Fraud Prevention in the Age of 5G

Telcos lose about **$29 billion** (USD) annually to fraud, according to the Communications Fraud Control Association. For telcos, mobile operators, and communications service providers (CSPs), dealing with declining margins from traditional voice business, **protecting** existing revenue sources has become critical.

These increasing concerns about fraud and other types of revenue loss have incited a new approach to revenue assurance. Simply put: the current methods won't cut it anymore because they focus on **repairing leaks** instead of preventing them.

But with $29 billion of revenue leakage occurring each year—and the rate of losses rapidly accelerating with the arrival of new technologies like 5G and IoT—telcos and CSPs clearly need a **new approach** to Fraud Prevention. Whether it's for business systems (BSS), customer management, or fraud prevention, this approach needs to be agile, flexible, and fast. **A ninja, yes, but also a nerd: intelligent decision-making will be key.**

Key Challenges (& Solutions)

1 New Fraud Tactics

New technology has brought an onslaught of new telecom fraud tactics. The latest strategies are very hard to track because of their frequency, anonymity, and globally distributed nature. The three major types of telecom fraud are:

- Schemes to defraud **telecom service providers**, such as traffic pumping, Wangiri fraud, SIP trunking, and regulatory loopholes.
- Schemes to defraud **subscribers**, meaning gaining access to someone else's account to make free phone calls.
- Phone fraud, or fraudulent acts conducted over **phone calls.**

2 (Almost) Impossible New Latency Demands

5G and machine-to-machine communication have raised the bar on latency. With so much more data coming in, so much more data to analyze, and so much more needing to be done with that data, the **250-millisecond latency gold standard has shrunk to under 10 milliseconds.** That's because there's no longer time to let data travel to and from the data lake or warehouse. By the time it's made that trip, it's too late: the fraudsters are in and you are once again repairing leaks instead of preventing them.

3 Fighting Fire With Fire

With IoT and machine-to-machine communication making revenue leakage both more prevalent and harder to track for telcos, a new strategy has appeared: fighting machines with machines. **Machine learning** has now become table stakes for competent Fraud Prevention in the age of 5G, and telcos are increasingly using it to generate predictive analytics. By applying complex rules and algorithms to check against fraud identification patterns in real time, telcos can identify anomalies and block a fraudulent call before the device can connect.

4 Real-Time Decisioning Intelligence

Using **real-time intelligence** combined with machine learning and complex event processing, telcos can analyze thousands of attributes—including subscriber behavior, geolocation, device information, transaction type, etc—in real time. These attributes are compared to correct behavior and **statistical anomalies are identified and blocked in real time and in-event,** prior to the transaction occurring. This hybrid approach means that arbitrary, rule-driven false positives can be avoided, as can equally arbitrary machine learning decisions based on aggregate behavior.

5 Downtime Elimination

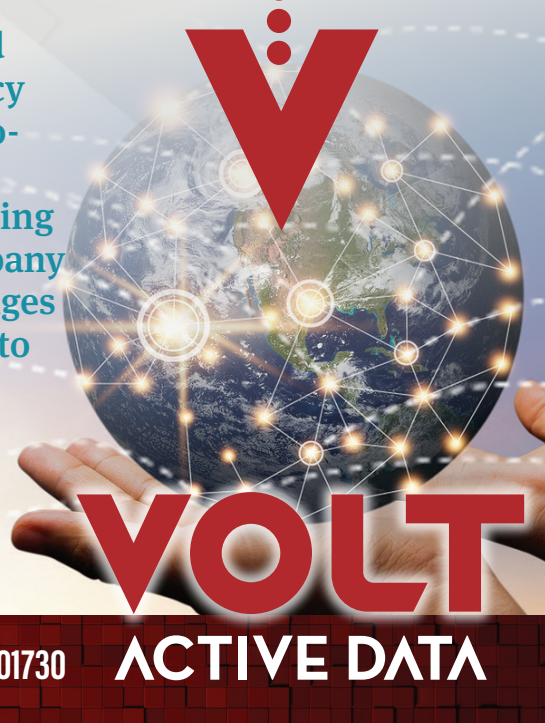
Potentially nothing else leads to more revenue leakage than network downtime. One estimate puts the annual, per-server cost of network downtime at **$6 billion.** But enterprise customers are no longer willing to put up with downtime, and to eliminate it, telcos are turning toward things like cloud-native, cross data center replication, and in-memory data storage, all three of which contribute, in their own way, to keeping a network running.

6 Stack Simplification

To be able to pull off all of the above, telco-space vendors are also trying to simplify their tech stacks. To truly achieve real-time decisioning, the less layers you have in your stack the better, because each layer adds latency. **Ideally you want a unified data platform that can handle the full ingest-to-decision data packet lifecycle and do it quickly, without compromising on data accuracy.**

Conclusion

Volt Active Data was designed to help telcos master Fraud Prevention in the age of 5G. Combining relational accuracy with NoSQL scalability, our data platform empowers telco-space vendors to build mission-critical applications that avoid downtime and enable real-time intelligent decisioning on fast-moving data. We're the only data technology company that has worked on real-world revenue assurance challenges for the last five years, and we know exactly what it takes to resolve today's Fraud Prevention issues.



To see why more and more leading telcos are betting on Volt Active Data in the 5G era, START A FREE TRIAL TODAY.