USE CASE

Financial Institutions - IT Security

Primary Key Alert Investigation and Resolution

THE SCENARIO:

Financial institutions security systems are configured to identify potential threats on a client's profile. These threats are identified by rules, algorithms based on historical data, typologies, trends etc. An alert is raised when a threat within the client's profile is identified. Certain of these alerts - often referred to as Primary Key alerts - are designed to instantaneously freeze the entire account, blocking any further transactions.

Some examples are:

Suspicious or illegal activity

Unpaid debts through creditors

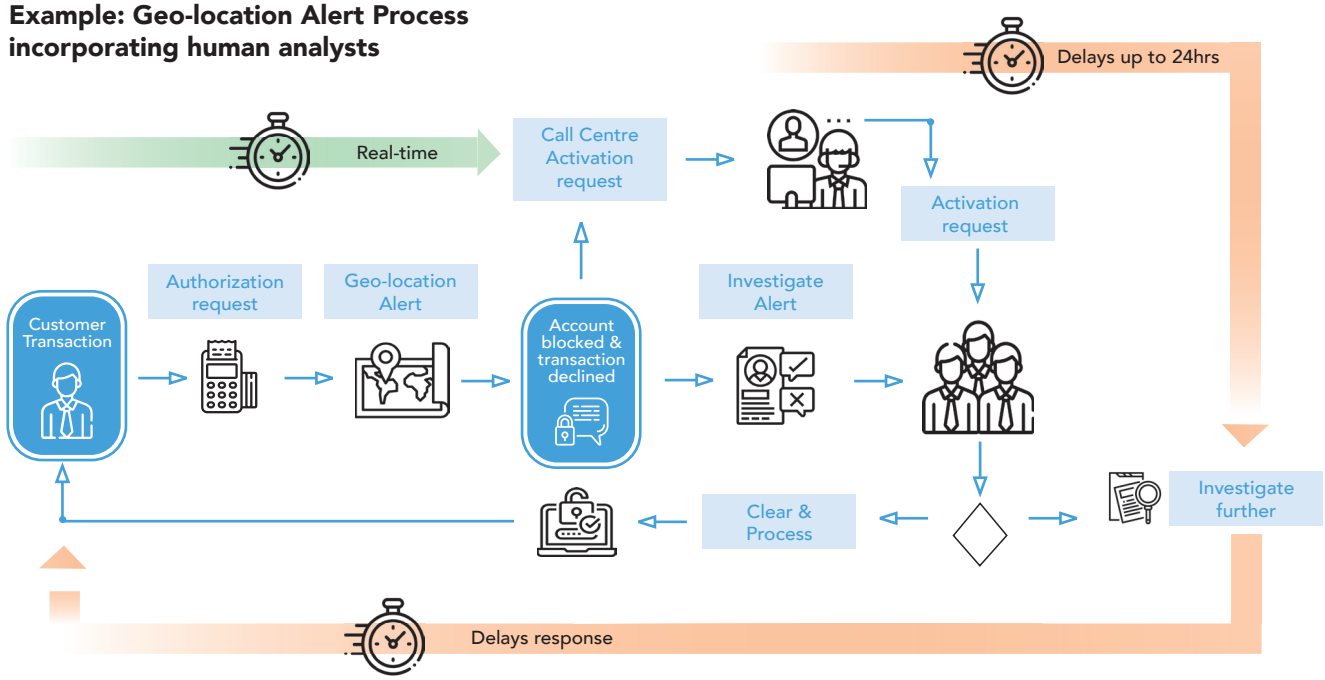
Unpaid debts to the government

A common Primary Key alert is an 'unusual IP address' – a notification or alert that the geo-location is out of the ordinary, this is often caused by international travel of which the bank is unaware.

Depending on the alert type various workflow streams are triggered to investigate and either clear the alert (unfreeze the account); or flag for full investigation.

Although the declined or denied transaction is designed to protect the customers assets, it is usually a very distressing and/or embarrassing experience for the customer, frustration is heightened by delays of up to 24 hours caused by internal processes and limited skilled personnel to efficiently manage the alert.

Example: Geo-location Alert Process incorporating human analysts



Technology with Conscience

THE CHALLENGE

Primary Key Alert screening is a high risk, high consequence activity. Incorrect key activations potentially enable fraud, identity theft or any number of illicit activities to be perpetrated, leading to major reputational damage for the financial institution. Fraudsters constantly evolve their modus operandi to outsmart and bypass systems. In a fluid risk environment rules are unable to accommodate constantly shifting parameters and data driven AI takes time and numerous records to recognize trends.

Screening decisions are therefore entrusted to experienced analysts who have, over time, developed and honed the intuition and judgement required to accurately identify suspicious activity, as well as the know-how to, under pressure, consider and analyze all relevant risks and make the right decision before action is taken.

Action is binding - once a key has been activated the process to deactivate is complex, therefore decision accuracy is of paramount importance.

Banks are obligated to ensure that the security of client accounts are dealt with in an accurate, consistent and efficient manner. The challenge to execute on this with limited expert resources, is a globally challenge.

CASE STUDY

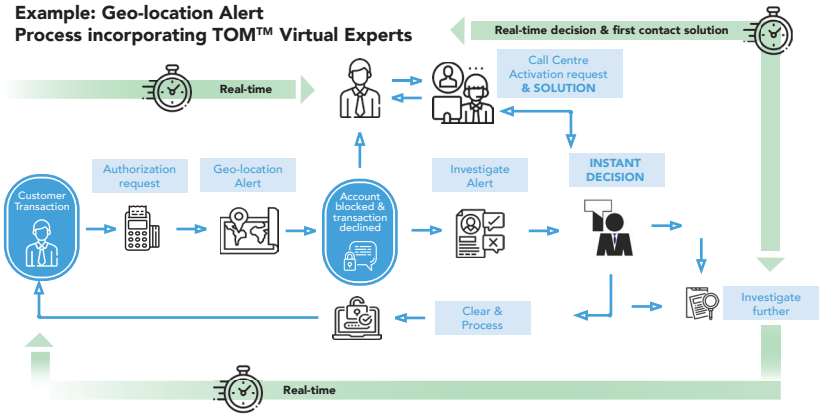
A multinational retail and commercial banking customer identified the need to create efficiencies without compromising risk, within its alert monitoring operations. Merlynn's Tacit Object Modeler - TOM™ was identified as the AI technology to digitize existing human expertise providing real-time access to decisions made by the analyst, thereby enabling the bank to automate this high-risk process.

PREVIOUS PROCESS

Due to the dependence on human expertise Primary Key alert screening and activation was handled through a manual work-flow and only available during office hours.
The process was initiated when the call center captured a primary key activation request on the workflow system. The existing SLA required the assessment team to provide a security decision within a certain timeframe, and then manually execute the necessary action.
Turnaround times on requests submitted outside of office often exceeded the group's SLA negatively impacting customer experience
In cases where the activation request was denied, the client would contact the call center to appeal the decision. This request would then be sent through for further investigation by a security assessor.

TOM SOLUTION

TOM™ was used to model and scale the analysts expertise. The bank now enjoys 24/7 access to digitized expert decisions via the TOM API. Models were deployed and integrated into existing RPA and workflow systems automating the process, dramatically improving activation response and first contact resolution times for legitimate transactions. This has had a positive effect on customer service and experience, risk management and scarce resource optimization.



1. PROCESS & RESOURCE OPTIMIZATION

a) Real-time 24/7 turnaround with zero human intervention.
b) call center able to approve or decline the request at first point of contact with the client - enhanced customer experience
c) Team spends time investigating true exceptions.

RESULTS & RETURN ON INVESTMENT:

	Prior to TOM	Post TOM
Activation requests (Annual average)	24,000	24,000
Average turnaround time within office hours	± 4 hours	2000 per second (real-time)
Average turnaround time outside office hours	±12 hours	2000 per second (real-time)
Capacity, availability	9am-5pm weekends 0 holidays 0	24/7 365 days a year

2. ENHANCED RISK MANAGEMENT

a) Reduced human error - model provides consistent high-quality decisions of best analysts
b) Real-time response to suspicious activity / true alert
c) Rapid refinement functionality - changes to policies/ regulations / threats etc.
d) Decision, consistency and reasoning visible for auditing purposes
e) Team capacity to research new security/ cyber and financial crime risk typologies and threats

For more information visit
www.merlynn-ai.com

Technology with **Conscience**