Advanced AI/ML for detecting Subscription fraud in an African Telecom Network

A case study on how Mobileum and AWS joined forces to stop the usage of stolen and synthetic identities to commit fraud

mobileum

Action driven by intelligence

About the Communications Service Provider

Our customer is a leading communications service provider in Africa, providing a wide range of services, including data, mobile and fixed voice, messaging, financial services, Enterprise IT and converged services to over 40 million subscribers. As a technology leader, the CSP's key drivers have been to deliver excellence and differentiation from its competition by offering seamless, frictionless and personalized digital experience to its customers. This CSP promotes the concept of connecting subscribers to a better future and, as a result, multiple sales channels are being employed to offer services and subscriptions to them. Our customer is evolving towards being a digital tech company, by providing additional financial services, on top of their traditional functions of voice, SMS and data. As part of this transformation, it is re-strategizing end-to-end engagement processes as well as make data-driven decisions to keep up with customers' increasing demands for exceptional digital experiences.

Decomposing the fraud challenge

Subscription fraud, despite the many controls in place, is still vicious and widespread, especially in the telecommunications industry. According to surveys, virtually every service provider is affected by subscription fraud. The CFCA reports that subscription fraud leads to roughly USD1.3 billion of revenue loss annually to operators. With multiple sales channels running across online and offline mode, our CSP started witnessing a significant increase in services and content usage at the same time as a parallel decline in revenue, leading to the realization of potential subscription fraud in their network.

Subscription fraud is the starting point for multiple other telecom fraud scams and, as such, it is recognized as the most damaging of all non-technical fraud types. Perpetrators don't just stop with obtaining legitimate services illegally; they usually use it as a precursor to other types of fraud such as Revenue Share Fraud, Bypass Fraud, Device fraud, Content theft, etc. The effects can be catastrophic in terms of escalating complaints, poor customer experience, dissatisfaction among support staff, and diminishing investor confidence.

To combat this, our customer needed a solution that could validate, authenticate and authorize subscribers by analyzing personal identification data coming from the multichannel environment as well as ensuring no disruption to the customer experience - and without compromising or delaying real sales.

Due to inefficient authentication and authorization of services across multiple channels, the operator experienced the following challenges:

- **Increase in unknown access to services and content;**
- **No means of evaluating multichannel services subscriptions;**
- **Lack of systems to evaluate false credentials and digital identities during the acquisition of services;**
- **Increase in fraud that led to device loss and as well as the impact on brand and customer loyalty;**
- **Financial costs of fraud investigation;**
- **Separating fraudsters from legitimate customers and increase acceptance rates with confidence;**
- **Keeping pace with the ever-evolving identity theft techniques.**

Peeling back layers of an onion

A result-oriented approach

For an operator executing a multichannel strategy, implementing and managing a fraud protection solution can seem like a costly exercise. It's like buying life insurance: you think you don't need it until it's too late. One of the main problems of using outdated tools when addressing fraud is that once the system starts catching fraudulent activity, the fraudsters themselves will change their strategy, making static tools of little value.

Subscription fraud not only impacts the CSP's revenue, but it also leads to poor customer experience and potentially massive data losses resulting in security threats such us stealing subscribers PII information. The theft here is plain and simple, but it is difficult to detect the subscriber's 'intent' at the point of sale.

The customer required that the chosen vendor would need to provide outsourcing services for all aspects of the fraud management function with rigorous SLAs and fraud detection targets associated. More than just implementing a tool, the vendor would be fully responsible for implementing the CSP's fraud strategy and would be accountable for any fraud losses based around agreed key performance indicators and SLAs.

Although it can be hard for a telecom operator to release control of something as crucial as fraud protection, our customer identified the following benefits to outsource this function:

Multichannel approach

The solution should be able to evaluate multichannel service' subscriptions and should be able to detect cases in the Online and Instore space.

Comprehensive insights

A dedicated fraud prevention provider has access to more diverse data points than an in-house team, enabling the provider to identify patterns and recognize fraud before transactions are processed.

Frictionless buying experience

A trusted partner can quickly and seamlessly make decisions on a transaction, meaning fewer transactions are flagged for manual review, and more transactions get approved immediately.

Fewer false positives

Mobileum's solution combines artificial intelligence and a rule-based approach to more accurately identify fraudulent behavior, which means fewer legitimate transactions will be incorrectly flagged as fraud.

Better technology

An external vendor will utilize innovative screening techniques and will have its fraud protection software always updated, saving the operator from having to make those investments directly.

Less drain on resources

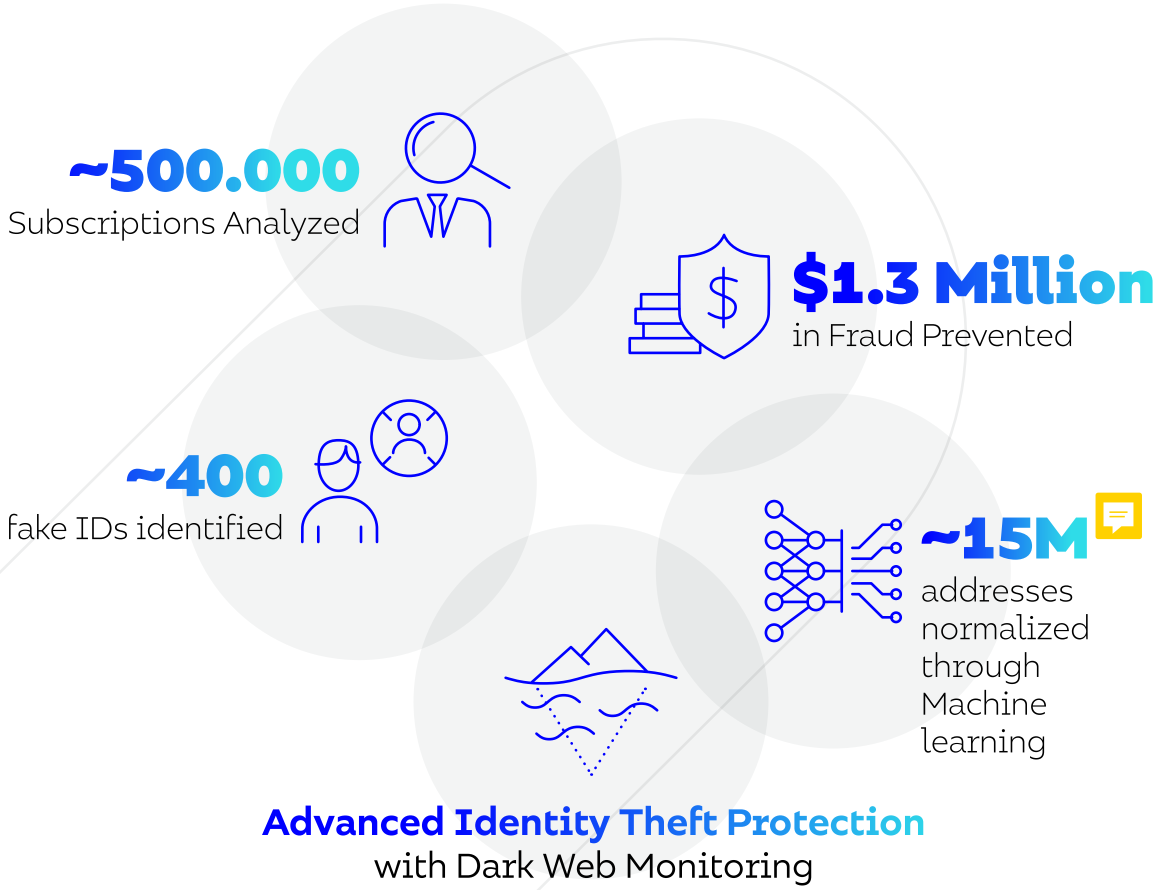
A trusted fraud protection partner frees up sales and engineering teams, allowing them to refocus their time, attention and manpower onto critical business tasks, like product analysis and market development.

Addressing subscription fraud through advanced AI/ML analytics

Communication service providers trying to achieve a multichannel strategy are quickly becoming targets for fraudsters, mainly via online channels, as fraud methodology and its sophistication continues to evolve. The digital era has given fraudsters a huge opportunity, especially with millions of personal credentials readily available on the dark web. It is now far easier for fraudsters to hide behind false details and cover up their tracks.

Fraud management systems such as the one provided by Mobileum, rely on many micro-decisions to make an accurate assessment of potential fraud to create an identity risk profile. These decisions are based on knowing the customer through the real-time synthesis of data (social, demographics, purchases, documentation, etc.), monitoring transactions across online and offline channels, and analyzing patterns in real-time. One of the key advantages of Mobileum's subscription module is that it provides a multilayered approach to multichannel identity theft scenarios. By combining a disparity of data, our solution processes the customer's existing data together with third party external data from a variety of sources. In conjunction with adaptive rules, our solution employs Artificial Intelligence (AI) and Machine Learning (ML) models, enabling it to process vast quantities of data across multiple channels in near real-time and detect fraudulent patterns that can then be investigated further by a team of anti-fraud experts. By using AI/ML technology, the system can perform multiple web crawls to detect compromised personal information such as social security number, drivers license, phone number, email addresses, etc. during the opening of online accounts and for product and service activations.

By using supervised and unsupervised algorithms in tandem, Mobileum is able to optimize fraud detection and reduce false alarms. It applies a layered, fraud analytics approach to frustrate the fraudsters in every step of the application process and deter the attacks. This allows collaboration on training data, the creation of shared models, inference results, and the validation of those results.



~500.000
Subscriptions Analyzed

$1.3 Million
in Fraud Prevented

~400
fake IDs identified

~15M
addresses normalized through Machine learning

Advanced Identity Theft Protection
with Dark Web Monitoring

Mobiluem's hybrid AWS based cloud architecture guarantees CSP data privacy

According to a 2017 TM Forum CTIO survey, the majority of CSPs had less than 10% of their BSS in the cloud (private or public). That has probably increased somewhat during the last two years, but, overall, OSS/BSS is still primarily hosted on physical servers and in a telco's own data center. Our customer had implemented a strategy to take advantage of the cost-saving and agility benefits of public cloud for their core business. Mobileum, in partnership with AWS, deployed an advanced fraud detection solution, offering the ability to ramp things up very quickly, without the pain of maintaining physical infrastructure. Despite having a cloud policy in practice, the ownership and the geographic placement of data was a major topic when it comes to data processing when it comes to sensitive data, such as the need to validate a person's identity. We knew that the command and control over sensitive data meant housing the confidential information locally on-premise. Following a hybrid cloud approach (i.e. workloads distributed across on-premise and commercial cloud environments) Mobileum, together with AWS and the customer, designed a hybrid cloud approach where specific workloads are kept on-premise due to data privacy issues.

The security capabilities that are native to a hyper-scale cloud provider like AWS empower customers to create unique architectures for mitigating access risks. On-premise and similar facilities lack the homogeneity, economies of scale, visibility, and automation that can bring significant security advancements. Leveraging the AWS cloud benefits of flexibility, reliability as well as cost savings, enabled Mobileum to meet the CSPs key business requirements. The impressive RoI, achieved in just three months after the system went live, showcased the solution from an engineering and business perspective. Mobileum's fraud and cloud teams had designed such an amazing fraud detection system with very high availability, scalability and accuracy, that is capable of serving telecom customers globally.

Benefits of adapting to the AWS cloud architecture

Technology has changed the way business works, making computing power more available and cost-effective, and regularly surpassing previous performance benchmarks. Businesses are connecting with customers via social networks, analyzing data trends, and creating new must-have products and services - all by harnessing the power of cloud computing. Successful businesses are adapting to a dynamic new way of operating, one that can have positive effects on a company's bottom line.

Mobileum's objective for moving to the cloud was not just about saving costs on IT; it was about creating an advanced technology-driven environment that lets customers' business thrive. The digital revolution has made it easier than ever to connect with customers, develop ground-breaking new insights and scientific breakthroughs, and deliver innovative new products and services.

Our decision to choose the AWS cloud-based architecture was to clear away all obstacles in our path of innovation and leverage on the default architectural benefits offered by AWS, such as:

High Availability and Elasticity with a high fault-tolerant and self-healing storage built for the cloud.

AWS offers complete control and confidence needed to securely run solutions and services with the most flexible and secure cloud computing environment available today.

Data Protection Compliance Assured by complying with CSP data protection standards adopting ISO27001 requirements.

Infrastructure Protection, where AWS protects web applications by filtering traffic based on defined rules.

Ready to Serve. Since launching, Mobileum has been able to maintain at least 99.58% service availability for the CSP applications

Massive economies of scale. By using AWS cloud infrastructure, Mobileum and its customers were also able to achieve a lower variable cost that was one of the main requirements for the CSP.

In Summary

Subscriber behavior is complex because users now log in from multiple devices, locations, and channels. Smart authentication relies on genuinely understanding not only the digital identity of a connecting user but their history too. By using advanced machine learning algorithms in combination with global shared intelligence, it is possible to streamline onboarding, prevent account takeovers, combat multiple fraud challenges as well as to detect insider threats

Mobileum is driving rapid innovation and time-to-market by embracing the paradigm shift to a microservices architecture. RAID for Subscription Fraud along with its machine learning models deployed on the AWS cloud infrastructure, offered smooth launch and training of new ML models for addressing ever-evolving subscription fraud attacks across multiple channels. The access to content and services across multiple channels has substantial authentication requirements. For this reason, the solution automatically executes due diligence machine learning algorithms that gather information on the subscriber across online and offline data stores to understand the risk they might represent to the CSP. The ML/AI solution operates with near-human intelligence to counteract the counterfeiters and reduce losses. Every transaction the model processes increases its accuracy of detection and adds to its enormous repository of historical information, so it is continually learning the practices of habitual fraudsters to defeat them.

“Mobileum is driving rapid innovation and time-to-market by embracing the paradigm shift to a microservices architecture. RAID for Subscription Fraud along with its machine learning models deployed on the AWS cloud infrastructure, offered smooth launch and training of new ML models for addressing ever-evolving subscription fraud attacks across multiple channels.”

fraud & risk
intelligence
Mobileum platform

About Mobileum

Mobileum is a leading provider of analytics solutions for the Telecom industry. More than 750 communications providers rely on Mobileum Active Intelligence platform to increase roaming revenues, improve network security, minimize fraud and risk, and optimize business operations. With a strong record of innovation, Mobileum is recognized for its ability to extract deep network and customer insights and to convert them into real-time actions that increase revenue, improve customer experience and reduce costs. Headquartered in Silicon Valley, Mobileum has global offices in Argentina, Dubai, Hong Kong, India, Portugal, Singapore and UK.

Learn more in www.mobileum.com
and follow @MobileumInc on Twitter.

MOBILEUM, INC.
20813 Stevens Creek Boulevard, Ste. 200
Cupertino, CA 95014 USA

Phone: +1-408-844-6600
Fax: +1-408-252-1566

mobileum.com