Pattern analysis of fraud case in Taiwan, China and Indonesia

A H Kusumo[1], C-F Chi[2] and R S Dewi[3]

[1] Department of Industrial Engineering, University of Surabaya, Raya Kalirungkut, Surabaya 60293, Indonesia
[2] Department of Industrial Management National Taiwan Univ. of Sci. and Technology 43 Keelung Road, Section 4 Taipei, Taiwan 106
[3] Department 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