Proposal for an RIT Software Engineering Sr. IT Project
Providing a
Telephone Fraud Monitoring and Detection System

1. General Background

PAETEC Communications is a Integrated Communication Provider (ICP). This means that PAETEC competes with Incumbent Local Exchange Carriers (ILEC) such as Frontier and Verizon, Long Distance Carriers such as MCI and Sprint, and Internet Service Providers such as Time Warner and Verio. The ILECs maintained a monopoly on selling these services until the Telecommunications Act of 1996 required them to open these markets to ICPs like PAETEC.

2. Project Description

PAETEC currently operates its day-to-day business in a heterogeneous environment including servers from Dell, Sun, and Hewlett-Packard, storage arrays from EMC, network equipment predominantly from Cisco, and software including Solaris, Windows 2000, Windows NT, linux, Microsoft Exchange and Oracle. We have many commercially-developed applications, and a comparable number which have been developed in-house, which perform necessary functions which include provisioning, billing, monitoring, and managing a large and complex set of data.

One of the critical challenges which face any telecommunications company is the abuse of their phone circuits through fraudulent activity. "Toll Fraud" as it is commonly known, can take many forms – from the simple theft of authorization codes, to elaborate schemes in which calls are placed through devices which generate false billing records, or to certain telephone exchanges which charge the carriers excessive monies which are subsequently funneled off to the perpetrator. Because of these and other threats, it has become necessary for telecommunication providers to install systems which monitor and provide assistance to humans who monitor the calling activity for fraud.

At PAETEC, we currently employ multiple safeguards to prevent loss from fraudulent activity, including a system which aids in detecting such activity. The system is a commercially-purchased software and hardware package which handles the 5 million long distance call records produced by PAETEC network subscribers each day. This information is maintained in a database for a user-definable retention period, and can be manually analyzed and reported on by many different dimensions. In addition, the software has access to historical trending data, and will automatically monitor call activity to see if it falls within certain boundaries based on historical analysis. The system will also generate alerts in the event that certain user-definable conditions are detected (relating to various parameters of the call record and external conditions such as time of day, frequency of calls placed to this region, length of call, etc.).

PAETEC has determined that it would like to develop its own fraud monitoring, detection, and alerting system. This system would have all the features found in its current software, but would have several additional capabilities, including the ability to: operate against an Oracle database; operate in a "customer partitioned" mode whereby PAETEC customers could have secure access to just their own fraud-detection data; incorporate new pattern detection algorithms for fraud types not yet existing; access and operate the system entirely from a web interface; provide automatic escalation of both customer & PAETEC alerts, utilizing different media types (such as cell phone, pager, email, etc.); provide a design which will facilitate future integration with SS7 signaling fraud (a different type of activity than toll fraud).

Some potential deliverables to be considered for this software will include the ability:

- To accept call-detail-record data feeds from one or more sources, on a continuous (stream), polled (buffered stream) or manual (file) basis
- For a user to view and report on the data, in both a detail and summary basis, with multiple selection criteria
- Automatically purge records from the database based on a record-aging or storage-capacity limits
- To monitor the call database and to identify potentially-fraudulent patterns of activity based on various thresholds, configuration criteria, and historical analytics; This capability should also allow relatively easy development and integration of future pattern algorithms
- Based on criteria, to initiate an alert to one or more parties that fraud-detection has been triggered
- To operate in a "partitioned mode" whereby users are associated with a specific account and can only access call data related to that account; Also, separate alarm and escalation settings should be maintained for each "partition"

This project could be completed in multiple phases, depending on the scope as determined from the initial analysis. Specifically, a reasonable first phase would be the development of a system comparable in features to our current one, yet based in java with a back-end in Oracle, and a web user-interface. A second phase could then be made which would include the realization of the "partitionable interface," new algorithms, and the alert escalation features.

The software must adhere to PAETEC's development standards, which specify that the programming language will be Java, in a J2EE / Web-Services framework, with an Oracle database. It is expected that a PSP / TSP methodology will be followed for this project, and that substantial further definition will be provided as an input to the requirement gathering / analysis steps. Test scenarios and sample data will be provided to the software development team.

3. General Technical Assumptions

Database Engine:	Oracle
Fraud Programming Language:	Java in a J2EE / Web-Services Framework
Web-based User Interface:	HTML / XML with business logic in Java
Development Environment:	Determined jointly by development team and PAETEC
Platform:	Solaris

4. Scope of the Project

- Analyze the various requirements, and develop an initial scoping document from which a decision will be made to proceed in a single or multiple phase project
- Construct a project timeline to scope and sequence the tasks necessary to develop this software
- Develop a design document based on software and database requirements to enable telephone fraud detection and monitoring
- Design & develop the database and fraud monitoring software
- Test and verify all aspects of this software