



KYC Guide UK

A comprehensive guide to KYC
and AML compliance in the UK

Table of Contents

02 Introduction

03 What is Know Your Customer?

04 What is AML?

09 Regulations for KYC, AML, and Data Privacy for the Businesses Operating in the United Kingdom

09 Know Your Customer

10 Anti-Money Laundering

14 Data Privacy

16 A case of AML Compliance failure

18 Industries Requiring To Comply With Regulations

20 Financial Sector

21 FinTech

22 Gaming

23 Cryptocurrency

24 Real Estate

25 E-Commerce

26 Methods to perform KYC and AML

26 Private or official database

26 Online verification from ID documents

27 Two-factor authentication

27 Knowledge-based authentication



Introduction

As technology has connected beyond traditional barriers of languages and distance, it has created a world of unprecedented economic opportunity. But in doing so it has also significantly increased the risks for doing business both globally and locally. Businesses are under immense regulatory pressure to perform robust customer due diligence, especially to diminish the international threat of money laundering and terror financing. This regulatory pressure manifests itself as Know Your Customer (KYC) regulations and Anti Money Laundering (AML) directives.

KYC and AML requirements are a key focus for organizations to ensure they are following compliance requirements for meeting the increasing regulatory demands. While these regulations vary from region to region and in some countries, even state to state, major compliance requirements are mainly uniform across the international business environment and are under the supervision of the Financial Action Task Force (FATF) ^[1]. Any organization doing business internationally also needs the agility to meet KYC and AML requirements in a specific region.

This comprehensive guide will provide you an overview of how to achieve KYC and AML compliance in the United Kingdom.



What is Know Your Customer?

Knowing your customer (KYC) in simple words is verifying customers to confirm they are who they claim to be and that they aren't a potential risk to your business. Finding KYC information has been tiresome and difficult.

Even so, financial institutions are required to gather this information around the world for over a decade. Lending money to or servicing a person who presents a high risk, or who may be involved in illegal activities, can be incredibly damaging for any bank or financial institution.

Many other industries are also now required to ensure KYC compliance and unfortunately this is an entirely new activity for many organizations, especially for small businesses and startups,

and analyze the information correctly.

It is an organization's responsibility to ensure its KYC compliance. This involves verifying the information that a customer provides and analyzing the risk involved in dealing with certain customers, including the funding sources and business details. Failure to do so brings with it significant risk in terms of financial cost, reputational damage, and potential judiciary consequences.

At a minimum, organizations are generally required to verify clients' identity, business type, source of funds and wealth, the purpose of specific transactions, and the expected nature and level of transactions.

There are four primary objectives when gathering KYC information, using a risk-based approach:

- ✓ **Identify the customer**
- ✓ **Verify the client's true identity**
- ✓ **Understand the customer's activities and source of funding**
- ✓ **Monitor the customer's activities regularly**

Customer Due Diligence (CDD)

Customer Due Diligence ^[2] is the control procedure that financial services apply to exist and new customers to identify and prevent risks. CDD plays an important role in eliminating risks related to money laundering, terrorist financing, fraud, corruption, arms trade, bribery, drug trafficking, and other illegal financial activities.

When opening a customer account according to legal requirements, a number of checks are required to follow the Know Your Customer procedures. One of the control methods implemented for risk assessment is a sanction, PEP, and adverse media screening.

Identity Verification

Verification is performed to check the authenticity of the information provided by the customers. The whole process of verifying identity is very important. It begins with authenticating the user i.e. verification of ID documents. After identity verification, the business checks whether it poses any threat to them. In this way, companies can conduct due diligence, prevent money laundering, and terrorist financing. Since businesses are mostly operating online manual identification is exhausted, cumbersome and in most cases impossible to perform so the financial institutions use an online identity verification.



What is Anti Money Laundering?

Money laundering is the process of hiding the source of money earned from illicit crimes to bring a legal image to this income. Anti-Money Laundering (AML) refers to rules and regulations implemented to hinder criminals from money laundering. It also includes laws and procedures to identify and counter financing terrorism (CFT).

Money laundering is a serious financial crime and there are rules and regulations on both global and local levels to prevent criminals from making illegal funds run into mainstream legal financial systems. Apart from global regulations, each country has its own AML policies. Companies have to comply with these regulations else they will be subjected to criminal sanctions imposed by regulators.

In the year 2019, only 58 AML fines were issued by the regulators worldwide and the total amount for these fines summed up to \$8.14 billion. Out of these 58 fines, regulators in the United Kingdom imposed 12 fines totaling \$388.4 million. (Fintechfutures)

The Financial Action Task Force (FATF) is responsible to provide comprehensive global AML regulations and policies recommendations. The purpose of the establishment of FATF is to build an international standard for the prevention of money laundering and FATF has 37 member jurisdictions and 2 regional organizations representing major financial centers in all parts of the globe.

AML Screening and Monitoring

AML screening and monitoring are some of the basic requirements of a comprehensive AML program. Audits and penalties by the regulators are expected to increase further. The sanctions and PEP lists are growing and changing every day in the world. Due to the dynamic nature of these lists, businesses need to scan sanctions, PEP, and Adverse Media data regularly. The following checklists could be applied for AML screening and Monitoring:

The Risk-based Approach

In the risk-based approach, the organization performs AML controls according to its risk perception and the risk level of their customers. The risk perception and risk level for each firm and every customer are different. It will be insufficient to apply the same AML controls for every customer. Therefore, organizations should take 2 basic steps for a risk-based approach. The first one is the assessment of the risk and the second is the implementation of the control processes appropriate to the risk levels.

Enhanced Due Diligence

Enhanced Due Diligence (EDD) is required when a customer is deemed to be a higher risk than the expected. These high-risk customers normally include Politically Exposed Persons (PEPs) or anyone originating from the high-risk countries list as outlined in the Fifth Anti-Money Laundering Directive (5AMLD)^[3]. EDD measures usually include high monitoring of customers.

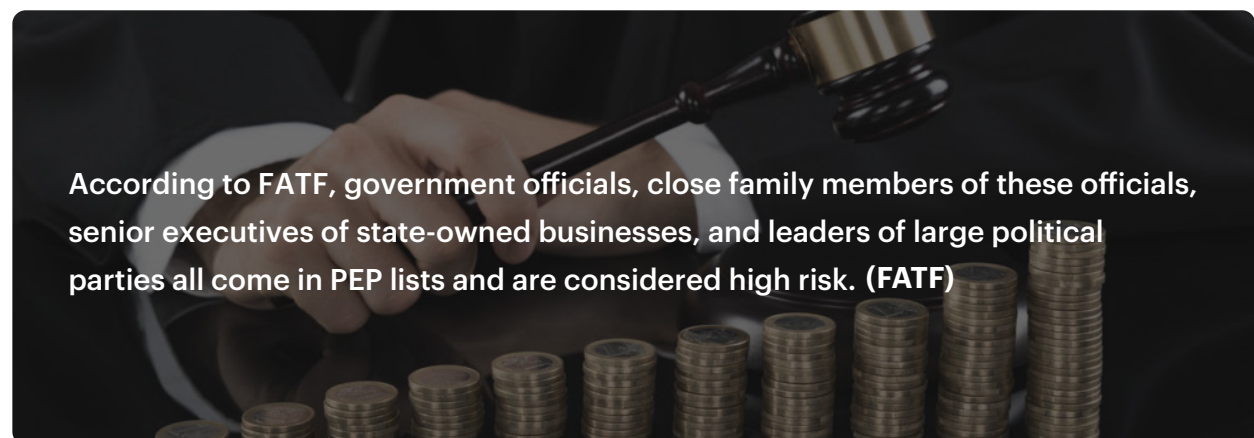
The most efficient way to become AML compliant is to conduct through customer screening. That being said, it can be difficult and time-consuming to execute these processes consistently at scale. To address these issues, automation plays an increasingly large role in AML compliance.

Sanction Checks

Individuals or institutions that do not comply with laws and rules are served with penalties and these penalties are called sanctions. Usually, the sanction decisions are made by governments or global regulators. Sanction checks are special searches from a list of different governmental and international databases to identify persons banned from certain activities or sectors. Political exposure, terrorism, money laundering, and corruption are the most popular reasons for sanctions. Businesses must verify that the customer they are dealing with isn't on any of the sanction lists and this process should be ongoing because sanctions lists are updated regularly.

Politically Exposed Persons Check

An individual with a high profile political role, or has been entrusted with a prominent public function is known as a Politically Exposed Person (PEP). As they have a high position in a country or jurisdiction, they are more open to bribery, corruption, and other offenses related to money laundering. This doesn't always mean that they are offenders but to be on the safe side they are declared as high-risk customers.



According to FATF, government officials, close family members of these officials, senior executives of state-owned businesses, and leaders of large political parties all come in PEP lists and are considered high risk. (FATF)

If an enterprise encounters any of these as their customers they should be put in high-risk profiles and should be screened against sanction lists and their transactions should be monitored on an ongoing basis.

Ultimate Beneficial Ownership

The legal entities of a company whether a corporate or an individual are Ultimate Beneficial Owners (UBOs). Financial institutions have to identify UBOs in order to prevent money laundering and terrorist financing. People with at least 25% shares in the capital of a legal entity, have 25% of voting rights inboard or are beneficiaries of at least 25% of the capital of a legal entity acquire UBO status. According to FATF, UBOs carry potential ML/TF risks, so financial institutions must have important obligations and information regarding UBOs ^[4].

Adverse Media Screening

Any negative information about the customer or business from various sources in the commercial world is adverse media. These are mostly news covering the individual or a business. It reveals whether a person or a business is involved in any criminal or illegal activities that could affect your organization if you do business with them. This is why it is important to perform adverse media screening.

>> Do you know?

FATF emphasizes on adverse media screening of high-risk customers to identify the customer reputation. (FATF)

AML Transaction Monitoring

Monitoring transactions is one of the crucial AML and anti-fraud security processes. Transaction monitoring helps in detecting suspicious transactions and determining the risk level of transactions carried out by the customers. Financial sectors like money service businesses (MSBs), Insurance corporations, financial services, money transfer companies mediate a large number of financial transactions on a daily basis. Transaction screening is one of the crucial AML obligations to detect any suspicious transaction. Ongoing transaction monitoring is necessary to meet AML obligations.

Suspicious Activity Report

Suspicious Activity Report (SAR) is used to track suspicious activity that will not be flagged normally in normal monitoring. The main purpose of SAR is to check for illegal activities such as money laundering, terrorist financing, tax evasion, and other financial frauds.

In the UK, alone, the number of Suspicious Activity Reports rose 9.6% between 2017-2018. In the US economic crime increased by 17% between 2016 and 2018. (National Crime Agency)



Currency Transaction Report

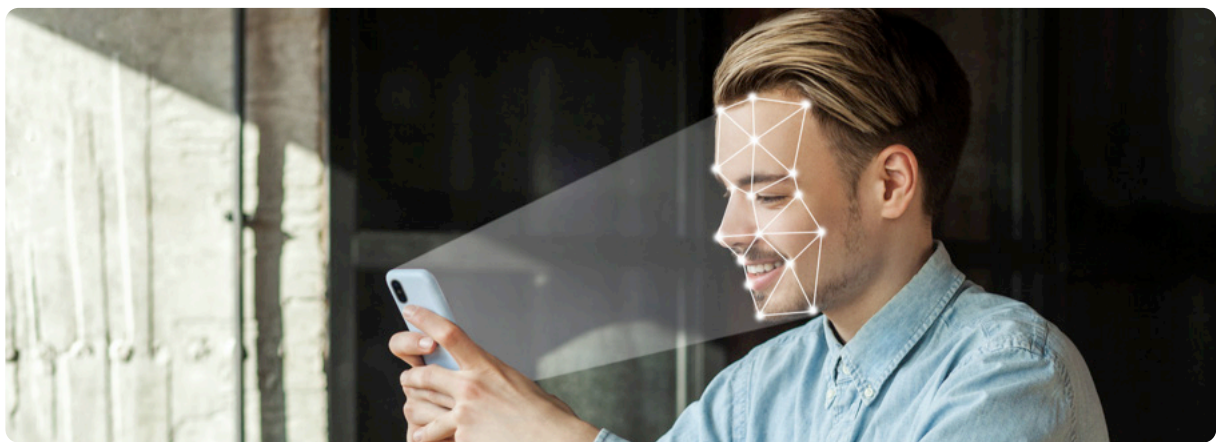
Currency Transaction Report (CTR) is generated by banks to help prevent money laundering. According to AML laws in most countries, the CTR report is an AML compliance obligation for financial institutions. Banks use CTR to report any bank transaction exceeding \$10,000 to relevant regulators ^[5]. This is a crucial part of AML transaction monitoring failing to report could lead to fines and penalties.



Regulations for KYC, AML, and Data Privacy for the Businesses Operating in the United Kingdom

The UK has the most robust KYC and AML regulations and is named as “Global leader in promoting corporate transparency” by FATF. Financial Conduct Authority (FCA)^[6] is well known for its risk-based approach to innovation. This means that in general, it focuses on the outputs rather than specific AML laws and rules. Firms must have policies and procedures in place for KYC and AML compliance. Here are some practices suggested by the regulatory bodies;

Know Your Customer



Know Your Customer compliance is obligatory for businesses dealing in finance. The businesses are required to collect evidence of identity from the individual as well as corporate customers.

According to FCA, evidence of identity can be in documentary or electronic form. From individual clients this identity information is required:

- a. Full name
- b. Date of birth
- c. Residential address
- d. Government-issued identity document (Passport, Driving License with a photo)
- e. A supported second document either issued by a government or a judicial authority, a public sector body, or any other FCA regulated firm in the UK financial services sector

From corporate clients, a firm should collect this information:

- a. Full name
- b. Registration number
- c. Government-issued identity document (Passport, Driving License with a photo)
- d. For Private/unlisted companies additional data is required:
 - i. Names of all directors
 - ii. Name of individuals who own or controls over 25% of companies share
 - iii. Name of any individual with otherwise exercise control over company

The firm should verify the existence of the corporation either confirming the company's listing on a regulated market, conducting a search of the relevant company registry, or obtaining a copy of the company's Certificate of Incorporation. For private/unlisted companies, the firm may decide, following a risk assessment, to verify one or more of the directors as appropriate in line with the CDD requirements for individuals. In respect to beneficial owners, the relevant person must take risk-based and adequate measures to verify the identity of the beneficial owner(s).

Anti-Money Laundering



The UK anti-money laundering regime requirements are set out in the Proceeds of Crime Act 2002 (POCA)^[7] (as amended by the Serious Organised Crime and Police Act 2005 (SOCPA)^[8]), the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017)^[9] and the Terrorism Act 2000 (TA 2000)^[10] (as amended by the Anti-Terrorism, Crime and Security Act 2001 (ATCSA 2001)^[11] and the Terrorism Act 2006 (TA 2006)).

As per the Financial Conduct Authority (FCA), a firm has to fulfill the following responsibilities under money laundering supervision:

You must apply customer due diligence measures:

- When you establish a business relationship with a customer (or another party in a property sale)
- When you suspect money laundering or terrorist financing
- When you have doubts about a customer's identification information that you obtained previously
- When it's necessary for existing customers - for example, if their circumstances change

7. UK Govt - Proceeds of Crime Act 2002

8. UK Govt - Serious Crime and Police Act 2005

9. UK Govt - ML, TF Regulation 2017

10. UK Govt - Terrorism Act 2000

11. UK Govt - Anti Terrorism Act 2001

- As a high-value dealer, when you:
 - Make a payment to a supplier worth €10,000 or more
 - Carry out an 'occasional transaction' worth €10,000 or more
- If you are not a high-value dealer when you carry out an 'occasional transaction' worth €15,000 or more

Establishing a business relation:

A business relationship is one that you enter into with a customer where both of you expect that the relationship will be ongoing. It can be a formal or informal arrangement.

When you establish a new business relationship you need to obtain following information:

- The purpose of the relationship
- The intended nature of the relationship - for example where funds will come from, the purpose of transactions, and so on

You need to obtain this type of information:

- Details of your customer's business or employment
- Copies of recent and current financial statements
- The expected level and type of activity that will take place in your relationship
- The source and origin of funds that your customer will be using in the relationship
- The changing circumstances of your customers
- Details of the relationships between signatories and any underlying beneficial owners

You need to keep up-to-date information on your customers so that you can:

- Amend your risk assessment of a particular customer if their circumstances change
- Carry out further due diligence measures if necessary

In case of following changes you may need to update your information:

- A big change in the level or type of business activity
- A change in the ownership structure of a business

Carrying out enhanced due diligence:

In some situations, you must carry out 'enhanced due diligence'. These situations are:

- When the customer is not physically present when you carry out identification checks
- When you enter into a transaction with a person from a high-risk third country identified by the EU



- When you enter into a business relationship with a 'politically exposed person' - typically, the non-UK or domestic member of parliament, head of state or government, or government minister and their family members and known close associates
- Any other situation where there's a higher risk of money laundering

If the customers are not physically present you may need to take following enhanced due diligence measures:

- Obtaining further information to establish the customer's identity
- Applying extra measures to check documents supplied by a credit or financial institution
- Finding out where funds have come from and what the purpose of the transaction is
- Making sure that the first payment is made from an account that was opened with a credit institution in the customer's name

While dealing with politically exposed persons you need to take following enhanced due diligence measures:

- Making sure that only senior management gives approval for a new business relationship
- Carrying out stricter ongoing monitoring of the business relationship
- Taking adequate measures to establish where the person's wealth and the funds involved in the business relationship come from



In the UK there are multiple anti-money laundering regulatory bodies for different sectors. For example, the banking and financial sector are looked over by the Financial Conduct Authority (FCA).

Regulatory bodies governing AML and KYC compliance in different industries

Similarly, there are multiple bodies for the non-financial sector:

- FCA is the supervisory authority for trust or company service providers who are authorized persons.
- Money service businesses and trust or company service providers are all underlooked by HM Customs and revenues.

These include high-value dealers, bill payment service providers, and telecommunications digital and IT payment service providers, estate agency businesses and accountancy service providers.

- Casinos and online gaming are supervised by The Gambling Commission.
- The Institute of Chartered Accountants in England and Wales ("ICAEW") is the supervisor for Chartered Accountants.

The latest money laundering regulation amendments were made in 2019 that were to ensure that the United Kingdom's money laundering regulations are in place with the European Union's 5th AML Directive and are in line with FATF's money laundering regulation standards.

These regulations make some limited but important amendments to the existing Money

Laundering, Terrorist Financing, and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017). These include extending the scope of the regulated sector, changes to customer due diligence, and enhanced due diligence, in particular, a new requirement to make reports to Companies House concerning discrepancies between information collected during customer due diligence and information on the Persons with Significant Control register.

Data Privacy



Customer data protection is a serious issue. You are responsible for securing your customer data and protecting it from fraudsters. Customer data is any identifiable personal information held in any format, for example, National insurance records, addresses, dates of birth, family circumstances, bank details, and medical records. This information must be kept securely to comply with your obligations under the Data Protection Act 1998^[12], but also because criminals can use it to commit offenses such as identity theft.

Data security is not purely an IT problem, nor is it just a problem for large firms. Firms of all sizes should think carefully about how they secure their data. Having good data security policies and appropriate systems and controls in place will go a long way to ensuring customer data is kept safe. However, you need to make sure your employees understand the policies and procedures and your firm keeps up-to-date when people move on.

Since the United Kingdom is a part of the European Union as of now, General Data Protection Regulations (GDPR)^[13] are also applicable to businesses of all sizes operating in the United Kingdom. At its heart GDPR identifies seven key principles for the way personal data should be:

- a. processed lawfully, fairly, and transparently concerning individuals. “lawfulness, fairness, and transparency”.
- b. collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes (‘purpose limitation’).

- c. adequate, relevant, and limited to what is necessary with the purposes for which they are processed ('data minimization').
- d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').
- e. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality')."
- f. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the implementation of the appropriate technical and organizational measures required by the GDPR to safeguard the rights and freedoms of individuals ('storage limitation').

A case of AML Compliance failure

Commerzbank fined £37 million by FCA

On June 17, 2020, the Financial Conduct Authority said that it had placed a penalty of £37,805,400 against the Frankfurt-based Commerzbank's London Branch ^[14]. The reason for imposing this fine was the failures in Anti Money Laundering systems and controls between October 2012 and September 2017. The firm received a 30% discount on the fine under the FCA's settlement agreement as the bank agreed to solve the matter at an early stage, FCA's final notice states. The original amount of fine before the discount would have been £54,007,800.



In the Final notice FCA specifically identified the followings:

- There were shortcomings in Commerzbank London's financial crime controls applicable to intermediaries (i.e. introducers and distributors).
- Certain business areas did not always adhere to Commerzbank London's policy of verifying the beneficial ownership of clients, including high-risk clients, from a reliable and independent source.
- Risk and issue owners were not clearly articulated or understood by Commerzbank London's committees. This led to a "lack of clarity around responsibilities", which impacted the Front Office, CLM, and Compliance.
- The Skilled Person identified instances where the way that Commerzbank London identified and considered the risks associated with politically exposed persons ("PEPs") was inadequate.
- There was no comprehensive documented process or criteria for terminating a relationship with an existing client for financial crime risk.
- Commerzbank London's automated tool for monitoring money laundering risk on transactions for clients was not fit for purpose and did not have access to key information from certain of Commerzbank's transaction systems.

- A significant backlog of existing clients being subject to timely refreshed know-your-client (“KYC”) checks developed during the Relevant Period, in part because Commerzbank London’s first and second lines of defense tasked with carrying out key AML controls were, throughout the Relevant Period, understaffed.
- In one example, a high-risk client, who was nearly 5 years overdue KYC refresh, entered into 16 transactions with Commerzbank London whilst overdue KYC refresh, with Commerzbank London generating net revenue of £273,799 from these transactions.
- An exceptions process put in place from May 2016 to permit existing clients to continue to transact with Commerzbank London despite not having been subject to timely periodic KYC checks, became, as at the end of 2016, out of control, with both senior branch management and Compliance lacking understanding and adequate awareness of the process.

Significant takeaways from this penalty

This penalty is significant for financial institutions because they are reassured that it is important to meet the expectations of their regulatory bodies and that authorities are always ready to promptly address any issues that are identified. In particular, the regulators remain focused on ensuring that:

1. Banks dedicate enough resources for AML compliance.
2. Financial institutions should formally document and clearly define the roles and responsibilities for AML compliance programs.
3. They should properly measure the transactions to monitor any suspicious activity. institutions should formally document and clearly define the roles and responsibilities for AML compliance programs.

Moreover, the notable amount levied that even though no evidence of the financial crime is identified by FCA but the risk of financial crime is as serious as the crime itself. This means that FCA considers the risk of crime important. Nonetheless, the FCA emphasized that Commerzbank London’s conduct created a meaningful risk that the firm might be used to promote financial crime.

Also, this conduct from FCA stresses that the firms need to fix issues identified by the regulators at their earliest. In this case, even though the bank initiated significant measure in 2017, the FCA charged the organization for not moving fast enough to update automated transaction monitoring systems, remove the backlog of customers requiring to perform KYC Checks at the London branch, and compliance team management concerning the AML compliance program.

Industries Requiring To Comply With Regulations

Fenergo posted a report towards the end of 2018 revealing that there were \$26bn (or £20.2bn) in fines related to AML and KYC legislation, and regulations in the decade following the financial crisis ^[15]. There were 83 fines issued in Europe alone, with a total of \$1.7bn (approx. £1.3bn). The majority of these fines were imposed by the Financial Conduct Authority (FCA) with the UK being the most active issuer of AML and KYC fines in the whole of Europe, accounting for 24%. The average fine

for the whole decade sits at \$15.7m (approx. £12.2m).

HM Revenue and Customs (HMRC) oversees compliance with AML regulations by businesses, and between 2017-2018 they fined companies a total of £2.3 million, which is double than of the previous year when £1.2m of fines were issued. On average, businesses were fined just under £2,500 per breach. Many of the fines have been issued to corporations in the property sector.



Damages of non-compliance

- **£163 million charge (\$203.83 Million) – Deutsche Bank**

In January 2017, the FCA levied £163 million (\$203.83 million) ^[16] in fines against the German lender Deutsche Bank – the most significant penalty the FCA has ever applied. Due to a lack of customer due diligence, along with other deficiencies, the bank was abused by unidentified customers who transferred approximately \$10 billion from Russia to offshore bank accounts in a way that is highly suggestive of financial crime.

- **£102,163,200 — Standard Chartered Bank**

FCA fined Standard Chartered Bank £102,163,200^[17] for Anti-Money Laundering (AML) breaches in two higher risk areas of its business. This is the second-largest financial penalty for AML controls failings ever imposed by the FCA.

- **£215,000 fine — Countrywide estate agents**

HMRC on March 4, 2019, imposed a fine of £215,000 (about \$283,000)^[18] to Countrywide estate agents for failing to conduct due diligence, proper verification, and record-keeping, and failing to ensure compliance with policies and controls in violation of the UK money laundering regulations.

Every industry sector has a different threshold, standard, and regulators so it's imperative to understand the specific requirements for each sector individually.

Financial sector

Banks and financial institutions in the UK are required by law to comply with AML and KYC regulations to stop criminals, terrorists, and fraudsters from using financial products or services to store and move around their money ^[19]. In the UK these requirements come primarily from the Money Laundering Regulations Act 2007 (MLRs) and apply across a range of sectors and institutions.



Customer Due Diligence

Under the updated 2017 AML regulations, the financial organizations are required to perform three due diligence measures, such as:

- Identify and verify the customer's identity through documents, data or information obtained from a reliable and independent source
- Identify any beneficial owners (where applicable) and verify their identities on a risk-sensitive basis
- Obtain information about the purpose and intended nature of the business relationship and things like source or origin of funds. Also, perform enhanced due diligence for Politically Exposed Persons (PEPs), specifically around the source of their wealth.

Under the risk-based approach, financial entities have to obtain sufficient data to develop a comprehensive profile of the customer and beneficial owners and to understand the risks associated with the business to ensure it's within the risk appetite of the financial entity.



FinTech

The UK is ranked as one of the most 'fintech friendly' regions in the world.

The initiatives like the Financial Conduct Authority (FCA)'s 'project innovate'^[20] and 'regulatory sandbox,' in the UK have helped companies to introduce and test new financial projects and distribution methods, which in turn, has helped establish the UK as a leader in fintech and a global authority on fintech regulation.

Currently, there are no specific laws for fintech companies, which fall under the existing body of UK financial regulation. Fintech firms will fall within the regulatory limits if they perform certain regulated operations including traditional financial services, such as the provision of banking, consumer credit, insurance services, and crowdfunding.



UK regulatory fintech sandbox

FCA's sandbox^[21] is open to authorized and unauthorized firms that require authorization, and technology businesses. For eligibility, companies need to show that they will deliver innovation that is either a regulated business or supports regulated business in the UK financial services market.

Other requirements include the need to show that:

- The innovation is ground-breaking or a significantly different offering in the marketplace
- The innovation offers a good prospect of identifiable benefit to consumers (either directly or via heightened competition)
- There is a genuine need to test the innovation in the FCA's sandbox

Gaming

Gaming operators in the UK must adopt efficient verification tools to provide a quick and convenient onboarding experience to users while meeting compliance requirements at the same time.

Here's what you need to know about these requirements:



Customer Due Diligence

The UK Gambling Commission has placed a general rule for remote casinos to perform CDD on a risk-sensitive basis (tailored to the risk attributed to the specific customer), but **due diligence is mandatory in respect of all customers who trigger the CDD threshold of €2000** ^[22].

To fulfil these identity verification requirements, gaming operators must:

- Verify the name, address, and date of birth of a customer before any gaming or gambling activity
- Ask for any additional verification information promptly
- Inform customers about what identity documents or other information is required before they can deposit funds, the circumstances in which the information might be required, and how it should be provided to the licensee
- Take appropriate steps to ensure that information on their customers' identities remains accurate.

Age verification

The new rules set by the commission prohibit new users from any gaming activity before the age verification process, obligating gaming operators to refrain from accepting any bets before the user's age is verified. These new verification rules also apply to "play-for-free" games, which look and feel like gambling but do not involve any stakes.

Cryptocurrency

Any crypto asset business that is carrying out the activities listed below must comply with the MLRs 2017 ^[23]. These activities include:

- Crypto Asset exchange provider [including Cryptoasset Automated Teller Machine (ATM)]
- Peer to Peer Providers
- Crypto exchanges e.g Initial Coin Offering (ICO) or Initial Exchange Offerings

According to FCA, any crypto-asset business or other institutions, such as existing financial services firms, e-money institutions, or payment services businesses undertaking crypto-asset activity are required to register under FCA.



Customer Due Diligence

All registered businesses under FCA must follow the following guidelines for verification of their customers.

- Identify and assess the risks of ML and TF which their business is subject to
- Have policies, and controls to mitigate the risk of the business being used for money laundering or terrorist financing
- Appoint an individual who is a member of the board or senior management to be responsible for compliance with the MLRs
- Perform CDD when entering into a business relationship or occasional transactions
- Apply enhanced due diligence for high-risk customers, including clients who fall under PEP definition.
- Perform ongoing monitoring of customers according to the customer's business and risk profile.

Real estate

According to the comprehensive guidance produced by HMRC (Her Majesty's Revenue and Customs) [24] department in the UK, the estate agents and real-estate companies have to comply with the KYC and AML regulations to combat money laundering activities.



Customer Due Diligence

The key obligations that these businesses or individuals have to follow are:

- Identify and verify clients, and perform additional checks on 'high risk' clients including the understanding of their source of wealth. Both buyer and seller need to perform these checks.
- For entity clients, beneficial ownership must also be established, and there must be an individual assessment of the AML risk posed by each customer.
- Perform regular monitoring and appoint an officer for identifying unusual activity or transactions by customers and reporting it to the relevant authorities
- Maintain adequate records of CDD and other documentation of clients
- Train your staff to ensure they understand their obligations and are equipped to spot money laundering and terrorist financing by clients

When should CDD be performed

HMRC considers that CDD should be performed when the terms are agreed, normally on the signing of a Memorandum of Sale in residential sales or Heads of Agreement in commercial sales. Other requirements related to systems, controls, policies, and procedures include the following:

- Prepare a written risk assessment to identify risks of ML and TF
- Monitor the effectiveness of the compliance program and keep it updated.
- Perform enhanced due diligence on PEPs, and individuals entrusted with prominent public functions, held in the UK or abroad

E-commerce

E-commerce stores in the UK have to follow the regulations in place for verifying the age of customers who want to purchase age-restricted goods online. Selling these products to minors is a major crime. The minimum age for purchasing alcohol in the United Kingdom is 18, and the minimum age for purchasing liqueur confectionery is 16 ^[25]. **The maximum penalty for selling to a minor is a fine of £20,000 and a forfeiture of your license.** These penalties vary for different age-restricted products



Customer Due Diligence

The online retailers should take positive steps to verify the age of the purchaser when selling age-restricted products. Here are some of the checks that are traditionally performed by retailers.

- Relying on the customers to confirm their age
- Using simple disclaimers to make an assumption
- Using an accept statement for the users to confirm that they have read all the terms and conditions and are eligible to purchase their product
- Accepting payments through credit card without verification that the card belongs to the person making purchases.
- Placing tick boxes to ask customers to confirm that they are of legal age

Age verification checks that retailers can adopt

There are a few age verification checks that online retailers can adopt for additional verification:

- Retailers could use age verification checks at the point of delivery by ensuring that delivery drivers request valid proof of age
- Requiring the customer to provide a valid/acceptable proof of age, which can then be appropriately checked.
- Introduce collect in-store policy. (This strategy may work for some of the retailers having both online and street presence)

Methods to perform KYC and AML

There are various methods to perform KYC and AML that businesses employ for the verification of their customers or clients. Let's discuss a few of the most common methods.

Private or official database

Databases are systems that house data previously collected and verified as part of a registration system. They can be private databases run by profit organizations or public databases run by governments. For example, private databases include credit bureaus and telephone directories and public databases include government identifiers (social security, tax or voter numbers) or the DMV (Department of motor vehicles) that houses driver's license data and numbers. While using databases for identity verification, certain things must be considered first including the cost of access, the fact that previous data breaches (if any) may have compromised the credibility of the data, and whether it can be used commercially under current privacy regulations.

Online verification from ID documents

In online verification, various techniques including artificial intelligence, human intelligence, and facial recognition, are used to determine if a government-issued id document belongs to the user trying to enrol in the system. This method typically requires users to provide a picture of themselves holding an ID document in their hands. By comparing the unique facial features of the live picture with the photo in the ID card we can confirm the facial similarity and the authenticity of the user.

Government-issued ID documents might include:

- National identity card
- Driver's license
- Passport
- Residence permit
- Voter identification document
- Tax identification document

There are several ways to evaluate the ID and user, which can help identify possible tampering and impersonation from multiple perspectives:

Document template comparison: Comparing the submitted ID image against the known document template can identify errors or fake formats.



Font anomalies: Scammers often try to change fields of data but will leave behind font inconsistencies while doing so.

Security features: All ID documents have some form of built-in security features which while evaluating can ensure authenticity or reveal errors.

To further explain how this method is or can be performed, let's take [Shufti Pro](#) – Identity verification solution -- as an example. Shufti Pro requires the end-user to capture a live picture by showing their face to the camera. Then by using 3D liveness detection, it ensures the presence of the user. After performing all facial checks a facial signature is created which is verified against the image on the document. And being a highly equipped KYC solution it can perform certain other functions as well as anti-spoofing checks, fake image detection, human face attributes analysis, AI mapping techniques, and microexpressions analysis.

Two-factor authentication (2FA)

This method requires users to provide a form of personal identification, also known as a token, in addition to the usual username and password details before they can access an account. The token is like a code that can be a number or an alphabet that the user receives from the authenticating agency during the sign-up or login process. 2FA is particularly useful for creating accounts and resetting passwords, however, this method typically requires users to have their cellphones with them during the authentication process. Most identity verification solutions including [Shufti Pro offer 2FA](#) as a security feature. It allows businesses to integrate an extra layer of security for customer onboarding and verification.

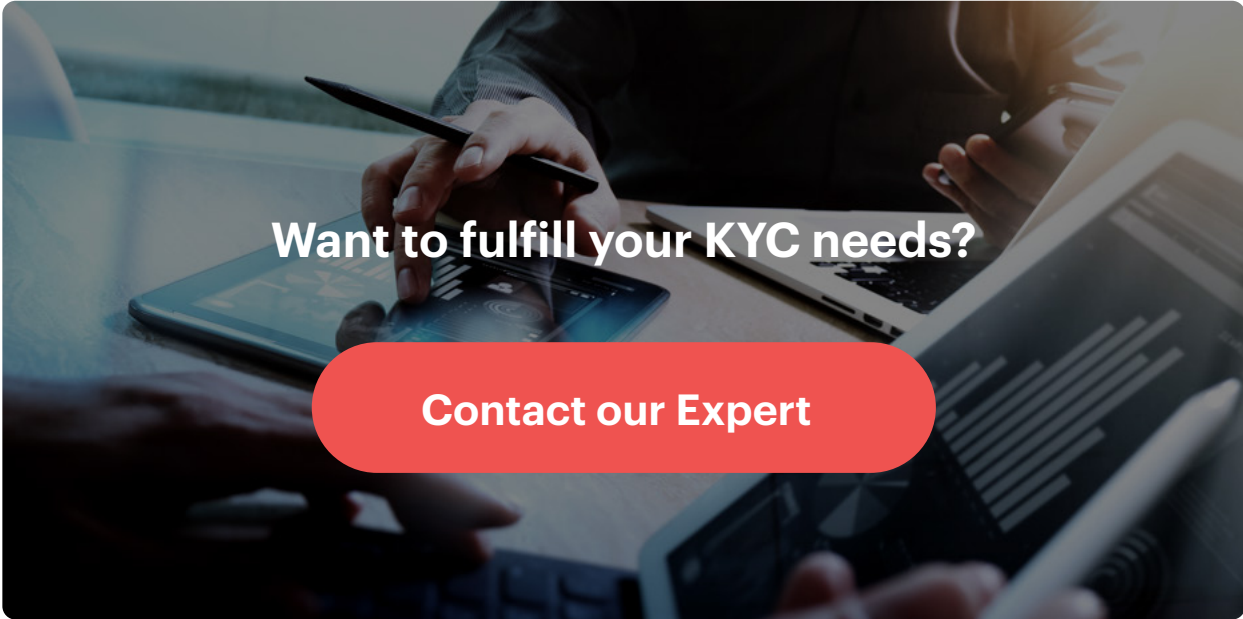
Knowledge-based authentication (KBA)

KBA verifies a person's identity by requiring an answer to security questions. These questions are generally designed to be easy for the user's to easily remember them. For additional safety, this method allows you to place a requirement for users to answer the questions within a specified time limit. KBA being the easiest verification method for users to understand has a drawback, as it is getting increasingly easy for hackers to discover the answers via social networking sites and other more traditional forms of social engineering.

Conclusion

To avoid penalties, businesses need to follow KYC and AML laws in the UK. With the financial growth in every sector the crime ratio is increasing as well. Hence, the regulatory authorities are increasing the scrutiny to keep bad actors in check. With the availability of technologically advanced verification solutions, KYC and AML compliance operations have now become effortless. These technologies perform verifications in seconds and help in regular monitoring and record keeping of your customers, and ensure that your business does not fall prey to any criminal activity.



A background image showing a business meeting with people's hands and arms around a table, interacting with tablets and laptops. The image is dimmed to allow text to be visible.

Want to fulfill your KYC needs?

Contact our Expert

A background image showing a close-up of a fingerprint being scanned, with blue light patterns highlighting the ridges. The image is dimmed to allow text to be visible.

Test our services yourself for 15 days

Get Free Trial

 www.shuftipro.com

 sales@shuftipro.com



Expanding services to 230+ countries and territories in a short period of time, Shufti Pro envisioned playing a pivotal role in creating cyberspace where every transaction is verifiable and secure. With enough experience in technologies like machine learning (ML), OCR, artificial intelligence, and Natural Language Processing (NLP), Shufti Pro strives to provide the best identity verification services to verify customers and businesses online.

Shufti Pro's cost-effective solutions help businesses to prevent fraud and illicit crimes that can ruin the integrity and brand reputation of your business. Our perfect solution suite consisting of KYC verification, AML screening, ID verification, Facial Recognition, Biometric Authentication, Video KYC, OCR, and KYB helps to improve your company's fraud prevention, Know your Customer (KYC) and Anti Money Laundering (AML) regulatory efforts by automating the workflow. With single API integration, Shufti Pro empowers you to verify customers with document checks from 3000+ ID templates and business entities from 200 million companies data.

Disclaimer: No warranty or claim is herein provided that information contained in this document is accurate, up-to-date, and/or complete. All information provided in this document is limited for general informational purposes only. In no circumstance(s), does such information constitute as legal or any other advice. Any individual or company who intends to use, rely, pass-on, or re-publish the information contained herein in any way is solely responsible for the same and any likely outcomes. Any individual or company may verify the information and/or obtain expert advice independently if required.