Research Sponsored by Mitek

WHITE PAPER

The cost of compliance and how to reduce It

consult hyperion
securing tomorrow's transactions

Executive summary

Banks and other financial services providers are legally required to establish the identity of their customers. These "Know Your Customer" (KYC) requirements are vitally important in helping to prevent financial crime and to protect society. However, they require banks to perform costly and cumbersome checks on customers, which impact both their bottom and top lines.

The bottom-line cost of meeting these requirements is very high – as high as €50m for a typical bank with 10m customers. And when banks fail to comply, these costs can be dwarfed by the punitive fines that regulators have demonstrated they are willing to mete out.

Often banks resort to sub-optimal manual processes to meet these KYC requirements. These manual processes create a very poor user experience, resulting in new customers abandoning applications in droves preferring challenger banks or fintechs that offer a more fully digital experience. For a typical bank we believe this could hit the top line by as much as €10m in the short term but with a much greater lost opportunity in the long term as these important new customers go elsewhere. After five years the cumulative lost opportunity cost could be in excess of €150m.

These problems are not going to go away. Quite the opposite in fact. Over the past few years the EU has introduced a series of directives that extend the scope of Know Your Customer (KYC) requirements, make more organisations subject to these requirements and increase the sanctions on organisations and individuals that fail to meet those requirements.

Financial institutions must find efficient and effective ways to undertake it in order that they remain competitive, do not exclude legitimate customers, and play their role in protecting their communities.

This paper explores the ongoing pain points that KYC creates for financial institutions – with examples from the Netherlands, Spain and the UK. We consider the following areas of cost:

Internal costs
especially those arising from needing to rely on the branch network

External costs
including the variable available data to support KYC processes depending on the country concerned

Fines
when financial institutions get it wrong

Lost opportunity costs
that arise when potential customers abandon applications due to the friction placed in KYC processes

Copyrighted material, all rights reserved | **consult hyperion**

Many of the issues with KYC today are linked to the need to frequently revert back to manual processes, such as requiring a person to visit a branch or send documents in the post.

These manual processes are:

Costly to operate

Significant friction for the customer

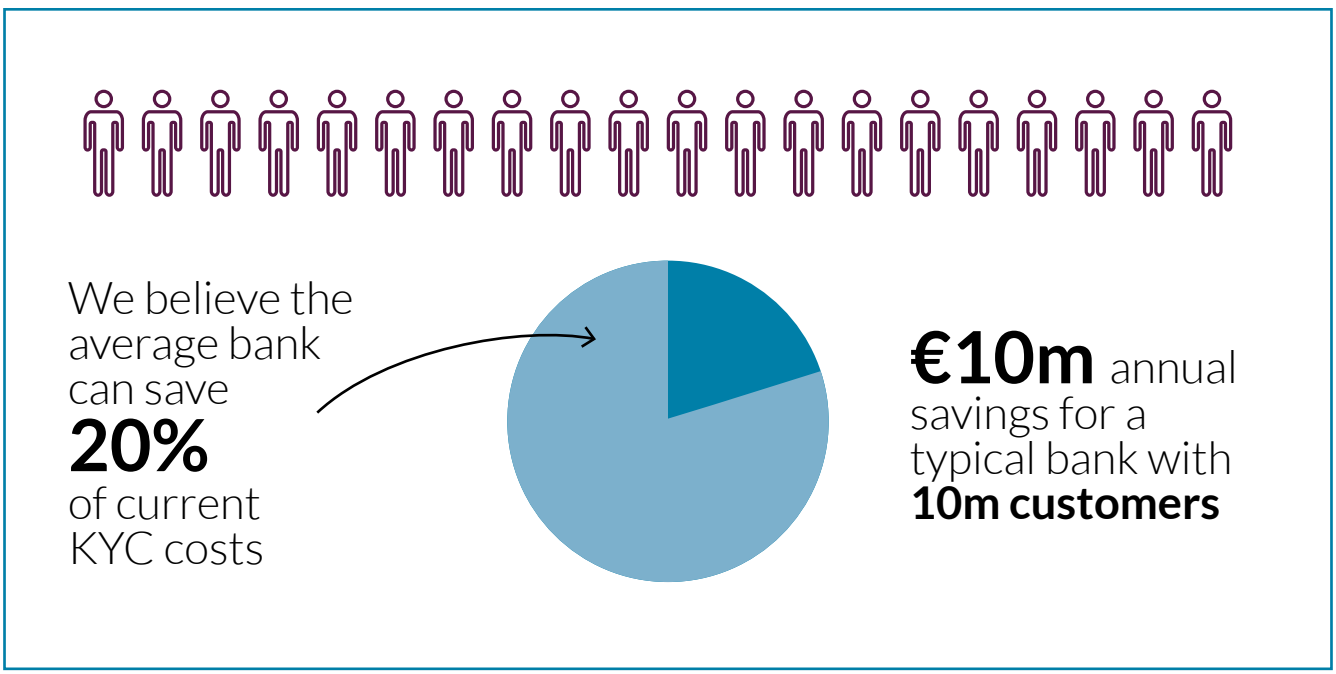
Unreliable

This paper outlines how technology can address many of these issues.

Employing mobile technology to verify physical documents and capture biometric information is rapidly maturing and becoming mainstream.

This technology enables KYC to be performed fully in digital channels for many customers. It works well in a face-to-face environment too, removing the human element from manual checks. Some digital identity technologies and services may help in the future but many of these are years away from maturity.

Employing robust technology is one of the the only ways to ensure that the complex array of KYC requirements is satisfied and is key to addressing the cost issues.



Copyrighted material, all rights reserved | consult hyperion

KYC: more relevant than ever

Over recent years significant regulatory changes have resulted in greater demands on the financial services industry. Banks continue to discuss the pros and cons of collaborating on KYC and in the meantime, numerous fintech companies have emerged with digital KYC solutions.

Despite all the discussion, **KYC compliance continues to pose a challenge to the financial services industry.** For good reason, regulators have been tightening the screws by strengthening KYC requirements.

As more and more commerce shifts to the digital channel, these requirements are essential to:

- **Counter criminal activity**
- **Prevent fraud**
- **Ultimately protect society**

To satisfy these requirements, banks need to employ a whole host of measures. Far too often, however, they still rely on manual processes which are costly to the bank, as well as time consuming and cumbersome for the customer.

Furthermore, when banks get it wrong, the consequences are dramatic. In recent years, there have been a series of highly publicised AML failings in major financial institutions, such as Danske Bank [1], ING Group[2] , Standard Chartered[3] and UBS[4] to mention a few. These have resulted in enhanced regulatory scrutiny both at EU[5] and national[6] levels and seen regulators willing to mete out punitive fines, such as the colossal €775m handed down to ING.

So, what is exactly KYC?

KYC is the process employed by a bank to ensure it knows the identity of the customer.

This may involve using identity documents and background data sources to both establish who the customer claims to be and then taking steps to confirm that the customer is actually that same person. KYC is performed during onboarding to financial services, but it does not stop there. Banks are required to ensure that they "know" the customer for the lifetime of the financial service in question. For retail customers, this includes detecting and confirming when a customer's circumstances change, such as when they move. For business customers, it also includes changes of ownership or control.

KYC is also a key element of AML and Counter-Terrorist Financing (CTF) compliance. It is the foundation on which the rest of AML is built. If you don't "know your customer" then you cannot assess whether there is a risk of you facilitating criminal financial activity.

This paper explores the rising costs that financial institutions face in meeting KYC requirements – with specific examples from the Netherlands, Spain,

1 Danske Bank - 2018 Actor of The Year in Organized Crime and Corruption
2 ING bank fined €775m over due diligence, client on-boarding
3 FCA fines Standard Chartered Bank £102.2 million for poor AML controls
4 FCA fines UBS AG £27.6 million for transaction reporting failures
5 EU Lawmakers Adopt Plan to Create Multiple Financial Crime Agencies
6 MPs in renewed attempt to force money laundering crackdown

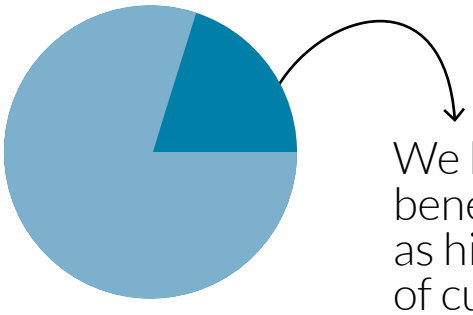
Copyrighted material, all rights reserved | **consult hyperion**

and the UK. As the paper also shows, there are numerous pain points impacting both banks and their customers. Many of these revolve around the reliance banks still have on manual processes. The answer, therefore, is to employ technology that enables these processes to become digital, reducing or removing the reliance on human operators and providing solutions that are effective over fully digital channels.

Fortunately, new technologies are being developed specifically in this space. Mobile technology to digitise KYC processes is now maturing and an essential part of any KYC solution. In the future, broader developments in digital identity will allow customers to present portable and secure, fully digital identities to banks and other services.

Our analysis suggests that the right technology will bring significant financial benefit to banks by:

- **Cutting costs**
- **Improving efficiency**
- **Preventing application abandonment**



We believe this benefit could be as high as **20%** of current KYC costs

or up to **€10m** **for a large bank.**

Why is KYC so hard?

There is no silver bullet solution that works for all customers.

To know your customer, you need to take them through the process that establishes and verifies their identity.

For some customers this could involve them presenting identity documents and leveraging credit bureaux data. For others this may not work – particularly for people without an established credit history, good address evidence and beneficial owners in other countries.

Copyrighted material, all rights reserved | **consult hyperion**

Making the process work seamlessly at the point of need can be difficult. Suppose someone wants to borrow money to buy a car they have just taken on a test drive. It is unlikely the person will want to go home, mail a copy of their passport or utility bills and wait days or weeks to get financing. In this "on-demand" era, it is much more likely that they will borrow the money from a provider who can perform their KYC real time and provide the funds instantly.

The liabilities associated with KYC, including the risk of fraud and penalties for non-compliance, has often left banks feeling that they need to do it themselves, controlling the processes as far as possible. This has resulted in the great fragmentation and duplication of costs we see in the market today. For a bank to be open to using KYC from somewhere else, the risk of non-compliance and fines need to be outweighed by the benefits (savings) of doing so. Even then, risk-averse compliance managers are going to need some persuading to move away from processes over which they have control.

Further complicating the regulatory landscape, AML requirements vary from country to country. In Europe, AML regulation is derived from a series of directives which are then interpreted and transposed into local law which is then enforced by the country specific regulator(s), following country specific guidance. This creates complexity for regulated organisations operating in multiple countries as they need to build localised processes and customised solutions for each country in which they operate.

	Spain	Netherlands	UK
Regulator	SEBPLAC	DNB AFM Belastingdienst	FCA Gambling Commission
Guidance	SEBPLAC	DNB AFM Belastingdienst	FCA JMLSG Gambling Commission ICAEW HMRC The Law Society
KYC evidence	Government issued	Government issued	Issued by government, public sector, or regulated entity.
KYC verification	Documents presented certified by appropriate person	Confirm documents issued by government	Verification in person or electronically with checks determined by risk

Figure 1, AML/KYC Regulation in Netherlands, Spain, and UK

The complexities of KYC do not stop there. In response to evolving financial crime threats regulators need to continually review and where necessary extend the scope of KYC regulation.

Copyrighted material, all rights reserved | **consult hyperion**

The growing scope of KYC

In recent years, the EU has introduced a series of directives targeting money laundering and terrorist financing, each of which refines and adjusts the approach taken in each country. These have progressively increased the number of organisations that are in scope and types of services for which KYC processes apply.

Regulation	Adopted	Effective	Features
4AMLD	May 2015	Jun 2018	• Central register of beneficial owners • Broader definition of PEPs • Risk based approach • Sanctions and penalties (see below)
5AMLD	May 2018	Jan 2020	• Beneficial owner register made public • Member states required to issue list of functions performed by PEPs • Additional services and organisations brought into scope (see below)
6AMLD	Nov 2018	Dec 2020	• Harmonised definition of money laundering predicate offences including aiding and abetting • ML offences committed anywhere in the world can be taken into consideration provided the offence is declared an offence in the ember state • Tougher punishments including prison sentences for both natural and legal persons – based on "identification principle" • Extraterritorial reach – member states' jurisdiction covers money laundering offences committed by their nationals or for the benefit of domestic organisations domiciled in their territories, no matter where in the world the offences were committed

Figure 2, Summary of AML Directives

4 and 5AMLD focus on risk management and transparency respectively, while 6AMLD focuses on making High-End Money Laundering (HEML) unattractive to 'Professional Money Launderers (PMLs)[7] .

4 and 5 AMLD expand the list of obliged entities and services that are in scope. This reflects the wide range of ways that criminals use to launder money. As well as banks, the regulation has expanded the scope of KYC to cover auditors, accountants, and tax advisors. It also includes organisations involved in the trading of physical assets such as estate agents, art dealers, free ports, storage providers and other intermediaries. And of course, virtual currency exchanges and virtual currency wallet providers are included too.

7 http://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf

Copyrighted material, all rights reserved | **consult hyperion**

The number and extent of checks has been increased too. Enhanced Customer Due Diligence (ECDD) is required for customers from a recently expanded list of high-risk countries.

The requirement to identify, verify and continuously monitor the Ultimate Beneficial Owners of legal persons including trusts and trust-like entities, especially where the UBOs are domiciled in a blacklisted high-risk third countries or offshore tax havens, creates particular challenges for KYC programmes.

Area impacted by 5AMLD	Main impact
Prepaid cards	Lower limits (annual €2500 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 third countries	Additional verification of both the sender and the recipient, source of funds and source of wealth, 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 overly complex, for example, when indirect beneficial owners could reside in another jurisdiction making KYC much more difficult.
Safe deposit boxes	CDD of owners of anonymous passbooks and safe deposit boxes, their proxy holders, and beneficial owners should be fully identified just as in for a payment/bank account.
Rental properties	CDD on properties of monthly rental value of €10,000 or more.
Art traders, free ports, storage providers and intermediaries including art galleries and auction houses in works of art	CDD for works of art where the value of the transaction or a series of linked transactions amounts to €10,000 or more.

Copyrighted material, all rights reserved | **consult hyperion**

Keeping pace with regulation is a challenge. It requires significant investment on top of the already substantial KYC costs at a time when banks desperately need to innovate to ahead of the competition.

What does KYC cost?

The operational costs associated with KYC are significant. Thomson Reuters, in their landmark study, reported that the average bank spends €50m[8] a year on KYC and CDD ("Customer Due Diligence") compliance with some banks spending up to €450m[9]. Based on conversations with a number of banks, the scale of KYC costs remains consistent with these numbers and may indeed be higher as a result of increased regulatory requirements.

It can be difficult to isolate KYC compliance costs. KYC is an integral part of the customer acquisition and onboarding process but can take many routes depending on:

- **The channel used for onboarding**
- **The ability of the customer to provide the right evidence**
- **Other checks that may need to be performed as part of the wider CDD**

Furthermore, KYC does not stop at onboarding. To remain compliant, evidence must also be regularly refreshed and archived for the applicable retention period.

Nonetheless, the costs surrounding KYC compliance can be broken down into the following key areas:

1. INTERNAL COSTS

Internal costs will include the KYC processes themselves as well as all the activities required to ensure the bank remains compliant. Hundreds, and in some cases thousands, of compliance staff will be employed to monitor transactions, deal with alerts, work cases, phone customers, deal with false positives and so on.

These costs, especially around staffing with trained AML professionals are rising. The waves of regulation hitting financial services have placed compliance officers in great demand resulting in additional recruitment and substantial pay rises[10].

There are numerous hidden costs as well. For example:

In-branch checks:

Depending on the local KYC requirements, with current processes, it will often not be possible to fully complete the KYC processes through a digital channel. Students and immigrants for example will often not be able to provide the legally acceptable evidence of long-term in country address. In these cases, the KYC process will need to be completed manually in-branch. This could, for example, involve examining a letter of invitation from a recognised university. Undertaking these checks interferes with and interrupts the normal commercials activities of the branch.

8 Reuters reported $60m which is approximately €50m
9 Reuters reported €500m which is approximately €450m
10 https://www.ft.com/content/baf70664-2795-11e8-b27e-cc62a39d57a0

Copyrighted material, all rights reserved | consult hyperion

Training in-branch staff:

In order to perform checks in-branch, it is necessary to ensure that those staff are trained and have the necessary expertise. Doing this consistently across a disparate branch network can be difficult and costly.

Record keeping:

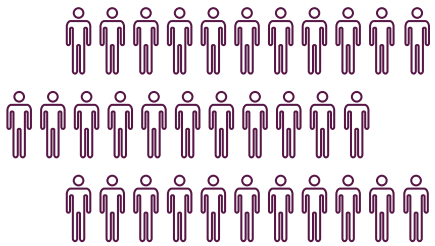
Keeping evidence of the checks undertaken is vitally important and inevitably more costly when checks are manual.

The cost of KYC does not stop at onboarding. Regulated entities are obliged to perform ongoing customer due diligence. This will involve monitoring financial transactions for suspicious activity. It should also include responding to changes to the customer's circumstances (e.g. change of beneficial ownership for a business customer) that could indicate an issue.

Established banks often have the additional headache of needing to re-verify existing customers who were not onboarded correctly in the past.

We estimate that for a bank with **10m customers** KYC programme itself will have internal costs up to

€25m including the costs of back office compliance staff as well as the cost of sending some customers into branches.



2. EXTERNAL COSTS

External suppliers will be an essential part of any KYC programme. Credit bureaux and background data sources have been essential points of reference to corroborate the identity claims made by prospective customers, as well as providing inputs to ongoing customer due diligence processes.

The availability of credit data varies between country. In the UK, large credit bureaux provide repositories of financial credit activity including payments (or defaults) on loans, mortgages, subscription phone bills and credit cards. The same organisations aggregate numerous other data sources providing counter-fraud signals amongst other things.

In the Netherlands and Spain however, the credit bureaux only hold negative credit records (e.g. defaults). Consequently, they do not provide full coverage of the banked population, meaning that as a source of identity evidence they are incomplete. This means that in these markets completing KYC online will be more difficult, resulting in higher numbers being required to go into branches.

Copyrighted material, all rights reserved | **consult hyperion**

Spain	Netherlands	UK
Negative credit records only	Negative credit records only	Positive and negative credit records

Figure 4, Credit Bureaux in Netherlands, Spain, and UK

Of course, in all these countries, performing KYC on new immigrants is a challenge as no in-country records of any type exist.

Isolating external KYC costs is difficult as often KYC checks will be bundled with credit score and other checks.

We estimate that for a bank with **10m customers**

KYC programme itself will have external costs up to **€5m** depending on the market in which the bank operates.

3. SANCTIONS

As well as the internal and external costs, there is constant risk of sanctions on financial institutions that do not meet the regulatory requirements.

The cost of getting KYC wrong are substantial with the risk of financial, reputational, and personal cost. The specific sanctions for AML failings 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:

Copyrighted material, all rights reserved | **consult hyperion**

Sanction introduced in 4AMLD	Impact
Fine of twice the benefit derived from the breach or €1m. For credit and financial institutions, this is increased to €5m or 10% of total annual turnover	Financial Loss
Public disclosure of the breach	Reputational Loss
Withdrawal or suspension of authorisation	Business continuity
Temporary ban or €5m fine against management (6AMLD introduces the potential for criminal convictions)	Personal responsibility
Order to desist from non-compliant conduct	Warning

Figure 5, 4AMLD Sanctions and Penalties

The Netherlands and UK have both seen regulators taking an aggressive stance. The UK Financial Conduct Authority (FCA) has intensified its regulatory enforcement strategy by adopting 'dual track' AML investigation practices, i.e. "investigations into suspected breaches of the Money-Laundering Regulations that might give rise to either criminal or civil proceedings[11]" , apart from substantial fines issued to some banks in recent years for failing to comply with AML requirements.

SO FAR IN 2019:

- **the FCA has fined Standard Chartered Bank £102m for poor AML controls[12].**
- **Goldman Sachs International, £34.3m for failure to provide complete, accurate and timely information in relation to reportable transactions[13].**
- **UBS AG, £27.6m for transaction reporting failures[14].**

IN RECENT PAST,

- **Deutsche Bank was fined £163 million for serious anti-money laundering controls failings.**
- **Barclays Bank, £72m for failing[15] to subject a number of ultra-high net worth clients (PEPs) to enhanced levels of due diligence and monitoring.**
- **These are dwarfed by the €775m fine levied on ING by Dutch authorities.**

11 https://www.fca.org.uk/news/speeches/partly-contested-cases-pipeline-and-aml-investigations
12 FCA fines Standard Chartered Bank £102.2 million for poor AML controls
13 FCA fines Goldman Sachs International £34.3 million for transaction reporting failures
14 https://www.fca.org.uk/news/press-releases/fca-fines-ubs-ag-276-million-transaction-reporting-failures
15 https://www.fca.org.uk/news/press-releases/fca-fines-deutsche-bank-163-million-anti-money-laundering-controls-failure

Copyrighted material, all rights reserved | **consult hyperion**

Spain	Netherlands	UK
€1,000,000	€776,000,000.00	£176,519,136

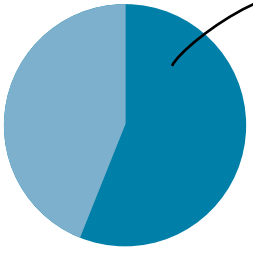
These figures may not represent fully the extent of AML fines. In the Netherlands for example not all AML fines are published. This is also true of Luxembourg and Germany which take advantage of loopholes in AMLD making it not compulsory to publish these fines.

Sanctions are not the only risk of course. KYC failings are likely to result in fraudulent activity resulting in financial loss to the financial institution. For example, card ID theft in the UK rose in 2018 by 59% to £47.3 million[16] . This occurs where a criminal uses a fraudulently obtained payment card or card details, along with stolen personal information, to open or take over a card account held in someone else's name. This is precisely the type of fraud KYC is supposed to prevent.

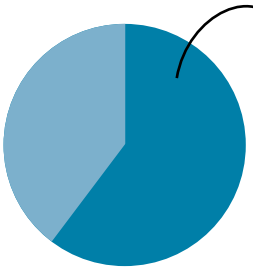
For a bank with **10m customers** the annual cost of fines, based on fines issued over the past 10 years and assuming all banks are equally vulnerable, would be **€3.5M** Clearly when things go wrong the costs can be a lot higher.

4. LOST OPPORTUNITY COST

Perhaps the biggest concern for banks should be the lost business when customers abandon applications for financial products because the KYC processes are too cumbersome. Recent research from Sapio[17] suggests that :



abandonment is a staggering **56%** (up from 40% two years ago).



retail customers are **60%** more likely to complete an application if it can be done completely online - something that is recognised and embraced by many start-up banks.

16 https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf
17 https://www.signicat.com/wp-content/whitepapers/signicat-battle-to-onboard-II-v6.pdf

Copyrighted material, all rights reserved | **consult hyperion**

There is a marked difference between the onboarding processes of traditional banks and internet or app-only challenger banks. These challenger banks are completely focused on simplifying the user experience and removing friction wherever possible.

For most customers, the challenger banks complete the KYC process in a fully digital and seamless manner. Where customers are not able to complete the process, rather than send those customers into a branch, challenger banks will place limitations on the accounts in question to mitigate the AML risks. They may for example place limits on the number or value of transactions. The average customer however will not notice the limitations – they just see the better user experience.

If a bank's onboarding process is in any way cumbersome, then some potential customers will give up. This is especially critical for key groups of new customers such as young people and students who represent the future business of the bank.

Even if this is only a few percent of these new customers, for a large bank that would equate to millions of Euros in lost earnings.

Given the scale of application abandonments we believe it is likely that large banks are losing out on at least €10 million now and a much higher lost opportunity in the future.

After 5 years the cumulative lost opportunity cost could be in excess of €150m.

How will technology help?

Large banks have already invested and continue to invest in sophisticated internal systems to help manage AML risks. These often employ "waterfall" screening that enable the bank to identify high-risk customers and high-risk events so that effort can be focused where it is most needed. These are clearly essential when dealing with the retail and SME business banking volumes. Often these internal systems are home grown and so between banks there will be significant variation in approach and capability. Some banks will actively monitor for and detect mules accounts, others will be more reactive.

Well designed and managed data analytics systems are essential in managing AML risks. These systems don't provide all of the answers, but they do help to identify quickly where there could be problem. It is then often necessary to revert to a manual process requiring a customer to bring documents to a branch or to post a notarised document, for example, leading to the inevitable application abandonments.

Copyrighted material, all rights reserved | **consult hyperion**

Technology can help remove these manual identity verification processes by:

Removing the human element:

Fully digitising onboarding processes will reduce the number of checks in branch, ideally with the branch just being used for exceptional cases. Technology can also be deployed in branch as well, digitising in-person processes. Then even though the customer is being served by a customer service representative, the risk of mistakes is minimised.

Making processes more auditable:

Fully digitising processes ensures that a complete and accurate audit trail of KYC processes can be created avoiding the inefficiencies and unreliability of depending on manual processes.

Streamlining the user experience:

Getting the user experience right is vital for digital services. Placing fully digital KYC processes at the optimal place (or places) in the user journey will help avoid customers giving up.

Key technologies that will help to bring these benefits include:

Mobile identity document verification:

Mobile identity document verification technology is already being used widely to digitise KYC processes. This technology provides a bridge between the physical and digital worlds. The technology includes the ability to scan physical identity documents with a mobile device and then perform biometric comparison of the customer against the scanned document. This technology is effective for digital channels and in-branch KYC processes alike. In branch, the technology can be provided to and operated by the customer services person – digitising a manual process.

Digital identities:

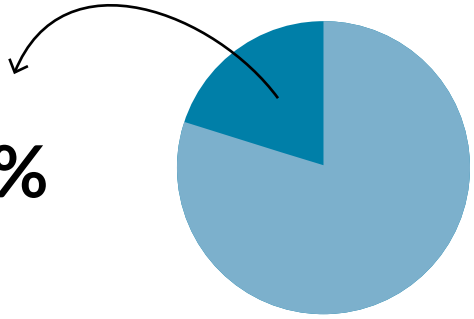
Where customers have a pre-verified identity that can be relied upon by banks and other service providers. The digital identity market is nascent in some markets (e.g. the UK and Spain) and more developed in others (e.g. the Netherlands).Furthermore, eIDAS has created an interoperable framework for government issued electronic identities in Europe. It will be some time before we have ubiquitous digital identities that banks can depend upon.

Self-sovereign identity:

Where customers are provided customers with the means to collect and share cryptographically verifiable personal data or digital documents. A number of scalable and extensible decentralised identity networks are being established for this purpose. From a KYC perspective, they provide the ability for a financial institution to go back to the source and draw their own conclusions about the veracity of the data or document being shared. Again we anticipate it will take several years for these to become widescale.

Copyrighted material, all rights reserved | **consult hyperion**

For a bank with **10m customers**
We believe effective use of technology could benefit the bank as much as **20%** of its current KYC compilance cost



through a combination of:

- **Reducing the reliance manual processing such as in-branch checks**
- **Reducing the lost opportunity cost**
- **Reducing the risk of compliance failings with the consequent fines and brand impact.**

This could be worth as much as **€10m.**

So, what should you do?

KYC is a first line of defence against financial crime. Criminals continually adapt and adjust their approaches to look for weak points. Manual processes are always a weak point and therefore a common place for criminals to target. Replacing these manual processes with identity technology is essential to avoid these common weak points and to enable you to keep pace with the rapidly changing landscape.

Technology is key to protecting both your business and your customers. It is key to meeting KYC requirements in an efficient and cost-effective manner. And it is key to ensuring you provide your customers with the best possible user experience and, in doing so, avoid the unnecessary levels of application abandonment many banks see today.

Today, mobile identity document verification is the primary technology to digitise KYC processes. It has already been adopted by many banks – large and small – and has reached a level of maturity where it should be part of every banks KYC approach.

This technology provides a bridge from the physical to the digital, that can be deployed in both remote and face-to-face channels. It is available now and should be part of every banks digital strategy.

Other digital identity technologies are more nascent. Much effort is being put into building broader digital identity ecosystems, that provide customers with portable digital identities that work across the digital economy. Government, banks and technology providers are all investing heavily in these systems. It will however be some time before these capabilities become mainstream.

Copyrighted material, all rights reserved | **consult hyperion**