

Pattern analysis of fraud case in Taiwan, China and Indonesia

A H Kusumo¹, C-F Chi² and R S Dewi³

¹Department of Industrial Engineering, University of Surabaya, Raya Kalirungkut, Surabaya 60293, Indonesia

²Department of Industrial Management National Taiwan Univ. of Sci. and Technology 43 Keelung Road, Section 4 Taipei, Taiwan 106

³Department of Industrial Engineering, Sepuluh Nopember Institute of Technology, Kampus ITS Keputih, Sukolilo, Surabaya, Indonesia, 60111

Email: argohadi@gmail.com, chris@mail.ntust.edu.tw, ratna.sari.dewi80@gmail.com

Abstract. The current study analyzed 125 successful fraud cases happened in Taiwan, China, and Indonesia from 2008 to 2012 published in the English online newspapers. Each of the case report was coded in terms of scam principle, information media (information exchange between fraudsters and victim), money media (media used by fraudsters to obtain unauthorized financial benefit) and other additional information which was judged to be relevant. The Chi-square Automatic Interaction Detector (CHAID) was applied to the coded data of information, scam principle and money media to find a subset of predictors that might derive meaningful classifications. A series of flow diagrams was constructed based on CHAID result to illustrate the flow of information (scam) travelling from information media to money media.

Keywords: coding scheme; flow diagram; CHAID

1. Introduction

Fraud can be associated with injury. One person can injure another either by force or through fraud. The use of force to cause bodily injury is frowned on by most organized societies; using fraud to cause financial injury to another does not always carry the same degree of stigma or punishment [1]. The internet crime complaint (IC3) received more than 250.000 complaints every year associated with the internet crime reaching the amount of one billion in 2015 [2].

A cyber scammer can operate in multiple countries on multiple victims in parallel. A single person or a unit of individuals can realize a large remuneration for the smallest possible investment of time and effort, even when such syndicate might be loosely-coupled and geographically distributed. Whilst there is a constellation of classification schemes available, a consistent classification framework is seemingly nonexistent. Some themes seem to be agreed upon throughout the current literature [3]. Laleh and Azgomi [4] proposed taxonomy of different kinds of frauds including credit card frauds, telecommunication frauds, insurance frauds, internal fraud, computer intrusion, web network fraud and customs frauds. Other taxonomy by Wang, technology-based financial fraud offences, can be divided into two categories: system attacks and non-system attacks [5]. However, variance of taxonomy is difficult for comparing sensible transnational or conceiving coordinated operations. To



aid in the detection and interception of fraud, a clear and consistent classification scheme needs to be developed.

For classification, the coding scheme is designed to be mutually exclusive individually but complete collectively [6]. A total of 125 successful fraud cases happened in Taiwan, China, and Indonesia from 2008 to 2012 in the English online newspaper were coded and analyzed based on a classification scheme.

Online newspapers as web based computerized data were also being used in several researches. A content analysis of the top 100 circulated daily newspapers in the United States was conducted to provide an understanding as to the current status of these online newspaper sites. A number of categories were examined including newspaper circulation size, updateness, cross media partnership/ownership, and level of convergence [7]. Poria also explored the possible uses of online news discussions that emerge following the publication of news on the Internet [8].

The current study proposed CHAID analysis and Flow Diagram to analyze fraud cases. The CHAID Analysis (Chi Square Automatic Interaction Detection) was applied to the coded data of fraud cases to select the independent (predictor) variable that had the strongest interaction with the dependent variable. Categories of each predictor were merged if they were not significantly different with respect to the dependent variable. The data flow diagram (DFD) was a good process model for such a visualization technique because of its strong hierarchical structure and due to the fact that it was a classic tool for process analysis [9].

A series of flow diagram was constructed based on the information media and money media to illustrate how the fraudsters exchanged information with the victims and how the fraudsters obtained unauthorized financial benefit similar to the prevention of electrical injury [10]. Each of the flow diagrams could be directly linked with feasible prevention strategies by cutting the flow of information or money.

2. Materials and methods

The current study analyzed 125 successful fraud cases happened in Taiwan, China, and Indonesia from 2008 to 2012 in the English online newspaper. This study used the following internet search engines to locate newspaper in each country: Google.com. The case reports were obtained by searching online newspaper with the terms “fraud” and “scam”.

The articles used in this study were chosen based on three criteria as follows [11]: First, Duplicated or reprinted stories eliminated the number of articles included in this study significantly. Second, the case report had to contain information about scam principle, information media and money media. If the critical information were not available in English, it had to be discovered from other sources such as newspapers published in Chinese or Bahasa. Third, articles presented unsuccessful case of fraud or announcement from any institutions were discarded. These kinds of articles were common in the online newspaper. Besides, traditional frauds such as corruption, insurance scam, investment scam, magic/special power ability, trading was also excluded from the analysis.

Using the inclusion criteria above, articles describing specific incidents of fraud and scam could be identified. Articles which did not meet these criteria were eliminated. By only analyzing specific newspaper articles, the report of this issue could be examined. The list of English online newspapers in Taiwan, China and Indonesia is shown in Table 1.

Table 1. English online newspapers in Taiwan, China, and Indonesia.

Country	Newspaper
Taiwan	China Post; The Taipei Times; Taiwan Economic News; Taiwan Today
China	China.org.cn; China Daily; China News; Economic Observer; Global Times; People's Daily; Shanghai Daily
Indonesia	Inside Indonesia; The Jakarta Globe; The Jakarta Post; The President Post; Tempo Interactive

CHAID and flow diagram were used to identify feasible prevention measures from each distinguishable pattern of flow diagram. The coding scheme was designed to be mutually exclusive individually but complete collectively. The coding schemes were developed based on the flow of scam from fraudsters to victims as shown in Table 2, in terms of scam principle, information media, and money media as variables. However, victim's age and gender were difficult to be defined due to insufficient data in the online newspaper. Besides the ones mentioned in each case, there were many people becoming a victim.

Table 2. Developed coding scheme.

Coding Scheme		Detail
Scam	Principle [12].	• Distraction Principle (Advance fee/price/lottery) • Social Compliance Principle • Kindness Principle (Charity) • Time Principle (intimidation) • Unnoticeable Scam
	Information media	• Face to Face [13]. • Mobile Phone (Voice and Text Based) [14]. • Internet (Person to person/email and Forum/web) [15]. • ATM fraud [16]. • Other
	Money Media	• Financial gain through money transfer (wire transfer, prepaid money card) • Financial gain through stolen information (loosing bank account debit/credit) • Financial gain through direct hit (cash/product)

3. Results

Our current study focused on CHAID analysis of the Scam Principle: Distraction principle, Social compliance principle, Kindness principle, and Time principle (4 out of 7 principles). Other principles from seven principles were not found in data collection. One more principle was added, which was unnoticeable principle such as hacking, manipulated ATM machine, etc.

CHAID divided total population into more distinct groups, based on categories of the “best” predictor of a dependent variable (i.e. the information media) and split each of these groups into smaller subgroups based on other predictor variables, e.g. scam principle and money media. Scam principles were found to be significant predictor variables and identified as the “best” or most critical predictor ($p < 0.001$) which divided total population in the format of hazard pattern into five different

groups (nodes). Money media were found to be the second critical predictor, and it was nested under the levels of the most critical factor, scam principle.

According to the constructed flow diagram as shown in Figure 1, it can be analyzed that the fraudsters can employ more than one media type to deceive their victims. In many cases on online newspaper can be found that the distraction principles which are advance fee/lottery/prize, romance/relationship scam, and job scam employ almost all media type such as mobile phone (voice and text based communication), internet person to person (email), forum/broadcast (website, etc.), magazine/newspaper, etc. In this principle type, while people are distracted by what grabs their interest, fraudsters can do anything to them and they will not notice it [12].

To deceive their victims, the fraudsters use not only one media, but also more than two or even three information media. From one media to another, the fraudsters must use simultaneously the first media before going to another media. In the example of winning lottery story, Fraudster called the victim via voice communication (phone) saying that they won a lottery. Some of the callers who believed in the sweet talk would send money to the suspect, which was requested by him as tax for their premium. Besides contacting the victim by voice communication, fraudsters also use text messages and emails. They also put the bait about lottery in magazine and newspaper. When a victim is interested, they will call the criminal.

From this flow diagram, the information shows that the fraudsters can obtain money from cash/product (that ended with directly met or "face to face" with the victims) or ask the victims to do a wire transfer from bank or ATM machine (however, the most cases is via ATM) or ask the victim's personal information in a way that the victim must provide credit card number and card security code before their application could be processed. Then they found out that overseas transaction had just been added to his credit card bill.

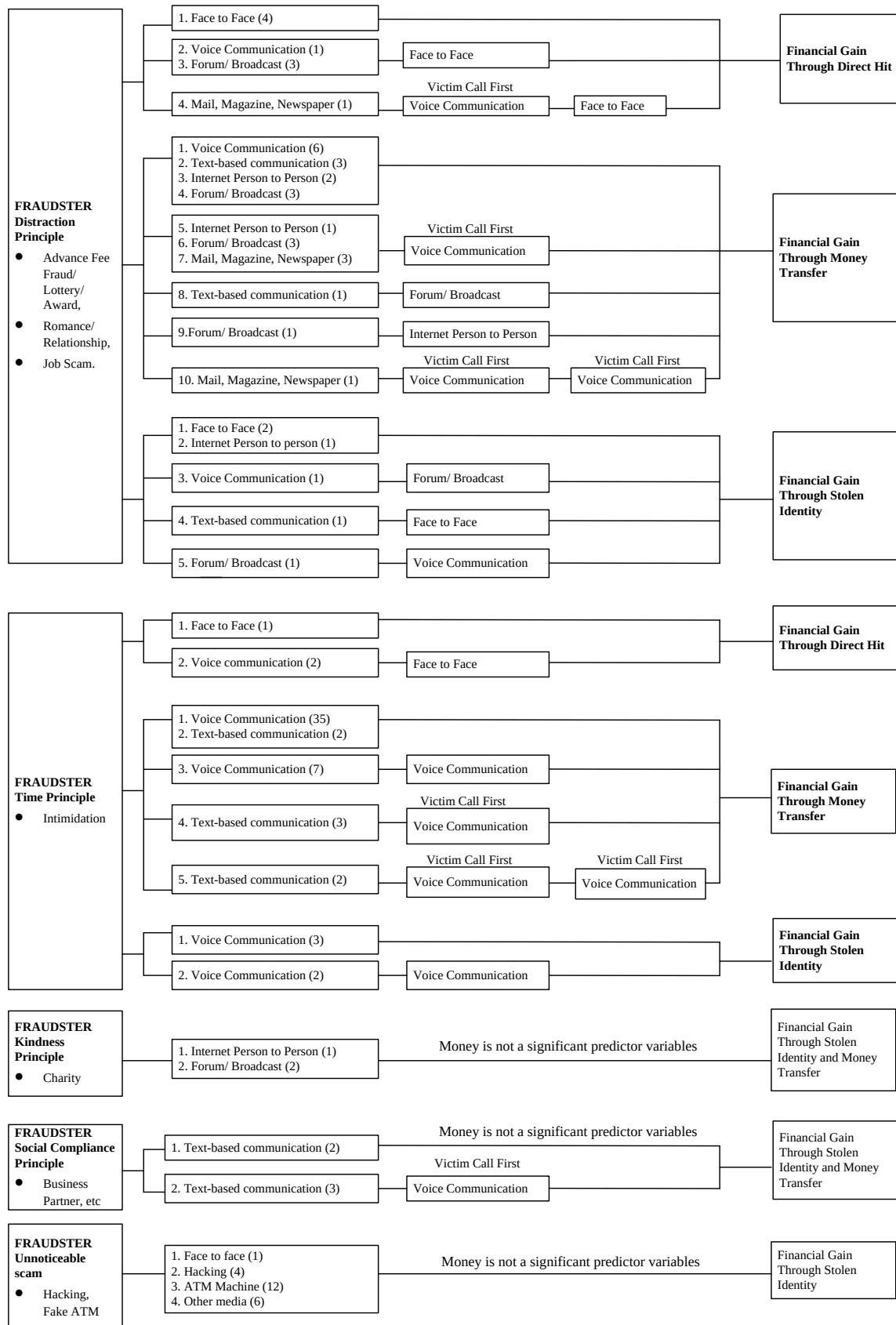


Figure 1. Flow diagram of fraud case.

For time principle (intimidation scam), when under time pressure to make an important choice, people tend to use a different decision strategy. Fraudsters then steer them toward one involving less reasoning [12]. Since there was a time pressure, the media used by perpetrators that can be found in this study was only direct communication media, such as mobile phone. Most of the cases, fraudsters randomly called the victims, but there were several cases that fraudsters only sent the text message. Since the victims were panic, they called the fraudsters first. This principle can also happen "face to face". When it happens, fraudsters ask for cash/products. In this flow diagram, besides cash/product, fraudster can also obtain financial benefit from wire transfer and stolen identity from the victims.

In Kindness principle (3 cases), social compliance principle (5 cases), and unnoticeable scam (23 cases), money media were not found to be a significant predictor variable by CHAID. It is possibly caused by the lack of sample data. However, in this condition, it can be analyzed that the media used for charity scam was found only in internet. Fraudster can obtain financial benefit from wire transfer and stolen identity of the victims.

In addition, in social compliance principle, Fraudsters employed mobile phone since it could convince the victims. For unnoticeable scam, for example, the thief performed the scam through a scam called "card copying" or skimmer. Scammers use some technological facilities to steal the card's data when the cardholder uses it at a particular ATM. The data is copied to another card, which is then used to withdraw money from the account. Photographs of the suspects withdrawing money at the ATMs have been obtained and handed over to the police. Beside using skimmer, they do hacking/phishing, make a fake ATM Machine, ask bank employee's help, set up pinhole camera around ATM, collect the information from customer's receipt, and also get customers' information because they have access on it.

4. Discussion

This study collected 125 fraud cases, but the pattern was not clearly seen. We assumed that if the data was collected more than the current study, it would be possible to show the better pattern. This flow diagram cannot be adopted from electrical injury in that each of the flow diagrams can be directly linked with feasible prevention strategies by cutting the flow [10]. Since it is dynamic, it means that Fraudster can have the other scenario if one scenario is not successful, e.g. if the fraudsters' demand for wire is not successful, the fraudsters can only ask for the private identity.

We also believed that age, gender and psychological factor of the victim contributed to successful fraud, e.g. there were cases that the youngest victims were in their 50s and lived alone. These people were vulnerable as they were generally less familiar with bank-account transfer practices and rules. To get the money, the fraudsters falsely claimed to be police officers, procurators or bank employees, and then persuade them to transfer money into a certain account due to legal problem or lacking personal information.

Other examples, more than 100 people were taken advantage of in the phone sex scam, most of them were men over the age of 50, divorced, widowed, or inexperienced with relationships. The men falling for such scams was desperately looking for love and was easily exploited by a charming woman who was called by them several times a day and showered them with affection. Victims thought that they have found their "dream girl," and many were willing to do everything for the object of their desire. However, victim's age and gender were difficult to be defined due to insufficient data in the online newspaper.

5. Conclusion

People nowadays face a much higher risk of fraud because they interact with various kinds of information media and money media as a technology to connect them.

This study developed a pattern and a flow diagram based on 125 fraud cases reported by online newspaper in Taiwan, China, and Indonesia 2008–2012. Nine patterns of flow diagrams were generated according to information media, scam principle, and money media. The information media had a significant association with scam principle, proven that scam principles were found to be

significant predictor variables and being identified as the “best” or most critical predictor ($p < 0.001$).

Flow diagram has shown that fraudsters can employ more than one information media type to deceive their victims. By using distraction principles, they can employ almost all the information media. However, in time principle, since there is a time pressure, the information media use that can be found in this study is only a direct communication media, such as mobile phone.

References

- [1] Singleton T W and Singleton A J 2010 Auditing and forensic accounting *Fraud Principles* vol 4 ed Rivera S (Hoboken: Wiley) chapter 2 p 40
- [2] Anonymous 2016 *Internet Crime Report* (Washington, D.C.: U.S. Department of Justice)
- [3] Stabek A, Brown S and Watters P A 2009 The case for a consistent cyberscam classification framework (CCCF) *Proc. Symp. and Workshops on Ubiquitous, Autonomic and Trusted Computing (Brisbane)* (Piscataway: IEEE) pp 525–530
- [4] Laleh N and Azgomi M A 2009 A taxonomy of frauds and fraud detection techniques *Proc. the 3rd Int. Conf. on Information Systems, Technology and Management, ICISTM* (Ghaziabad) vol 31 (Cham: Springer-Verlag Berlin Heidelberg) pp 256–267
- [5] Wang J H, Liao Y L, Tsai T M and Hung G 2006 Technology-based financial frauds in Taiwan: Issues and approaches *Proc. IEEE Int. Conf. on Systems, Man and Cybernetics (Taipei)* vol 2 (Piscataway: IEEE) pp 1120–24
- [6] Chi C F, Yang C C and Chen Z L 2009 In-depth accident analysis of electrical fatalities in the construction industry *Int. J. Ind. Ergon.* **39** pp 635–644
- [7] duPlessis R C 2003 *A Convergence of Modes: Present Status of Online News Sites A Content Analysis of 100 Online Newspaper Web Sites* (LA: Louisiana State University)
- [8] Poria Y and Oppewal H 2003 A new medium for data collection: Online news discussions *Int. J. Contemp. Hosp. M.* **15** pp 232–236
- [9] Turetken O and Schuff D 2007 The impact of context-aware fisheye models on understanding business processes: an empirical study of data flow diagrams *Inf. Manage.* **44** pp 40–52
- [10] Chi C F, Lin Y Y and Ikhwan M 2012 Flow diagram analysis of electrical fatalities in construction industry *Saf. Sci.* **50** pp 1205–14
- [11] Archbold C A, Lytle D, Weatherall C, Romero A and Baumann C 2006 Lawsuits involving the police: A content analysis of newspaper accounts *Int. J. Police Strat. & Mgmt.* **29** pp 625–642
- [12] Stajano F and Wilson P 2011 Understanding scam victims: Seven principles for systems security *Commun. ACM* **54** pp 70–75
- [13] Nardi B A and Whittaker S 2002 Distributed Work *The Place of Face-to-Face Communication in Distributed Work* (Cambridge: MIT Press) chapter 4 pp 83–110
- [14] Schiefer G and Decker M 2008 Taxonomy for mobile terminals - A selective classification scheme *Proc. of the Int. Conf. on e-Business (Porto)* (Setúbal: SciTePress) pp 255–258
- [15] Long B and Baecker R 1997 A taxonomy of internet communication tools *Proc. WebNet AACE (Toronto)* (Charlottesville: AACE)
- [16] Utakri N 2007 The phantasm of ATM withdrawal *Proc. 5th Australian Information Security Management Conf. (Perth)* (Perth: Edith Cowan University) pp 207–215.