Icon UK - Fraud incidents: prevention using video-enabled document and identity management systems (Session 3/5)

Business Reporter asked Icon UK some probing questions concerning online fraud incidents and how to prevent them using video-enabled document and identity management systems.

In this session, we're going to examine a couple of recent fraud cases. In a world increasingly moving towards digital processes and staff in remote offices, how do we reduce fraud and deception? We explore how digital smart meeting enablement could have prevented problems.

Fraud incident examples.

The first is a case of mortgage fraud, also applicable to many more types of loan in nature. When we lose the ability to see the people we're dealing with, such as in an online remote self-service transaction, we open ourselves up to potential deception. Without being able to verify individuals using visual, audio, and behavioural insights for face-to-face in-person meetings, how can we be sure that they are who they say they are?

Take the example of banking customer who made a joint application to remortgage his house with his wife. His company was going through some financial problems, and he needed access to some cash. The mortgage application was completed online, and a follow-up call was made to the customer to confirm details.

After a short confirmation call, the application was approved, and funds were deposited in the customer's account. The customer subsequently failed to make repayments on this mortgage, slipping into further debt until the bank decided to repossess his home.

The customer's wife was surprised to find agents at her house and made a frantic call to the bank to find out for the first time that she was party to a new mortgage agreement. As it turned out, the customer had used his PA to pretend to be the wife during the confirmation call. The banker processed and accepted the application with little more than confirmation of the wife's agreement.

A second type is more common. It's a high-value contract executed online using simple e-signing tools, in this case, from a well-known US provider. However, this type of technology is often inappropriate providence for higher value transactions.

How could these incidents have been prevented by digital fraud prevention tools?

There are measures to stop fraudsters signing up in the first place and also to detect impersonation or misrepresentation throughout the years of engagement subsequently with bona fide customers. These include biometric face and voice recognition, identity document validity checks, and video recordings of all parties.

What are the main behavioural benefits of these video-assisted functionalities?

Fraudsters do not want to be videoed. The ability to conduct credit reference checks on the fly also reduces fraud. But the recording of individuals reduces their inclination to lie, exaggerate, or misrepresent, whether it's client side or agent side. Having automated recording of all elements in an online meeting enables a full picture.

How can a business identify the solution that suits it best?

Identify and focus on the high impact areas first, pairing internal knowledge of the as-is process with an external understanding of best of breed options to create a new and clear desired future state plan. Find complete platforms that can be used flexibly for a spectrum of future use cases across the enterprise, whether that's selling, onboarding, AML, KYC, compliance, advice service and support, or whatever.

What are the challenges of implementation, and how can they be overcome?

There's a challenge of fragmentation of technology across organisation. Changing working practises and data privacy are major challenges also. They can be overcome by finding platforms for self-serve as well as human assisted processes; data privacy by design within fast integration using pre-integrated or connectors or low code approaches and for legacy applications; and easy-to-use systems and attention to working practises, such as a professionally suitable environment within call centres as a backdrop to video.

What are the biggest issues that hold businesses back from grasping these processes?

It comes down to internal knowledge, external support, and tools or platform choice. Not all transactions have the same value nor risk and consequences. Solution flexibility's key. External specialist support, such as from ourselves, helps here.

We work with customers with high demands. And we aim to anticipate and respond to an ever-changing set of explicit and latent requirements. Challenging the current ways of working works well, working smarter, not just the same faster. And that means providing educating on the options, guiding from experience to solve problems and highlighting the right tools to compliantly simplify the complex.

Hands-on experience with a range of advanced tools enables new visions of the big picture to be created. With well-designed, highly configurable yet standardised technologies to support digital automation initiatives, process mapping does not need to constrain happy customer journeys.

In the next session, we'll discuss how anti-fraud capabilities can drive conversion rates and customer retention, thus improve the ROI of deployment.