Deloitte.

Data synthesis in fraud detection and prevention for telecommunications service providers

Executive Summary

Growing transaction numbers and advances in technology are increasing the potential for fraud attacks on the telecommunications industry. The heavy dependence of telecom service providers (TSPs) on automation, the Internet, IP networks, and wireless networks can provide fraudsters with many opportunities to act. And, suspicion or evidence of fraud, waste, or abuse can present TSPs with numerous legal, compliance, and related issues.

Facing such situations, TSPs historically have performed "look back" analysis to determine how likely and how large an alleged scheme may be. However, the inefficiency of this reactive approach can potentially impede investigation and resolution. This article discusses an alternative approach — data synthesis — which can help TSPs navigate their complex organizational structures and target and collect relevant fraud data when the need arises.

Introduction

Large TSPs can face numerous legal actions, compliance requirements, and other issues related to fraud, waste, and abuse. In situations requiring investigation, such as a chance discovery of fraudulent activity or an allegation by a whistleblower, involved parties frequently scramble to collect data or perform legal holds.

Historically, many TSPs have responded to such matters by performing "look back" analysis based on data subsets collected by different departments or geographic locations. For example, when a TSP detects potential fraud, an investigative team may be assigned to determine the likelihood and scope of an alleged scheme, sometimes leading to a damages calculation.

For a variety of reasons, this reactive approach can be inefficient and time consuming, potentially impeding thorough investigation and timely resolution. In assisting with several such investigations, Deloitte has observed that many TSPs may not have a clear procedure for collecting needed data. A lack of synthesis — or merging of data — between a TSP's fraud detection unit and finance department can impair the acquisition and conversion of extensive data sets often required for meaningful analysis.

This article discusses potential strategies to help TSPs create a road map for implementing data syntheses on an enterprise level. These strategies are specifically designed to help TSPs navigate their complex organizational structures and help them target and collect relevant data when the need arises.

Fraud's Impact on the Telecommunications Industry

In 2012, telecommunications was estimated to be a $1.1 trillion business in the United States alone, employing more than 860,000 workers.[1] Over the past two decades, the rapid expansion of broadband and wireless services has fueled the evolution of telecommunications services and supporting technologies. Many TSPs, including local and long-distance phone carriers, cable operators, wireless carriers, and Internet service providers, as well as networking equipment companies, are working to adapt their organizational structures and operational models to this shifting landscape.

TSP structures are often intricate, designed to accommodate business functions but engineered for cost efficiency. Such structures can challenge organizations that are pressed to gather data for a fraud-detection investigation, an anticipated or ongoing litigation matter, or a government-mandated compliance review.

[1]Introduction to the Telecommunications Industry, Plunkett Research, Ltd. http://www.plunkettresearch.com/telecommunications-market-research/industry-trends

With telecom-related fraud estimated to cost approximately U.S. $40 billion[2] per year, detection and prevention remain TSP priorities. However, preparedness for and efficient response to incidences may continue to be a challenge. Meanwhile, fraudsters are likely to continuously evolve and create new ways to exploit weaknesses in TSP internal controls.

With dramatically increasing telecom transactions and advances in technology, the industry may become an increasingly attractive target for fraudsters. The heavy dependence of TSPs on automation, the Internet, IP networks, and wireless networks can provide fraudsters with many opportunities to act. One study estimates that more than 200 types of telecom fraud exist, including schemes to manipulate a TSP's operator network or exploit a billing system.[3] Common fraud scenarios include:

Billing system related frauds

- **Subscription fraud:** up to 10 percent of a carrier's bottom line can be lost to simple subscription fraud and other low-tech scams.[4] Fraudsters may open accounts and sign up for service using fake names and/or addresses. Personal information exposed to criminals can be used to change existing customers' addresses or phone numbers, often resulting in abuse of services.
- **Assaulting security weaknesses in databases:** fraudsters may hack a customer database containing billing names and address information, which they can use to send unsolicited commercial email or spam mail to unsuspecting end users. The information can also be used to disguise a calling party's identity by falsifying telephone numbers and names relayed as caller ID information.
- **Credit card fraud:** fraudsters could make payments using another person's credit card and CVV number.

Network related frauds

- **Bypass fraud:** unauthorized manipulation or exploitation of an operator's network is one of the latest and most severe threats to a telecom operator's revenue.[5]
- **Hacking IP addresses:** by hacking IP addresses behind the phone numbers of VoIP users, fraudsters and hackers can penetrate a company's VoIP system and route calls via its server.
- **Other:** Network related fraud schemes are continually being created and may include prison call forwarding, compromised PBX/voicemail systems, and hijacking of a network device, which could then be used to attack the vulnerabilities of a telecom network.

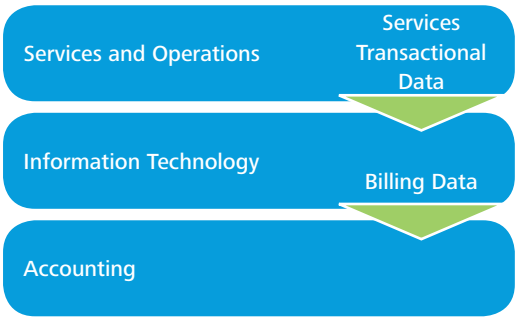
The impact of telecom-related fraud on a TSP may take the form of a reduced financial bottom line. Ultimately, the effects may extend to the TSP's clients as well in the form of degraded services and support, potentially eroding its client base. These risks may compel some TSPs to detect fraudulent activities and protect themselves by developing customized rules and tests for fraud detection.

Big Data in Telecom

The emerging concept of "big data" may aptly describe data possessed by a TSP, as well as define the challenges associated with making effective use of these data. TSPs typically collect and maintain massive amounts of data, including telecom service transaction records, finance data, and human resources data. They often decide what data to collect primarily based on internal departmental requirements and geographic data needs.

Data are usually separated logically across departments and geographical regions, and the types of data being collected and managed can be quite complex. Data types can include service transactions, customer information, and product and service types, as well as definitions for varying pricing and billing data models with overlapping life cycles. The data themselves may be subject to internal or governmental agency retention requirements. Data may also be shared across a TSP based on departmental needs (Figure 1).

Figure 1: A typical model for sharing data across TSP departments:



[2] "Telecom frauds cost $40B globally", Swati Prasad, http://www.zdnet.com/telecom-frauds-cost-40b-globally-7000008466/
[3] http://www.scribd.com/doc/24765507/Telecom-Fraud-Management
[4] http://www.billingworld.com/articles/2004/07/telecom-fraud-on-the-rise.aspx
[5] http://www.allround.net/images/stories/attached_files/Bypass_Fraud.pdf

Typically in large organizations, each department with specific functions develops its own criteria for capturing, cleansing, normalizing, storing, searching, sharing, analyzing, and retaining required data. Data that need to be moved and shared across departments or locations are generally provided in a summarized format and are limited to supporting specific functions, such as finance (e.g. customer billing, salaries) or operations (e.g. network traffic enhancements, customer support response time).

Data analysis teams are typically composed of subject matter specialists (SMSs) from the TSP's fraud detection unit, who work in conjunction with data analytics specialists. The scope of an investigation can compound data collection challenges, particularly when the investigation requires data residing in decommissioned legacy systems, including those of another company acquired through merger or acquisition.

Data Extraction and Analysis Challenges

Data extracted and analyzed for fraud investigations typically consist of transactional data (e.g. phone call records), financial data (e.g. AR and AP records), and other reference data. The size and complexity of data sets can make them difficult to manage and process using available database management tools, legacy systems, and related applications. Aggregating and analyzing data reactively can be time consuming due to several factors:

- Inadequate synthesis between a TSP's fraud detection unit and finance department can make exceptional effort necessary to obtain and convert extensive data sets for meaningful analysis. Much time may be spent attempting to collect complete and useful data, as well as understand data definitions. Mergers and acquisitions may negatively affect the quality and completeness of data collection and interdepartmental information sharing.
- Understanding business rules and the policies and procedures behind data can be arduous and iterative. Often, data owners and subject matter specialists have to be brought in to gain insight into the multifaceted data.
- Data analytics specialists may encounter difficulties in reverse engineering complex data collection systems by tracing events through summarized data sets that cross departmental boundaries.

Data Synthesis for a More Effective Solution

Telecom fraud is prevalent and can have potentially significant financial impact. The collection and strategic distribution of data critical to detecting and preventing fraud across departments should be an enterprise- level effort properly prioritized in a TSP's strategic management initiatives (Figure 2). Prioritizing fraud detection and prevention efforts can begin with a cost/benefit analysis that objectively assesses fraud's true impact on the TSP, along with development of a plan for making the required enterprise-level changes.

Figure 2. Proposed model for sharing data across departments

Continuous addition of new telephone services and possibly mergers and acquisitions can lead TSPs to maintain disparate customer information databases. This approach can be attributed to the complexity of data collection and the highly customized manner in which large organizations manage data. If databases are not managed properly, each one may contain different information for the same customer. Outdated addresses and misspelled names can create confusion in billing and customer care. Merging data into a single database of accounts for many services may reduce confusion and improve efficiency.

Developing an Enterprise Fraud and Misuse Management (EFM) Plan

Integrating fraud management efforts under the umbrella of enterprise fraud and misuse management (EFM) can bring the pieces of the fraud puzzle together to provide a clear picture of a carrier's fraud risk and help develop a path to mitigating it. The effectiveness of this overarching solution hinges on how a TSP's departments develop and implement appropriate plans for fraud-related data collection, management, and distribution.

A typical TSP organization includes large departments such as telecom services, information technology, accounting, and marketing. Each department possesses a distinct set of institutional knowledge that, when shared across the enterprise, can play a key role in detecting fraud.

An example of this would be a sharp rise in fraud calls. According to Pindrop Security, approximately 1.3 million fraudulent calls were made in the first half of 2012, a 29 percent increase from the second half of 2011. Fraudsters have been targeting large banks and other financial services providers by calling people and claiming to represent these institutions. Mobilizing resources from different departments to promote interdepartmental collaboration and communication could be an effective approach for TSPs to fully detect this type of fraudulent activity.

To help increase the effectiveness and return on investment of its EFM program, a TSP can consider these steps:

- Establish a results management office (RMO) and steering committee to manage the EFM program and serve as a single point of contact for oversight
- Develop cost models to identify the true impact of discount abuse, bad debt, and handset fraud and to measure the benefits of the new EFM approach
- Apply an integrated approach to the use of advanced analytics and continuous monitoring systems for identifying and tracking the different fraud types
- Enforce discount usage and credit collections recovery policies and procedures through internal-audit back-testing and regular training sessions
- Track fraud down to specific handset type and taking a multidimensional approach to fraud management, including subscription type, geography, usage characteristics, timing of subscriptions, and discount type

An EFM solution can provide benefits beyond the primary goal of mitigating fraud. Establishing designated points of contact for data-collection-related questions within each department can be used for other purposes, such as improving overall operating efficiency. A holistic view and comprehensive catalogue of enterprise data can provide the organization with an opportunity to "clean house" and reorganize itself as appropriate to improve operations. And, interdepartmental understanding of business rules and policies, which may be niche knowledge within specific departments, can be enhanced.

An Actionable Solution

TSPs may want to consider a four-step process for improving decision making and predictive capabilities in support of early fraud detection and mitigation:

1. **Obtain or create relevant information —** Questionnaires can be distributed to capture detailed listings of information repositories and databases owned by each department within the company. Information to capture can include data dictionaries, data flow and process flow diagrams, data owners, and subject matter specialists. Network analysis diagrams can indicate how information repositories relate to and interact with one another. Issues may arise during the process that could impact timing, such as identifying the proper SMSs to provide applicable business rules and obtaining reference data, even when the data resides on systems owned and maintained by the TSP's IT department. SMSs may also reside outside of the department in which the data is being collected, another potential challenge. Following the initial information gathering, participating departments can periodically inventory their databases and catalog and update information related to the data sources they own.

2. **Form an interdepartmental committee of data owners and SMSs** — After the relevant information is collected from each department, a committee can be assembled to assess the data sources and develop standardized, enterprise-level antifraud business rules. The committee can fairly represent the departments and help "connect the dots," especially when many information systems are involved.

3. **Conduct joint design sessions —** Regular meetings between data owners and SMSs can help flesh out antifraud business rules and identify key performance indicators. Organizations should consider potential timing issues that may arise during this process such as identifying the proper SMSs to provide the applicable business rules. Once the committee develops an understanding of existing rules, alerts, and data analytics frameworks, the committee can define business requirements and the analytical processes needed to meet them. Committee members can work closely with business and technical users to identify and document existing business use cases in support of analytical processes. Overviews of technical systems, dependencies, and key assumptions used for each of the business processes may be needed to develop meaningful and effective fraud detection mechanisms. To target areas for enhancement, SMSs can leverage their experience and knowledge of leading practices in data architecture and analytics to evaluate the technical and functional components of existing business rules. Harvested business rules can be independently reviewed and approved by a designated group of organizational stakeholders. Potential antifraud areas to considered include:

- Payment fraud (duplicate invoices, ghost employees and vendors, and segregation of duties)
- Telecom fraud (call forwarding and calling card scams)
- Consumer scams (identity theft and fraud calls)
- Early case assessment
- Litigation readiness

4. **Develop and document a standard process to collect and catalog data —** the interdepartmental data committee can implement standard operating procedures (SOPs) to provide rules and oversight for data collection in response to new litigation matters or internal investigations. Along with capturing data sources, data descriptions, and points of contact for relevant information systems, the SOPs can document committee-developed antifraud business rules. The rules can reflect the departmental knowledge that is now being shared across the enterprise as a major component of antifraud initiatives.

In planning for deployment of a new antifraud solution, TSPs can benefit from considering the solution's potential effects on employees and operations. Employees in some departments may be concerned that participating in the program could require significant time and resources. Internal politics and job security concerns may restrain SMSs from sharing niche knowledge of specific business rules and policies. Operationally, adding a new process may adversely affect efficiency and flexibility. And, even if SMSs willingly participate in joint design sessions, developing an inclusive roadmap that captures data points and institutional knowledge from various parts of the organization can be difficult.

Conclusion

The telecom industry has accumulated vast fraud knowledge, often through costly experience. The emergence of big data, combined with advanced and predictive analytics, can provide a powerful fraud-prevention weapon. At a high level, TSPs can turn to telecom fraud specialists to help mitigate the challenges

of capturing, managing, and sharing relevant information from vast data repositories. These specialists can analyze the TSP's current state, provide an extensive gap analysis against recommended industry standards, and offer a plan to close identified gaps.

TSPs that embrace telecom-related fraud prevention efforts and business processes and establish a complete set of available data can identify potential instances of known fraud types and ongoing and evolving fraud schemes. While many TSPs continue to use reactionary methods for detecting fraud, forward-looking industry players can reap the benefits of combining experience with technology. They can strengthen fraud reduction and prevention efforts and potentially predict areas of vulnerability.

Case Study

A TSP engaged Deloitte to assist in identifying potentially fraudulent call routing activities detected by the company's internal fraud detection and prevention unit. Our team consisted of a lead partner with a background in forensic investigations, as well as analytics practitioners.

The engagement began with a series of meetings involving the Deloitte project team, the client's in-house counsel, and specialists from the client's fraud detection and prevention unit. The fraud unit provided a high-level understanding of the business processes related to the investigation, as well as offering a hypothesis of how the fraudulent activities were perpetrated. The fraud unit also presented sample data that appeared to show clear examples of anomalous and potentially fraudulent activities.

To help define the scope of the investigation, the Deloitte team worked with the client to identify business process subject matter specialists (SMSs) who could offer detailed insights into how the potentially fraudulent activities differed from normal activities. For example, our team wanted to understand how to categorize phone call activities by call type and tariff-zone jurisdiction, as well as leverage available data for the purpose of calculating damages. The analytics practitioners worked with the SMSs to identify key data points to be collected for analysis.

The engagement revealed that providing the client's operations team with real-time access to reference data could aid in detecting, and potentially preventing, fraudulent activity. Transactions could be tested against client data and business rules in the accounting department's database to test transactions as they transpire. Because constant monitoring of transactions could come at a performance cost, methods such as sampling were identified as potentially helping meet both performance and risk mitigation goals.

Contacts

David Wallis
Partner, Deloitte Forensic
Deloitte Financial Advisory Services LLP
+1 404 220 1053
dwallis@deloitte.com

Dimitri Saad
Senior Manager, Analytics
Deloitte Transactions & Business Analytics LLP
+1 404 942 6981
dsaad@deloitte.com

Hong Zhou
Manager, Analytics
Deloitte Transactions & Business Analytics LLP
+1 202 220 2604
hzhou@deloitte.com

Young Lee
Analytics Specialist Master
Deloitte Transactions & Business Analytics LLP
+1 404 220 1630
yolee@deloitte.com