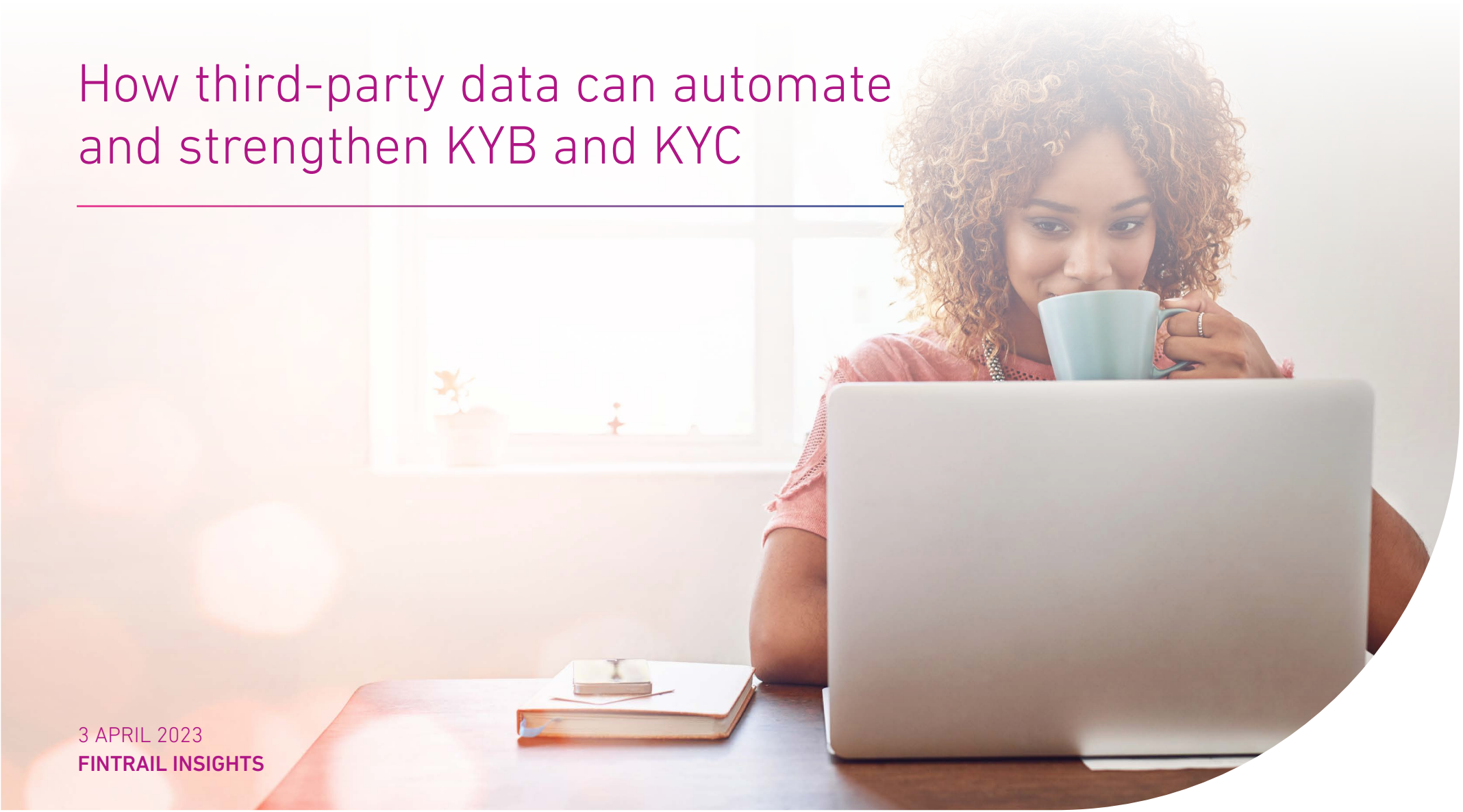
How third-party data can automate and strengthen KYB and KYC



3 APRIL 2023

FINTRAIL INSIGHTS

Table of contents

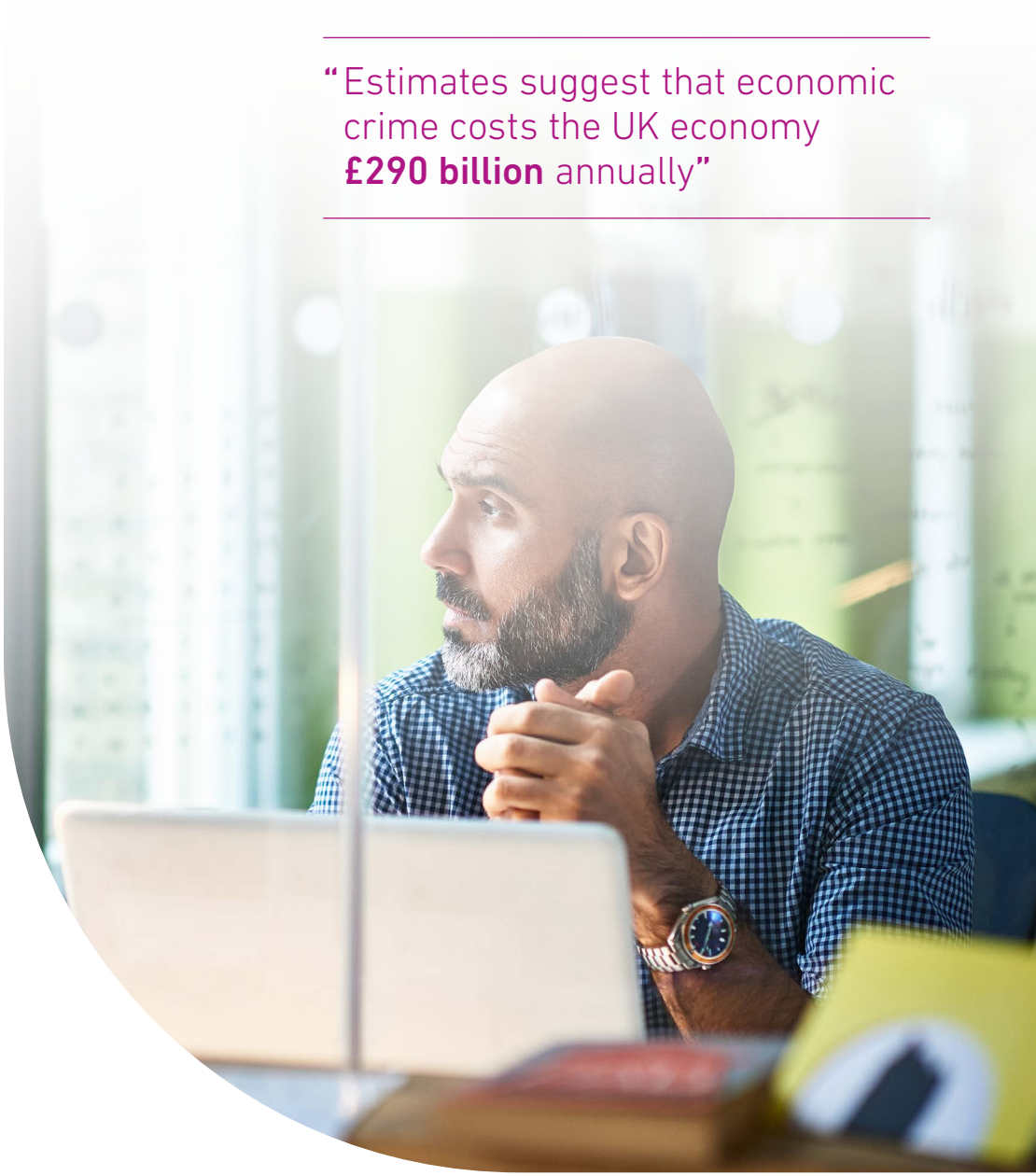
Introduction

The UK is front and centre when it comes to persistent and evolving financial crime threats and is widely reported as a global hub for money laundering[1].

As countless scandals and investigations reveal, the UK is often seen as a prime target for illicit activity. Estimates suggest that economic crime costs the UK economy £290 billion annually[2]. There are a few reasons for this. The UK enjoys a level of credibility and reputation as a leading global financial market, with a government that champions growth and international trade. Although being seen as having some of the most robust anti-money laundering legislation globally, it has, until recently, lacked the political will to enforce this and tackle dirty money. Despite having one of the most transparent and public beneficial ownership registers in the world, the use of corporate vehicles with opaque ownership structures, such as the anonymity that the controversial Scottish limited partnerships afford, have been used to launder illicit funds worldwide.

Given the penchant for using UK businesses as a vehicle for financial crime - what more can financial institutions do to protect themselves? And more practically, how can critical parts of the anti-financial crime workflow be optimised? This paper addresses some of the challenges with conventional Know Your Customer (KYC) and Know Your Business (KYB) methods in a UK context while proposing a complementary solution for the compliance toolkit - using aggregated third-party data. Highlighting the UK's unique position of having a wealth of data to source from, this paper draws on case studies and practical examples to demonstrate how enriching and automating KYC and KYB data can not only protect UK financial institutions from malevolent actors — but also provide a wealth of benefits to their overall business.

"Estimates suggest that economic crime costs the UK economy **£290 billion** annually"



[1]Transparency International

[2]The Financial Times

Spotting dirty money

Following industry campaigning, investigations, and media scrutiny, which accelerated post-Russia's invasion of Ukraine, the UK government is taking more proactive steps toward corporate transparency.

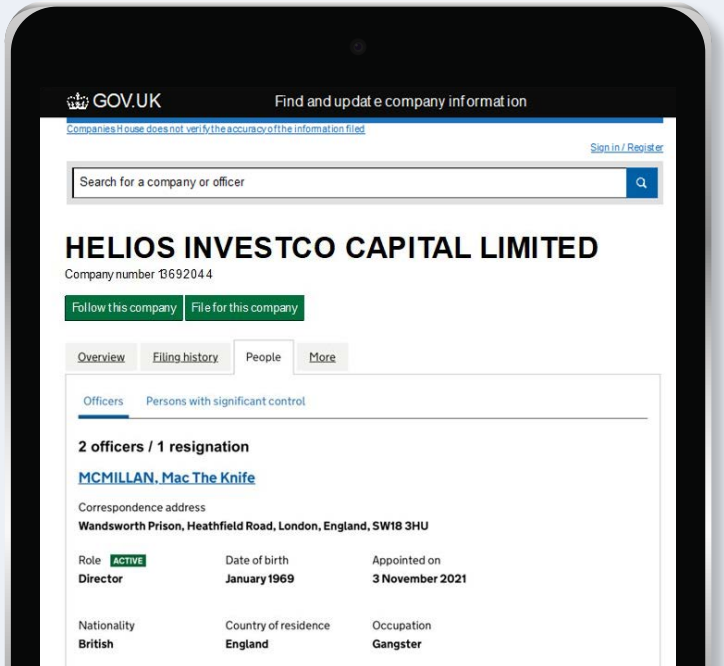
The well-known and documented issues with Companies House have been one specific area of focus. Currently, it costs only £12 to incorporate a UK-registered business (versus nearly €300 across the EU), and at present requires only self-reported information, meaning virtually anyone can register a company. Pranksters and criminals demonstrate the ease at which the register has been manipulated. Additionally, UK companies are often readily sold 'off the shelf' around the world, allowing people to capitalise on the UK's favourable reputation and consequent lack of scrutiny.

Alarming trends in Companies House

Analysing Companies House data exposes some emerging threats and alarming trends. In the last three years alone, there's been a 116% increase in businesses connected to EU-defined high-risk third countries (those countries most commonly associated with financial crime), rising from 19k in 2019 to 40k in 2021. In the last decade, there's been a doubling of UK businesses where there are no UK-based directors (35k in 2011, rising to 70k in 2021).[3] Another trend is the rise of zombie company directors. Zombie company directors occur when criminals steal the credentials of the deceased, appointing people to become directors of active businesses after their death. There are 6,452 new incorporations today where the directors were already dead at the point of formation.[4]

Examples:

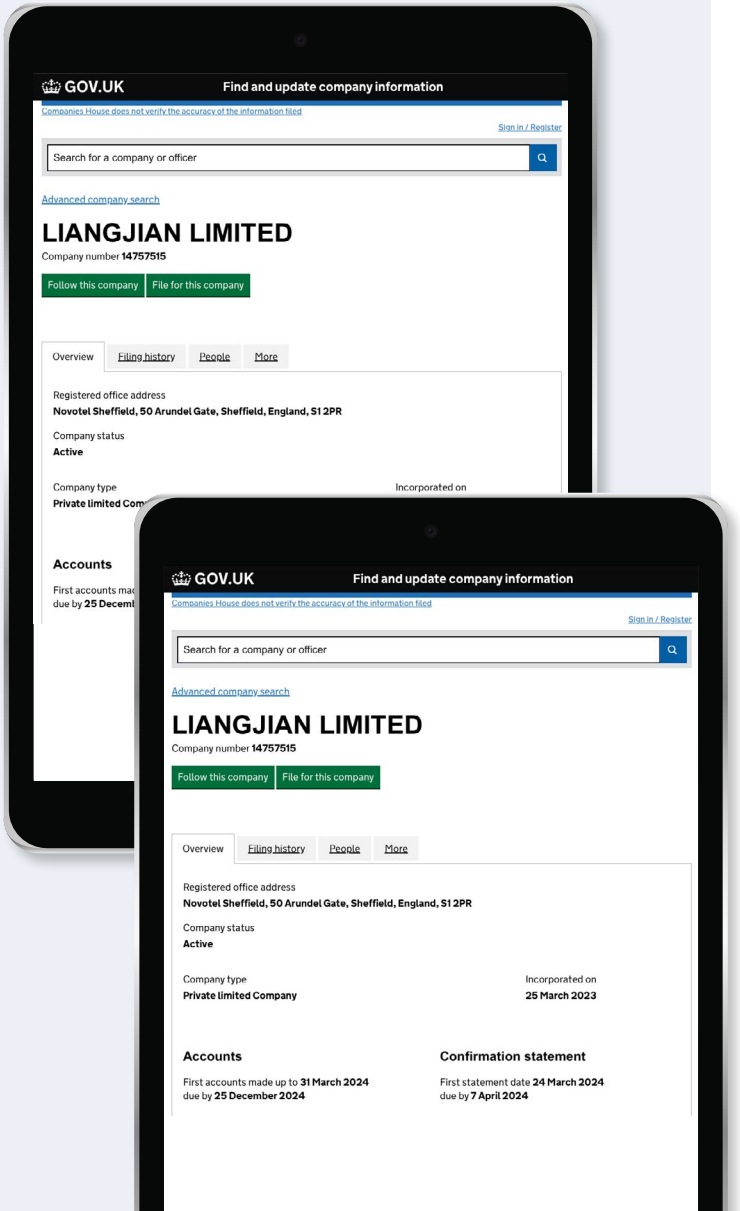
The below example shows a real new company where the director, Mr 'Mac the Knife McMillion', has registered Helios Investco Capital Limited, with Wandsworth Prison as the correspondence address. You may note that his occupation is a Gangster.



[3]Experian, Why multi-sourced this-party data is key for detecting and preventing financial crime

[4]Experian, Zombie Company Directors

Another example, by Graham Barrow, Director of the Dark Money Files, pointed out the bizarre practice of individuals registering their businesses in hotels, including the Novotel Sheffield hotel.



Once criminals set up these bogus businesses, they use them as mechanisms to launder illicit money. Tens of billions of pounds are laundered in UK-registered corporate structures annually.[6] As ever, financial institutions must stay alert to money laundering red flags for businesses, which include unusual customer behaviours, high volumes of cash, or unusual corporate structures. Recently, pertinent and illustrative failures of banks in preventing money laundering through commercial clients have emerged.

National Westminster Bank (NatWest) was fined in 2021 by the Financial Conduct Authority (FCA) concerning a jewellery business, Fowler Oldfield. Despite many instances of suspicious activity, such as large cash deposits, the commercial customer continued to conduct business with the bank over a four-year relationship. This not only resulted in a fine of £265m for NatWest but made history as the first time that the FCA pursued criminal charges for money laundering failings. Details of the case highlight the importance of KYB and customer oversight, stressing that firms must maintain a sound knowledge of a customer's business, activity, and financial flows, particularly for companies with potentially higher risk profiles.

Exemplifying another common red flag involving unusual transactions or corporate structures, the National Crime Agency (NCA) recently dismantled a criminal network that laundered over £70m. A sophisticated, large-scale money laundering scheme using shell companies and a complex web of transfers to obscure funds was at play. A network of bank accounts was used to deposit cash received from criminal operations, and through bogus corporate structures, the criminals then sent the money to international accounts in Germany, the Czech Republic, the United Arab Emirates, Hong Kong, and Singapore.[7]

[5] The Guardian

[6] NCA

[7] NCA, 2023

Common money laundering red flags for businesses:

- Unusual customer behaviour
- Identification deception or misrepresentation
- Unusual transactions
- High volumes of cash
- Trade with high-risk countries or with industries irrelevant to the business
- Significant adverse media or no online presence at all
- Unusual or unnecessary complex corporate structures or use of formation agents
- Unusual financial transactions (e.g. how loans are structured)
- Nature of business is different from activity
- Anticipated activity is different from actual activity or filed accounts
- No UK directors or directors associated with high-risk jurisdictions
- The use of a residential or mailbox address, especially suspicious for companies with a large turnover
- The same company registration address or directors home addresses across many companies

Despite Companies House, including its register of Persons of Significant Control (PSC), being the subject of much abuse, its status and calibre as an official government source remain. Freely available to the public, the Register allows people to search both legal entities and individuals, making it an essential KYC and KYB tool for many financial institutions. With work underway to provide Companies House with the power to check and query data provided by reporting companies, to date, criminals have been easily able to submit false data to create seemingly legitimate companies, significantly compromising a firm's onboarding processes. Recent reports have highlighted how fake UK identities are increasingly used for fraud, including 'pig butchering' scams that are elaborate schemes involving organised criminal groups and modern-day enslaved people. One investigation found 168 UK companies "accused of running fraudulent cryptocurrency or foreign exchange trading schemes", of which half have possible links to pig-butchering.[8]

Outcries for reform of UK corporate records have been partially addressed by Part Two of the Economic Crime Bill, finalised and released in March 2023. The Bill equips the registrar with new powers to act as an active gatekeeper upholding the accuracy and reliability of the data it collects. There will finally be checks confirming and verifying the identity of anyone who sets up, owns or runs a company is actually who they say they are. These enhanced intelligence capabilities enable Companies House to eliminate companies from the register and proactively share information with law enforcement if there is evidence of anomalous filings or suspicious behaviour.[9] While it will take time for these reforms to settle in and for concrete benefits to manifest, they will likely still fall short of fixing all of Companies House's vulnerabilities. In reality, while these reforms are welcomed and commendable, Companies House will not become a reliable or full-proof tool overnight.

[8] The Guardian

[9] HM Government, Economic Crime Plan 2

Enriching KYB and KYC with multi-source data

The UK as a jurisdiction is rich with data sources restricted to the general public, signalling a massive opportunity for banks and financial institutions.

Many other official government registries, such as the VAT Register, Charities Commission, Gambling Commission, and the FCA, can enrich KYC and KYB data to improve accuracy for financial institutions. Open Government Licences facilitate re-using a wide range of public sector information. For example, if a financial institution wants to gain more knowledge about a customer operating a pub, they may reference Licensed Premises data. Similarly, a firm may consider the Food Standards Agency if they run a restaurant. If the client is a dentist, they may look at the Care Quality Commission or Edubase if they are a school.

How the business presents itself to potential customers can provide another face of the customer to enrich and verify data. For example, how a business positions their offering and when they started marketing can provide rich insights to support nature of business assessments, even providing evidence in the form of shop front images.

Alternative registers and multi-data sources

Referencing and incorporating key third-party data sources is instrumental in optimising KYB and KYC processes.

Data sources could include:

- VAT Register
- Gambling Commission
- Charity Commission for Northern Ireland
- Charity Commission for England and Wales
- Scottish Charity Regulator
- FCA Financial Services Register
- Jersey Financial Services Commission
- Care Quality Commission
- Edubase Schools Register (DoE)
- Driver & Vehicle Standards Agency
- Food Standards Agency
- Licensed Premises databases
- Organisation Data Services (NGS Digital)
- Postcode Address File (PAF)
- Marketing and web databases

> "Fraudsters and money launderers will typically misrepresent themselves across multiple databases."

Fraudsters and money launderers will typically misrepresent themselves across multiple databases. Look for discrepancies in the way they present themselves across numerous sources. Experian research has even identified one such director with over ten companies registered with Companies House, but where his country of residence is entirely different for each business. Multi-sourced data corroboration is key for verifying your business customers.

While there is no single source of truth for any industry, multi-source data corroboration and verification can better identify misleading claims. If a customer is found consistently against five or six third-party data sources, that should instil confidence. Conversely, if a customer has presented themselves across five data sources inconsistently, does not appear in the sources as they should, or has an image evidencing they provide otherwise undisclosed services i.e. money service activities, this should give cause for concern. In this way, these additional data points are invaluable for onboarding and KYB and KYC processes.

From a practical standpoint, besides helping with corroboration, using multiple data sources reduces customer friction at onboarding. Banks can populate data point information where possible, allowing for a quicker and smoother customer journey. Streamlining the process means an overall increase in efficiency, translating to a reduction in overall costs. As compliance teams benefit from saving time, overall effectiveness will increase, allowing them to more accurately identify red flags of illicit activity with more precise and better-vetted information.

This stress on effectiveness and using resources efficiently is a crucial part of a well-functioning risk-based approach, advocated for by the global anti-money laundering watchdog, the Financial Action Task Force (FATF) and the UK regulators. At its core, a risk-based approach means identifying, assessing, and understanding exposure to money laundering and terrorist financing risk and taking appropriate measures in accordance with that level of risk.[10] It truly focuses on knowing your customer throughout the relationship, emphasising the importance of consistent quality data. Harnessing multi-source data points during onboarding plays an essential and cost-effective role in championing a risk-based approach.

[10] FATF, Risk-Based Approach for the Banking Sector

Optimising financial crime controls with third-party data

Onboarding

Recent trends show how data is frequently and easily manipulated on Companies House, coupled with firms seeing an increase in the number of applications from high-risk sectors in the market, such as pubs and clubs. This means compliance teams must simultaneously contend with lower-quality Companies House data when verifying customer information and higher-risk accounts that require more involvement.

At its foundation, validating customer information can require a huge amount of manual outreach, making it costly and time-consuming. In reality, internal resources are not always adequate for the task - leaving a firm with overwhelming backlogs or poor quality KYC and KYB data that expose it to unwanted financial crime risk through inaccurate customer risk assessments. Third-party and multi-source data can use information held by the government to verify critical points, such as appropriate licences or government-required business records. Coupled with open-source findings, Experian bureau data, and other commercial and consumer information, this can enhance and speed up the onboarding process. A multi-pronged approach to data is more valuable and accurate than relying only on Companies House, which many financial institutions still do.

From a customer standpoint, using aggregated multi-source data reduces friction at onboarding. Up to an astounding 150 questions are asked to businesses opening a new account and roughly 50 for personal accounts. Reducing these touchpoints with pre-populated information and less back-and-forth between banks and clients means banking customers can access facilities quicker and easier. Reducing friction and improving the customer journey without compromising anti-money laundering procedures is vital for a successful, thriving business.

Remediation

UK banks have incurred huge fines for anti-money laundering failures, with penalties more than doubling in 2023 compared to 2022.[11] As outlined in one of the FCA's 'Dear CEO' letter, some common and consistent areas of weakness include risk assessments and due diligence.[12] One recent regulatory enforcement involving Santander UK showed that the bank did not sufficiently understand nor verify a customer's nature of business, in one case incorrectly onboarding a money service business that was outside of the bank's risk appetite.[13]

Remediation is a costly, expensive, and painful exercise. KYC remediation programmes have become UK banks' largest operational burden.[14]

Many firms spend upwards of £100m on remediation activity per year, with data showing that significantly higher expectations for remediation activities are anticipated in the next three years.[15]

While remediation will always entail a cost, the right tools, like third-party data, can help make it more efficient and cheaper. During periodic remediation exercises, firms can establish whether the data supporting KYC and KYB is consistent and unchanged from what was previously captured from the customer. If the data shows no change, customers can be 'risk accepted' and suppressed from remediation activity.

This streamlined and efficient approach to remediation benefits both the customer and the financial institution. While the customer avoids unnecessary contact with the financial institution to confirm information, compliance staff aren't burdened with unnecessary customer outreach, a waste of already limited resources. Experian's research shows this method saves around £30 for each instance that consumer outreach could be avoided and up to £1,000 for business outreach cases.

For work recently completed for a Tier 1 bank, using Experian's third-party data automated 85% of consumer records, 45% of sole traders and 30% of limited companies, generating estimated operational savings exceeding £30m.

[11]FCA
[12]FCA, Dear CEO
[13]FCA, Santander UK Final Notice
[14]Experian
[15]LexisNexis

Continuous KYC and KYB

In contrast to updating client data in periods of remediation, actively managing financial crime risks means continually monitoring for changes in data.

Known as continuous or perpetual KYC, monitoring client behaviours and substantial risk profile changes is advantageous to fixed and periodic reviews because it more accurately depicts actual risk. As a result, it allows for the more efficient and strategic allocation of resources and is more in line with a risk-based approach. Contacting a customer every time there is a data change will create expensive and onerous backlogs. Instead, concentrating resources on making contact only when there is a relevant data change that changes the risk profile and the Customer Risk Assessment is a better use of time. In this way, compliance teams can focus on the highest and top-priority risks.

Continuous KYC and KYB are data-driven strategies that leverage internal sources such as initial onboarding files and transaction patterns with external sources like publicly available information, government registries, and proprietary databases.

With significant and game-changing technological advancements, regulators have long advocated using technology for better results. The FATF has expressly recognised technological innovation as holding great potential for anti-money laundering efforts. Within the push for overall effectiveness, technology adoption will continue to be an instrumental part of the solution.

In an evolving trigger-based KYC and KYB approach, leveraging third-party data sets can enrich internal data to identify discrepancies, trigger further investigation, and monitor for relevant changes. Financial institutions benefit from this because a continuous KYC and KYB approach will eliminate costly periodic reviews. Because data is maintained continually, customers are only contacted when absolutely required, minimising friction and inefficiency.

Transactional data

While transaction monitoring is undoubtedly a vital process and defence in fighting financial crime, the current model of systems has inherent limitations.

In its current state, transaction monitoring doesn't capture an accurate cross-industry view. Criminals and acts of financial crime are becoming increasingly complex, often entailing a web of transactions designed to obscure the origins of funds. In practice, this means that money is usually transferred between a very high volume of accounts across multiple banks and jurisdictions in an attempt to confuse investigators and financial institutions. This challenge should not be understated - even for the most seasoned investigators.

Approaching transaction monitoring with more valuable and insightful data is a key solution to tackling more complex crime. Aggregated industry transaction data plays an instrumental part in optimising financial institutions' defences. Establishing peer group profiles defines an understood level of 'normal' that provides the basis for a useful comparison. All businesses can then be profiled to establish what account activity is 'normal' or expected for each one.

Given this baseline, three patterns that are key indicators of money laundering include a sustained increase in credit turnover that outperforms peers, income always being transferred out of the account, and low average balance as a proportion of credit turnover. Accessing this type of information and comparing and checking them over these three key indicators can more effectively detect suspicious activity.

This type of data sharing and usage is set to become the norm, as regulators have shown their support for data-sharing initiatives to combat financial crime. This sentiment has been expressed by global authorities such as The Wolfsberg Group, which has stressed the need for public-private information-sharing systems in a recent paper.[16] Overall, the push for effectiveness in fighting financial crime will entail smart data-sharing initiatives and strategies that employ already-existing information to improve key processes. The UK is in a perfect position for this, with a rich third-party data ecosystem that can optimise a firm's KYC and KYB processes, eliminate inefficiencies, and reap operational benefits.

[16]Wolfsberg Group

Aggregate Transaction Data: Current Account Turnover data

In March 2015, the Small Business Enterprise and Employment (SBEE) Act was passed, intending to stimulate the economy by increasing the flow of lending to small and medium-sized enterprises (SME). The Act was designed to address one of the perceived barriers preventing SMEs from gaining access to the best finance options: the inequality of information available to banks of different sizes. While the established main banks held current account relationships with more than 90% of SMEs and had the data to match, other smaller lenders had little or no access to information about current account behaviour.

That all changed because of the SBEE Act. Now, Current Account Turnover (Commercial CATO) data is available via the rules of Mandatory Credit Data Sharing (MCDS) that are set out in the Act.The Act mandates the nine largest banks (by market shares of SMEs in the UK and Ireland) to share with Experian the data they hold on their SME portfolios. For the first time, financial institutions are able to leverage the valuable aggregate transaction data provided by the UK's largest banks to uncover previously hidden risks of financial crimes.

What does this mean for transaction monitoring?

As part of transaction monitoring efforts, most UK banks build and use complex rules to closely scrutinise each and every financial transaction. But without capitalising on a true-cross industry view, the transaction monitoring systems of today can only go so far. Experian has carried out extensive market research, analysing the characteristics of money launderers and how they use firms to help carry out their crimes. As part of this analysis, Experian looked specifically at the rules set up by banks to spot questionable transaction behaviour. Building on this, Experian has further looked at how aggregated industry transaction data can identify concerns that might be overlooked by any individual transaction monitoring system.

Conclusion

With financial crime becoming ever more sophisticated, it's more important than ever that you know who you're in business with. UK banks and financially regulated institutions are spending millions each year fighting financial crime, with much of this effort being manual or happening in intra-company silos.

There is a better way - blending the latest technology, data, and insight to build slick, automated financial crime prevention and remediation processes. It should only require manual intervention when the data calls for it, hugely reducing the time, cost, and effort involved.

About Experian

Experian is the world's leading global information services company.

During life's big moments – from buying a home or a car, to sending a child to college, to growing a business by connecting with new customers – we empower consumers and our clients to manage their data with confidence. We help individuals to take financial control and access financial services, businesses to make smarter decisions and thrive, lenders to lend more responsibly, and organisations to prevent identity fraud and crime.

We have 20,600 people operating across 43 countries and every day we're investing in new technologies, talented people, and innovation to help all our clients maximise every opportunity. We are listed on the London Stock Exchange (EXPN) and are a constituent of the FTSE 100 Index.

Experian KYB data coverage

Experian has identified key third-party data sources and aggregated them to enable the multi-sourced corroboration required to uncover hidden risks associated with a business or the people behind the business. With FinCrime becoming ever more sophisticated, it's more important than ever that you know who you're in business with. UK banks and financially regulated institutions are spending millions each year fighting financial crime.

Learn more at **www.experianplc.com** or visit our **global content hub** at our global news blog for the latest news and insights from the Group.

About FINTRAIL

FINTRAIL is a global consultancy passionate about combating financial crime.

We've worked with over 100 global leading banks, FinTechs, and other financial institutions, RegTechs, startups, venture capital firms and governments to implement industry-leading approaches to combating money laundering and other financial crimes. With significant hands-on experience in the UK, we help you prepare, assure, and fortify your controls to meet evolving regulatory requirements and overcome the challenges of 2023 and beyond.

Get in touch **here**

Registered office address:
The Sir John Peace Building, Experian Way,
NG2 Business Park, Nottingham, NG80 1ZZ

www.experian.co.uk

C-01708