



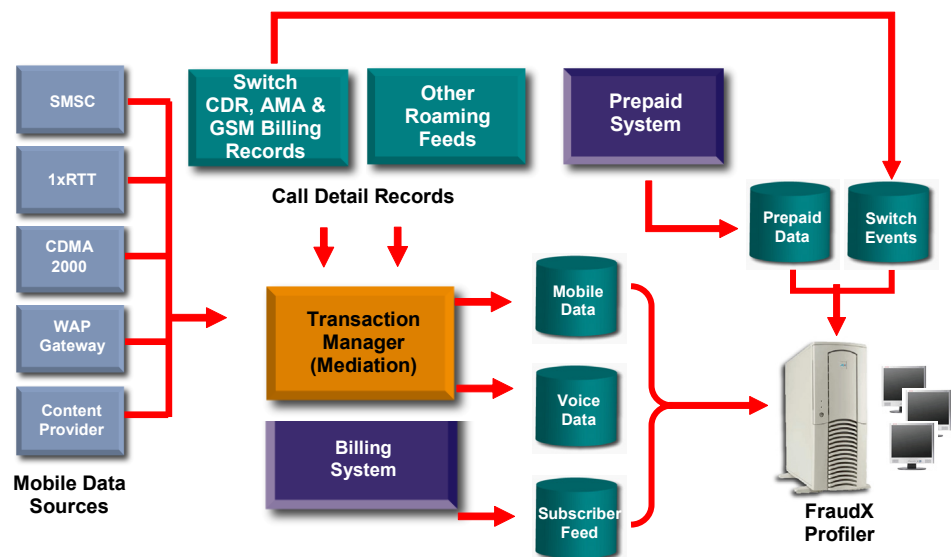
## Fraud Detection for GSM and ANSI-41 Operators - FraudX®

With FraudX, you are able to take control of mobile fraud in your home and roaming markets while paving the way for prepaid and next-generation mobile data fraud.

**FraudX**, a Syniverse fraud detection system, is a knowledge-based software application that uses artificial intelligence to identify potentially fraudulent activity, specifically cloning and subscription fraud, on your wireless network. With FraudX, you are able to take control of mobile fraud in your home and roaming markets while paving the way for prepaid and next-generation mobile data fraud.

### Benefits of FraudX

- Works as your single fraud platform with its ability to accept multiple data feeds.
- Reduces losses associated with roaming fraud.
- Achieves more timely fraud detection with near real-time processing.
- Increases productivity of fraud analysts with advanced analytics and user-friendly, feature-rich graphical user interface.
- Capitalizes on Syniverse's extensive fraud expertise.
- Complies with the GSMA's NRTRDE initiative.





- Works as your single fraud platform with its ability to accept multiple data feeds.
- Reduces losses associated with roaming fraud.
- Achieves more timely fraud detection with near real-time processing.
- Lets you determine the types of fraud most prevalent in your market and the types of fraud on the rise.
- Allows customization with its threshold, table and parameter value-setting capabilities

## Features of FraudX

To identify potentially fraudulent activity, FraudX uses near real-time data from mobile switches and creates a unique profile for each of your existing subscribers based upon a subscriber's incoming and outgoing call records. After the subscriber profile is established, FraudX continually compares each subscriber's calling activity to his or her profile, constantly monitoring events. However, FraudX does allow for subtle variations in subscriber activity and updates the subscriber's profile with new, legitimate calling patterns as they emerge. Any significant deviation from a subscriber's normal profile generates a system alarm and a case to be reviewed by a fraud analyst.

FraudX, which is scalable and flexible, also:

- Lets you determine the types of fraud most prevalent in your market and the types of fraud on the rise.
- Allows customization with its threshold, table and parameter value-setting capabilities as well as with its:
  - User-defined pattern capabilities, allowing you to define specific conditions for identifying call records with certain fraud-associated characteristics.
  - User-defined rule capabilities, allowing you to use if/then statements that alter FraudX's programming logic for assigning fraud types and confidence levels.
  - User-defined automatic actions, allowing you to instruct FraudX to execute certain routines in response to defined fraud types and alarms with or without human intervention.
- Accepts data from your billing system, including customer subscription information, that is used to detect subscription fraud and is available for customized user-defined rules.
- Provides defense against subscription fraud by detecting excessive usage among new subscribers.
- Accepts a feed from your prepaid platform, monitors recharge activity and evaluates the information against call activity.
- Monitors mobile data and SMS activity to identify potential fraudulent activity.
- Stores in the system's history all actions, such as call marking, performed by fraud analysts.
- Employs a historical subscription fraud database that analyzes incoming subscriber information against confirmed fraudulent subscriber data, so alarms are generated when matches occur.
- Gives you the opportunity to outsource fraud analysis to Syniverse's Fraud Resource Center, a comprehensive, multilingual, customer service-oriented fraud department that is knowledgeable in fraud detection and resolution and is available to provide coverage seven days a week from 8 a.m. to 8 p.m. ET on weekdays and 9 a.m. to 5 p.m. ET on weekends.



## Syniverse Technologies

Serving more than 800 communications companies in over 160 countries, Syniverse Technologies (NYSE:SVR) offers market-leading solutions that simplify the complexities of roaming, messaging, network interoperability and business intelligence for mobile operators, MSOs, enterprise verticals and emerging mobile providers.

## How It Works

When you provision a new mobile subscriber, FraudX starts the process of building a unique profile for that particular subscriber. Since profile data is based upon actual subscriber usage, it generally takes about a month for FraudX to collect the data on a new subscriber and to determine what is normal for each subscriber. In the meantime, FraudX allows you to track a new subscriber's usage during a probationary period against operator-defined thresholds. Once a historical profile is established, FraudX compares that historical data with each subscriber's current profile data. By taking this cumulative approach, FraudX accounts for fluctuations in call activity due to activities such as vacations or excessive travel.

Once a profile is determined, the following process takes place:

1. FraudX accepts and performs edits on call records received from fraud data collection systems.
2. The system evaluates the edited call records for:
  - Call pattern matching
  - Suspicious dialed digits
  - Suspicious electronic serial numbers (ESNs/MEIDs/IMEIs)
  - Subscription fraud
  - Collision and velocity (SIM cloning detection)
  - Profile-specific variables, such as call cluster, call count and duration, source and destination, and fraud call area
3. The profiler assigns fraud probability and creates alarms when the fraud confidence levels you set are exceeded. It then updates the profile components with the resulting call detail and sends the alarms for fraud analysis.
4. When an alarm is generated, FraudX applies a set of knowledge-based, system-defined rules, which can be customized with your additional rules, to determine if a case is presented.
5. When enough fraud evidence is generated, the system creates a case and continually updates it.
6. The profiler performs the following steps to prioritize highly probable fraud cases:
  - Tracks by fraud type
  - Accumulates evidence
  - Assigns automatic actions, if needed
  - Assigns confidence level
7. A fraud analyst reviews the cases and performs additional research as needed, following your company's policies to determine what actions should be taken in response to each case.
8. As appropriate, a fraud analyst updates and/or closes cases in FraudX and marks calls as fraudulent. These fraudulent calls can then be sent to your billing system to ensure the charges from those calls do not appear on the legitimate subscriber's bill.