Risk Management for Convergent Communications

Version 1.5.1

February 3, 2000

Contributors: Nguyen, Heiss, Embry, Carabelos

BMS Corporation
1999 Broadway Suite 3135
Denver, CO 80202

TABLE OF CONTENTS

Introduction

Fraud is a growing problem that continues to have an enormous financial impact in telecommunications and other industries. Far from its origin as the work of small-time thieves several years ago, today telecommunications fraud is a worldwide sophisticated criminal enterprise. Many telecommunications companies are now discovering that their fraud losses constitute a serious problem that needs to be monitored, managed, and controlled. As a result, industry awareness and a concerted effort to combat fraud are increasing.

Telecommunications Fraud

Booming Industry

Fraud is a booming industry that costs the telecommunications industry around $13 billion per year, a figure that rises 10% to 15% annually. Fraud perpetrators can capitalize on quick and easy money from defrauding the telecommunications industry because of low start-up costs, almost no overhead, and a low margin of consequential risk.

As new telecommunications companies emerge, they are vulnerable to fraud due to the market necessity of obtaining new customers rapidly, which leaves little room for thorough credit management and proper customer screening. Existing telecommunications companies are facing the same type of pressure to gain new customers due to fierce competition in the industry. Established telecommunications companies tend to react after the fact and often mistake fraud for bad debt.

If telecommunications companies realize that organized crime is booming, they must take action to combat fraud, or suffer the consequences to their own profitability. It is interesting to note that the return on investment of telecommunications fraud intervention typically provides cost savings within 12-24 months when appropriately implemented.

Types of Fraud

Fraud perpetrators can cause serious damage to the telecommunications industry through many different types of fraud, such as:

Access fraud - any unauthorized use of service through intentional tampering. This type of fraud is the major contributor to overall fraud losses.

Subscription fraud - the perpetrator obtains the subscription of a service with no intention of paying. This may occur through the normal application process using false identity information.

Cloning - the practice of programming the electronic serial I.D. of a legitimate mobile phone into another phone.

Teeing-in - physically connecting into someone else’s phone line.

Shoulder surfing – the use of binoculars and cameras to watch the user (often occurs in public places such as airports) enter the codes or recording devices to eavesdrop on numbers spoken to the operator.

Hacking – fraud perpetrators' repeated attempts to figure out code combinations by random entry.

Surfing - the use of someone else's service without having the necessary authority.

Ghosting - refers to technical means of deceiving the network to obtain free calls.

Prepaid cards - fraud perpetrators recharge a calling card by illegitimate means, without paying for service on a prepaid card.

Line tapping - clip-on access to customers' line.

Accounting - exploitation of the accounting and billing processes to reduce charges or obtain credits; this usually involves insiders.

As new services are created, the list of known types of fraud is expected to expand and fraud perpetrators will continue to discover new ways to exploit services and compromise security.

Fraud Perpetrators Motives and Benefits

Fraud perpetrators are motivated financially, the need to cover their crimes and the challenge of beating a system. They most commonly benefit from fraud by:

Using a service without paying - For those who are not willing to pay for the service, fraud is usually the answer. In this category, losses are difficult to differentiate from bad debt. They average about $600 per case.

Selling information - Insiders exploit information by selling it to others. Very commonly, the information is sold to a professional network of criminals that resell it worldwide to counterfeiters. In 1995, two US carriers reported losses suffered of $55 million from the activities of two employees.

Impact of Fraud

The cost of fraud is significant and often hidden within an organization. The financial losses can be extremely large. For example, a fixed network provider can lose up to 3% of its annual revenues to fraud. Mobile providers lose 5% of their revenues every year. This can have a serious effect on operating margins and crucially impact the earnings of the company.

Fraud impacts other areas of the telecommunications industry, including marketing. Vulnerability to fraud may constrain a company from offering advanced services that their customers desire and for which their existing network infrastructure may already support technically. For example, the ability to provide on-line subscription of a service may provide a competitive advantage to a carrier. However, because the Internet is not perceived as a safe place or previous fraud losses have been high, many carriers hesitate to offer such feature.

The cost of fraud is also reflected on customer relations. Fraud can impact customer billing statements and lead to disputes and negative customer perceptions. The service is seen as poorly protected and unreactive to fraud. Significant losses may also affect the perception of both shareholders and the market for publicly held telecommunications companies.

Case Study

A medium-sized telecommunications company relied on simple reports from their billing system to detect fraud. Detected frauds were allowed to run for some time to facilitate prosecution. Losses climbed rapidly, peaking at more than $4.5 million per month and threatening the viability of the organization. A fraud detection system and set of management procedures were implemented and over the following three months fraud losses reduced to approximately $80 thousand per month.

This case demonstrates what can happen when fraud management focuses entirely upon investigation. Although there were considerable resources deployed, it was focused in the wrong direction and was not addressing the issues that would have reduced the problem to manageable proportions.

Recommended System Requirements

For any system to be effective in fraud loss prevention or risk management, two basic functions must be considered: *fraud detection* and *fraud case management*. In accomplishing these functions, the system should be robust, process extremely large amounts of data quickly, customizable, and user friendly.

Fraud Detection

An effective Fraud Management System (FMS) should be able to detect multiple types of fraud. The FMS should be able to process calls originating from one switch, and calls which originate on a global basis and are run against one authorizing server. The types of fraud suspected should be user definable, to address new types of fraud yet to be defined. It should be able to process multi-thread rules, with multiple dependencies to tailor rules against different customer types. It should be able to process rules against a real time Call Detail Record (CDR) feed, and against a historical repository of call data. The FMS should have provision to send out signals to tear down a call in progress, or to disable a customer account. The system should have a standard, published interface layer to facilitate integration with other network components.

Fraud Case Management

Fraud cases should automatically be generated on a Case Management System (CMS). The CMS should have the ability to dispatch automated responses based on user definition. It should be able to dispatch cases to human intervention based on user definition, and it should maintain a hierarchical record of activity. The CMS should be based on a user-friendly Graphical User

Interface (GUI), with provision to customize both the display screen attributes and the process work flow of managing a fraud case. The CMS should correlate and notify the user of multiple fraud cases against a single account or ANI. The CMS should automatically escalate cases which are not resolved within the time period prescribed by the authorized user.

The TCS DEFEND™ Solution

Since there is no "cure" that can prevent attempts to perpetrate fraud, the only way to manage it is through intervention. Early detection and consistent monitoring are the keys to successful fraud intervention. Designed specifically to intervene in all (both known and future) types of fraud in a telecommunications environment, TCS DEFEND™ uses the latest technology to provide a comprehensive packaged application that supports risk management with user-defined rules and the ability to handle enormous call volumes. It possesses all of the features and benefits expected from a custom solution, while retaining the ease of use of an off-the-shelf product.

How TCS DEFEND Works

Rule Definition

TCS DEFEND operates as a rule-based Event Manager. User-defined rules are applied to any data element, or event. Rules can be applied to data from historical analysis or an on-line source.

DEFEND can store the historical data and link this information with the billing server to provide a profile of traffic that has not been paid for.

DEFEND is delivered to the customer with a base set of fraud rules. In addition, the user can define new rules as business requirements change.

DEFEND supports complex rule conditions such as parent/child rules, thresholds, and group-by functions. New rules are easily created within the system using the GUI. Once fraudulent activity has been defined, it is possible for the system to detect new instances of fraud with similar patterns.

CDR Scan

TCS DEFEND provides real-time processing of events including analysis of CDRs and any other information loaded into the TCS database, such as customer billing records or previous fraud history. The information must be available to TCS either through the TCS database repository, or by interface to an external source. Once data is available, it can be stored and retrieved for use in fraud detection and analysis. DEFEND supports a standard interface to the Inet Geoprobe for SS7 information.

Conditions/Rules/Actions

TCS DEFEND supports the ability to automatically trigger external systems for the suspension of accounts, calling card deactivation, ANI blocking, tear down of calls in progress, or blocking of destination numbers. As data is continuously filtered when received, action is taken by recognizing the condition and sending an alarm to the governing system through a standard or custom interface.

When the defined conditions are met, DEFEND recognizes the event, fires the applicable rule, and automatically triggers an action previously defined by the rule.

Benefits Of TCS DEFEND

Flexible

TCS DEFEND supports call-based rules definitions that trigger alarms and/or fraud cases. These rules can be changed dynamically while DEFEND is in operation. Not only do users have the capability to create their own rules, they can also change and apply them against any field or group of fields in the CDRs. This gives telecommunication companies the flexibility to customize and tailor the system to specific needs.

Expandable

Utilizing powerful Oracle Parallel Processing methods and servers expandable up to 128 processors, TCS DEFEND is flexible in the size of volume it can handle. All service types (components) defined in DEFEND are object-oriented and new network elements and services can be created rapidly and easily by the user, without programming changes.

Common User Interface

TCS DEFEND supports a wide range of interface technologies including TCP Socket, FTP, DCE/RPC, CORBA, Telnet and a published API. Direct interfaces (typically using Socket) can communicate directly with network equipment such as switches and mediation devices. On-line or batch interfaces, typically using the API, are used to retrieve customer and billing information.

Customizable

TCS DEFEND supports group-by functions to manage and customize rules and the customer categories to which they are applied. This allows the user to manage which type of customers a particular rule applies to or is excluded from. DEFEND also supports priority and severity levels and multiple and complex alarm escalation, including threshold functions based on individual customer calling patterns.

Case Management

TCS DEFEND includes a full graphical Case Manager. Generated fraud cases can be dispatched to automated processes and to the Case Manager for human intervention.

Reports

TCS DEFEND includes several packaged reports. Since it is an Oracle application, it is also compatible with common Oracle reporting tools for creation of new reports.

Architecture

Events, Rules and Actions

TCS DEFEND is a rules-based Event Manager. It is comprised of the TCS Database Server, TCS CONTROL, interfaces to external systems, and TCS Client workstations. In addition, source CDRs must be provided as input into TCS. For some types of automated action it may be necessary for a governing system to be available to receive information or signals from DEFEND.

An Event is defined as the specific combination of data and conditions. For example, data "x" occurs in conjunction with "y", or at a specified time, or at a specified frequency. In TCS DEFEND, events are correlated against specific rules. Rules and data are both stored in the database. When an event or combination of events is processed against rules, if the pre-determined criteria is met, then an action is taken by the system.

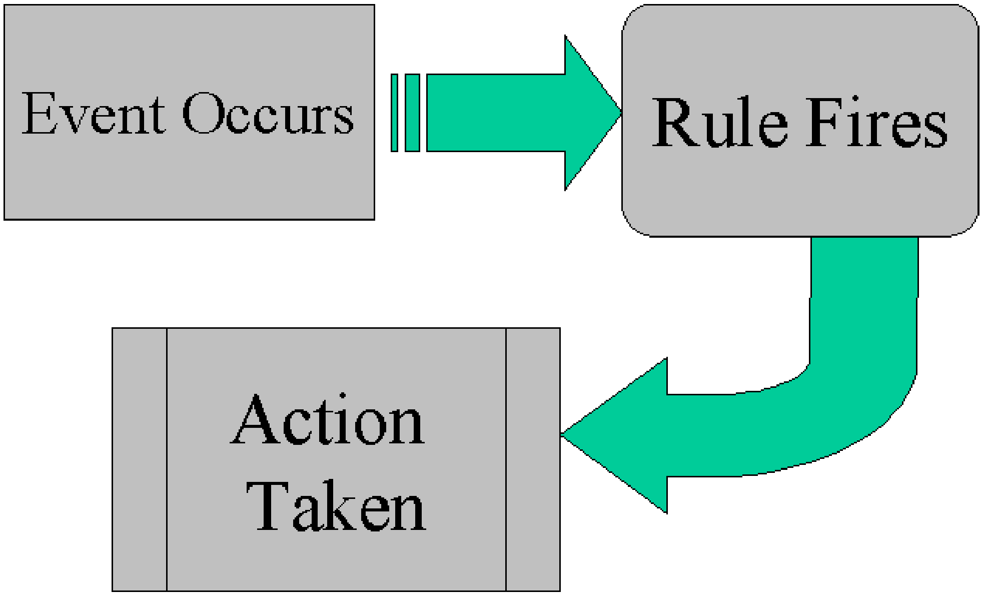

Figure 1: TCS Control Rule Based Action

TCS DEFEND Process Flow

In using TCS DEFEND for telecommunications fraud intervention, events are usually related to telephone calls or account usage. Data that defines most events is contained within the DEFEND database. It originates from network switch feeds, external systems, and alarms.

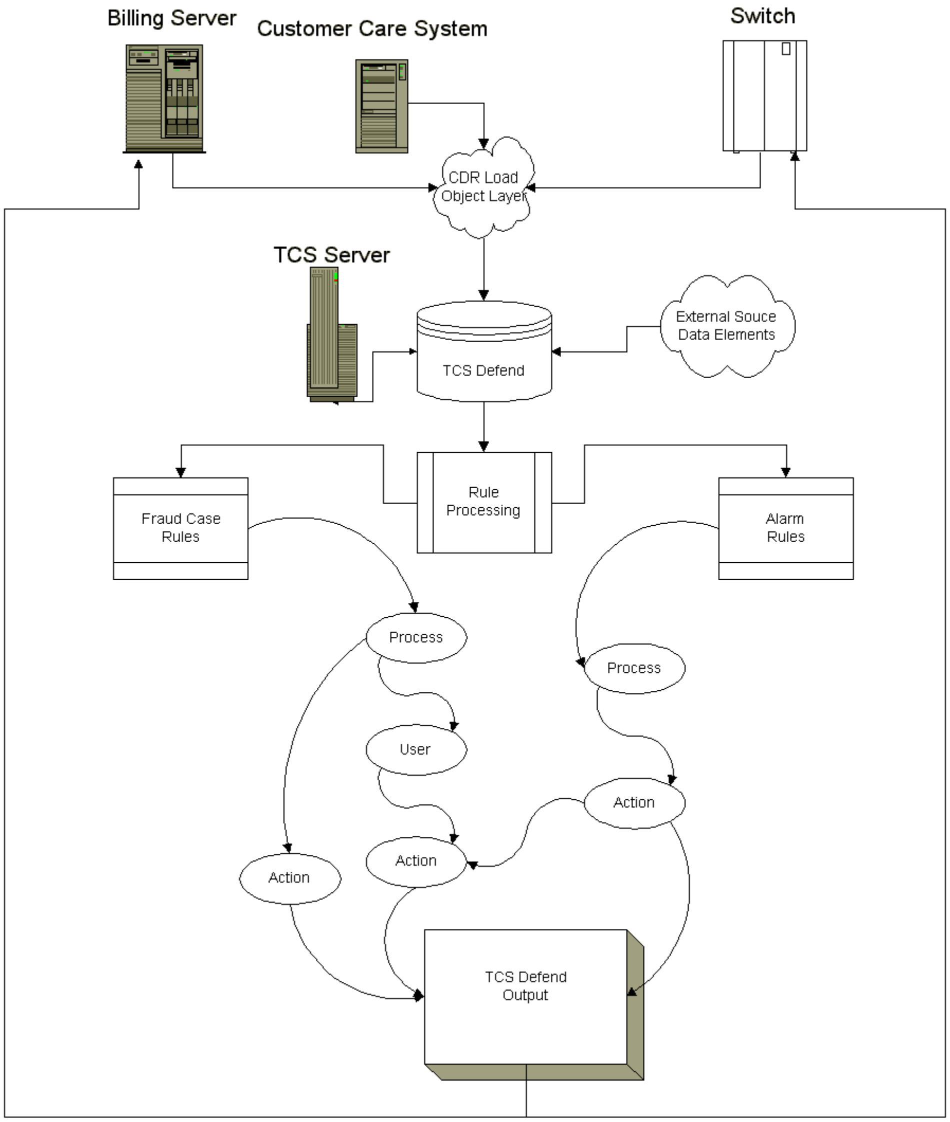

Figure 2: TCS DEFEND Process

For instance, a Geometric Velocity (or ballistic) rule might state that two events are not allowed to occur at a sequential rate faster than 700 mile per hour between earth coordinates. Another rule might be a Simultaneous Restriction rule, which states that the owner of an account is not permitted to have simultaneous occurrence on his account from two different points of origin. Multiple parameters can be set, such as in a Duration rule. The first condition might be set to flag calls which exceed a specific duration. The second condition is to take action only if the call is between certain city pairs that have previously been demonstrated to exhibit an unusually high occurrence of fraud. The third condition is that the account owner does not reside in one of the cities.

The output of events processed by rules in TCS DEFEND is distributed to processes for automated actions, or sent to Case Management for human intervention. Because DEFEND includes an integrated Case Management System, the actions taken through human intervention can then cause the case to re-enter the system of automated process as defined by the authorized user.

The final result is an integrated system that processes massive call volumes consistently, according to user defined complex rules, and manages the output in an automated and controlled fashion.

Summary

TCS DEFEND provides an effective means of telecommunications fraud intervention, through the use of fraud detection and integrated case management. Benefiting from real-time processing of customer information, CDRs, external data, automatically generated dispatching, and the ability for users to define rules “on the fly”, TCS DEFEND is a comprehensive solution to reduce the financial impact of fraud.