CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

Analysis

E-KYC in the Era of Rising Digital Crime

James Roche

James Roche
Senior Consultant for Authentication, Identity and Scams
FICO

Biography

James Roche is a Senior Consultant for Authentication, Identity and Scams covering the EMEA region at FICO (https://www.fico.com). He joined FICO in early 2020 after working in fraud and business transformation functions at a number of major global banks.

James has substantial experience in both UK and European markets and has focused on delivering strategy and solutions for fraud, driven by regulatory initiatives including 3D Secure 2, PSD2 and Strong Customer Authentication and Open Banking.

Keywords Electronic Know Your Customer (e-KYC), Anti-money laundering (AML), Identity validation, Identity verification, Authentication
Paper type Research

Abstract

Even before COVID-19, the risks of online fraud were being highlighted by industry professionals. Earlier this year Cifas, the UK's fraud prevention service, reported that in 2019 over 364,000 cases were recorded to its database[1] – the highest ever recorded. Online retail saw one of the most significant rises in cases – with a 100% increase. Technology was identified as playing a key role in facilitating fraudulent conduct, with 87% of identity fraud in 2019 occurring through online channels. And in a separate study[2] by Cifas, three quarters of fraud prevention professionals said COVID-19 will have a 'significant' impact on fraud, and more than 90% warned of fraud spikes in 2020 and 2021.

Against this backdrop compliance teams face huge challenges in balancing KYC with customer satisfaction. When consumers move their financial lives online, they expect a simple streamlined process and less paperwork. Digital on-boarding is, however, impeded by regulations, legacy systems and a disjointed approach to customer due diligence (CDD), also known as KYC in online or in-app environments. In this article, the author examines how compliance teams can adapt for a digital environment.

Introduction

The regulations say customers need to prove their identity online using official documents and authoritative data records. Customer Due Diligence (CDD) / Know Your Customer (KYC) also asks a provider to understand the affairs of the applicant to a sufficient degree in order to set expectations for how they will make use of a

CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

service, especially a financial one. At each stage of the process, the applicant wants to know that the business values them and their time, and that their personal information is safe. This is likely to frustrate existing customers who would have previously been asked for and provided this information, and many may find the need to confirm details throughout the process tiresome.

There are, however, serious concerns associated with removing all friction. If a fraudster can take over an account and apply for a product without all the necessary checks, the real customer may be harmed. If lax KYC processes allow money laundering to occur, the bank can face massive fines and loss of reputation. Therefore, having some customer friction in the process can bring a positive benefit: awareness that security is going on behind the scenes provides customers with peace of mind.

Compliance can alleviate costs

The choice of identity verification solution often lies with those tasked with providing excellent customer service. Customers are directly involved with proving their identity, making it vital that this process is not so difficult or time-consuming that they abandon their application. That said, if the identity proofing put in place is not adequate to meet the regulatory requirements for KYC, then customer friction downstream is inevitable as compliance teams reach out to the customer for additional proofs of identity. Compliance is too often seen as a cost of doing

CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

business, but done right it protects the organization from loss of reputation and substantial fines – involving compliance teams in the design and choice of identity proofing solutions is vital.

The applicant's identity and data should drive the process

The applicant, their identity and data are the key to understanding the process and therefore businesses which architect their procedures around their customers will see better conversion rates and lower risk.

Applicants appear from many different routes. In some cases, the business may have no information, little information, an identifier in an existing customer database, or a complete set of data. The on-boarding process must therefore be flexible enough to cope with these different situations.

An applicant-focused on-boarding process should be designed to request only the necessary information at the right time. The functions of "identity proofing" and "credit and affordability" within financial institutions can overlap much more than they already do to reduce customer friction and improve efficiencies.

A consistent journey through the application procedure builds customer confidence and results in the capture of higher quality data. At the same time, as the applicant moves through the process, the business builds up confidence in their identity and


CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.
The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

information. In some cases, analysis of the flow may develop a better order to prompt the user for data or identify another source where data can simply be looked up.

The key steps to e-KYC

1. **Basic** – The on-boarding process for a regulated entity which must perform customer due diligence or KYC, fraud prevention for a new customer starts with basic data – contact information, including email address.

2. **Identity validation** – The next step is to gather any identity evidence necessary – for example passport number or official name – and check the identity against public lists of politically exposed persons (PEPs) and companies or individuals subject to sanctions.

3. **Identity verification** – Having proved the claimed identity exists, the next stage is to prove that it belongs to the applicant. Matching the person to identity evidence, for example using facial matching to the photo in a passport, establishes the official identity of the application.

4. **'Liveness checks'** – Criminals that attempt to open accounts using a stolen identity try to break through the integrity of digital onboarding with recordings or a photograph of the legitimate identity holder. The key to detecting these is to identify when a recording or photograph is in use; this is known as a 'liveness' check. Liveness detection in digital channels generally falls into three categories:

5. **Passive** – Often using machine learning, an assessment of the applicant for signs that it is a photograph or recording.

6. **Active** – The system asks the applicant to carry out certain activities such as look up and down, blink etc.

7. **Live video link to an operator** – less scalable, more expensive and adds friction to the customer experience but a regulatory requirement in some countries.

Depending on the level of risk and regulatory requirements, organizations can use one or more of these techniques. For example, a passive liveness check could form a 'first pass' with any borderline decisions resulting in stepping up the check to active liveness detection or video contact with an operator.

Data matching

Fraudsters operating at scale cannot have a completely unique data set for each fraudulent application, so some data elements are re-used across applications or re-used with only minor variations. For example, the same mobile phone number might be used across multiple applications or names reused with slightly different spellings. Data matching and analytics will help to spot similarities across applications and reveal any links between them.

CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

Compromised account checks

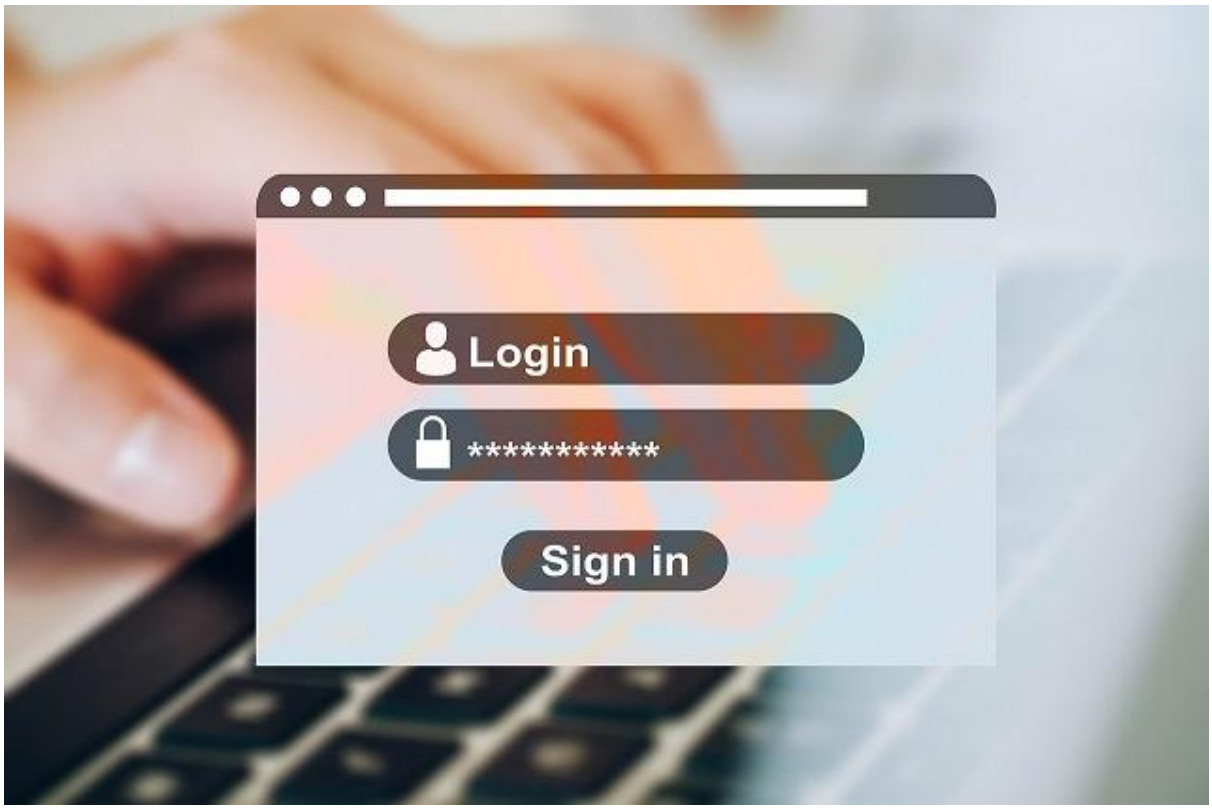
Any system relying on people can never be totally secure. Customers store their login details unencrypted, re-use passwords and lose mobile phones and security tokens. Techniques must be used to spot signs of a compromised account, and these techniques include geolocation, device identification and behavioural data.

Source of wealth and funds

One way to look for money laundering is to gain an understanding of applicants' source of funds. It is important to explain why these questions are asked.

Re-authentication in future transactions

The last step before opening the account is to determine how a customer will be re-authenticated in future interactions. Existing customers may already have methods in place, but it is good practice to allow them to update authentication factors to increase security, or to update a biometric which might change over time.



In conclusion – the applicant should be central focus for each business discipline

During the on-boarding process is it vital to obtain good, accurate data from applicants. Data which the business already holds could be verified if it might have changed, but applicants may ask why they are being prompted again for static data. It is only as the applicant makes their way through the on-boarding process that the


CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.
The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

questions and data required become apparent. It is important to build a flexible process which can adapt to each applicant's particular circumstances.
Through this approach, the applicant becomes the point of focus for the internal disciplines of the business:

- The customer experience group is tasked with ensuring positive customer outcomes in a streamlined manner.
- Compliance ensures legal obligations and regulations are met efficiently.
- IT security is concerned about session, application and endpoint security and resilience.
- Software engineering must ensure systems are robust, secure and maintainable.
- Fraud management is focused on balancing losses and liability against preventative measures.
- Business owners are focused on increasing cost-effective generation and protection of revenue.

Only once these skills are brought together, with an emphasis on improving the customer journey, can a business build smart on-boarding processes and benefit from happy customers, reduced risk, compliant procedures and increased revenue.

Reference

[1] https://www.cifas.org.uk/newsroom/highest-numbers-2019
[2] https://www.cifas.org.uk/newsroom/survey-reveals-4-in-5-unprepared-for-2020-fraud-levels