THAMMASAT REVIEW
PRINT ISSN: 0859-5747 ONLINE ISSN: 2630-0303
Volume 23 No 1 (January-June) 2020 [Page 138-159]

Guidelines for the Management of Digital Evidence Gathering Concerning Online Shopping Fraud

Somkanae Akkarakantrakorn *

Faculty of Social Science and Humanities, Mahidol University, Thailand

Received 23 September 2019; Received in revised form 22 January 2020
Accepted 21 February 2020; Available online 9 June 2020

Abstract

Constant connectivity to the Internet has improved our quality of life by leaps and bounds. Convenience shopping is the ultimate game-changer which is fast becoming the norm. While globalization of the Internet is rapidly moving forward, online businesses and consumers are vulnerable towards online fraud due to increasing usage on online transactions. This mixed methods study aims to investigate the factors that contribute towards online purchases while gathering evidence to develop guidelines for collecting digital evidence. Quantitative samples from 95 police officers from the Technology Crime Suppression Division, whereas qualitative samples comprised of 6 police officers from the same division, and 13 senior executives in various agencies who had been coordinated work with the Public and State Agencies in coordinating work in digital data evidence collection. The study employed focus group discussion and in-depth interviews. Questionnaires, percentage, mean, standard deviation, t-test and ANOVA were also used for data collection and analysis.

Research outcomes revealed that online shopping fraud was done in 3 ways: 1) buyer fraud 2) seller fraud 3) buyer and seller fraud. The Computer Crime Act B.E. 2550 (2007) empowered the police to request information from the service providers regarding the communication, financial, shipping and delivery trail. Problems and obstacles were related to poor knowledge management, delays, late delivery of evidence, scope of police power, incompetent personnel without ability to manage the flow of internal and external knowledge effectively, including a lack of public awareness. The main contribution of this study is to build public awareness to prevent and reduce the risk of online shopping fraud as well as providing a guideline for the Technology Crime Suppression Division to further operations.

Keywords

Online Shopping Fraud, Digital Evidence, Buyer & Seller Fraud, Computer Crime Act B.E. 2550, Technology Crime Suppression Division

* **Corresponding author:** somkanae@gmail.com **DOI:** 10.14456/tureview.2020.7

Introduction

In the late 1970s, electronic commerce was identified as the facilitation of commercial transactions electronically, using technology such as Electronic Data Interchange (EDI) and Electronic Funds Transfer (EFT), transforming conventional business activities by allowing businesses to send commercial documents like purchase orders or invoices electronically. The growth and acceptance of credit cards, automated teller machines (ATMs) and telephone banking in the 1980s were also forms of electronic commerce. Presently, social development encompasses a rapid change in the economy, politics, culture and technology with information sharing happening worldwide through the internet. The borderless world has become essential for human existence (e.g. education, business, entertainment and data transmission).

Electronic commerce is the use of open networks over, the Internet, to conduct external transactions such as buying, selling, and exchanging products and services, which in turn creates an opportunity fraud (Hawkins et al., 2000).

The technological advancement in Thailand has quickly accelerated numbers of computer and internet users. Online shopping continues to grow rapidly from generating sales of merchandise in 2015 for 2,245,147 million baht to 2,560,103 million baht in 2016 and 2,812,592 baht in 2017 (ETDA, 2018).

There are many types of computer crimes such as unauthorized access to information, computer interception, and computer frauds (Kulnithet et al., 2013). Out of 2,576 complaint cases received by the Technology Crime Suppress Division in the 2015, 440 cases were online shopping fraud (Technology Crime Suppression Division, 2017). Crimes with the highest number complaints are highlighted in Table 1.

Table 1 Statistics on complaints of Technology Crime 2015-2019

Crime Types	Number of Cases				
	2015	**2016**	**2017**	**2018**	**2019**
Defamation	1103	1591	740	1122	1268
Online Shopping Fraud	653	343	440	573	857
Input factual or fake data into computerize system	492	446	496	499	516
Wrongful access of computerize system *	192	303	77		
Input obscene information* *	58	151	165		
Fraudulent email	31	183	41	71	51
Lese Majeste ***	19	14	4		
Damaged destroyed or altered data	17	0	0	499	516
Hacking	8	0	0	623	697
Using or possessing other electronic cards ****	3	1	0		
Total	2,576	3,032	1,963		

Source: Statistical complaints of Technology Crime 2015-2019, Technology Crime Suppression Division, 2019

Remarks: *, **,***,**** No data available in 2018 & 2019 due to change in categories

The Technology Crime Suppression Division (TCSD) is an agency under supervision and command of the Royal Thai Police and has been assigned to prevent and suppress crimes as well as perform other duties stipulated by law. In the course of litigation against cybercrime offenders, the division is assigned to seek evidence to testify and prosecute offenders throughout the entire Kingdom of Thailand.

This mixed methods study intends to examine the occurrence of online shopping fraud, situation intervention, problems and drawbacks, including agency and third party involvement, as well as propose various approaches to prevent on line shopping fraud.

Literature Review

Concept of Fraud

Fraud happens in a social setting and thus produces severe effects not only on the economy, but also businesses and individuals (Silverstone & Sheetz, 2007). According to Albrecht et al. (2009) fraud is an individual's attempt to gain a benefit from others through deception or inappropriate means. Scholars such as Kovanich (2008,) also defines fraud as a concealment or false representation through action that injures others.

While the existing literature on social commerce provides insights on social commerce development in terms of its advantages and adoption, other studies offer understanding of the dark side of social commerce, particularly with regards to the occurrence of social commerce frauds. Although studies have been conducted by many authors, the research in this area remains limited.

Fraud is a product of personality and environmental or situational triggers according to Duffield & Grabsy (2001) , and it can be varied, depending on each individual case (Pedneault 2009) . Moreover, Albrecht et al. (2009) mentioned that perpetrators who committed fraud are motivated by perceived opportunities and rationalizations which coincide with the Fraud Triangle Theory as shown in Figure 1 in which:

1) Pressure is something that has happened in perpetrators' lives causing stress and pushing them to steal.

2) Opportunity is interpreted as a condition that perpetrators identify as weak control of others to use these weaknesses to steal from the victims successfully.

3) Rationalization is perpetrators' justification why they decided to commit fraud.

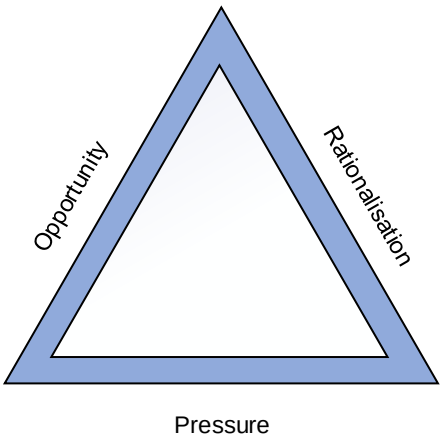

Figure 1 Fraud Triangle: A Framework for Spotting High-risk Fraud Situation

Source: Retrieved from Brunell Group/WWW.brunellgroup.com

Moreover, customers' motivation to online purchase has been investigated and found several interesting concepts such as Lu & Su (2009) demonstrated in their studies that customers online purchase intention is influenced by enjoyment, usefulness, compatibility and anxiety. In addition, a few studies also revealed that trust of sellers has a positive and significant impact on purchase intentions using e-commerce, which implies that the more customers trust sellers, the more customers intend to transact using e-commerce. This concept is supported by Kim et al. (2008), Liu et al. (2005), and Tung et al. (2008).

Nonetheless, this study focuses on 3 patterns of fraud committed as follows:

1. Seller Fraud

1.1 The seller failed to deliver the merchandise as agreed even though the payment had been made.

1.2 The seller delivered different merchandise what was advertised, counterfeit, poor quality, expired merchandise or claimed that the merchandise had been delivered by showing a fake delivery statement.

2. Buyer Fraud is when the buyer forged the proof of transfer and sent the fake slip to the seller or the buyer claiming that no merchandise was delivered to the buyer.

3. Both Buyer and Seller Fraud is when the fake seller contacts the real seller with intention to obtain merchandise without payment. In the meantime, the offender advertises merchandise that does not existed, just to gain the attention of a prospective buyer. After the prospective buyer transferred payment to the bank account set up for fake selling, the fake seller would show the transfer slip to the real seller so that he could deliver merchandise to the offender. In this case, the buyer who paid the money for the merchandise would not receive the merchandise. Figure 2 provides concise explanation of the aforementioned patterns:

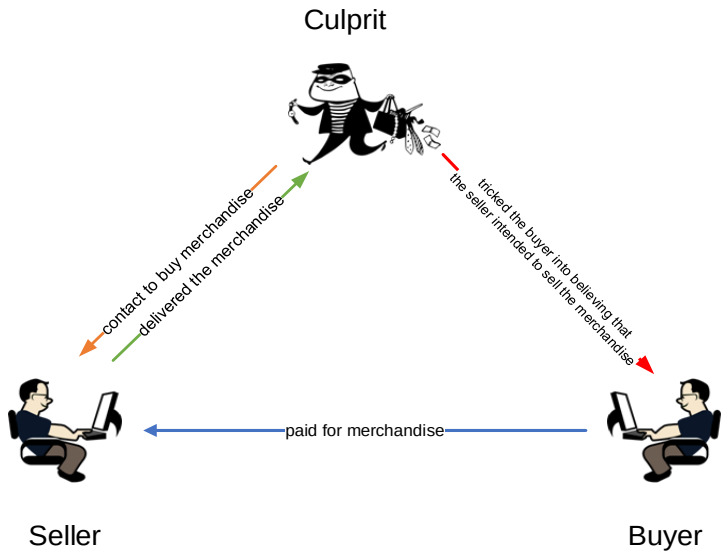

Figure 2 Fraud Patterns

Source: Constructed by the author from interviewing and gathering information

Fraud in Cyberspace

With the advent of the Internet, e-commerce is a prime target of perpetrators to increase fraudulent activities because it is borderless, low-cost, and accessible, has a global reach and does have a capable guardian. Huge money lost in e-commerce each year is becoming a serious problem and damaging the economy, with victims from both sides, customers and vendors alike (Clough, 2010, p. 185).

In addition, the study employed the Crime Control Model as a tool for the police officers to exercise the power as prescribed by law while collecting digital evidence of online shopping fraud for the police officers to exercise power as prescribed in the law for effective crime control and suppression as well as track down the offender and bring him or her to justice.

Prior to the passing of Computer Crime Act B.E.2560 (2017), the Thai Criminal Code had incorporated section code on fraud such as, Section 341 on Fraud, Section 342 on Special Circumstances of Fraud, Section 343 on Public Fraud, Section 344 on Fraud for Services, Section 345 on Fraud for Theft of Food, Drink, or Shelter, Section 346. Fraud for Theft of Property and Section 347on Insurance Fraud. Nonetheless, there is no specific section on Computer Crime, the closet section is Section 341 with the following provision:

Section 341. Fraud

Whoever dishonestly deceives a person with the assertion of a falsehood or the concealment of the facts which should be revealed, and, by such deception, obtains property from the person so deceived or a third person, or causes the person so deceived or a third person to execute, revoke or destroy a document of right, is said to commit the offence of cheating and fraud, and shall be punished with imprisonment not exceeding three years or fined not exceeding six thousand Baht, or both.

Therefore, the Computer Crime Act B.E. 2550 (2007) was enacted to cover specific provision and punishment for violation in such area. In Thailand, online shopping fraud is considered the direct violation of Computer Crime Act B.E. 2550 (2007), Section 14(1) amended by the Computer Crime Act B.E. 2560(2017), Section 8(1) which prescribed as follows:

In Thailand, online shopping fraud is considered a direct violation of Computer Crime Act B.E. 2550 (2007), Section 14(1) amended by the Computer Crime Act B.E. 2560(2017), Section 8(1) which is prescribed as follows:

Section 14: Whoever commits the following offences **shall be punished with imprisonment not** five years, or a fine not exceeding one hundred thousand Baht or both.

(1) Dishonestly or by deception, entering wholly or partially distorted or false computer data into a computer system in a manner likely to cause damage to the general public; which is not a defamation under the Criminal Code*;*

(2) In case the offence under Paragraph (1) is not committed against the general public but rather against a certain person, the offender, the disseminator or. forwarder of such computer data shall be liable to an imprisonment for a term not exceeding three years, a fine not exceeding sixty thousand Baht or both; and such offence shall be deemed a compoundable offence.

As mentioned earlier, Thai Act prescribed the offense on fraud in the criminal code, section 341 (Chanunchai, 2006) as anyone intentionally deceived other by displaying false statement or any other methods such as verbal gestures or written statement, including the action through television, radio, Internet network or concealed the fact that should be told, making the doer gain assets or the deceived victim or third person pull out or destroy the ownership right documents. Therefore, online shopping also has the components of fraud in line with the criminal code Section 341 apart from Section 14 of Computer Crime Act 2550 (2007).

The study also explored problems and obstacles in collecting digital evidence online shopping fraud of the Technology Crime Suppression Division. Based on the recent studies, the main questions were then developed:

Q1: What are problems and obstacles in collecting digital evidence of online shopping fraud of the Technology Crime Suppression Division?

Q2: Which directions were chosen for administering procedures on collecting evidence related to online shopping fraud of the Technology Crime Suppression Division?

Research Methodology

Data Collection Instruments

The study employed mixed methods through documentary research, qualitative and quantitative research materials. In-depth interview and questionnaires, including the statistical application of percentage, mean, standard deviation, t-test and ANOVA used for data collection and analysis.

Research Populations and Samples

Quantitative samples of 95 police officers, from the Technology Crime Suppression Division, Sub-division 1-3, mostly Squad Leaders, Deputy Superintendents, Operational officers, all possess expertise in collecting computer crime evidence. The Multistage Random Sampling, namely, Purposive Random Sampling and Quota Random Sampling were the criteria for mixed sampling based on the targeted population characteristics.

Qualitative samples of 6 police officers assigned to a focus group, 13 senior government and corporate officials for in-depth interview. Questionnaires, percentage, mean, standard deviation, t-test and ANOVA were used for data collection and analysis. Samples size was calculated from 123 persons with the application of Yamane formula (Yamane, 1967) and final samples were 95 police officers under the Jurisdiction of the Technology Crime Suppression Division, mainly, operation level and experienced working in collecting computer crime evidence.

Questionnaire Development and Measurement

The quantitative survey method was conducted by distributing the questionnaires to selected samples participate in the study. The questionnaire was divided into two parts.

Part 1 was proposed to collect the respondents' demographic information such as gender, age, level of education, monthly income level of the respondent, including closed-ended questions that the respondents were asked to provide their rating on their perception using a five-point Likert Scale measurement that ranged from 1=strongly disagree, 2=disagree, 3=neutral, 4=agree, and 5=strongly agree for measuring level of opinion on the police officers under the jurisdiction of Technology Crime Suppression Division collecting digital evidence (Panpinit, 2006).

Part 2 included open-ended questions to allow the respondents expressed their opinions, and provided suggestion freely on the development of guidelines in digital evidence collection of the Technology Crime Suppression Division.

The acquired data was subjected to interpretation of results, summary of problems and obstacles in collecting digital evidence on subject of online shopping fraud of the Technology Crime Suppression Division as well as forming the guidelines for further operation in collecting digital evidence.

Research Results

Origin of Online Shopping Fraud

As the internet continues to reshape consumer purchasing habit, with retail apps and social media stores, cybercriminals are also keeping pace. The typical shopping scam starts with attractive bargain and a bogus website or, mobile app. Some imaginary e-stores are invented purely just to scam the public, and many mimic trusted retailers, with familiar logos and slogans and a URL that's easily mistaken for the real thing.

The research findings suggest that Digital Evidence online shopping fraud occurred when buyer and seller used the device such as Computer, Smart Phone and Tablet to conduct activities, followed by the Internet Service Provider provided a service when the user has own device joined the Internet network to access computer system at the end and lastly,

the user connected the equipment from Internet network to computer system at the end trail such as Social Network, e-Marketplace, e-Classified or Internet Banking to advertise selling products, agreed on the sale transaction, including transfer fund for merchandise payment and most of times, which evident in a Log File.

The start of collecting digital evidence online shopping fraud is categorized into communication trail such as communication and telephone, financial trail such as Bank Account, Internet Banking and e-Money and shipping and delivery trail is the evidence on delivery and receiving merchandise such as receipt on delivered merchandise and the merchandise authorization.

Revisiting the Research Questions

The aim of this study is to investigate the factors that contribute towards online purchases fraud, study problems and obstacles while gathering evidence to develop guidelines for collecting digital evidence by reviewing the applicability of a selection of theories and documents from the discipline of criminology and online shopping fraud related. As outlined earlier, online shopping fraud encompasses a range of elements depending on the nature and intention of the offender. The research will also focus on online interactions and related behaviors to answer for the formulated questions, the research questions are then re-stated as to supply answers.

Q1: What are problems and obstacles in collecting digital evidence of online shopping fraud of the Technology Crime Suppression Division?

Problems were found in 5 areas:

1. Body of Knowledge

The overall results indicated high level of knowledge among the police officers of the Technology Crime Suppression Division found with the Mean 3.53 and the item with the highest Mean of 3.67 regarding knowledge on laws, followed by Mean 3.49 on knowledge regarding evidence and 3.42 on network knowledge, respectively.

As for the body of knowledge regarding the laws, it was found that the police officers had knowledge and understanding on the elements of offence as related to online shopping fraud.

Also, the findings suggest that the police officers understood the rules for maintaining Creditability of evidence, Chain of custody and Evidence validation as well as effectively operate Website and Internet application, Social network, internet function system, Domain name, URL, IP Address, work and its use, e-Classified.

The findings reveal that the police officers of the Technology Crime Suppression Division have sufficient knowledge in law, evidence collection by learning and practicing until

able to develop, and accumulate essential knowledge and work experience. The police officers of the Crime Suppression Division of the Ministry of Science and Technology are regarded as a specialized unit in the field of computer crime. They are, the only unit of the National Police in charge of eradicating technology crimes, hence, they should have knowledge at the highest level for effective performance and they should always be on constant training to maintain expertise and the maximum knowledge level for efficient duty.

Even though these police officers have a high level of knowledge, the findings from quantitative research suggest that they had high opinions regarding problems with knowledge management at the Mean of 3.52 and consistent with the outcomes from focus group discussion and in-depth interview. Problems were also found regarding the police officers approach to accumulate cumulative knowledge from their work experience and a lack of organizational support to set up proper systematic knowledge transfer and training. Moreover, the timing of the provided training was insufficient since most police officers were on duty at the training time so they could not attend all training courses. Quite often the police officers must acquire their own knowledge from self-training which is time consuming. If the Technology Crime Suppression Division can provide suitable training courses to transfer information, knowledge, and information and set up a systematic approach for disseminating knowledge, it will make staff work more efficient. Moreover, the division needs to enlist a field specialist or appointed expert to advice on inquiry, investigation, prove of evidence and other police-related works so that the police officers could seek consult in various areas.

2. Division

The findings on division related problems suggest the police officers had a high opinion on division problems, having the Mean of 3.62 which coincided with the focus group discussion and the in-depth interviews that mentioned shortage of personnel and the police officers to handle the workload. Besides, the job rotation from personnel administration disrupted the work flow, making the police discontinued gathering knowledge, and build up skill in performing tasks. Regarding the appointment in the division, there should be specific guidelines for qualification such as passing the test of the division or possessing technological knowledge.

The division is responsible for handling technology crime cases in Thailand. Even though the victim could file the complaint with the police officer in such jurisdiction, the public have more confidence in the work of the Technology Crime Suppress Division. Moreover, the inquiry officer at the station usually that the victim files a complaint with the division. This makes a heavier workload for the division since they only have 162 police.

Also, the rotation of personnel had disrupted the learning process of the police officers who try to accumulate knowledge and develop their skills.

3. Cooperation

The findings suggest that problems in gaining cooperation were rated at a high level, with the Mean 3.54, mainly lacking cooperation from the Mobile Service Provider, the Internet Service Provider (ISP) when receiving the request for Log File from the police officer but delay sending data, including the service provider of e-Money who failed to cooperate with the police officer receiving the request for account data and statement, including Log File for accessing e-Money system. Collecting digital evidence online shopping fraud is the crucial beginning of gathering other evidence that is the Log File that the police officer must send the request to the service provider involved. According to the Computer Crime Act B.E. 2550 (2007), the service provider or business operator must keep the Log File open and available for the officer to inspect for at least 90 days, often the police officer received delayed data from the Internet Service Provider beyond 90 days which disrupted the connection to other evidence.

4. Legal

The study on legal problems indicated the existence of problems at a high level, having the Mean 3.55, and the most found problem on the legal authority of the competent officials with the Mean of 3.56 and the Mean on rules, regulations, principles and practices equaled to 3.53.

Regarding legal authority problems, it was found that the service provider who received the request for data on the offence and Log File may refuse to give information to non-official officers appointed by the Computer Crime Act B.E. 2550 (2007), Section 18. The Act itself specified that the service provider must act immediately after receiving the request or within the specified times at least 7 days or not exceeding 15 days in which the Internet Service Providers were often delayed sending the data to the police officer within the specified time. Further from the police officers in requesting Log File due to the legal interpretation of the Computer Crime Act B.E. 2550 (2007), Section 18 (1)-(3) such as questioning or calling the third party involved or sending the explanation on Log File. Because the Act has clearly prescribed the appointed officials' authority, it had obstructed the investigation in collecting evidence base on the code of conduct when some service provider refused to give up information. As for the service providers, they must act per request immediately at least in 7 days or not exceeding 15 days. If the Internet Service Provider and the Mobile Service Provider failed to act within the specified time, the Act already imposed the penalty, but there had not been any prosecution case by the officials caused problems to the case proceeding and unable to apprehend the suspect.

The impact from having the Computer Crime Act B.E. 2550 (2007) and the State policy with the Freedom of Speech suggest that the officials' request of data from the service providers of IP Address received cooperation if only the officials were appointed legally.

Regarding problems on rules, regulations, procedures and practice, it was found that the registration for Prepaid to confirm the user identity was lacking control for effective operation, having the registration for each other that could be the loophole for committing the offence. Internet Service providers and Internet access providers such as Internet Café, Game Online, Coffee shop, Restaurant, Hotel, Dormitories mostly had not kept Log File as required by laws and the service provider in e-Money lacking the program Know your Client (KYC) to confirm identity of the users enough and appropriate so that the offender could use such loophole to committee the offence. The problems on rules, regulations, principles and practice as the guidelines for the Telephone service providers, Internet service providers and e-money service providers need the control to ensure that those providers comply with the laws. As a matter of fact, the law prescribes the preventive measures for the offence, but the agencies involved neglected to follow as well as the state agencies responsible for law enforcement had not actively exercise their authorities, causing damages. As for the problem on registered telephone number for each other and lacking the identity verification system for the users of e-Money, the quantitative research results matched the focus group discussion.

5. People Awareness

The findings from the in-depth interviews suggest that the public lack of awareness in keeping their own identity confidential by opening the bank accounts to allow the using such bank account in exchange for minor compensation, also registering own telephone number for the culprit to use, which may become criminal offense. This finding coincides with the National Strategies on Anti-money Laundering and Combating the Financing of Terrorism B.E. 2560-2564 (2017-2021) that found that some Thais became the criminal's instrument for committing online business fraud through e-commerce by opening a bank account. Often, it is the buyer and seller's carelessness neglecting to check the payment thoroughly, leaving the loophole for the culprits to commit fraud by disguising themselves as the online seller and buyer.

The quantitative study outcomes indicated overall knowledge level of the police officers' was at a high level, their opinions regarding assessment of their own knowledge and at the end of questionnaires also suggested that they lacked knowledge and understanding in collecting evidence and there was no field expert to provide advice. Suggestions were made to build officers' knowledge in investigation and evidence collection as well as arranging training for the police officers in the line of work for the officers to work extensively. As for the outcomes from the focus group discussion, it was found that frequent promotion and relocation of the police officers caused discontinuity in accumulating experience. Moreover, the Division lacked a proper system of Knowledge Management as well as the technique in transferring knowledge. The recommendations from the focus group discussion are that the division give priority to Knowledge Management by having the division personnel, with work

experience help to build knowledge for work as well as transferring knowledge. At the same time, staff should have the incentive to develop knowledge for work in order to seek career advancement. The In-depth interview results suggest most police officers lacked the proper knowledge in collecting digital evidence enough to start the case and unable to continue collecting evidence.

The in-depth interview suggested the need for increasing development of specific knowledge for actual practice in collecting evidence through rules, regulations, procedures and principles of laws for manual preparation, as well as arrange training to transmit knowledge to the officers. The qualifications for a specific position must be clearly stated especially the qualification in information technology and communication, leading to career advancement.

Q2: Which directions were chosen for administering procedures on collecting evidence related to online shopping fraud of the Technology Crime Suppression Division?

To answer Q2, directions for the Management of Digital Evidence Gathering Concerning Online Shopping Fraud of the Technology Crime Suppression Division had been developed and suggested mainly in the Knowledge Management area.

Steps for Police Officers Collecting Digital Evidence

The digital evidence collecting process began when the victim filed their complaint with a police officer. The police officer then conducted an inquiry of what actually happened during the online shopping process. The initial evidence presented to the police officer consisted of sale advertisement of merchandise the victim bought, the record of conversation and phone number of the offender and the evidence or copy of transfer payment. After the police realized the trace advertised on Social Network, e-Marketplace or e-Classified, a letter requesting details on the advertise and log file was issued and sent to the advertiser, including the Log File, first name-last name, address, e-mail, telephone number, bank account information and the payment methods. Besides the advertise on selling merchandise, the communication trail allow the direct communication such as contact thru Instant Messaging (IM), namely Facebook Messenger, Line Chat and Telephone contact which are all the trace to confirm the offender.

After knowing the Log file information to access the computer, the police officer proceeded with checking the IP Address from the Internet Service Provider (ISP) anyone to call for data, detail of the user of IP Address as appeared in the Log File from the Internet Service Provider.

Another crucial piece evidence that leads to the offender is the Financial Trail in which the police officers received this fact from the victim, which is the evidence of payment for

merchandise, either the pay-in slip ,or e-Payment via Internet Banking, e-Money and Payment Gateway that indicated the account of recipient, date time and amount.

Both Log File and Internet Banking would show IP Address and the police officer can check the Communication Trail to accompany the actual evidence. Internet banking stores data of IP Address and the system access and enables the police to identify the culprit as well. Another type of evidence is the shipping and delivery trail accompanied to confirm whether the merchandise had been delivered.

Discussion

Criminal Cases Management

The online shopping fraud evidence collection begins when the victim comes to see the police officer to file the complaint against the offender. Once the evidence for the investigation have been established for fraud with complete element of illegal action, enables to identify the offender. Nonetheless, it was found that the victim delay filing the complaint beyond the time lapse on requirement to keep Log File, then, the police office was unable to check the data for apprehending the offender. The findings from quantitative and qualitative studies, the focus group discussion, and the in-depth interview indicated that knowledge in computer and Information Technology network, including knowledge of laws, regulations and principles of law can be formulated into guidelines for collecting digital evidence.

1. As soon as the victim files a complaint, the officer begins an inquiry to consider if the case is online shopping fraud as stated in the Computer Crime Act B.E. 2550- before proceeding to collect evidence.

2. Consider the case details by making the inquiry with the victim regarding when and what type of merchandise, price and the method of payment. The police officer issued a letter to the Webmaster to request detail on advertise, advertiser data and IPO Address. A registered member system should provide the name of the user, address, E-mail, telephone number, bank account or channel of payment. The IP address was subjected to check for the place of Internet Service Provider (ISP). The user IP Address was called with the detail of the user as well as user telephone number. The victim detail of account owner, name, address, telephone number, statement, the Internet Banking Application and the shipping and delivery were used as the evidence to confirm the delivery of merchandise and receiving merchandise.

3. In the case which the evidence could be found and gathered, the police officer must send the evidence for validation to seek the truth. The outcome from validation would be used to link with other evidence, which required the experts and specific process for digital evidence validation. The police officer may sent the evidence at the following place

1) Technology Case Support Group, Technology Crime Suppression Division and 2) Computer Crime Forensic Group, Central Forensic Section, Office of Forensic Science.

4. After the evidence was collected at the site based on the set procedures and the reason to believe who committed the offence established, the police officers would issue a warrant to call a suspect for questioning. If the suspect failed to show up, the police officer can request warrant of arrest to track suspect to make the arrest. Figure 3 illustrates the trial of site evidence.

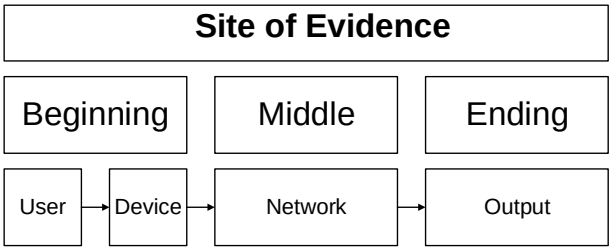

Figure 3 Site of Evidence

Source: Constructed by the author from interviewing and gathering information

Research Conclusion and Recommendation

The research finding indicated that the investigation to collect evidence online shopping fraud began with the victim came to file the complaint on the offender to take legal action.. As soon as the police officer received the complaint, he started to gather evidence to determine the facts in the fraud case. In the beginning, the advertiser announced the sale of merchandise through a Social Network such as Facebook, Timeline of Line, Instagram, and e-Marketplace such as Lazada, Lnwshop or e-Classified such as Kaidee, Pantip Market. When the prospect buyer found the advertisement and became interested in buying the merchandise, the prospect buyer contacted the seller through various channels such as Instant Messaging (IM) for example, Facebook Messenger, Line Chat, telephone communication between buyer and seller agreed on the sale transaction, making the payment through bank counter or e-Payment such as Internet Banking, e-Money, or Payment Gateway.

Validation of facts based on the digital evidence that the police officer collected with the authority of the competent officers based on the Computer Crime Act B.E. 2550 (2007) to call for data from the third party involved (Vichitcholchai . 2007) is explained as follows.

1. Communication trail is to prove the existence of the offender through the advertise for sale of merchandise in the computer system, website, the communication methods, agreement on the transaction, the type of merchandise, price and payment method

by requesting data from the Inter Service Provider. Mobile Service Provider Webmaster, Internet Café, and Game Online.

2. The financial trial is used to prove merchandise payment method, and recipient by requesting information from the Bank or Payment Gateway.

3. The shipping and delivery trail is used to prove the shipping of merchandise to the buyer by collecting data from a Log File.

Examining the evidence from the Communication Trail collected at the outcomes of ending system of Log file to find which IP Address came from which Internet Service Provider, the middle system comprised of the Network. The internet service providers have the data, time identified IP address available and thus able to tell who the user is, and this may lead to the arrest of the offender. Another piece of evidence in online shopping fraud is the financial trail which can prove that the offender acquired property or money illegally from the buyer through the record of bank transfer funds.

Ramifications for online shopping fraud prevention

There are certain implications for fraud prevention strategies based on the data in this search. Throughout the next section, suggestions are made for potential approaches to prevent online shopping fraud.

Recommendations

To facilitate the police operation, it is helpful to set procedures for gathering the following information.

- Complainant's details – including name, date of birth, age, address, phone number, email
- Summary of allegations – prepare a summary of events in chronological order
- Evidence – include a brief description of the evidence which support the events described
- Suspect/offender –a particular individual, provide details such as date of birth, age, address, phone number, email
- Witnesses – provide details of any witnesses, including name, address, phone number and a brief summary why this person is a witness

In addition to the aforementioned suggestions, the researcher recommends the following actions:

1. Appoint the Work Committee among members including the field specialists in collecting evidence. For example, the police officers from the Technology Crime Suppression Division, the office of Forensic Science and the Ministry of Digital Economy and Society, including the prosecutor together had collected knowledge in performing legal and related

network tasks, information technology, evidence and knowledge in other practical relevant areas. This collection was conducted for preparing the manual for laws, regulations, and practical guidelines on collecting digital evidence online shopping fraud for the division officers.

2. Provide training on a regular basis to transfer knowledge, including the appointment of specialist for advice in performing tasks, including support for the police officials in the same line of work to advance in their career as well as continue to update their knowledge for work efficiency.

3. Inform the public of the necessity to file fraud complaints immediately for the benefit of collecting evidence as well as arrange the request form for the victim to describe the incident in detail and prepare the primary evidence as the data to assist the police officer in investigation to speed up the process.

4. Organize collaboration among third parties involved since most police officers argued that the Internet Service Provider, Mobile Service Provider had not given full collaboration with the police officers from delay sending data on Log File or returning the answers beyond the90 day legal requirement to keep log, making the police officers unable to verify data. The Central Computer System should collaborate with the Technology Crime Suppression Division and the service providers of different computer systems in transmitting evidence data for effective and quick operation.

5. Seek collaboration with the service providers who had in possession the evidence for online shopping fraud consisted of beginning, middle and ending trails for the Internet Service Provider, e-Marketplace and e-Classified, including Social Network and Instant Messaging (IM), Internet Banking, shipping and delivery providers to speed up the data delivery.

6. Engage the Ministry of Digital Economy and Society in supporting frequent use of Information Technology (The Ministry of Digital Economy and Society: http://www.mdes.go.th/view/Ministry-related) to gather digital evidence online shopping fraud, through training and appointment of competent police officer as the encouragement to boost their morals as well as giving priority to validate the delivered evidence to speed up the legal process.

7. Raise public awareness on the-necessity to take the time to check the seller and buyer creditability before making the decision to buy. Importantly, online shoppers need to pay close attention in preserving their own identity, as well as not allowing anyone to use their personal information to open an account. This may constitute a criminal act and eventually work against them.

Research Overview

Due to technological innovation, the Internet has fundamentally changed consumers' ideas on convenience, speed, price, and product and service information. Buyers love online trading for its convenience, while sellers benefit from lower costs and a greater reach than a physical store provides. To ensure that both parties continue to benefit from online commerce, it must remain a safe and secure channel, allowing legitimate consumers' access as needed. Although online shopping has brought consumers a lot of advantages, there are some negative concerns as well. This study discusses the detection and investigate aspects of fraud as well as providing a workable framework for dealing with the existence of online shopping fraud and its implications. As a matter of fact, prevention and detection of online shopping fraud complement and supplement each other, nonetheless, both are difficult tasks because fraudsters always come up with newer ideas of fraud whenever old ideas get detected by fraud detectors. One crucial goal of this thesis is to expand on a current field of knowledge and explore various venues. Apparently, researching the topic of online shopping fraud is an ongoing investigation as the field is constantly evolving, and with the rapid speed of technological advancements, new forms of criminality are bound to develop. New theories, methods and techniques in criminological research are expected. Therefore, it may be suggested that the most effective approach begins with the profound study in various relevant issues to seek more alternatives in dealing with the obvious problems. Results from this study could be very useful to develop strategies for organizations and businesses interested in preventing e-commerce crimes. By implementing proper strategies, businesses could reduce their umber of losses thus increasing their businesses' sustainability. There is still a lot of research that needs to be done in this area for our society to benefit and become aware of various types of newer fraudulent activities happening day by day in the online commerce. We need to seek ways to safeguard individual assets through citizens' collaboration with the police and other relevant agencies. Because the police officers have a key function and authority in keeping peace, maintaining public security and safety, as well as preserving common property for citizens, the work effectiveness of police officials is then extremely crucial. If the police officers have high effectiveness, awareness, and alertness in their work performance, it would positively affect the Royal Thai Police and the country's developing social and economic system.

References

Act B.E. 2560 (No. 2). (2017). Regarding the offence related to the Computer Crime Act B.E.2550, Graduate Studies, Mahidol University, Ph.D. (Criminology).

Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2009). *Fraud Examination* (3rd ed.). Ohio: South - Western Cengage Learning.

Amornpinyokiet, P (2010). *Explanations on the Computer Crime Act B.E. 2550*. Bangkok: Provision Publishing.

Arnusasananun, V. (2007). *The Investigation officers' authority in collecting electronics evidence: A comparative Study between Thailand and U.S.A*. Bangkok University. Bangkok.

Association of Chief Police Officers. (2009). Good Practice Guide for Computer-Based Electronic Evidence. Retrieved February 27, 2016, from https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence[1].pdf

Boonthum, K. (2002). *Social Sciences Research Methodology*. Bangkok.

Bunting, S. & Wei, W. (2006). *The OFFICIAL EnCE: EnCase Certified Examiner Study Guide* (pp.126). Indianapolis: Wiley Publishing.

Chalermchai, L. (2009). *The Development of Evidence Collection and Storing Electronic Evidence* (Master of Sciences). Rangsit University. Bangkok.

Clough, J. (2010). *Principles of cybercrime*. Cambridge, UK: Cambridge University Press.

Duffield, G & Grabosky, P, (2001). The psychology of fraud. *Trends & Issues in Crime and Criminal Justice*, *199*, 1-6.

Electronic Transactions Development Agency (Public Organization). (2015). (Draft) Standard Practice in digital evidence validation, Bangkok, The Ministry of Digital Economy and Society.

Jintasathien, C. (2010). *Overrule on non-admissible evidence acquired illegally based on Section 226/1 Code of Law on Criminal Procedures* (Unpublished Thesis, Master of Laws). Thammasat University, Bangkok.

Kasaemsaeng, S. (2000). Problems and Obstacles in Performing Tasks of the police officials regarding the Suppression of Corruption and Misconduct among the officials.

Kim, D. J., Ferriny, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, *44*(2), 544-564.

Kitpreedaborisut, B. (2002). Social Sciences Research Methodology. Bangkok: Books Center, Chulalongkorn University Chadarat Pipatnun (2011). Computer Crime Act

B.E. 2550 section related to the Office University of Thai Chamber of Commerce Journal*, 31(2),* 142-157.

Kittisomboon, N. (2006). *In Search of Evidence from private information from Electronics Data in Computer Crime* (Unpublished Master of Law). Dhurakij Bundit University. Bangkok.

Kittivarakul, S. (2012). *The Impacts of Freedom of Speech Concepts with the police arrest, A comparison between Thailand and the People Republic of China* (Master of Laws). Chiangmai University. Chiangmai.

Kovacich, G. L. (2008). *Fighting fraud: how to establish and manage and anti-fraud program*. London: Elsevier Academic Press.

Kruse, W. G. & Heiser, J. G. (2002). Computer Forensics: Incident Response Essentials. Indianapolis: Addison-Wesley.

Kulnithet, N. et al.. (2013). *Network and Knowledge Management in Computer Crime*. Suan Sunandha Rajabhat University. Bangkok.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C-S. (2005). Beyond concern: a privacy-trust-behavioral intention model of electronic commerce. *Information & Management, 42*(2), 289-304

Lu, Y., Yang, S., Chau, P. Y. K., & Cao, Y. (2011). Dynamics between the trust transfer process and intention to use mobile payment service: a cross-environment perspective. *Information & Management*. *48*(8), 393-403.

Ma, G., Wang, Z., Zou, L., & Zhang a., Q. (2011). Computer Forensics Model Based on Evidence Ring and Evidence Chain. The Central Institute for Correctional Police. *Procedia Engineering*, *15*(2011), 3663 – 3667.

Seecharoen, M. et al. , (2010). *Guidelines in developing higher education and Excellence in Police Career*. The Thailand Research Fund. Bangkok.

Mandia, K., Prosise. C., & Pepe. M. (2003). Incident Response & Computer Forensics (2nd ed.). (pp.200-206). McGraw-Hill/Osborne: California.

Mukherjee, A., & Nath, P. (2007). Role of electronic trust in online retailing: A re-examination of the commitment-trust theory. *European Journal of Marketing*, *41*(9/10), 1173-1202.

Na Na Korn, K. (2006). *Code of Conduct Law. Published* (7th ed.). Viyuchon Publishing: Bangkok.

Naetivanich, V. (2008). *Manual for Legal and Information Technology Communication*. Kampaengpetch: Srisawat Printing Co., Ltd.

National Statistical Office (2016). *Survey of Household Use of Information Technology and Communication 2015, March 1st 2016*. Retrieved from http://service. nso.go.th/nso/web/survey/surtec5-1-3.html.

Newby, T. , & Carroll, O. (2008). Rethinking the Storage of Computer Evidence. Retrieved February 27, 2016 from https://www.justice.gov/sites/default/files/usao/legacy/2008/02/04/usab5601.pdf

Ngamsaeng, N. (2004). *Computer Crime: A Case Study on Factors affecting Internet Crime* (Unpublished Master Thesis, M.A). Thammasart University.

Office of National Broadcasting Telecommunications Commission. (2016). *Market Analysis on Thai Fixed Broadband Market*. Bangkok.

Pedneault, S. (2009). *Fraud 101: Techniques and Strategies for Understanding Fraud*. New Jersey: John Willey & Sons, Inc,.

Research Group, Strategy Police Office. (2016). *Research for developing investigation and inquiry process of the Police Officers to combat computer crime*. Royal Thai Police, Bangkok.

Ruijiravinijchai, K. (2014). *Developing Effectiveness in Administering Investigation of Metropolitan Bureau, Royal Thai Police*. Unpublished Dissertation. Public Administration, Eastern Asia University, Pathumthani.

Silverstone, H., & Sheetz, M. (2007). *Forensic accounting and fraud investigation for non-experts.* Hoboken, New Jersey: John Wiley & Sons, Inc.

Scientific Working Group on Digital Evidence (SWGDE). (2014). *SWGDE Best Practices for Computer Forensics Version: 3.1*. Retrieved February 28, 2016, from https://www.swgde.org/documents/Current%20Documents/20140905%20SWGDE%20Best%20Practices%20for%20Computer% 20 Forensics%20V3-1.

Software Alliances. (2015). *Computer Crime*. Retrieved from https://www.microsoft.com/thailand/piracy/cybercrime.aspx.

Suksri, S. et al. (2012). *Affects from the Computer Crime Act B.E. 2550 and the State Policies with the Freedom of Speech, Internet for the public (iLaw).* Thai Volunteer for Service. Bangkok.

Sukhum, S. (2000). Factors Affecting Computer Crime Prevention of the police Office at the Economic Crime Suppression Division (Unpublished Master of Sociology). Chulalongkorn University, Bangkok.

Tung, F-C., Chang, S-C., & Chou, C-M. (2008), An extension of trust and TAM model with IDT in the adoption of the electronic logistics information system in HIS in the medical industry. *International Journal of Medical Informatics*, 77, 324-335.

United States Department of Homeland Security, United States Secret Service. (2006). Best Practices for Seizing Electronic Evidence v. 3 A Pocket Guide for First Responders. Retrieved February 27, 2016 from, https://info.publicintelligence.net/Usssbestpractices.pdf.

UNODC. (2013). *Comprehensive Study on Cybercrime, Retrieved August* 20, 2015 from, https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

Unsri, V. (2001). *Problems on collecting Electronics Evidence in the Criminal Case.* (Unpublished Master of Laws). Thammasat University, Bangkok**.**

Vichitcholchai, P. (2007). *Explanation for the Computer Crime Act B.E. 2550*, Retrieved from http://www.chandra.ac.th/th/doc/ICT/ban.pdf amended by the Computer Crime.

Vithitanon, V. (2006). *Criminal Investigation*. Retrieved from http://wutthi.central.police.go.th/images/510912/510912a.pdf.

Yamane, T. (1967). Statistics, an Introductory Analysis (2nd Ed.). New York: Harper and Row.

Yungyuen, S. (2015). *Computer Crime*. Retrieved from http://202.29.22.164/e-learning/cd-1687/HUM07/topic3/linkfile/print5.htm.