web sites as a result of complaints from Hong Kong investors (Securities Commission, 2007c). Immediately after, the Swiss Embassy issued a statement on its official Web site on May 18, 2006 which read:

[…] the Swiss Mutual Fund (1948) and or Swiss Cash are not registered companies in Switzerland. Until proof of the contrary, the Embassy doubts that the remarks about these funds and their historic links to Switzerland as outlined on their original website are genuine. The original website is indeed registered in the USA and the contact telephone number is from New Jersey (USA). […] (Switzerland Embassy, 2006).

On September 5, 2006, the Securities Commission and Bank Negara Malaysia (BNM which is the Central Bank of Malaysia) issued a joint press release, whereupon the Malaysian public was warned against investing in the Swisscash investment program as well as with Swiss Mutual Fund (1948) S.A. (Bank Negara, 2006). The Securities Commission has launched a thorough, exhaustive investigation into the operations of a few Swisscash-related companies, namely, Dynamic Revolution Sdn Bhd, Swiss Mutual Fund, SMF International Limited, SMF (1948) International Limited as well as the parties – Albert Lee Kee Sien, Kelvin Choo Mun Hoe and Amir bin Hassan – alleged to be the mastermind behind the scheme in Malaysia.

On April 19, 2007, a second joint press release was issued, whereby the public was cautioned against Internet investment schemes by and large. In June 2007, three Web sites, namely, www.swisscash.biz, www.swisscash.net and www.swissmutualfund.biz, were blocked by the Securities Commission working together with Malaysian Communications and Multimedia Commission and Cyber Security Malaysia. On September 13, 2007, the regulators blocked a new Web site, www.swisscashguide.com,

which had surfaced amid the regulators' pre-emptive actions and efforts to "combat" and block illegal investment Web sites. This has brought the total of Swisscash scheme-related Web sites blocked to four.

The key players, Mr Lee, Mr Choo and Mr Hassan, had actually used Swisscash Mutual Fund, a non-regulated company which did not even exist, i.e. it existed merely on paper and on Web sites, to induce Malaysian investors to send monies to the accounts with the promise that the investors would enjoy unusually high profits. Investigations showed that Swisscash's New York-office was merely a virtual office with forwarding services provided by a so-called "executive office". Even the Web site, a replicating one, was made available to Swisscash fund's investors and which they could utilize to further promote the Swisscash scheme. This was essentially put in place to enable and to encourage investors to recruit other investors. All mails addressed to Swisscash were actually forwarded to Mr Lee's office in Petaling Jaya. Investors were given the impression that Swisscash and Swiss Mutual Fund were actually schemes linked to Switzerland. The ruse was based on the perception that these schemes were bona fide investment schemes, as they are linked to Switzerland, renowned for being a sophisticated financial center. In actual fact, the funds were not even registered in Switzerland, as evident from Kuala Lumpur's Swiss embassy's public statement mentioned earlier.

The Securities Commission also took decisive steps to ensure that investors' rights are protected. On June 7, 2007, the Securities Commission filed a civil suit against Mr Lee, Mr Choo, Mr Hassan as well as Swisscash-related companies, namely, Dynamic Revolution, Swiss Mutual Fund, SMF International Limited and SMF (1948) International Ltd. The litigation was initiated to restrain and to prohibit them from carrying on the business of the Swisscash scheme; targeting, soliciting and/or collecting funds from the public for investments purposes in the Swisscash scheme; and hosting or even operating Swisscash's or Swisscash's related Web sites. The basis for the action was that the whole scheme was a fraud or scam and the parties were involved in dishonest or fraudulent conduct and carrying out fund management activities and holding out to be investment advisors without a license.

The Securities Commission had managed to freeze 22 Malaysian bank accounts of the defendants amounting to RM2.9 million[1]. But, what could be described as a milestone in the history of Securities Commission's enforcement action was the procurement of the worldwide Mareva injunction against the scheme's perpetrators, so as to prevent them from dissipating assets in and outside Malaysia (Securities Commission, 2007a). This pre-emptive strike enabled the Securities Commission to ensure that if the litigation against the defendants were successful, the regulators and the investors will not be deprived of the fruits of judgment by the defendants, possibly, dissipating the funds or transferring the funds out of the companies to put the money out of reach of the regulator or investors. If this were to occur, the enforcement action would have been an exercise in futility. Through the Mareva injunction, the three defendants were also required to

disclose information pertaining to all of their assets in and outside of Malaysia, the companies they have incorporated as well as the bank accounts that they operated. A court order was also obtained in September 2007, in which Mr. Hassan was directed to transfer RM35 millions of Swisscash monies back to Malaysia. Upon the transfer, the said monies were subjected to the Mareva order granted earlier by the court on June 21, 2007 (Bernama News, 2007). Since then, the Securities Commission has led a meeting of seven regulators to intensify cross-border cooperation and exchange of information on the Swisscash scam.

As a result, the Securities Commission was able to recover compensation for the investors to the Swisscash funds. The judgment was obtained against Albert Lee Kee Sien, Kelvin Choo Mun Hoe and Dynamic Revolution Sdn Bhd, obtained on September 25, 2008, which ordered them to pay USD83 million, and any further amounts traced by the Securities Commission, for the purpose of compensating investors of the scam. In consequence to a consent judgment entered into with Albert and Amir, on November 13, 2009, the Securities Commission entered into a settlement amounting to RM31 million. The monies were to be used via a restitution scheme to compensate eligible investors who suffered losses as a result of the scam. The restitution scheme was administered by PricewaterhouseCoopers Services Sdn Bhd, appointed by the Securities Commission. On November 2, 2011, the final report (setting out the restitution process as well as the payment criteria to eligible investors) was issued. It is to be noted that a total of 29,885 claims amounting to RM188 million were made, both from Malaysian as well as foreign investors. However, only RM30.532 million were made to 19,625 eligible claimants. Investors, basically recruiters or up-liners, as well as those who invested after Securities Commission issued the warning on November 5, 2006 are among those not eligible for the compensation (Securities Commission, 2010).

The Crude Palm Oil Ponzi scheme: *PP* v. *Raja Noor Asma bt Raja Harun* [2013] 9 MLJ 181

Around the time the Swisscash saga unfolded, another scheme was brought to the attention of the regulators. On May 9, 2008, the Securities Commission issued a press statement via its official Web site that it has launched an investigation into FX Capital Consultant (M) Sdn Bhd, and its director, Raja Noor Asma (Securities Commission, 2008b). It was alleged that she had duped an estimated 4,200 investors of over RM100 million between February 2007 and May 2008 under the pretext that the money would be invested in crude palm oil Futures.

A popular definition of a futures contract is a contractual agreement, generally made on the trading floor of a futures exchange, to buy or to sell a particular commodity or financial instrument at a pre-determined price in the future. The term “trading in futures contract” has a broad and expansive connotation, as defined in Schedule 2, Part 2 of the CMSA 2007. It encompasses entering into and the closing out of a futures contract such as that of hedging, foreign exchange (forex), commodities etc., and includes

preliminary acts such as that of offering or making an offer to enter into a futures contract or soliciting or accepting an order to enter into a futures contract or even inducing or attempting to induce a person to enter into such contracts.

In the case of Raja Noor Asma, she was charged on December 17, 2008, with conduct to defraud investors of the company and for trading in futures contracts without a license between May 7, 2007 and September 27, 2007 and between September 28, 2007 and May 2008 under the Futures Industry Act 1993 and the CMSA 2007, respectively. The charges under the Futures Industry Act 1993 were for offences alleged to have been committed prior to the Futures Industry Act being consolidated into the CMSA 2007. Additional charges were made under Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (AMLATFA) for receiving, possessing and using the money obtained from the said scheme. On December 21, 2010, Raja Noor Asma pleaded guilty to the charges of fraud for using a scheme to defraud investors and trading in futures contracts on behalf of others without a license.

Consequently, on January 10, 2011, she was convicted and sentenced to imprisonment of five years for each of the four charges, which were to run concurrently, as well as a RM5 million fine in default of six months' imprisonment. As for the charges under the Anti-Money Laundering Act, she was sentenced to two-year imprisonment for each of the 50 charges that are to run concurrently but consecutively after the five-year imprisonment (Securities Commission, 2011a). In total, Raja Noor Asma had to serve a seven-year jail-sentence. The Securities Commission convinced the court to impose a retributive and deterrent sentence on the grounds of public policy, i.e. to preserve the interest of the public considering the huge amount of investors' funds (The Sundaily, 2011).

Subsequently, the regulators issued a notice under Section 61 of the AMLATFA to inform any "bona fide third party with interest" to be present in the court to show cause as to why the properties valued at more than RM8 million that were seized could not be forfeited to the Government of Malaysia. It is to be noted that monies or properties seized as a result of this type of illegal scheme are subject to forfeiture as provided under Section 55 of the AMLATFA, unless the victims can show that the money should be returned to them instead of forfeited by the government. On April 1, 2011, more than 600 victims of Raja Noor Asma's illegal scheme turned up at the Jalan Duta Sessions Court (on the court's order) in relation to their third-party claims as to the money recovered from Raja Noor Asma. The victims sought to reclaim their monies invested in the scam[2]. A total of RM8.3 million had been recovered from Raja Noor Asma's personal, fixed deposit as well as the company's accounts. At the hearing, eight investors appeared on behalf of the 700 victims. One investor, Mohd Imran Razali, stated that he invested RM630, 000 in the scheme and got back only RM54,000, while another investor, Shahrom Hadi, beseeched the court to take into consideration their plight and return the money that they have invested (AsiaOne News, 2011). There were allegations of regulatory failure in the assertion by the solicitor

acting on the victims' behalf that the Securities Commission and Bank Negara Malaysia had not been "vigilant".

Under the AMLATFA, for the "victims" to recover their money, they must be able to fulfill the requirements under Section 61(4):

The court or enforcement agency shall return the property to the claimant when it is satisfied that:

a) the claimant has a legitimate legal interest in the property;
b) no participation, collusion or involvement with respect to the offence under subsection 4(1) which is the object of the proceedings can be imputed to the claimant;
c) the claimant lacked knowledge and was not intentionally ignorant of the illegal use of the property, or if he had knowledge, did not freely consent to its illegal use;
d) the claimant did not acquire any right in the property from a person proceeded against under circumstances that give rise to a reasonable inference that any right was transferred for the purpose of avoiding the eventual subsequent forfeiture of the property; and
e) the claimant did all that could reasonably be expected to prevent the illegal use of the property.

At the trial court, the judge decided in their favor on April 14, 2011, on the grounds that they have been able to fulfill the requirements of the above section.

The regulators, however, were not satisfied with the decision and appealed to the High Court. The High Court, however, was sympathetic to the predicament of the victims and upheld the decision of the Sessions Court (*PP* v. *Raja Noor Asma bt Raja Harun* [2012], MLJU 515; *PP* v. *Raja Noor Asma bt Raja Harun* [2013], 9 MLJ 181). Unfortunately for the victims, their exhilaration in being able to recover their investments was short-lived. On October 3, 2013, the three-man bench members of the Court of Appeal unanimously allowed the appeal by the prosecution (who acted on behalf of Bank Negara of Malaysia and the Securities Commission) to forfeit the money [3]. The Court of Appeal was of the view that the respondents, i.e. the victims in Raja Noor Asma's case, had failed to discharge the burden of the requirements under Section 61(4) of the AMLATFA (*PP* v. *Raja Noor Asma bt Raja Harun* [2013], 9 MLJ 181, pp. 182-184). Section 61(4) requires certain circumstances to be fulfilled by the third-party claimants (like Raja Noor Asma's victims in this case) to ensure that the claims are actually bona fide claims. The Court of Appeal was of the view that these have not been fulfilled. Perhaps, one of the reasons for the court to conclude that the claims were not bona fide lies in Section 61(4)(c) of the same Act, i.e. the claimants in this case are not lacking in terms of knowledge of the illegal use of the monies invested in Raja Noor Asma's scheme, as some of the victims were lawyers and judges.

The enforcement action in the crude palm oil investment scam raises some interesting issues. Note that the investors and/or victims in the crude palm oil investment scam made headlines in 2011, in their attempt to recover part of their monies invested in the scheme which they failed to recover as a result of the decision at the Court of Appeal. The AMLATFA does not provide the victims with the *locus standi* to sue for the recovery of the money where the regulator had not agreed to issue a notice to enable them to "join" in the proceedings. This is in contrast with the CMSA 2007. It must be noted though that the enforcement action for contravention of securities law by private litigant has not always been part of the statutory framework under the CMSA 2007. In the past, the predecessor statutes had neither provided for private enforcement nor given the right to private litigants to initiate suits. The predecessor statutes of the present CMSA 2007, namely, the Securities Industry Act (1983) and the Futures Industry Act (1993), originally as introduced focused mainly on public enforcement by the capital market regulators. Investors would have to rely on the law of contract or the law of torts to recover any loss. These had their challenges. The high cost of litigation, absence of contingency fee framework and class action as well as the "cost follow event" rule are considered as economic disincentives to investors' private action. Where there is a contingency fee arrangement, the client agrees to pay the solicitor a certain specified percentage of any settlement or even verdict. But, if the client lost the case, the solicitor is left with nothing. The "cost follow event rule" results in the losing party having to pay the winning party all costs (Securities Commission, 2011b). However, the Securities Industry Act (1983) was subsequently amended, enabling the Securities Commission to obtain civil compensation on behalf of the investors (Nariman Mohd Sulaiman, 2008). This was initially allowed for insider trading but was later expanded to cover other securities market contravention [4]. The right to bring civil action for securities law contravention that resulted in loss of damage was retained in the CMSA, under sections 199, 201, 210, 211, 357 and 358, when it was introduced in 2007. For contravention of the CMSA relating to futures contracts, the enforcement framework covers criminal prosecution, civil action by the Securities Commission under Section 211 and civil action by private litigants (i.e. investors) under Section 210. Despite this, hardly any private litigation has been commenced.

Excerpted from:

Sulaiman, A.N.M., Moideen, A.I., Moreira, S.D. (2016). "Of Ponzi schemes and investment scams: A case study of enforcement actions in Malaysia," *Journal of Financial Crime, 23*(1), 231-243, https://doi.org/10.1108/JFC-05-2014-0021

Case 2: (Supplementary Case) Bet365's $200 Free bets for new customers

(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, 98 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

Source: Phones, Internet, and E-Commerce Technical Module (pp. 97 – 98)

Appendix A.5: Cases – Session 5

Case for Role-Play: Sextortion in the Philippines

Cambridge Advanced Learner's Dictionary & Thesaurus (n.d.) defines sextortion as "the practice of forcing someone to do something, particularly to perform sexual acts, by threatening to publish naked pictures of them or sexual information about them." According to International Criminal Police Organization (Interpol), it is "sexual blackmail in which sexual information or images are used to extort sexual favours and/or money from the victim, with blackmail demands ranging between USD 500 and USD 15,000" ("INTERPOL-coordinated operation," 2014).

Interpol (as cited by BBC News, 2014) states that this crime is claiming "hundreds of thousands of victims." Criminals impersonate young men, luring them into sexual encounters via webcam, and then extort money from them (BBC News, 2014).

Daniel Perry, RIP

On July 15, 2013, 17-year-old Daniel Perry, an apprentice mechanic, jumped to his death off Forth Road Bridge in the town of Dunfermline, Fife County, Scotland, after having been victimized by an online sextortion ring based in North Hills Village, Bulacan, Philippines ("Teenager's death," 2013, Parry, 2017). Below is the chronology of events as gathered from different news accounts.

Sometime in 2013, Perry chatted on Skype with a young, pretty American girl, whom he met on the social media website ask.fm and with whom he shared sexually explicit pictures and a video chat (Teenager's death, 2013; Gutierrez, N., 2018). As it turned out, Perry had been chatting with blackmailers.

About three months before he committed suicide, Perry started receiving messages from his blackmailers, who demanded payment if he did not want his video to be made public (Crawford, 2014). Some of the messages were "kill yourself mate," "you need to let a blade meet your throat," and "I will make you suffer" (Teenager's death, 2013; Crawford, 2014). Perry pleaded with them, but the suspects allegedly replied, "Commit suicide now," and later: "Are you dead yet?" (Crawford, 2014).

On July 15, 2013, Perry received a message saying he needed to send money to an account if he didn't want his friends and family to see his images and video; otherwise, he should just kill himself ("Teenager's death," 2013). Perry's last reply to his blackmailers was "bye, bye" ("Sextortion, lies," 2017). An hour later, he was dead ("Teenager's death," 2013).

Operation Strikeback

Below is the Timeline of Operation Strikeback combating "sextortion" (May 2014) of the INTERPOL. The UK's Foreign and Commonwealth Office provided funding towards Operation Strikeback to support both operational coordination and a capacity building project to help tackle future cybercrime threats.

November 2013

During the 1st INTERPOL Eurasian Working Group Meeting in Singapore in November 2013, a presentation by Hong Kong Police and a social networking group highlighted the growing number of 'sextortion' cases, with some 440 cases reported in Hong Kong in 2013.

Following the meeting, officers from the INTERPOL Digital Crime Centre (IDCC) met with representatives from the Hong Kong Police Force, Singapore Police Force and the Philippine National Police (PNP) Anti-Cybercrime Group to formulate a joint investigation model to combat sextortion.

December 2013

PNP identified and shared information about the 'Bicol Group' based in Naga City as being involved in sextortion. More than 100 suspects were linked to this particular syndicate.

January 2014-February 2014

Hong Kong Police identified a second network, the 'Bulacan group,' involved in sextortion cases and operating out of the Philippines.

Investigations identified victims of this group in a number of countries/jurisdictions including Hong Kong (China), Singapore, the United Kingdom and the United States. Additional potential victims were also identified in Australia, Malaysia, the Philippines and Korea.

February 2014

Police Scotland officially joined the cybercrime taskforce to combat sextortion, after work with the UK's National Crime Agency (CEOP command) led to the identification of a criminal network linked to the death of Scottish teenager Daniel Perry.

March 2014

The INTERPOL Digital Crime Centre arranged a 2nd operational meeting in Singapore involving representatives from police and judicial authorities from the Philippines, England, Scotland, Hong Kong, Singapore and Australia. Details of a third organized crime group also based out of the Philippines were presented to the group.

April/May 2014

As a result of the intelligence sharing between the involved countries and the private sector, an operation targeting the organized crime groups was mounted in the Philippines on 30 April and 1 May 2014. Raids were conducted at premises in Bicol, Bulacan, Laguna and Taguig City, resulting in the arrest of 58 individuals and the seizure of 250 pieces of electronic equipment.

The Suspects

Arrested in connection with Perry's death were Vincent Regori Bravo, Jomar Palacio (alias Park Ji Man) and Archie (alias Gian) Tolin (INTERPOL-coordinated operation, 2014). They were charged with having violated the following (Parry, 2016):

1. Republic Act (RA) 7610, or the Special Protection of Children Against Abuse, Exploitation and Discrimination Act, specifically Article 5, Section 9, which states in part: "Any person who shall hire, employ, use, persuade, induce or coerce a child to perform in obscene exhibitions and indecent shows, whether live or in video, or model in obscene publications or pornographic materials or to sell or distribute the said materials shall suffer the penalty of prison mayor in its medium period."

2. RA 10175, or the Cybercrime Prevention Act of 2012;

3. RA 8484, or Access Devices Regulation Act of 1998; and

4. RA 9775 Anti-Child Pornography Act of 2009).

When interviewed by BBC, Palacio denied any wrongdoing: "I do not know him, I did not get any money, I did not do anything wrong to him, that's all" (Crawford, 2014). Similarly, Bravo protested, "I didn't do it, I don't know anything about it. They have no hard evidence against us…I send my condolences to [the Perry family], but I wasn't the one who did it. I feel sorry because he left behind a family which loves him" (Crawford, 2014).

The same BBC report states that Scottish authorities want the suspects to be tried in the UK, but
"They will first have to be tried in the Philippines and other legal actions might follow. They will have to serve prison or any verdict entered into by the court," according to Senior Superintendent Gilbert Sosa, director of the Filipino Anti-

Cybercrime Group (Crawford, 2014). The three suspects are out on bail. (Crawford, 2014).

In February 2016, The Crown Office and Procurator Fiscal Service of Scotland (COPFS) announced that a warrant had been issued for the arrest of Tolin, who has since gone into hiding (Musson, 2016). The COPFS is responsible for "the prosecution of crime in Scotland, the investigation of sudden or suspicious deaths, and the investigation of complaints against the police (Crown Office and Procurator Fiscal Service of Scotland, nd.).

The Alleged Mastermind

Bravo, Palacio, and Tolin are allegedly members of a gang headed by Maria Cecilia Caparas-Regalachuelo, known as the Queen of Sextortion (Parry, 2017). According to her neighbors, Caparas-Regalachuelo used to be dirt-poor, but now, she allegedly owns ten properties in Bulacan, "including a villa with a swimming pool and a two-storey block in the centre of the village where youngsters congregate in a billiard room lined with computer terminals" (Parry, 2017).

Caparas-Regalachuelo, was arrested along with Bravo, Palacio, and Tolin, but was released on bail in June 2014 supposedly after she had bribed officials. Rearrested in September 2016 in response to international pressure, she is awaiting trial for child abuse violation of RA 7610 and trafficking (violating of RA 9208, or the Anti-Trafficking in Persons Act of 2003) and has been charged with criminal cases 3715-M-14 to 3718-M-14 (Parry, 2017). Also arrested was her nephew Mark Andrey Rafol Sesaldo, who allegedly helped her operate the scam (Parry, 2016).

In an interview held at the Bulacan Provincial Jail where she was detained, Caparas-Regalachuelo, narrated how the North Hills-based sextortionists look in Facebook for professionals who are in their 20's and who are apparently most vulnerable to blackmail demands (Parry, 2017):

We worked in teams and targeted a lot of men in Hong Kong and Singapore because they are in the same time zone as us and they can usually communicate in English," she says. "We tease them to get them comfortable and we work to a prepared text. Some of the chatters can barely speak English and many are young gay men and transsexuals – but they only communicate by text and show pre-recorded video so the victim never knows. It only takes about 30 minutes of chat before they are persuaded to do things in front of camera. They nearly always pay up after we put the video on YouTube…

I am ashamed of what I did. I am so sorry for the victims. I was terribly shocked and sad when I heard what happened to the boy [Perry] in Scotland. I don't know anything about him but I'm very sad for his family's loss…

They are stupid. When I talked to them after they had paid their first [blackmail] demand I would tell them: 'Don't do it again – you have learnt a lesson from your mistakes.'"

Yet Caparas-Regalachuelo insists: "How could an uneducated woman like me organise a criminal syndicate?" (Parry, 2017)

The evidence against Caparas-Regalachuelo includes pictures from various Facebook accounts andscores of fake ID cards that had been used to collect blackmail payments from Western Union offices (Parry, 2017).

References:

Crawford, A. (19 December 2014). Sextortion' suspects deny involvement in Daniel Perry case. *BBC News.* Retrieved from http://www.bbc.com/news/technology-30494566

Crown Office and Procurator Fiscal Service of Scotland (n.d.) Retrieved from http://www.copfs.gov.uk/about-us/ about-us

Gutierrez, N. (2018, 9 February). Can the Philippine gov't protect you from revenge porn, hackers? *Rappler*. Retrieved fromhttps://www.rappler.com/newsbreak/in-depth/195653-revenge revenge-porn-hackers-cybercrime-cybersecurity-ph-israel

INTERPOL-coordinated operation strikes back at 'sextortion' networks (2014, 2 May). Retrieved from https://www.interpol.int/News-and-media/News/2014/N2014-075

Musson, C. & Brown, T. (2016, 6 April). Filipino suspect could face trial over teenage blackmail victim's suicide. *The Sun.* Retrieved from https://www.thesun.co.uk/archives/
news/187313/filipino-suspect-could-face-trial-over-teenage-blackmail-victims-suicide/

Parry, S. Inside the sleazy Filipino internet den where 'Queen of Sextortion' arrested over British teen's suicide 'made fortune duping men into stripping for cybersex and then blackmailing them' (2016, 9 December). *The Daily Mail.* Retrieved from http://www.dailymail.co.uk/news/article-4000652/Inside-sleazy-Filipino-internet-den-Queen-Sextortion-arrested-British-teen-s-suicide-fortune-duping-men-stripping-cybersex-blackmailing-them.html

Parry, S. Sextortion, lies and videotape: the Philippine cybercriminals who target men in Hong Kong and worldwide (2017, 10 February). *The Star Online.* Retrieved from https://www.thestar.com.my/news/regional/2017/02/10/sextortion-lies-and-videotape-the-philippine-cybercriminals-who-target-men-worldwide/

Republic Act 7610. Retrieved from http://pcw.gov.ph/law/republic-act-7610

Sextortion. (n.d.). In *Cambridge Advanced Learner's Dictionary & Thesaurus.* Retrieved from https://dictionary.cambridge.org/us/dictionary/english/sextortion

Teenager's death sparks cyber-blackmailing probe (2013, 16 August). *BBC News.* Retrieved from http://www.bbc.com/news/uk-scotland-edinburgh-east-fife-23712000

Timeline of Operation Strikeback combating 'sextortion' (2014, 2 May). Retrieved from https://www.unodc.org/res/cld/case-law-doc/cybercrimetype/phl/operation_strikeback_html/2014-075-Timeline-of-Operation-Strikeback.pdf

Case: **(Supplementary Case) Australian 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.

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 e-mail 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 (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.

Release number: MR 8/15

Source: Phones, Internet, and E-Commerce Technical Module (pp. 117 – 119)

Appendix B: Assessment Form

Module Assessment Form

Program Title:	
Date:	
Topic:	

Please encircle the number corresponding to your feedback for each of the ite*ms* below. We would also appreciate your *specific* comments for each section whenever applicable.

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
CONTENT					
The module is relevant to my work setting.	1	2	3	4	5
The module was able to meet the training objectives.	1	2	3	4	5
Each topic was given enough time to be discussed adequately and effectively.	1	2	3	4	5
The content is up-to-date and includes data from ASEAN context.	1	2	3	4	5
LEARNING MATERIALS					
The learning materials (training manual and PPT slides) were relevant and helpful in helping me to understand the topics.	1	2	3	4	5
The learning materials (training manual and PPT slides) were made with good quality (i.e. clear format and visuals) and understandable sequence.	1	2	3	4	5
Comments/Suggestions on the Learning Materials:					

What did you like best about the training/module?_____

What do you suggest to improve the training/module? _____

What other topics for training do you suggest that AADCP II to sponsor?

RESOURCE SPEAKER EVALUATION

Instructions: Please encircle the number corresponding to your feedback for each resource speaker.

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Name of Facilitator					
Demonstrates mastery of the subject matter.	1	2	3	4	5
Presents the subject matter and handles sessions in a timely and organized manner (i.e., starts and ends each session on schedule, spends enough time on each topic, links topics, and provides systematic review)	1	2	3	4	5
Communicates ideas clearly and effectively (i.e., uses simple words and familiar language, uses examples and visuals)	1	2	3	4	5
Able to establish rapport with the group (i.e., draws attention and sustains interest throughout the discussion)	1	2	3	4	5
Competently handles questions raised by the group	1	2	3	4	5
Encourages critical thinking and analysis while respecting the personal views and opinions of each participant	1	2	3	4	5

What are the facilitator's strong points?

Please provide suggestions for areas of improvement.

If you have other comments, please specify.