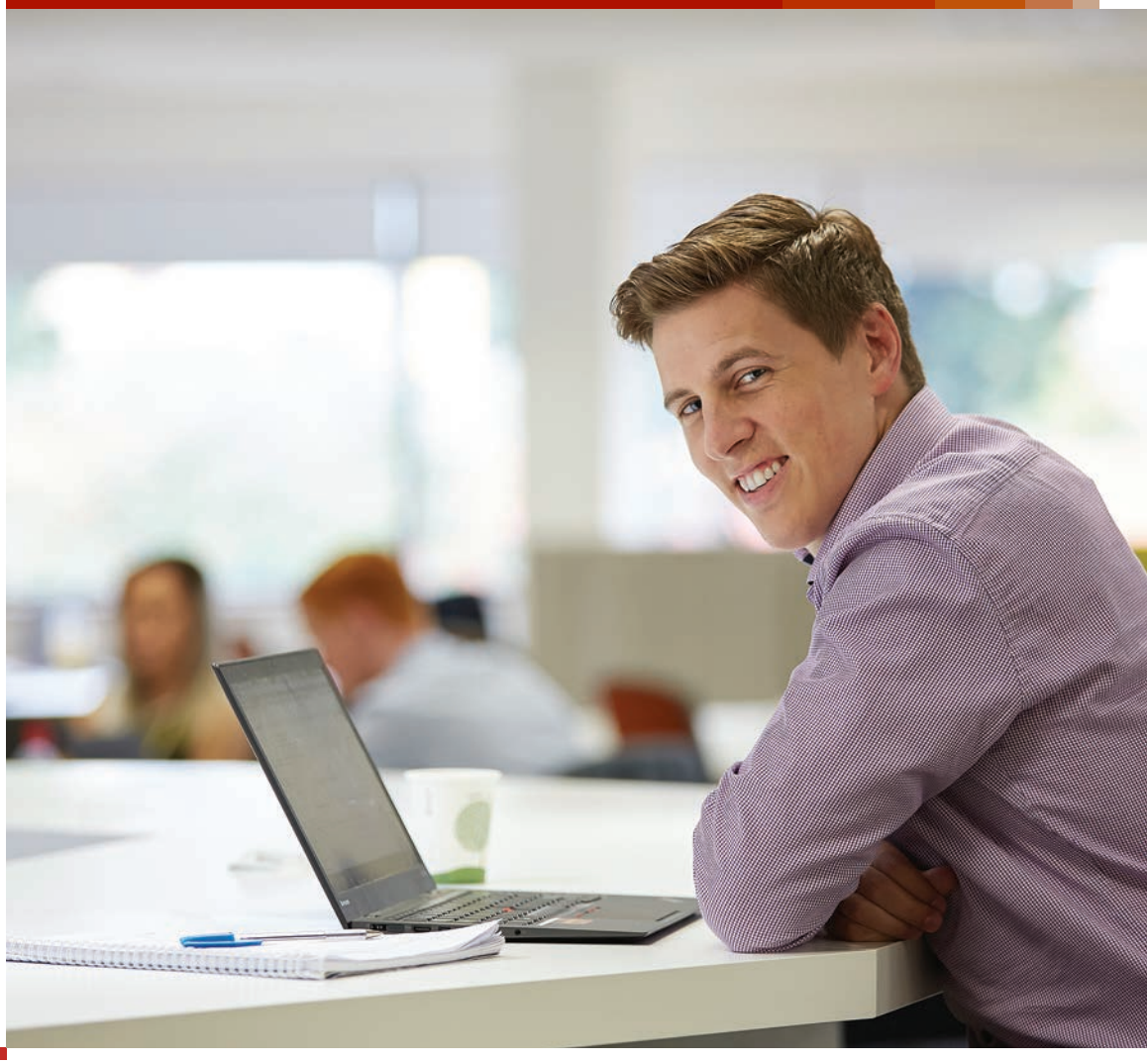
www.pwc.com/financialservices

# *The Future of Onboarding*

*December 2016*



pwc


BUS

**Contents**


| | |
|---|---|
| The Future of Onboarding | 4 |
| The Current State of Affairs | 5 |
| ***1.*** Digital Identities | 6 |
| ***2.*** Biometrics | 8 |
| ***3.*** Utilities and Blockchain | 10 |
| The Purpose of Financial Institutions | 11 |
| The Way Ahead | 12 |
| Contacts | 13 |

# *The Future of Onboarding*

*The current onboarding processes at many financial institutions are anachronistic. Fortunately, advances in technology offer solutions to the onboarding operation which are being deployed with enthusiasm. However, to be most effective the financial services community must all pull in the same direction…*

How can you prove who you are? This rather existential question sits at the heart of financial institutions' fight against the risk of financial crime and is the main challenge for the future of client onboarding. Particularly in an age where financial institutions rarely interact with their customers face-to-face, how can these institutions really know their customer?

Technology provides a solution to this conundrum, provided that regulations can keep pace with technological developments. Having visibility across the market of the full range of Know Your Customer (KYC) identification and verification innovations that are out there enables us to see how they are driving divergent approaches to customer onboarding.

We ask whether these divergent approaches are wasting an opportunity for the financial services industry. Enhancing the onboarding process could allow financial services to contemporise but at the same time help to raise the bar for financial crime risk management around the globe. We believe that enhanced standardisation in the customer onboarding process allows for efficiencies in time and cost, but also sets a clear goal for developing territories' financial crime risk management frameworks and will expedite their rise to meet global Financial Action Task Force (FATF) standards. In this manner, issues such as de-risking that have caused consternation among banks, money-service providers, customers, regulators and governments for some years can be overcome.

# *The current state of affairs*

Current processes for client onboarding employed by many financial services organisations involve collecting documents or individually engaging credit reference agencies to verify customer identity against other independent data sources on their behalf. However this poses a number of challenges which are set out in Figure 1.

We discuss below a number of technologies that are already having an impact on how financial institutions onboard customers.

**Figure 1**

| **Access:** | **Time consuming:** | **Variable quality:** |
|---|---|---|
| we are seeing a pressure from society for immediate services. Customers' expectations nowadays demand easy access to financial services and certainly no longer include physically coming into a branch. | numerous reviews that we have performed at financial services institutions have illustrated that the time it takes to onboard a customer can be very long. This is costly for the bank and frustrating for the customer. | the remediation exercises that we have performed have shown that compliance officers set due diligence standards to varying degrees of rigour, resulting in varying strength of KYC documentation obtained. |

Source: PwC

# 1 Digital Identities

*As a society, we are more and more comfortable with the concept of digitalisation. It is evident that we are integrating more and more of our lives with technology. In 2015, the UK performed 347 million payments through banking apps, a 54% increase from the year before[1] and this shows no sign of slowing down. While privacy remains a concern to many people, the increased convenience that technology offers is driving more and more people to embrace these new technologies.*

The creation of a digital identity – a unique identifier for you that verifies that you are who you say you are – seems to be the natural next step to facilitate society's desire to digitise.

A good example of where this has worked is Norway, where a bank ID can be used as a digital identity to both the public and private sectors, including all Norwegian banks. A study has shown that 80% of the adult population has a digital identity and through the use of this Bank ID, an individual can easily open a bank account and the financial institution will have comfort from a regulatory and an anti-money laundering (AML) perspective that the customer's identity has been verified[3].

Digital identities are also already offered in many other EU member states. However, some are more embedded than others. For example, Estonia allows a digital identity to be used for many purposes from opening a bank account to registering a company[4]. On the other hand, digital identities are available in the Netherlands, but their uses are limited to governmental and healthcare services. New EU regulation called the Electronic Identification and Authentication Services regulation (or 'eIDAS')[5] seeks to establish a single legal framework for recognising electronic signatures and identities throughout the EU as part of a wider programme by the European Commission to create a single digital market. One of the aims of this regulation is to allow the holder of a digital identity in one member state to use this to access services in other member states. This may be the start of the standardisation of identification that we need.

In May 2016 the UK government rolled out their own digital identity programme called GOV.UK Verify, the purpose of which, in its own words, is to 'prove who you are online'[6]. The process of how this is performed is set out in Figure 2. In short, this process requires a pre-approved third party provider to the government to perform verification checks over your claimed identity, providing you with a unique code that can unlock the ability to carry out governmental services such as completing your tax return. It is the intention of GOV.UK Verify to look to roll out these digital identities beyond governmental services.

1 https://www.bba.org.uk/wp-content/uploads/2016/07/TWWBN3_WEB_Help-at-Hand-2016.pdf

2 http://oixuk.org/wp-content/uploads/2016/02/Digital-Identity-Across-Borders-FINAL-Feb2016-2.pdf

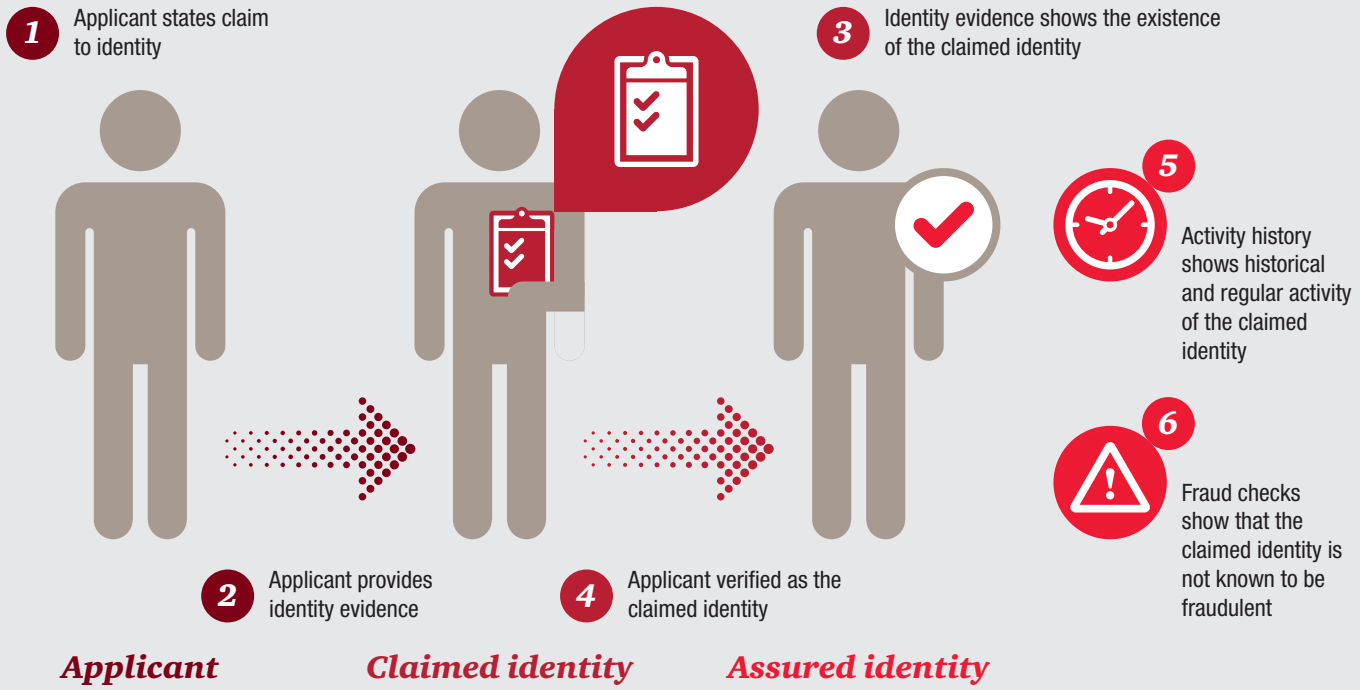
3 http://oixuk.org/?page_id=2367

4 https://e-estonia.com/

5 Regulation EU No. 910/2014

6 https://identityassurance.blog.gov.uk/2016/08/17/how-we-introduce-gov-uk-verify/

**Figure 2**




Source: Good Practice Guide No. 45 - Identity Proofing and Verification of an Individual, July 2014 Issue No: 2.3, CESG

We have completed a study to assess the extent to which GOV.UK Verify can be applied to the banking industry onboarding process. Even just in the UK we have seen a wide range of onboarding processes employed by different organisations and these organisations all obtain a variety of different data points as part of those processes. It is also apparent that the vast majority of banks collect further information for verification than is checked by GOV.UK Verify[7]. While these steps meet regulatory minimum standards for identification[8], in the UK banks approach the onboarding process with a wider lens. However, there is an important distinction to be made. Customer identification and verification is the cornerstone of a broader KYC process (this includes steps such as screening your customer to identify whether or not they are a Politically Exposed Person, for example). The onboarding process, however, includes KYC checks but also broader points such as the individual's tax residency or employment information as well as information to assist with the institution's customer profiling from a more commercial standpoint. Customer identification and verification, wider KYC, and other onboarding processes are often conflated into one broad concept.

Conflating these concepts can lead to the perception that regulatory requirements are a source of delay or friction at onboarding. It may be the case, however, that some of the information being requested from new customers, is actually not strictly required at onboarding – for example, data to help inform a future credit decision. To drive efficiencies most effectively, financial institutions must therefore determine what they want to achieve from their onboarding process. There is no one size fits all in this regard and all financial institutions should consider this as part of their business strategy.

Furthermore, the success of digital identities in Norway is often put down to the level of trust between Norwegian banks[9]. Some sources have also pointed to a strong trust in the state in Scandinavia[10] that has assisted the public and industry in taking to digital identification. If digital identities are to be rolled out in the UK and elsewhere, these are actions that will need to be emulated.

*To drive efficiencies most effectively, financial institutions must therefore determine what they want to achieve from their onboarding process.*

7 Name, Address, DoB and Gender

8 Refer Joint Money Laundering Steering Group (JMLSG) Part One, Chapter 5

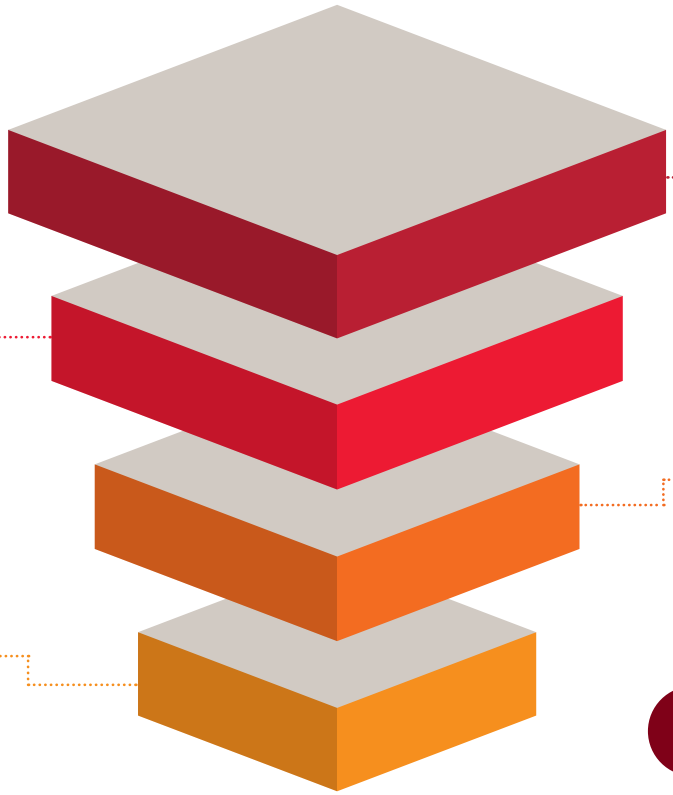
9 http://oixuk.org/?page_id=2367

10 https://www.theguardian.com/media-network/2016/jul/25/do-we-trust-digital-identification

# 2 Biometrics

*A further question raised by GOV.UK Verify is the level of assurance that is provided by any identification process. In the UK, there are considered to be 4 levels of assurance in the identification and verification process, with level 4 providing the highest level of assurance and 1 the lowest. These levels of assurance are set out in the Good Practice Guide 45 produced by by the Communications-Electronics Security Group (CESG), the UK Government's National Technical Authority on Information Assurance, and the Cabinet Office. GOV.UK Verify currently produces level 2 assurance.*

**Figure 3**



***Level 4***
This is an identity where further evidence is provided and which may be subject to additional procedures such as biometrics

***Level 3***
The same as level 2, with a higher level of proof which physically identifies the person as well as supporting the real world existence and activity of the individual.

***Level 2***
The applicant provides a claimed identity with evidence that supports its existence. Steps are taken to determine that the identity belongs to a real person.

***Level 1***
The applicant provides an identifier, however there is no requirement for the identity to be proven.

***Level of assurance provided by GOV.UK Verify***

Source: Good Practice Guide No. 45 - Identity Proofing and Verification of an Individual, July 2014 Issue No: 2.3, CESG

The challenge in the level of assurance provided by GOV.UK Verify boils down to the intrinsic issue of how you can prove who you are in a non-face-to-face scenario. The independent identity verifiers used by GOV.UK Verify perform electronic checks over individuals through use of credit agencies and other sources. Does this provide sufficient comfort as to the identity of the individual attempting to open an account? Also, what if the customer in question does not have a credit footprint?

Biometrics is an exciting field of technology that can help provide the answer. Biometrics describes the science of recognising an individual based on his or her physical or behavioural traits and as such, are widely considered to be more secure and reliable than alternative methods of identity verification. The increasing sophistication of mobile devices and the increasing use of biometric security features in Government-issued identity documents, present a significant opportunity to enhance the effectiveness and efficiency of customer identification and verification.

The human body is a catalogue of unique identifiers and biometric technology exists now to use our unique traits to verify our identity to a high level of assurance. Technology exists that can use an individual's face, iris, voice, pattern of veins in a finger or even your electro-cardiogram to identify who you are. Firms who use facial recognition technology to verify your identity, already have products in the market and indeed many banks already leverage biometric technology and are looking to expand its use across different product types and customer segments. However, the scramble to deploy these types of technologies means that divergent approaches and different biometric features are being adopted around the world.

The high level of assurance that can be provided by biometrics chimes well with emerging regulation in the form of the Payment Services Directive 2 (PSD2). PSD2 introduces the concept of Strong Customer Authentication, which means that authentication of a customer's identity must be based on 2 or more independent elements:

- **Knowledge** (something only the user knows) – this could be a password
- **Possession** (something only the user possesses) – this could be a mobile device
- **Inherence** (something the user is) – the biometric.

Biometrics is a solution to this regulation since through something that you possess - your mobile phone, and something that you are – your biometric, you can be identified. Matching this identification to a trusted government document such as a passport or drivers licence can verify your identity to a high level of assurance.

But how would this fit in with digital identities? Each customer could have a unique digital identity supported by biometric authentication. This would provide the cross-border flexibility of the digital identity with the high level of assurance provided by biometrics.

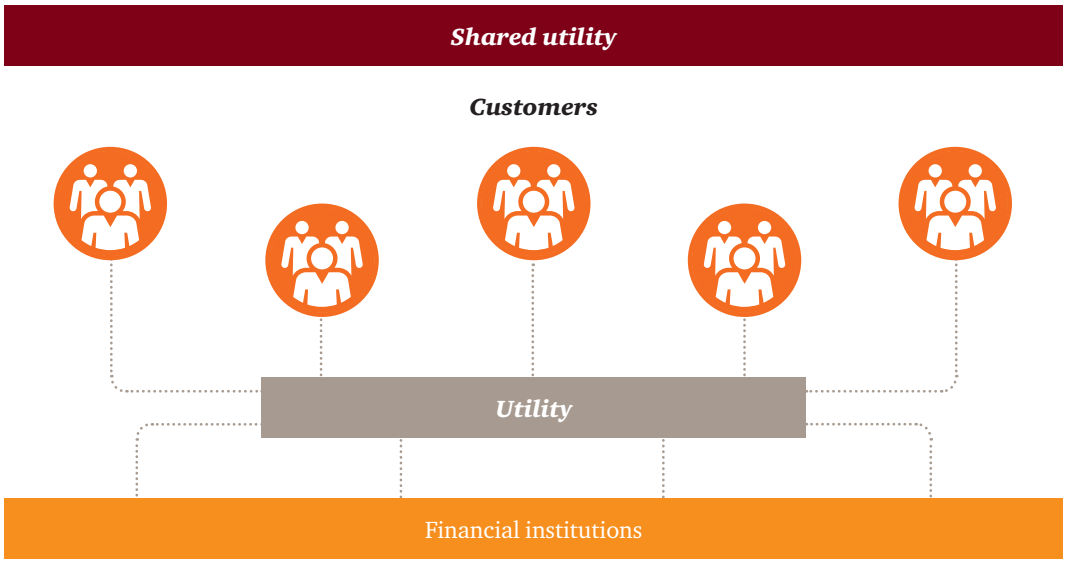
To date, many of the institutions that we have been working with have found that the biometrics offer more in terms of ongoing customer authentication, as opposed to onboarding. However, we anticipate that as the technology matures, particularly in terms of the compatibility of biometric security features, the opportunities within onboarding will open up.

There is also an interesting question over whether sanctions testing can be supplemented with biometrics. A search using your customer's biometrics over a biometrically enabled list of sanctions individuals would dramatically decrease false positives. However, it remains to be seen how many terrorists you would be able to ask for their photo or thumb print!

# 3 Utilities and Blockchain

*A further new development in the world of customer onboarding involves the use of blockchain technology to build Know Your Customer utilities. A KYC Utility provides a centralised location where customer identification and verification can be performed once for a customer, rather than several times by different organisations for the same customer. This concept is set out in Figure 4. Crucially, the adoption of KYC Utilities should lead to a much needed set of common standards for KYC.*

**Figure 4**




Source: PwC

Blockchain technology can facilitate the set-up of KYC Utilities by using the mutually distributed ledger technology to create a safe store of data that a customer can provide access to if they wish. At PwC, we have just sponsored a study, performed by Z/Yen, into the use of blockchain in the wholesale insurance market. A key use case for blockchain identified in this study is in KYC Utilities. Full details can be found in the report online, entitled 'Chain Reaction: How Blockchain Technology Might Transform Wholesale Insurance'.

# *The Purpose of Financial Institutions*

Following the global financial crisis, a large number of international banking groups developed mission statements that now included specific reference to looking after customers and the wider community. We believe that improving the customer onboarding process is a route to achieving, at least in part, these missions. But by working together the industry can create a gold standard for customer onboarding. As discussed above, we have seen this work in Norway for the use of digital identities.

The bigger picture benefit of all this is that a single standard practical approach to customer onboarding that takes advantage of these new technologies can empower the financial services industry to have a number of broader positive impacts for society. Can enhancements to KYC checks during onboarding drive changes to how and where financial services can be sold? Can this allow greater access to financial services for individuals in developing countries around the world?

Convergence towards a single industry best practice for onboarding will also set a clear goal for developing territories or those territories considered to be of higher financial crime risk. If this were to drive an increased adoption of the same or similar technologies in those territories then the gap between low and high risk territories, can be minimised. While this can help individuals from high risk territories gain access to financial services, crucially the same logic can apply to banks from high risk territories. We are aware of US correspondent banks spending the time and money to conduct site visits at their respondents in some overseas territories up to once every quarter. Furthermore, over the past few years the media has reported stories of money service providers' and charities' bank accounts being closed as they were considered too high risk. This de-risking agenda could be reversed by the smart application of technology to the customer onboarding process.

*The bigger picture benefit of all this is that a single standard practical approach to customer onboarding that takes advantage of these new technologies can empower the financial services industry to have a number of broader positive impacts for society.*

# *The Way Ahead*

**55%**

*of respondents considered that compliance spend would increase in the next 24 months*[11]

Digital identities, biometrics and KYC Utilities all offer different solutions to improve the identification and verification of new customers. It is a truism that technology is the future for financial services. However, in this case technology has arrived and the future is already here and is being deployed differently in different locations. In some developing economies the absence of significant banking infrastructure means that biometric identification is already operational as a necessity. Furthermore, many of the challenger banks now see customer identification and verification as a competitive advantage in their business model, rather than an overhead cost. If you can onboard customers more quickly and efficiently then business benefit will follow.

In terms of managing a bank's exposure to financial crime, onboarding is only one, albeit important, component. Another important objective of the onboarding process is to gather sufficient information to enable effective ongoing monitoring. From our experience of working with the more technology-enabled entrants to the financial services sector, these challenger institutions are better positioned to demand less of the static data typically gathered at onboarding and rely more on the transaction and activity data to highlight unusual behaviour. They will often have a single source of customer data, enabling profiling for business, as well as ongoing (financial crime risk) monitoring, purposes. As such there is considerable scope for minimising the perceived friction at onboarding.

PwC's Financial Services Global Economic Crime Survey identified that 55% of respondents considered that compliance spend would increase in the next 24 months[11]. However, rather than investing in incremental individual enhancements with occasional remediation projects, investing in these new approaches to onboarding as part of a consensus of international industry best practices can get right to the heart of the issue and drive real positive change for financial services.

11 PwC Financial Services Global Economic Crime Survey (http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html)

# Contacts


***David Grace***
Global Financial Crime Leader
PwC UK
+44 (0)20 7212 4881
david.w.grace@uk.pwc.com

***Sean Joyce***
US Financial Crimes Unit Leader
PwC US
+1 703 918 3528
sean.joyce@pwc.com

***Andrew Clark***
EMEA Financial Crime Leader
PwC UK
+44 (0)20 7804 5761
andrew.p.clark@uk.pwc.com

***Vincent Loy***
APAC Financial Crime Leader
PwC Singapore
+65 62367498
vincent.j.loy@sg.pwc.com

For more information about the global Financial Services marketing programme, please contact Lara De Vido on +1 646 313 3635 or lara.de.vido@us.pwc.com.

pwc.com/financialservices