Icon UK - Online fraud types in high value transactions: are we doing enough to prevent it? (Session 1/5)

Business Reporter asked Icon UK some tough questions concerning online fraud. This session covers online fraud types in high-value transactions. Are we doing enough to prevent it?

In this series, we're focused on the role correct and timely KYC plays in the entire customer relationship, either during a specific financial transaction such as a loan application, or for repeated interactions years and years after initial onboarding, such as in wealth management and investments context.

Why is high-value fraud accelerating?

Well, there are many reasons. But some of the key ones include uncoordinated systems and silos of information and a persistent failure to address costly and inconvenient manual breakouts. Within that focus, unlike touch payments which have had huge attention, low volume, high-value transactions are real greenfields awaiting transformation.

Which industries and use cases are the most susceptible to such online fraud?

Industries with advised purchases or complex services. Many types of fraud are committed on both sides of these transactions including by overzealous misselling, such as in the banking PPI scandal, or loss exaggeration by insurance claimants, or amended payments via identity theft in loan applications and mortgages. It's prevalent in almost every industry where clients are engaging in transactions worth thousands of pounds or more.

The broad classes that are common in complex high-value business to consumer transactions are compromised data or documentation, such as for hacking, stealing of identity, and/or an advance-fee fraud, and misrepresentation or impersonation.

Why is high-value digital fraud expected to become more prevalent?

As regulated industries move through their digital transformation programmes, new risks emerge as physical processes are replaced with online ones unfamiliar to staff and to customers. Often the fraudsters will learn faster, and the business is struggling to keep up with genuine client expectations.

And policing is behind this. The National Fraud Intelligence Bureau's crime survey last year identified that there's almost no area of high-value transactions that's immune from fraud. Fraud is a crime of deception. Entire life savings or even houses can be wiped away. And customers will in time lose trust in computer-only processes. We must rehumanize but re-equip our processes for a digital age.

Consider a new customer for a loan, mortgage, or financial investment, pension or otherwise. Current business systems comprise many silos of data and process types, typically moving through steps of meet, share, guide, verify, convert, and serve. Now in these, there are multiple departments, multiple handoffs, multiple media types and formats. Often each department uses its own data store and uses different tools for collaboration and customer communication. No wonder it's so hard to get a timely and consistent understanding of clients.

In regulated industries, where we focus, it's about helping our clients tackle fraudulent behaviour whilst enabling sales acceleration and control. Robo-advisory and self-serve platforms are growing. But humans are currently still best at data and process integration when faced with real time customer demands across complex areas.

Until recently, many advisory type meetings occurred as expensive physical co-located meetings or via more impersonal chat or telephone support. Now organisations are experimenting with a solely self-service model. But this is also prone to fraud, in this case, unattended fraud, where fraudsters have plenty of time to test system weaknesses and are mostly doing so unobserved. However, when implemented correctly, remote human-supported meetings can outperform self-serve overall.

Are we doing enough to prevent high-value digital fraud?

No. In England and Wales alone, there's at least 5 million fraud and cyber crimes last year equaling all of the crime in total. Much police-reported fraud is for banking and credit accounts, whereas consumer retail fraud and advance-fee fraud are prevalent and under-policed. The real figures are probably five times higher.

It's a big and growing problem as transactions are increasingly digitised, so fraudsters adapt faster. And the most valuable transactions attract the best fraudsters, often in organised gangs, and are increasingly sophisticated. Add in a significant percentage of business fraud that's insider enabled, and threats come from all vectors.

What's the biggest threat?

Moving too slow to transform before customers are lost. That risks the entire business as customers' expectations rise exponentially. Technology is now there to easily rebuild processes to eliminate pay-per-use, like for wet signatures and documentation, and to replace most physical meetings. While so doing, we can eliminate all signature fraud and almost all impersonation fraud. Corporates too slow to implement sophisticated, online, anti-fraud and smart meeting solutions leave space for competitors to grasp the early mover advantage.

The difference is simply huge-- customer satisfaction and operational efficiency gains of 10 times the laggards. Solution platforms enable extraordinary scaling up of volumes, while simultaneously reducing fraud to easily manageable levels. Organisations need to rehumanize suitability to service processes. Buy, don't build. And manage change as well as selecting the right technology.

In the next session, we're going to talk more about such solutions and capabilities on the market that can help with managing and mitigating with the challenges from such siloed processes and combat online fraud.