Chapter V
New Technique to Detect CNP Fraudulent Transactions

Adnan M. Al-Khatib
Yarmouk University, Jordan

Ezz Hattab
The Arab Academy for Banking and Financial Sciences, Jordan

ABSTRACT

Money in the e-commerce network, represents information moving at the speed of light, where fraud (digital crime) within the banking and financial services happened very fast and can cost billions of dollars each year-undetected and unreported. In this chapter we present a comprehensive framework that mines and detect fraudulent transactions of Card-Not-Present (CNP) in the e-payment systems with a high degree of accuracy.

INTRODUCTION

Fraud can be described as "a dishonest actions to make false statements in order to gain money or benefit from an individual or from an organization". Electronic systems have increased the opportunity for fraud by providing easy and fast access to the organizations networks. Fraud on the Internet includes several types such as theft of funds through illegal transfers, theft of credit card details, illegal credit card use, and others (Commonwealth of Australia Report, 2000).

Fraud detection is a process that can use data mining techniques to detect fraudulent transaction. In this paper, we propose a comprehensive framework that mines fraudulent transactions of Card-Not-Present (CNP) in the e-payment systems with high degree of accuracy. Our research used the user account profiling techniques to discover fraudulent transactions in CNP payment systems. To detect fraud using profiling technique, it is necessary to determine the normal behavior of each user account with respect to certain indicators, and to determine when that behavior has deviated significantly.

This paper presents an overview of the proposed framework in section 1. Section 2 gives an overview of fraudulent activities in financial area. Section 3 describes our methodology of the system. Section 4 presents and evaluates the results. Section 5 gives an overview of related works. Section 6 discusses the method and compares it with other techniques. Section 7 concludes the research.

FINANCIAL CRIMES

Financial Crimes consists several types of fraud such as: Credit-Card Fraud, Card-Not-Present (Internet credit-card) Fraud, Loan Default, and Bank Fraud (Jesus, 2003). *Credit-Card Fraud* can be a result of a stolen card with the PIN number, or as a result of the theft of an individual's identification (Social security number and home address) in order to create a new account under false or stolen identities. Credit-card theft will defraud the card issuer or merchant. *Card-Not-Present Fraud* like Internet and phone-order sales transactions. They are also time-sensitive crimes. In this type of fraud, thieves leave characteristic footprints. For example, fraud rates increase at certain time of the day, and order coming from certain countries exhibit a higher percentage of fraud. *Loan Default fraud* involves the manipulation and inflation of an individual credit rating prior to performing a "sting", leading to a loan default and a loss for the financial service provider. *Bank Fraud* involves the creation of fictitious bank account for the conduit of money and the siphoning of other legitimate accounts.

The critical factors for detecting all of these financial fraud crimes is to know the behavior of credit, bank accounts, and loan accounts and developing an understanding of the categories of customers. Data mining can be used to spot outliers or account usage that are normal and out of character.

RESEARCH METHODOLOGY

Problem Statement

Our research purpose is "*to present a high accuracy method or prototype to detect Card-Not-Present (CNP) Fraudulent transactions in the e-payment systems by integrating data from multiple databases (e.g., bank transactions, federal/state crime history DBs); and then using suitable and effective data mining and artificial intelligence (AI) tools to find unusual access sequences*". Accuracy means high detection rate (percentage of fraudulent transactions that are detected) and low false positive rate (percentage of normal transactions that is falsely determines to be fraudulent) (Andreas, 2000; Salvatore, 1997).

Researchers have developed two general categories of detection techniques; misuse and anomaly detections. In misuse detection, well-known fraudulent transactions are encoded into patterns, which are then used to match new transactions to identify the fraudulent ones. In anomaly detection, normal behavior of user are first summarized into normal profiles, and then used as yardsticks, so that run-time activities that result in significant deviation from the user profiles are considered as probable fraudulent transactions. In our research we are going to use the user account profiling techniques to discover fraudulent transactions in CNP payment systems. To use this technique three issues arise (Fawcett, 1997):

1. Which transaction features are important? Which features or combinations of features are useful for distinguishing legitimate behavior from fraudulent behavior?
2. How should profiles be created? Given an important feature identified in step 1, how should we characterize the behavior of a subscriber with respect to the feature?

Related Content