KPMG

Electronic onboarding — a guide for reporting entities

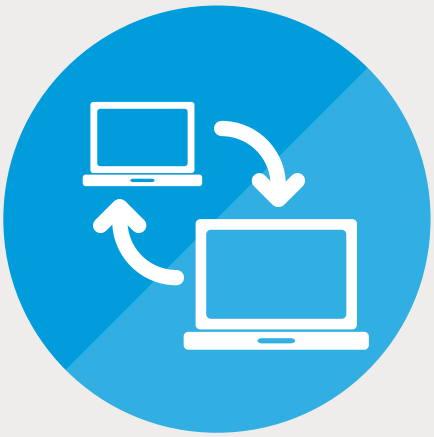
July 2016

kpmg.com/nz

So here we are… three years into the Anti-Money Laundering / Countering Financing of Terrorism (AML/CFT) regime, with reporting entities having largely navigated regulatory ambiguities and supervisory inspections. Given this, priorities are inevitably starting to change.

Now, the words 'AML compliance' are typically followed by words such as 'optimisation' and 'efficiencies'.

Electronic onboarding – a low-friction way to onboard new customers – is one such opportunity. This paper explores why electronic onboarding is becoming an increasingly hot topic; explains the New Zealand requirements; and assesses the risks. Based on our experience and observations in the market, we also highlight the key considerations when embarking on the electronic onboarding journey.



What's driving the change?

Increasingly, customers expect their financial providers to provide a digital customer experience – and they will go elsewhere unless that experience is fast and easy. Banks in particular are increasingly aware of the need to adapt, with the threat of non-bank competitors leveraging technology to disrupt traditional business models[1].

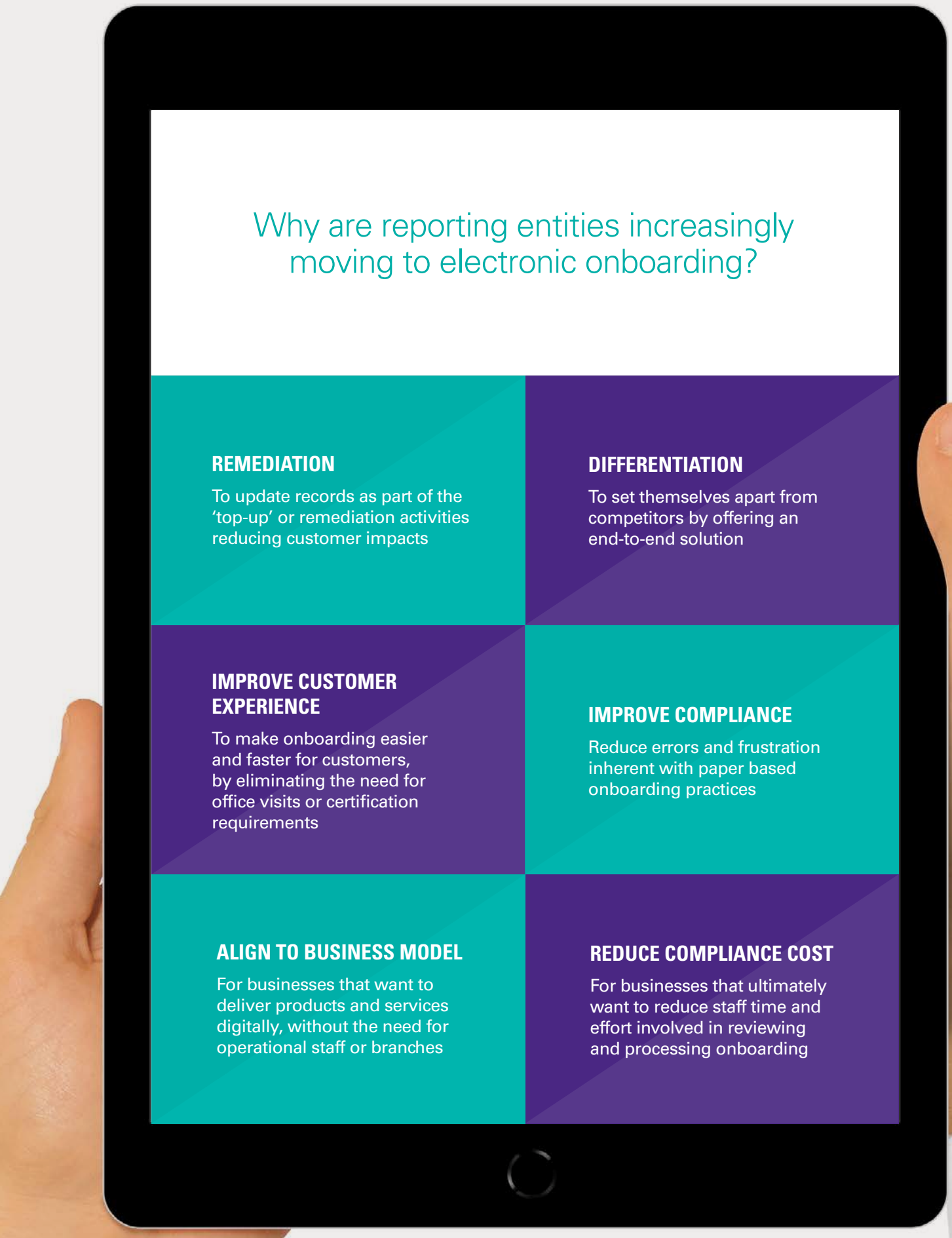
As organisations move towards digital models globally, regulators are showing more appetite to onboarding innovation; understanding that traditional paper-based models are becoming unsustainable. For example, the UK's Financial Conduct Authority and Australia's Austrac have gone on record to encourage the use of digital technologies.

The significant costs of traditional onboarding – coupled with advancements in digitisation, and the consumer's push for a convenient experience – has placed electronic onboarding squarely into the frame.

We see the following six factors as catalysts that are driving the shift to electronic onboarding...

1 For an overview of digital disruption in banking the recent RBNZ Bulletin provides useful analysis of the trends http://www.rbnz.govt.nz/news/2016/05/rbnz-bulletin-looks-at-digital-disruption-in-banking

Why are reporting entities increasingly moving to electronic onboarding?



REMEDIATION

To update records as part of the 'top-up' or remediation activities reducing customer impacts

DIFFERENTIATION

To set themselves apart from competitors by offering an end-to-end solution

IMPROVE CUSTOMER EXPERIENCE

To make onboarding easier and faster for customers, by eliminating the need for office visits or certification requirements

IMPROVE COMPLIANCE

Reduce errors and frustration inherent with paper based onboarding practices

ALIGN TO BUSINESS MODEL

For businesses that want to deliver products and services digitally, without the need for operational staff or branches

REDUCE COMPLIANCE COST

For businesses that ultimately want to reduce staff time and effort involved in reviewing and processing onboarding

The current New Zealand experience: a snapshot

Already in New Zealand, many reporting entities have or are incorporating electronic onboarding to some extent into their operations. Several New Zealand banks are moving quickly to provide an end-to-end digital solution with near real-time capability. Other reporting entities have opted to ease in more slowly, with a hybrid mix of face-to-face and electronic verification in the back-office.

Those organisations that operate on a digital-only platform and have no physical branches – such as crowd-funders or peer-to-peer lenders – use electronic onboarding in the customer-facing sense. However, they will still typically rely on manual interventions through their back-office function.

What's the relevant law?

The Amended Identity Verification Code of Practice 2013 ('the Code') is part of New Zealand's Anti-Money Laundering (AML) provisions. Organisations must comply with provisions of the Code in order to achieve 'safe harbour' status under the legislation[2].

The Code provides for two ways of verifying identity – documentary verification (i.e. manual) under Part 1 and Part 2, and electronic verification under Part 3.

2 The Code applies to the verification of 'name' and 'date of birth' particulars of identity. The Code is a best practice standard for natural persons assessed to be low or medium risk.

Part 3 of the Code

Part 3 of the Code permits reporting entities to verify the customer's name and date of birth via matching to electronic data sources.

There are two options for verifying the customer's 'name':

i) to a single independent electronic source that is able to verify an individual's identity to a high level of confidence[3]; or

ii) to at least two independent and reliable matching electronic sources

While not covered by the Code, Industry practice is that reporting entities also use 'reliable and independent' data to verify customer's address. This means verification can be completed without a face-to-face meeting with the client, or requiring them to get identity documents certified (sometimes an onerous step).

To verify identity electronically while maintaining a 'safe-harbour' status, reporting entities need to follow the direction set out in the Code; with two key steps being:

1. Determine what electronic sources they consider to be 'reliable and independent', having regard to:
   - » Accuracy;
   - » Security;
   - » Privacy;
   - » Method of collection;
   - » Linkage of customer to claimed identity;
   - » Data ownership and maintenance; and,
   - » Corroboration.
2. The reporting entity must document in their AML/CFT compliance programme the electronic verification methods they use, how they have had regard to the above matters and in what circumstances they will be used.

In our experience, many reporting entities have been light on documentation around electronic verification. Many are either not documenting their position, or might just replicate bullet points flagged by the vendor for illustrative purposes. Without appropriate thought, this may erode the effectiveness of identity verification and expose the reporting entity to regulatory sanction.

What are the risks of electronic onboarding?

As with any technology, electronic onboarding provides scope for criminal activity.

Globally, non face-to-face relationships are considered to be a factor increasing the risk of money laundering; and electronic onboarding, by its nature, reduces the need for customer interaction. The associated financial crime risks will depend on the robustness of the onboarding solution. There are significant risks where the electronic solution is vulnerable to identity being misappropriated (hence linkage is important); or counterfeit (hence robust validation is required to reliable independent sources).

Taking the example of loan fraud, counterfeit or misappropriated identity is one of the key enablers. Similarly, where false identities can be created, launderers can effectively operate as a shell company – with transactions and ownership becoming untraceable to law enforcement authorities.

The other side of the argument is that technology can better enable banks to detect errors/anomalies than their human employees. It is argued, for instance, that biometrics can more accurately assess photographs than the human eye. Technology can also assist the authentication of a document itself, or an assertion that a customer has made; by validating it to an independent source.

3 The industry views we observe is that the option to confirm 'name' to a single source able to verify identity to 'a high level of confidence' refers to DIA's igovt identity verification service operated through RealMe. The DIA website's direction on Identity Policy indicates the service verifies identities, 'to a high level of confidence'.

Key considerations

So, what are some of the key considerations on the electronic onboarding journey? Having seen the good (and not-so-good) in our audit and advisory capacity, we provide some guidance below.

Establishing the business case

An electronic onboarding solution can be costly – both in implementation and on-going matching fees.

"Therefore, to realise its value, it's important to establish a sound business case. Is it integral to your organisation's business model? Is it a key driver for your prospective customers?"

(E.g. perhaps your customer base is predominantly older and comfortable with traditional models); or your operating model suits manual onboarding for other reasons.

Defining the business requirements

It is important to determine the function your digital solution will play in the onboarding channel. Is it to support existing in-branch processes, for instance, or simply validate agency referrals? Or, at the other end of the spectrum, will it facilitate end-to-end near real time processing of 'new-to-entity' customers?

It is important to keep the complexity, cost and level of disruption proportionate to the fraud and regulatory risks. Where risks of misappropriation or counterfeit identity are higher, it is reasonable to expect the number or 'strength' of the electronic sources to increase, together with associated controls to mitigate any deficiencies.

Clear business requirements should be in place in advance of approval and vendor discussions. All relevant stakeholders should be engaged; with the business requirement sign-off involving process owners, IT, Application Development Team, and Risk & Compliance.

Remember, no solution will dispense with the need to have back-up or manual onboarding. Unsuccessful electronic matching will still require verification through traditional manual channels.

Engaging a vendor

We have seen a number of vendors in the market offering solutions to different sectors; as reflected in the capability and complexity of their offerings. A robust assessment of their proposed solution is essential, both from a business and a compliance perspective. When selecting a vendor, some of the key things to consider include:

» Sector fit and experience.

» Level of implementation and ongoing support (e.g. do you feel they take a 'we're part of the team' approach).

» Variety of data sources supported (i.e. that fit your clients demographic, with the ability to add further).

» Understanding of matching success rates and their applicability to your business. Make sure you drill down on statistics provided, as there is little point investing in a solution that fails to deliver the benefits pursued by its strategy.

» Capability to correct common data issues as part of the matching process. This helps to increase the solution's success, but needs to be tempered with impacts around match accuracy.

» Ability to support associated solution controls if required (e.g. document authentication, biometrics or comparative linking mechanism, IP limitations etc.).

» Ability to join up with Politically Exposed Person or Sanction screening, if required, to avoid system disconnects.

» Data matching speed and usability.

» Data security and privacy.

» Understanding of how matching records are retrieved for assurance and regulatory purposes.

» Ability to provide you confidence that you understand 'in the box' matching processes (in particular, the basis of any scoring mechanism).

Selecting sources

The determination of independent and reliable sources requires a balance of organisational risk appetite and the inevitable push for broad sources that increase matching success. Clearly not all sources carry the same credibility or capability to achieve high percentage matching; and vendors should be able to indicate those routinely adopted by your peers.

Selecting sources are a key decision, and it is essential to:

» Align to client demographic ensuring matching will be effective.

» Understand what data should be captured as part of the customer interaction to increase matching success.

» Ensure compliance is at the table due to the potential regulatory consequence of getting it wrong.

Establishing the link

In our opinion, there is an expectation in the Code that reporting entities consider whether their solution incorporates a mechanism to confirm the customer can be linked to the claimed identity. We see this as integral to mitigate the risk of identity misappropriation, and to combat fraud and money laundering risks.

We believe the method to 'link' should be proportionate to the risk of identify fraud. That 'mechanism' is not necessarily limited to biometrics, but could also include provision of document copies/images or associated information. For example, where the user provides something that a genuine person would reasonably be expected to know or have in their possession.

Pre and post deployment testing

Testing will depend on the complexity of the solution, and the extent of manual operation and intervention. Consideration should be given to testing matching accuracy (e.g. through positive and negative testing of input data).

For more complex solutions, it may be necessary to deploy through a pilot phase to assess user experience, effectiveness of the solution, and the interaction with back-end databases.

Document how the solution meets the Code's requirements

This will become the focal point for your auditor or sector supervisor; and your organisation should be able to talk to this in some depth. Remember, if an issue is identified through solution misuse or regulatory inspection, it is you as the reporting entity that needs to explain how you meet the requirements – not your vendor.

In summary

Electronic onboarding will increasingly become a 'must have' channel harnessing the power of digitalisation. The key to successful adoption is to clearly establish your requirements, engage the right vendor, develop a solution that is proportionate to your risks, and ensure your solution is Code-compliant. Getting it right will keep both your customers and sector supervisors happy.

Like to know more?

If you have any questions about electronic onboarding, we will be happy to assist.

Please contact any of our team below:

Stephen Bell
Partner
T: +64 9 367 5834
E: stephencbell@kpmg.co.nz

Stephen is the national lead partner for forensic services. Stephen started his career with KPMG in New York and has over 20 years of experience providing auditing, accounting, investigative, dispute resolution, arbitration, expert testimony and financial advisory services to clients in a number of industries.

Since the implementation of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009, Stephen has led numerous engagements involving banks, brokers, asset managers and casinos providing both advice on implementation of the Act, and review of risk assessments and compliance programmes required by the New Zealand AML regime.

Stephen is a Certified Public Accountant (CPA) and is Member of the board of NZ Council for CPA (Australia). He is also certified in Financial Forensics (AICPA).

Gareth Pindred
Director
T: +64 9 363 3633
E: garethpindred@kpmg.co.nz

Gareth leads KPMG's delivery of AML services. He spent seven years in the New Zealand Police before joining KPMG London in 2005 where he helped reporting entities comply with their AML/CFT obligations.

He has particular specialism in delivering remediation engagements having led projects in New Zealand, United Kingdom and several offshore jurisdictions. Gareth joined the New Zealand firm in 2013 where he has leveraged his experience to help clients bring a focused, proportionate approach to compliance.

Gareth has an LLB and is a Chartered Accountant.

Tim Goodrick
Senior Manager
T: +64 9 363 3620
E: tgoodrick@kpmg.co.nz

Tim Goodrick joined KPMG in March 2015 from the Financial Action Task Force (FATF) in Paris, France. Tim spent three years at the FATF working with industry and governments to develop international AML/CFT standards policies and assessments. Prior to the FATF, Tim was the Director of Financial Crime in the Australian Attorney-General's Department.

He has represented the FATF and Australia at international meetings of the United Nations, G20, Basel Committee and OECD. Tim also worked for AUSTRAC in compliance.

Tim has a Master of Laws and is a Certified Anti-Money Laundering Specialist (CAMS).

kpmg.com/nz