CASE STUDY

OUTWITTING FRAUDSTERS WITH DEEP ANALYTICS

Abstract

An Australian telecommunications firm was receiving an increasing number of complaints from customers whose accounts had been misused by fraudsters to place unauthorized orders. This case details how Johann Coker, Senior Manager for Business Analytics and Fraud Prevention, leveraged the company's 15-year partnership with Infosys BPM to identify such customer account takeovers with deep analytics. Infosys BPM's solution successfully stemmed the systemic fraud running into thousands of dollars, and thereby prevented the erosion of customer trust.

Infosys®
Navigate your next

A theft of identities and equipment

Johann Wagner is a Senior Manager for Business Analytics and Fraud Prevention at one of Australia's largest telecommunications firms. Over the last few months, Johann had been made aware that a rising percentage of customer complaints coming into the organization related to fraudulent activities by fraudsters.

Often using stolen credentials, fraudsters were taking over customer's accounts and placing unauthorized orders or modifying their existing orders. For instance, they would request ordered products to be delivered to addresses different from those specified by the customers. The identity theft quickly became a pressing issue. While the volume of such cases was not very large, the resultant financial losses borne by customers were quite high as most of the fraudulent orders were related to expensive hardware devices.

Clearly, the situation was not only leading to a significant loss in customer confidence and trust, but also in revenue. Johann's teams began expending a significant amount of time on post-mortem analysis to understand the top reasons for these frauds, using data science techniques to identify these transactions, later contacting affected customers to let them know about their accounts being compromised.

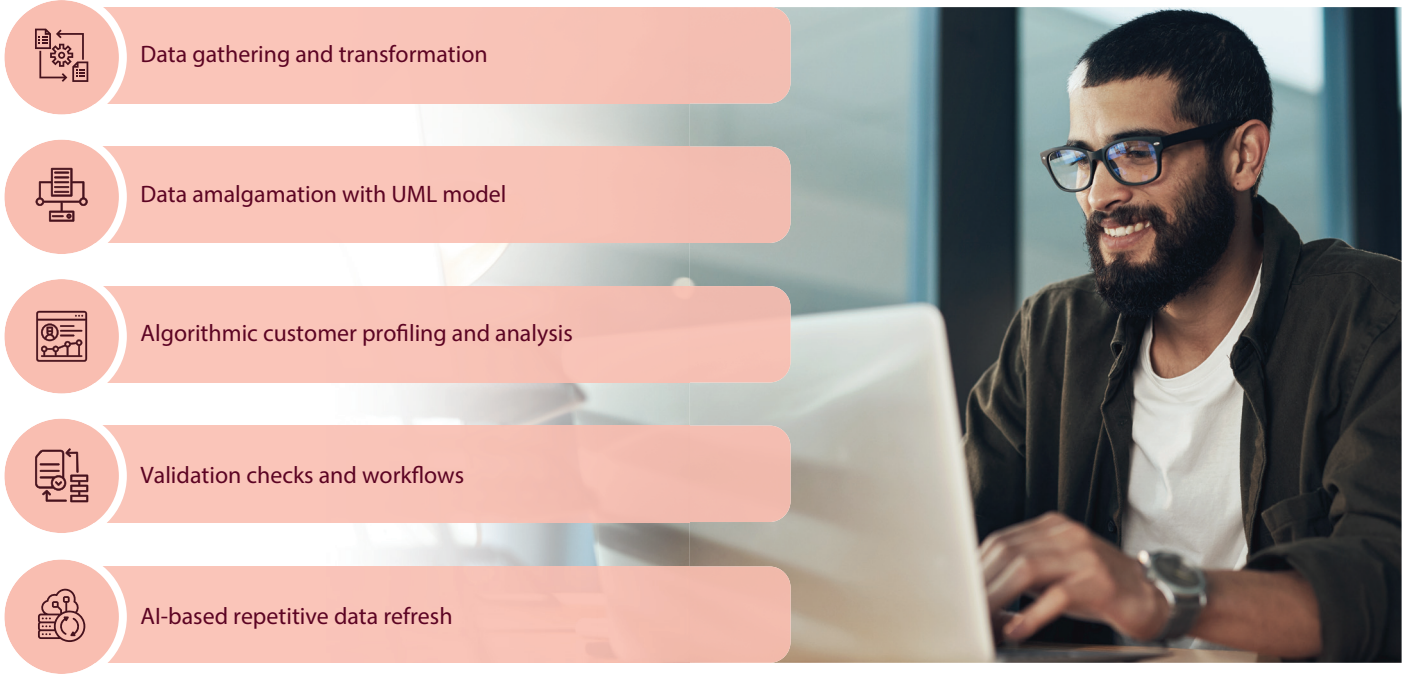
However, Johann was concerned by the challenges his teams faced in tackling these issues. The lack of structured preventive fraud controls meant that they were unable to stem the malpractices at source, and the post-facto analysis that they were doing had hardly stemmed the rising customer dissatisfaction and revenue loss.

Thankfully, Johann knew whom he could call on for help. He called for a meeting with Bhupendra Subba, an account manager with Infosys BPM, the telecom giant's trusted IT outsourcing partner since 2011. The partnership between the two companies had grown and evolved over the years into a strategic one, and Bhupendra and his team had played key roles in several transformation journeys that the telecom giant had undertaken earlier.

Unearthing the fraud, algorithmically

As he briefed Bhupendra on the situation, Johann highlighted his chief concern, the absence of structured preventive fraud controls for the sales and business functions. Bhupendra also understood that Johann's teams had made limited use of machine learning and deep analytics. Thus, they found it difficult to analyse the high volumes of telecom data, especially when faced with the complicated business rules and mix of legacy and cloud-based systems that the enterprise employed.

Approach Summary



The challenge was both massive and complex, but Bhupendra and his team were ready to tackle it head on. They first collected various data points attributed to sales behaviour. This included activation vs disconnection data for the different products offered by the company, data linked to customers' payment behaviour, credit volumes, and address changes, as well as demographic heatmaps. Then the team carried out transformation activities on all the data they had collected, also creating new measures to further improve its quality.

Next, Bhupendra set his team to develop a unified modelling language (UML) model that amalgamated all the different types of data points. After this, the team profiled all the company's customers based on their demographic data, payments, and recent changes in details. Finally, they applied an Isolation Random Forest model using Python scripts to analyse the behaviour of customers and detect any anomalies.

Through randomly partitioning the data sets and isolating outliers, the Isolation Random Forest algorithm was designed to efficiently detect anomalies in the complex, multi-dimensional data sets of the customers' historical purchases. So, with the system fully built, the team moved on to validate its model by running it on historical data, ensuring cross- validation and a continuous feedback loop from the stores and back-end operation teams. They also incorporated workflows to validate all orders before the actual shipments took place. Finally, when satisfied with the solution's effectiveness, they hosted the entire process in the organization's CRM suite, baking in an AI-based repetitive refresh function to gather the latest data.

When the data yields up its secrets

Initially several stakeholders in the organization were hesitant about applying the machine learning based solution to the organization's data, unsure that it would yield the desired results in terms of detecting and preventing the fraudulent activities. However, its effectiveness would soon change their minds.

Key benefits

- 50K AUD fraud prevention
- 2500 fraud customers identified
- Active sleeper cells identified
- 80% reduction in complaint call volumes
- 99% reduction in enquiries on unauthorized device billing

Not long after Johann rolled out the solution, feedback pouring in from the business and sales units indicated that the new fraud detection system had already identified and prevented close to 50K AUD in customer account takeover fraud. Using historical data patterns, the solution identified 2500 fraud customers in the existing customer base of 7700. Its network model also identified active sleeper cells of probable fraud customers who were deeply connected with previously identified fraud accounts, whether active or inactive. With the widespread fraud checked at source, there was soon an approximately 80% reduction in call volumes relating to device sales complaints, and close to 99% reduction in enquiries relating to unauthorized billing.

Johann was delighted with these early outcomes and so were the other stakeholders. And then, apart from preventing account takeover fraud in device sales, the solution's all-encompassing, nearly 100% profiling of customers, now also provided the business with near real-time insights.

But even as the accolades poured in praising the success of the solution, Bhupendra and his team did not have much time to celebrate. Because of growing demand from across the enterprise, Johann soon handed them another mandate. They are now busy migrating their fraud detection model to the cloud for more advanced features such as fully automated business intelligence with feedback loops and preparing for its more widespread deployment across other sales units in the coming days.

**Names have been altered to preserve the identities of the people involved.*

For more information, contact infosysbpm@infosys.com

Infosys®
Navigate your next