WEBINAR REPORT

How KYC, AI and regulation shape the financial crime landscape in 2026



Daniel Orchard
EMEA KYC Specialist,
NICE Actimize



Jessica Cath
Managing Partner,
Thistle Initiatives



Dave Laramy
Head of Group Fraud,
ABC & TEP, Danske Bank

Finextra® | NICE Actimize

Contents

00 | Market Context 03
01 | Introduction 04
02 | Fraud in the time of AI 05
03 | How AI is being effectively deployed by banks 06
04 | Organisational challenges and regulatory impact 08
05 | Conclusion 11
06 | About 12

00 | Market Context

AI in the hands of fraudsters is becoming an increasingly sophisticated foe for financial institutions, with recent data finding that as many as four out of five companies have experienced payment fraud attacks in 2024. Going forward, financial institutions must not only keep up with these evolving threats but also anticipate and mitigate them effectively.

In order to keep up with the developments in financial crime, financial institutions need to embrace AI, keep up with regulatory frameworks, and make collaborative efforts with industry counterparts, regulators, and consulting firms in order to leverage wider data pools. KYC becomes crucial in this process, in order to ensure the right information is available from the start of the customer relationship.

This report summarises the discussion from a Finextra webinar, hosted in association with NICE Actimize, featuring a panel of industry experts, including:



Daniel Orchard
EMEA KYC Specialist,
NICE Actimize



Jessica Cath
Managing Partner,
Thistle Initiatives



Dave Laramy
Head of Group Fraud,
ABC & TEP, Danske Bank

01 | Introduction

When it comes to financial crime controls, fraud, KYC and AML developments are posing key questions for financial institutions going into 2026. AFP's 2025 Payments Fraud and Control Survey finds that 79% of organisations were victims of payments fraud attacks in 2024. Simultaneously, regulatory bodies across jurisdictions are taking strong action against fundamental AML failings.

As fraud grows more sophisticated and regulatory scrutiny intensifies, KYC emerges as a critical link in the fraud prevention chain. Yet the overall KYC process can only be as good as the sum of its parts, so how are financial institutions adapting to innovations in technology and the increasing availability of AI tooling?

Meanwhile, sweeping regulatory changes are reshaping the compliance landscape. The new EU AML package establishes a new Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA), with the aim of strengthening EU-wide AML/CFT rules and harmonising requirements across member states. What do these changes mean for financial institutions? And how do they need to adapt their KYC processes and technology to address this new regulatory reality?

This webinar report seeks to answer:

1. As fraud is becoming increasingly more sophisticated, what is the financial crime outlook for 2026?
2. What are the key AI use cases in KYC, AML, and fraud applications?
3. How are financial institutions adapting their KYC technology and processes, and consolidating their systems to enable KYC across functions?
4. How are financial institutions balancing the competing priorities of improved risk management while maintaining smooth customer experiences?

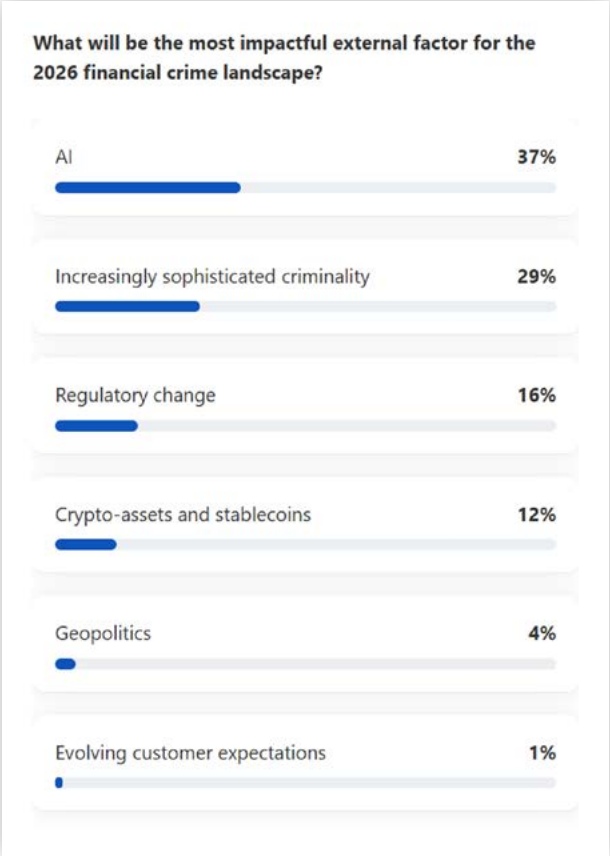
02 | Fraud in the time of AI

Laramy highlighted that fraudsters today are “doing more of the same, but with a higher level of sophistication. They have volume, scale, the ability to switch language, and the ability to change the tactics that don’t work and thus adapt really quickly. The barrier to entry for scams has definitely reduced. Organised crime is moving from some of the traditional higher risk activities, such as drugs, into scams, which is seen as a lower risk activity with lower sentences and lower prosecution rates. So, we are definitely seeing that ‘scamdemic’ attack across the industry.”

With AI coming into the picture, he also emphasised the development of something he calls ‘victim triage’, where the initial conversation happens with an AI agent, and human fraudsters are brought into the scam when it appears worthwhile to do so. This often happens via false websites, which typically involve cryptocurrency scams, that delay the customer reporting the fraud to the bank, as they believe it to be legitimate for a longer period of time.

Another blind spot for banks lies in not knowing exactly what kind of AI has been used in which fraud cases, because it can be difficult to get specific information from customers. This can cause problems in the investigative processes, since banks likely do not see the true scale and extent of modern, AI-driven fraud.

An audience poll (pictured on the right) confirmed that AI, and the resulting increased criminal complexity, is indeed expected to be the most impactful external factor in 2026. This problem can be exacerbated in different regions. Laramy gave a local example: “In the Nordics, we don’t see the reporting of some of the scams that are happening because customers don’t get refunded in the same way as they do in the UK. So, you can be a little blind to the scale of the problem.”



03 | How AI is being effectively deployed by banks

"Although it's difficult to measure, the asset recovery rates globally from financial crime are staggeringly low," Orchard highlighted. "But in terms of the levels of success that organisations are having, there are some really interesting use cases and successes that are happening. They are looking across broader data sets, even as part of consortiums, and collaborating with other institutions. This gives them the ability to then pick up on networks and criminality across a wider scale. There are some really interesting and exciting things happening in that space."

Cath added that AI deployment in financial institutions can still be a "completely mixed bag". Yet the leveraging of different data points from different data sets is indeed one of the strongest use cases for AI, particularly when it comes to transaction monitoring.

"So, not only looking at transaction flows, but pulling in lots of different data points from across the customer profile to properly assess the holistic customer risk in a better way," she expanded. "We're seeing some really exciting things with pattern behaviours, as well as things like adverse media screening. This helps to add that extra layer for the reduction of false positives."

Laramy commented: "In the fraud world, we are lucky, because we've been using machine learning models for some 20-plus years. This isn't new for us. We have started calling it AI because it's a great buzzword."



We're seeing some really exciting things with pattern behaviours, as well as things like adverse media screening. This helps to add that extra layer for the reduction of false positives.

Jessica Cath, Thistle Initiatives

He added that, through AI, "we are seeing better precision and reduced false positives, which helps us to put humans in the areas where we need them. We don't need a human to decline a card transaction, but we absolutely do need a human to talk to a customer that might be in the middle of a romance or a cryptocurrency scam. And that allows us to invest our people and our time into those complex conversations."

Ultimately, the ability to switch strategies based on the level of risk appetite, capacity to deal with alerts, and current fraudster activity is greatly improved by recent developments in machine learning and AI. "There's opportunity to play in the sandbox, optimise, see what works best, and try some new things. Today, we have the ability to create a model much more quickly than before," Laramy concluded.



We don't need a human to decline a card transaction, but we absolutely do need a human to talk to a customer that might be in the middle of a romance or a cryptocurrency scam. And that allows us to invest our people and our time into those complex conversations.

Dave Laramy, Danske Bank

04 | Organisational challenges and regulatory impact

When it comes to regulatory scrutiny, the regulators' primary role is to make sure that consumers can engage with financial services without any harm being applied, which is why the industry is seeing such a focus on fraud prevention. "If we look at the UK, for example, we are a global hotspot for fraud, with around 40% of all UK crime being fraud," Cath emphasised. "So, of course, the regulator is focused on making sure that firms' fraud controls are much sharper than they have been. Historically, the regulators have really put the anti-money laundering agenda at the top of the tree."

Yet on the other hand, the panel emphasised that one of the themes that they are observing, particularly from 2025 and going into 2026, is a back-to-basics approach from the regulator. Since there are vast differences in product sets between different institutions, consequently there are also different risk profiles — meaning KYC and onboarding are crucial aspects of addressing the modern fraud landscape.

Orchard explained: "Governments are looking at regulation as a lever for growth, [to determine] where there might be opportunities to streamline, to scale back, or at least to target some of the regulation that is deemed to be anti-competitive or harmful in that respect. You often hear that regulation is on an ever-increasing trajectory, but I think that's slightly misleading. I think regulatory change is increasing, but not the amount of regulation itself. That certainly creates a challenge as we look into 2026 and ultimately creates some uncertainty."



Governments are looking at regulation as a lever for growth. You often hear that regulation is on an ever-increasing trajectory, but I think that's slightly misleading. I think regulatory change is increasing, but not the amount of regulation itself.

Daniel Orchard, NICE Actimize

Orchard explained that a common mistake he sees organisations make is to think about the end goal as being the application of AI, rather than choosing AI based on the business outcome they are planning to achieve. Determining the business outcomes, for example reducing risk exposure in a certain business area or introducing greater efficiency in another area, needs to happen before choosing the most effective tool. And this tool might or might not be AI.

Cath confirmed this observation, stating that, while some exciting things are happening, it's a learning phase. "We have also seen a number of people deploying AI but not understanding what that model is doing to reduce false positives. They end up missing hits because they haven't quite understood the model."

Another crucial point is adding extensive data to their AI tooling. Cath added that organisations need to "make sure that you are training [your AI] on synthetic data. If you are just using internal data, it will just be training itself on existing typologies instead of new typologies that might not have been targeted for quite yet. If you are part of networks and you are getting other data sets from different parts of the industry, that's excellent."

A second audience poll (pictured on the right) confirmed that data completeness and quality is currently the biggest internal challenge for organisations looking further ahead in 2026.

When looking at the data question, KYC is a crucial aspect for financial organisations that should be considered holistically. "There is a decision in terms of where and if to introduce friction that organisations should think about across the whole customer journey," Orchard commented. "It might be that you ask for an additional data point as part of onboarding, and therefore you introduce a degree of friction, but that enables more robust ongoing monitoring throughout the course of the relationship. And that in turn means that you don't have to re-request that data."



Rather than thinking about the controls in isolation — whether that's KYC, fraud, or AML — organisations need to consider the entire customer journey from the friction perspective. This enables them to understand where they might benefit from upfront friction throughout the course of the customer relationship.

"That's one of the things we're seeing the regulator focus on," Cath confirmed. "If firms don't understand their risk profile, then their control framework that runs off the back of that simply won't deal with their risks fully. Looking back at the KYC onboarding is really important because if you don't understand who your customers are, and the risks related to those customers, then all the other controls that you're building post-onboarding will fall flat."

Laramy added the importance of the real-time intervention in a real-time world. "I do feel very strongly about real-time intervention. That's absolutely critical in today's approach to broaden financial crime prevention overall. If we don't stop the transaction, then we just encourage it on our platform. One of the problems with the regulation on repayment of scams in the UK is that it doesn't actually stop the crime."

This is where the collaboration through public-private partnerships, as well as cooperation with government and law enforcement comes into play, to create international solutions that include data from telecoms and big tech.

"They all have their part to play across the lifecycle of fraud, since we, as banking, only see the end of it, once the payment is about to be made. We're missing some of that upstream vision on exactly what's going on. We can collect some threat intelligence, but we're not ever going to have the whole story," Laramy stated.

> **"There is a decision in terms of where and if to introduce friction that organisations should think about across the whole customer journey.**
>
> Daniel Orchard, NICE Actimize

05 | Conclusion

As fraud evolves, so does the need for more comprehensive fraud detection and mitigation in financial institutions. Not relying on one solution, adapting strategies, including more data points, and above all, testing, lie at the heart of modern fraud prevention in the age of AI.

In closing, the panel stressed the need to optimize core KYC processes before layering AI tools — while maintaining explainability and governance.

Finally, Orchard highlighted the importance of engaging with the regulator during consultation periods, as well as industry counterparts. “So get involved, speak to them, and use your influence as an organisation to shape changes. Equally, engage with your counterparts across different organisations or consulting firms. The more organisations collaborate and share information and ideas, the better place they are in to fight financial crime in 2026.”

About

Finextra Research

This report is published by Finextra Research.

Finextra Research is the world's leading specialist financial technology news and information source. It offers more than 130,000 fintech news, features and TV content items to some 800,000 monthly visitors to www.finextra.com.

Finextra covers all aspects of financial technology innovation involving banks, institutions and vendor organisations within the wholesale and retail banking, payments and cards sectors worldwide. Finextra's unique member community consists of over 40,000 fintech professionals and 200,000 social followers working inside banks and financial institutions, specialist fintechs, consulting organisations and technology providers.

The Finextra community actively participates in contributing opinions, ideas and comments on the evolution of fintech.

For more information visit **www.finextra.com** and become a member, follow **@finextra** or email us via **contact@finextra.com**.

NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti- money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

Find us at **www.niceactimize.com**, **@NICE_Actimize** or **Nasdaq: NICE**.

For more information

Finextra Research
77 Shaftesbury Avenue
London
W1D 5DU
United Kingdom

Telephone: **+44 (0)20 3100 3670**

Email: **contact@finextra.com**

Follow: **@finextra**

Web: **www.finextra.com**

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording or any information storage and retrieval system, without prior permission in writing from the publisher.

© Finextra Research Ltd 2026

Finextra® | NICE Actimize