BOSS TALK

CYBERSECURITY

DOROTHY NAKAWEESI

The one thing that criminals can't fake

As Uganda embraces digital transformation, the dark side of the web follows. In 2026, cybercrime is automated, intelligent, and more dangerous than ever. The National Information Technology Authority reports a 300 percent spike in automated attacks. *BD Life*'s Dorothy Nakaweesi spoke with Mr Mark Mwanje, the managing director of Creditinfo Uganda, a local Credit reference bureau, about their identity verification, and fraud detection solution, that protects businesses and financial institutions from cybercrime.

Could you explain how the platform uses credit bureau data and government records to verify a user's identity?

Ideally, the platform examines the credit bureau data associated with the presented identity, assessing the data we hold against four areas. It uses that information to generate an aggregate score. The four areas are:

Bureau Footprint assesses the breadth of the data we hold for the presented identity – multiple records from a range of contributing organisations, reflects a higher level of trust than thin file cases. Mature Anti Money Laundering (AML) regimes require multiple confirmations of an identity.

Activity history examines the payment behaviour over time – evidence of both recent and consistent long-standing payment activity is challenging for a bad actor to synthesise.

Data consistency looks at how stable a person's information remains over time, while AML regulations require those identity details to be verified across multiple sources. When the data doesn't match or shows anomalies, it signals a higher level of risk.

The third area is application velocity, which assesses the recent application history for the presented identity – moderate velocity is the expected observation, but excessive recent and declined applications are indicative of higher risk.

Then, the platform leverages government information services and registries to further verify identities.

Finally, the National Identity checks that use the National ID number to retrieve identity attributes, including the driving licence number, address, phone number and email address.

Phone ownership checks use industry data to check the name associated with the presented phone number while bank ownership checks use industry data to check the name associated with the bank account.

The data is cross-checked against the provided identity. The platform returns flags indicating the strength of the match and adjusts accordingly.

How does the platform integrate identity proofing and digital risk signals to detect fraudulent identity claims?

The solution draws on multiple sources of data generating comprehensive risk and trust signals. Single point verification presents an attractive attack surface for fraudsters. There is little challenge in synthesising a narrow set of data. This represents a single point of vulnerability.

Our solution creates a hostile environment for fraudsters—making it virtually impossible to build a consistent, anomaly-free credit and digital footprint across multiple identity attributes. We want to ensure that organisations are attractive providers for genuine customers but not for criminals.

What kind of watch lists will the platform screen against, and how will this strengthen the screening process?

The platform will screen against international and domestic watch lists including sanction lists and other risk indicators, to enhance detection of high-risk entities.

The platform's flexible configuration allows fine-tuning to reduce false positives and align screening rules with the local AML regime, ensuring stronger more accurate oversight.

Mr Mark Mwanje, the managing director of Creditinfo Uganda, explains that data consistency assesses the stability of personal information over time. PHOTO/MICHAEL KAKUMIRIZI

Cyber risks

- Uganda has made significant progress in recent years in strengthening its anti-money laundering (AML) framework, including its removal from the Financial Action Task Force's increased monitoring. But the rapid expansion of digital payments has introduced more complex fraud risks.
- The transaction monitoring system operates without capacity constraints and delivers risk assessments within 200 milliseconds.

How does the platform support KYC compliance and AML regulatory requirements?

Robust identity proofing is a core regulatory focus – organisations are required to confirm they are interacting with a genuine identity not a synthetic identity, particularly with the upwards trend we are seeing in synthetic identities being use to commit financial crime.

Additionally, organisations are required to confirm they are interacting with the owner of the presented identity rather than a criminal presenting a stolen identity.

Once robust identity confirmation is complete, organisations are required to check whether an individual has been sanctioned or is Politically Exposed (PEP), or is a relative or close associate of a sanctioned individual or PEP.

The platform can help organisations meet all three of these requirements with robust identity proofing across multiple sources, digital risk assessments and watch list screening against comprehensive sanction and PEP sources

Digital footprint

'The platform gathers insight from a large range of sources and can identity anomalies in the digital footprint.'

How does the platform balance fraud protection with customer experience, particularly during onboarding?

It delivers strong fraud controls through a streamlined, low-friction onboarding process.

This minimises unnecessary steps, so fraud checks do not disrupt the customer experience.

It also reduces abandonment rates while maintaining robust protection.

What benefits can organisations expect from using this unified platform, and how will it improve their risk management processes?

Uganda has made significant progress in recent years in strengthening its anti-money laundering (AML) framework, including its removal from the Financial Action Task Force's (FATF) increased monitoring. But the rapid expansion of digital payments has introduced more complex fraud risks.

Our platform equips organisations with robust, integrated tools to detect and mitigate these emerging threats earlier, without adding friction for customers. Overall, the unified platform enhances end-to-end risk management by improving detection accuracy, supporting compliance, and helping organisations protect both their operations and their customers more effectively.

How does the platform handle false positives or disputed transactions?

The platform provides a facility that enables users to review the results of the assessment. This presents all the results of the assessment within a comprehensive report enabling organisations to manually review the outcomes. False positives are a particular challenge when matching against watch lists – the platform provides highly flexible configuration options that can tighten the search criteria and name matching algorithms within a risk based approach to AML controls.

Can you give examples of the digital risk signals used to detect fraudulent activity?

Criminals exploiting stolen identities cannot present the victim's own email and phone number since they need to be in control of accounts that receive any one-time password or other confirmation steps.

Additionally, they need to avoid alerting the victim to the ongoing fraud. For a synthetic identity, creating a genuine active digital footprint – with long-standing email and phone numbers – actively interacting with social, messaging and service accounts – appearing in historical data breaches presents a significant barrier to criminals.

The platform gathers insight from a large range of sources and can identity anomalies in the digital footprint – for example, recently created email addresses, phone numbers not linked to any messaging services, profile pictures with no human face, phone numbers associated with multiple or many names in the identity graph.

None of these attributes are conclusive in their own right, but a combination of more than 200 attributes is strongly predictive of risk – and conversely predictive of trust – allowing organisations to stop fraud and provide a great customer experience to genuine customers.

How will the platform stay ahead of evolving fraud trends and emerging threats?

The platform offers highly flexible orchestration, allowing new data sources and services to be integrated with ease. As fraud patterns evolve, we continuously monitor outcomes and refine our decisioning and scoring models to address emerging threats.