> *"Today's fraudsters are not the opportunists of old, they are highly organized and technically sophisticated.*

The dramatic surge in card fraud during the pandemic has been well documented. More recently, market research is showing a reduction in the number of fraud cases as a result of payments organizations implementing modern fraud prevention solutions. However, while the volume of card fraud is declining, the monetary amount of fraud is not, as fraudsters continue their penetrative testing looking for easy targets. Our interview with Fabrice Daniel, Head of the AI team at Lusis briefly introduces some of the key factors that payments organizations should consider in respect of their fraud platform.

Q. Why should an organization consider upgrading their fraud decisioning platform?

F.D. : There have been significant advances in AI research for fraud detection in recent years. Advanced gradient boosting decision trees, deep learning models like Fraud Memory, rules extraction methods like Anchors, or even the Dempster-Shafer theory to combine many probability outputs are only some examples. Payments fraud is an ever evolving challenge and the older fraud prevention solutions are unlikely to cope with the newer fraud attacks. Today's fraudsters are not the opportunists of old, they are highly organized and technically sophisticated. If your fraud decisioning platform and procedures are out of date then you are significantly increasing the likelihood of a serious fraud attack.

Q. What should an organization look for in a new fraud solution?

F.D.: For one thing, you want to make sure that your strategic fraud solution can be deployed in the cloud and leverages the significant processing cost savings of cloud deployments. Additionally, a modern fraud solution needs to provide massively parallel processing to allow customers to deploy a comprehensive mix of rules and machine learning models without significant processing latencies or excessive cost.

The cost of fraud screening is a legitimate concern, both in terms of computational resources but also in staff costs. Each organization is likely to set their own balance between processing costs and the breadth of screening. However, as a rough guide a large organization should expect to process 50 million transactions using 40 rules with a per transaction latency of under 10 milliseconds. This level of performance ensures that they can deploy a sufficiently stringent fraud screening strategy in a timely manner.

The ability to run multiple rules engines simultaneously is another important capability. Trying to rely on a single all-encompassing rules set or model leads to greater inaccuracy. It is far better to use multiple models and rules sets, each tuned to catch a specific set of fraud attributes. This strategy results in higher accuracy and easier management.

Q. Is good fraud decisioning purely a matter of technology?

F.D.: Although the right technology is a critical element, it is even more important that the operational staff and analysts can interact effectively with the fraud decisioning system. The fraud team needs to establish a continuous learning environment whereby new transactions are assessed for emerging fraud patterns, new rules and machine learning models need to be developed and validated, and the approved rules and models need to be deployed into production with full change-audit transparency. Obviously robust version control needs to be an integral component of the learning process, as do the operational procedures used to manage the validation testing and governance.

Ideally the fraud decisioning platform should also include an integrated test transactions repository that enables analysts to create different libraries of transaction scenarios. These transaction sets can then be used with the built-in back-test system to validate new rules and models. For greatest efficiency the analysts should receive clear and intuitive reporting on the test results to optimize the model quality.

Q. When should organizations take action?

F.D.: The most important principle is don't wait. The nature of payments fraud is continually evolving. To successful prevent fraud organizations need to develop the operational skills and procedures to manage continual change. For many organizations this is a very different situation to what they are used to. Many organizations 'lock down' their systems and allow only limited changes. However, transforming your organization to a CI:CD methodology is not just about technology, it is also about helping people overcome their uncertainties of change.

The most successful organizations shift to this 'always changing' mindset by taking frequent, well defined, 'baby steps' and make extensive use of automated testing. The use of automated testing provides immediate feedback on progress and importantly helps the staff to build confidence within a backdrop of continual change. Establishing a continual learning environment of this type takes time so the quicker that organizations start the better.

TANGO AI Fraud technology results from a multi-year research program between Lusis and leading Paris Universities and institutes to provide the most effective anti-fraud solution available.

Lusis Payments proudly provides **TANGO AI Fraud (AIF)**, an advanced fraud prevention solution specifically designed to defeat the most determined thieves. Using a rich combination of rules, machine learning, and deep learning, TANGO AIF provides iron-clad defense against current and evolving card and merchant fraud. Already deployed with one of the world's largest merchant acquiring banks, TANGO AIF has the robustness and scale to tackle the most challenging of workloads and fraud threats. Contact us to learn more about TANGO AI Fraud.

lusis
Payments

The Proven Advantage

France:

5 Cité Rougemont
75009 Paris
France
(+33) 1 55 33 09 00

United States:

315 Montgomery St.
#900
San Francisco, CA 94104
(+1) 415 829 4577

Canada:

Eaton Centre
1 Dundas St. W, Suite 2500
Toronto, Ontario, M5G 1Z3

UK:

1 Northumberland Ave
Trafalgar Square
London, WC2N 5BW
(+44) 207 868 5288

Luxembourg:

321, route d'Arlon
L-8011 Strassen
Luxembourg
(+352) 31 35 02-1

Latin America:

Francisco Díaz Covarrubias #14,
Circuito Ingenieros, Ciudad Satélite,
Naucalpan de Juárez, Estado de México,
CP 53100
(+52) 55 9195 5136

www.lusispayments.com   sales@lusispayments.com