consult hyperion
securing tomorrow's transactions

AMLD4/AMLD5 KYCC

Know Your Compliance Costs

June 2017

Fola Ogunsola - Consultant
Steve Pannifer - Chief Operating Officer

Research Sponsored by Mitek

Executive Summary

The overhaul of the anti-money laundering legislation, in the fourth and fifth EU Anti-Money Laundering directives (referred to hereafter as 4AMLD and 5AMLD), will significantly increase the frequency with which financial institutions will need to conduct 'Know Your Customer' (KYC) checks. Even before the new legislation, with current methods, these checks place an enormous cost burden onto financial institutions.

KYC and associated processes cost the average bank $60m annually.

Much of the cost comes from the reliance of manual processing. The use of third party data sources helps but due to data quality issues, failure rates are high. Furthermore, the current processes employed are often cumbersome and do not translate well into digital channels.

In addition to operational cost, banks that do not comply with the new legislation risk extremely punitive fines. In January 2017, the FCA fined Deutsche Bank £163 million for serious anti-money laundering controls failings. This is the largest penalty for AML controls failings ever imposed by the FCA (or its predecessor the FSA). Under the 5AMLD, regulators will have the power to impose much higher fines than this, as high as 10% of annual turnover for serious breaches.

Key Findings

- KYC processes cost the average bank $60m annually.
- Total costs for KYC processes range from £10 to £100 per check.
- In the UK 25% of applications are abandoned due to KYC friction.
- 4AMLD and 5AMLD increases both the frequency and scope of checks.
- 4AMLD will impose fines as high as 10% of annual turnover for serious breaches.
- Mobile technology can significantly decrease the risk of sanctions, provide significant improvements in user experience and reductions in KYC friction, while delivering savings for the average bank of £5m in operational costs, rising to £10min three year's time.

To reduce risk of sanctions, KYC friction, and the operational costs, banks and other regulated entities should employ advanced identity technology that will drastically cut manual processing costs, be much less prone to error and not susceptible to social engineering.

One solution offered by the 5th AML directive is to use government-backed eID schemes, however, in many cases; these will not be ready in time and even when they are ready, to achieve scale deployment and adoption will take several years. There is therefore a need for alternative technologies to bridge this gap. Mobile technology can do just that. The high quality cameras on most smartphones can be used to capture images of documents, authenticate the document, and verify the identity of the individual. In combination with advanced image processing and machine learning, this technology can really make a difference.

The message to all financial institutions is clear:

- The cost of customer due diligence is much too high, placing toomuch reliance on inefficient and error prone manual processes.
- Getting it wrong is both costly and damaging. New rules will result in much higher fines when serious failures in compliance occurs.
- Advanced mobile technology provides a straightforward mechanism to reduce both costs and risks.
- The same technology will remove friction from the user experience increasing top line revenue.

In light of 4AMLD and 5AMLD there is a significant opportunity for banks to reduce the risk of sanctions, improve the user experience associated with KYC processes, and make significant operational cost savings. We conservatively estimate the average-sized financial institution can save £5m in operational costs, rising to £10m in three years' time. This is a low estimate. The actual benefit to banks has the potential to be much higher.

KYC costs are already huge

According to a recent Thomson Reuters Survey[1], the average bank spends $60m a year on KYC compliance. Some banks spend up to $500M annually on KYC and CDD ("Customer Due Diligence") compliance.

The BBA states that its members are spending at least £5bn annually collectively on core financial crime compliance, including enhanced systems and controls, and recruitment of staff (not including the direct costs from fines for AML/CTF breaches[2]).

These costs occur because there is still a great reliance on manual checks as follows:

Manual

For applications performed in branch, the customer will present original documents, which are checked and photocopied (with the photocopies being archived).

There are significant costs associated with document archival and significant inconvenience to the customer if the documentation provided is insufficient (and they have to make a subsequent visit to the branch with the correct documentation).

These processes will often involve hidden costs such as, the time spent by staff performing checks, the need for staff to receive specialist training and the need to employ compliance officers to ensure processes are being implemented correctly.

Whilst the cost of the basic KYC check may be around £2, the total cost once staff time is factored in could be much higher. We have seen estimated total costs for such processes as low as £10 per check and as high as £100 per check.

One online report[3] cites a bank, which saw its annual compliance cost per customer spiral from £60 to £300 in two years primarily due to the increase in staff needed for compliance purposes. The BBA reports that 2000 new UK AML roles were created in the banking industry in the past year alone.

Online

For applications performed online, customer-entered details are checked against third party sources. In addition, knowledge-based verification can be performed against a third-party source, such as a credit bureau.

These checks have a high failure rate, as high as 20%, due to data quality issues. When a failure occurs then it is necessary to fall back to a manual process with the resultant cost to the financial institution and inconvenience to the customer.

This will mean that on average online checks will range from £6 to £30. Furthermore, processes that rely entirely on customer-entered data are also prone to phishing attacks as well as other forms of identity theft.

UK challenger digital banks are reducing their onboarding costs and time by deploying online identity verification services and biometrics including facial and voice.

One of them also 'piggybacks' on other brick and mortar banks' verification by requiring details of a customer's UK current account for onboarding.

It can be difficult to isolate KYC compliance costs. Usually the KYC steps are part of the broader business processes of customer acquisition. These steps are used to comply with a range of legislation and regulations such as AML, FATCA, and the Immigration Act. Furthermore, KYC does not stop at onboarding. To remain compliant, evidence must also be regularly refreshed and archived for the applicable retention period.

It is however clear that a significant proportion of the cost is due to staff performing manual tasks. We believe that as the 4th and 5th AML directives take effect there is a significant opportunity for banks to reduce these costs by using technologies that allow KYC processes to be automated, resulting in fewer errors and simpler monitoring.

Our conservative estimate is that for a typical UK bank this could bring immediate savings of £5m rising to £10m as more customers move to mobile chanels, over the next three years.

The actual savings could be considerably higher. Failure to comply with KYC rules brings the risk of substantial fines. The reliance on manual processes increases the risk. Staff may cut corners and can be susceptible to manipulation in ways that technology cannot.

Compliance is not the only issue. Poor onboarding processes leads to abandonment of online and mobile banking applications and the associated loss of revenue.

In the UK as many as 25% of applications are abandoned due to the friction associated with KYC.[4]

Customer due diligence costs are increasing

4AMLD will be transposed into local law and come into force in June 2017. In the same month 5AMLD[5], which introduces a range of amendments to 4AMLD is expected to be adopted, with implementation occurring in June 2018.

Together these will result in significant increases in the cost of KYC compliance. 5AMLD, for example, introduces additional measures in response to the Panama Papers scandal and the increased terror threat in Europe[6]:

Area impacted	Main impact
Prepaid cards	Low limits (annual €2,500 limit replaced by monthly €150 limit) and removal of exemptions (e.g. for online-only, customers must be identified if their transactions amount exceeds €50).
Virtual currencies	Virtual currency exchanges and wallet providers brought into scope.
Payments to high risk countries	Additional verification of both the sender and the recipient, the nature of the intended business relationship and in some cases senior management approval.
Beneficial ownership for complex accounts	Indirect beneficial owners to be verified, including every trust-like legal arrangement whether a company or charity. This can potentially get very complex, for example, when indirect beneficial owners could reside in another jurisdiction making KYC much more difficult. Furthermore, current proposals are to reduce the beneficial ownership threshold from 25% to 10% including the number of individuals required to be KYC checked.

Table 1, Changes introduced by 5AMLD

Whilst the additional measures introduced in 5AMLD are very specific, they will serve to increase the already substantial cost of KYC compliance for many financial institutions.

Cost is not the only issue

Aside from the financial cost of meeting the requirements of 4AMLD and 5AMLD there is a potentially much greater cost to financial institutions in being prevented from delivering digital services. KYC introduces friction into the onboarding process.

This is clearly the case where KYC is performed over physical channels (e.g. branch or post). However even digital KYC processes can be cumbersome. Knowledge-based verification, for example, can be poor from a user experience as well as being susceptible to phishing.

Unless effective digital means can be found to efficiently perform KYC then there will be a significant impact to conversion rates for digital products.

This problem will be especially acute for migrant workers wishing to access financial services in a new country but without any financial history in that country.

What if you are not ready?

If you are not ready, you will be at increased risk of sanctions due to non-compliance. The specific sanctions are determined by each member state but are expected to be extremely punitive and highly damaging to the financial institution concerned. 4AMLD includes the following sanctions where there are serious, repeated, or systemic breaches of customer due diligence:

Impacted	Sanction
Financial Loss	Fine of twice the benefit derived from the breach or EUR 1m. For credit and financial institutions, this is increased to EUR 5m or 10% of total annual turnover.
Reputational Loss	Public statement about the breach.
Business continuity	Withdrawal or suspension of authorisation.
Personal responsibility	Temporary ban or EUR 5m fine against management.
Warning	Order to desist from non-compliant conduct.

Table 2, Failure is not an option

The UK Financial Conduct Authority (FCA) has fined some banks in recent years for failing to comply with AML requirements.

- Deutsche Bank was fined £163m for serious anti-money laundering controls failings[7].
- Barclays was fined £72m for failing to subject a number of ultra-high neworth clients (PEPs) to enhanced levels of due diligence and monitoring.
- Standard Bank was fined £7.6m for failings relating to AML policies and procedures over corporate customers connected to PEPs[8].
- The size and number of fines are increasing and it is in this area that most banks are vulnerable. Under new rules, the Deutsche and Barclays fines could have become a staggering £2.5bn and £2bn espectively (if 10% of previous year's total annual turnover was applied).

Consequently, UK banks have been 'de-risking' customers and relationships they associate with higher money laundering risk. This includes Money Service Businesses (MSBs), correspondent banking relationships, and FinTech start-ups. This de-risking affects diplomats, foreign students and the financially excluded unbanked population, as well as resulting in lost revenue to the banks.

One possible answer: eIDAS

5AMLD offers eIDAS[9], the EU's regulation on eID, as a route to efficient digital onboarding. But what exactly is eIDAS?

Europe has a history of government issued or recognised eID. Some countries, such as Belgium and Austria, have issued smart cards that contain cryptographic keys and digital certificates associated with the citizen's identity. In the Nordic countries, bank issued credentials can be used to access both banking and government services. The UK government's GOV.UK Verify[10] programme is seeking to establish a wide ecosystem digital identity provision and usage through partnership with the private sector. All of these schemes are country specific.

eIDAS requires EU Member States to recognise and accept any eID scheme issued in another Member State which has been "notified" to the Commission. eIDAS introduces infrastructure to enable cross border acceptance of these eIDs and provides a mechanism for countries to notify their scheme as being available for cross border use.

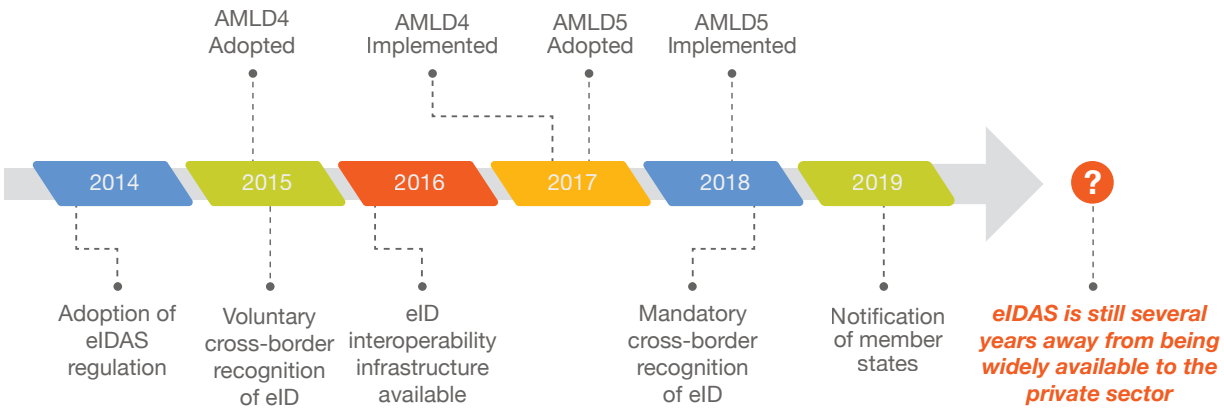


Figure 1, eIDAS timeline

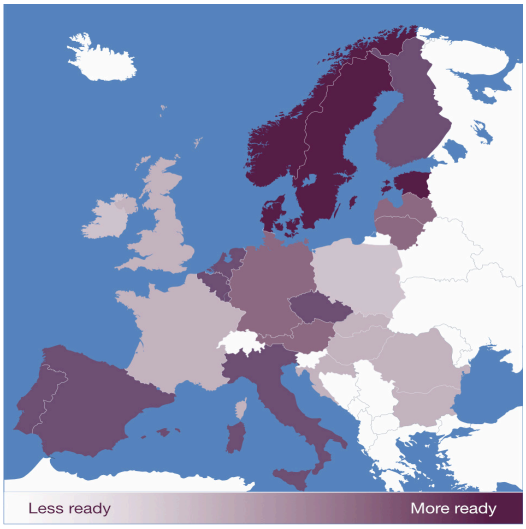
As the above timeline shows, whilst eIDAS has already been adopted into law and the central interoperability infrastructure put in place, individual countries are not required to be ready to accept other country eIDs until September 2018 and there is no timetable for when countries will notify their respective schemes.

As of the end of the first quarter of 2017, it is only Germany that is known to have formally notified[11] It is also not clear how or when eIDAS will be opened up to allow the private sector to access compliant digital identities. Realistically we believe it will be several years before eIDAS is widely available to the private sector.

So whilst eIDAS will provide a solution to KYC for digital onboarding in the future there is no clarity around when it will be available for 5AMLD compliance. Consequently, alternative approaches will be needed in the meantime. The European Commission itself recognises the need for "innovative digital tools for identifying customers"[12].

What about individual eIDs?

eIDAS is focused on cross border use cases. It does not prevent eID being used within a country for the purposes of supporting CDD. The majority of EU countries have an eID scheme of one form or another; however, the readiness of those schemes for integration into digital services varies widely.



Several of the eID schemes use smart cards, which do not integrate well into digital channels (especially mobile channels) due to the need for a reader device. Some countries (e.g. Norway, Sweden, and Estonia) have mobile versions of their eID. Others (e.g. Belgium, Denmark) have alternative solutions for online and mobile integration.

In some countries the use of eID is limited to specific government applications such as civil identity, so may not even be available for private sector use.

The GOV.UK Verify is designed for the digital space, but currently only available to government, whilst the scheme is established. There are ongoing projects to explore how to open up the scheme, or at least the services of the Verify-accredited identity providers, to the private sector. It is likely to be at least a year before these services are commercially available and ready for use in KYC for example.

The role for technology

For digital onboarding, there is a gap between what 5AMLD requires and what eIDAS provides both in terms of timing and suitability for digital channels, especially mobile. This gap can be addressed by using mobile technology that is already in the hands of many consumers.

1. Capture Document

MiSnap guarantees the capture of a quality image of all ID documents

2. Authenticate Document

Machine learning powers authenticity checks to validate the ID document isn't forged or tampered

3. Compare Face

Selfie compared to photo ID document to prove person holding document is who they say they are

Figure 2, Digital Identity Verification workflow

Most modern smartphones include high quality cameras that can be used to scan documents and take photographs or videos of the user.

Sophisticated image processing can be used to determine thegenuineness of a scanned document. Many official documents include security features such as the use of special inks, complex designs, watermarks, perforations and so on that can be analysed to show that the document is genuine. In addition, on many smart phones it is possible via the NFC interface to read and verify information from smart chips such as those embedded in passports.

‘Selfie’ photographs can then be combined with verified passport, driving licence or any other approved document data to confirm that the individual using the mobile device corresponds to the identity document presented.

Furthermore, several countermeasures can be employed to mitigate the risk of impersonation such as taking a ‘selfie’ of a picture, by incorporating ‘liveness’ tests where it is confirmed that it in fact is the true live person taking a selfie. ‘Liveness’ tests can include techniques such as recording video of the person reading randomly presented words, moving body parts in randomly directed order, or other real-time activity.

Machine learning can be used to continuously improve the analysis of all of the above inputs. This could allow, for example, systems to automatically detect new anomalies as they arise without needing to explicitly code instructions for them.

Finally, teams of highly trained experts can perform spot checks and perform exception handling.

Mobile technology employed in this way will provide a better and more secure onboarding journey for digital channels. Its application is however not limited there. For example, mobile deployed in branch could be used to provide essentially the same process taking out the human element from KYC, which currently places a reliance on the individual to recognise false documents and to match the person to the photo.

Most importantly it enables customer due diligence to be more automated reducing both staffing requirements and likelihood of mistakes, the two areas where most of current KYC costs and regulatory compliance risk arise.

You need to act now

4AMLD introduces stiff administrative sanctions for non-compliance. 5AMLD, which is expected to be adopted in June 2017, will further increase the already considerable costs and risks to financial institutions associated with KYC. Current ways of performing KYC are often inefficient and prone to human error. It is incumbent on every financial institution to examine how it can improve its KYC processes. Otherwise, it will be exposed to a massively increased risk of loss, through huge fines, brand damage, and increased fraud exposure.

Cumbersome onboarding processes also result in applications for financial products being abandoned by new customers, with the result loss of revenue. Without taking action to make digital onboarding better, growth in digital channels limited and incumbent financial institutions will start to see challengers take the lead.

Adopting mobile identity verification technology, such as that described above, is one very practical and immediate step financial institutions can take to both improve onboarding processes and significantly reduce compliance costs and associated risks.

References

[1]
Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity - https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html

[2]
BBA response to Cutting Red Tape Review – Effectiveness of the UK's AML Regime - https://www.bba.org.uk/policy/bba-consultation-responses/bba-response-to-cutting-red-tape-review-effectiveness-of-the-uks-aml-regime/

[3]
Drivers & Impacts of Derisking: https://www.fca.org.uk/publication/research/drivers-impacts-of-derisking.pdf

[4]
On-Boarding Report - The battle to on-board: why 40% of consumers abandon banking applications https://www.signicat.com/wp-content/whitepapers/signicat-onboarding-whitepaper.pdf

[5]
Directive of The European Parliament and of The Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC - http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf

[6]
EU Panama Inquiry Committee –http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587327/IPOL_STU(2016)587327_EN.pdf

[7]
FCA fines Deutsche Bank £163 million for serious anti-money laundering controls failings - https://www.fca.org.uk/news/press-releases/fca-fines-deutsche-bank-163-million-anti-money-laundering-controls-failure

[8]
Financial Conduct Authority – AML fines - https://www.fca.org.uk/search-results?search_term=AML%20fines

[9]
Regulation (EU) No 910/2014 of The European Parliament and of The Council on electronic identification and Trust services for electronic transactions in the internal market - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

[10]
Government Digital Service - GOV.UK. Verify Guidance - https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

[11]
eIDAS Notification of the German eID - https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/German-eID/eIDAS-notification/eIDAS_notification_node.html

[12]
European Commission Consumer Financial Services Action Plan - http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017DC0139&from=EN

About Consult Hyperion

Consult Hyperion is an independent strategic and technical consultancy, based in the UK and U.S., specialising in secure electronic transactions. We help organisations around the world exploit new technology for secure electronic payments and identity transaction services, from mobile payments and “chip and PIN” to contactless ticketing and federated identity. Our aim is to assist customers in reaching their goals in a timely and cost-effective way.

We support the deployment of practical solutions using the most appropriate technologies and have globally recognised expertise at every step in the electronic transaction value chain, from authentication, access and networks, to transactional systems and applications.

For more information, visit www.chyp.com or email info@chyp.com

About Mitek

Mitek is a global leader in mobile capture and identity verification software solutions. Mitek’s ID document verification allows an enterprise to verify a user’s identity during a mobile transaction, enabling financial institutions, payments companies and other businesses operating in highly regulated markets to transact business safely while increasing revenue from the mobile channel.

Mitek also reduces the friction in the mobile users’ experience with advanced data prefill. These innovative mobile solutions are embedded into the apps of more than 5,600 organisations and used by tens of millions of consumers for mobile check deposit, new account opening, insurance quoting, and more.

For more information, visit www.miteksystems.co.uk or www.miteksystems.co.uk/contact