



Strategi
Compliance

*Using software to ease the pain
of Customer Due Diligence*



WHITE PAPER

EMBRACING AML/CFT DIGITISATION

ADVICE YOU CAN
PROFIT FROM

Contents

- 01 Executive summary
- 02 Introduction
- 03 The benefits of digitising Customer Due Diligence
- 04 What does the FATF think?
- 05 Complying with IVCOP
- 06 How to choose an AML/CFT digital provider
- 07 AML/CFT digital providers list
- 09 Next steps

Email daniel.relf@strategi.co.nz
if you have any questions about this whitepaper.



Executive summary

- (i) Conducting Customer Due Diligence (CDD) is regarded as a nuisance and a chore by many, including the customer. Simplifying the process through digitisation can ease the pain.
- (ii) Digital AML/CFT offerings can help reduce business costs and business risk, while also improving the client experience.
- (iii) FATF believes now is the time to consider using a digital solution, but only one that is appropriate to your business needs and is robust, reliable, and accurate.
- (iv) IVCOP caters for digital solutions, but you need to select a provider who is fully compliant with IVCOP guidelines.
- (v) A checklist is provided to help you formulate your software provider selection criteria.
- (vi) View the list of quality AML/CFT software providers.

Manual solutions for meeting CDD requirements are onerous both to the business and the client.

David Greenslade

”

Introduction

Strategi Compliance is a leading provider of AML/CFT services, having completed over 1,000 AML/CFT audits since 2013. Each year Strategi interacts with hundreds of phase one and phase two reporting entities for AML/CFT audits and training.

Our experience has shown that reporting entities fall into two distinct camps.

(i) **Those that struggle with Customer Due Diligence (CDD):**

These businesses typically have paper-based CDD processes, which are time consuming. As a result, staff find it frustrating and difficult to ask long-standing clients to prove their identity.

(ii) **Those that automate CDD:**

These businesses have used technology to undertake CDD and store client records. Meeting AML/CFT obligations is integrated into their day-to-day processes and staff time input is kept to a minimum.

If a business is caught under the [Anti-Money Laundering and Countering Financing of Terrorism Act 2009](#) (AML/CFT Act), then it must comply with that Act, with the penalties for non-compliance potentially huge. When it comes to CDD, the penalties include fines up to \$200,000 for an individual and up to \$2 million for reporting entities. Therefore, it is worthwhile getting robust CDD processes in place, while simplifying these tasks at the same time.

This paper combines the collective experience of Strategi Compliance (based on its interactions with thousands of AML/CFT reporting entities), discussions with the AML

supervisors, and the March 2020 Financial Action Task Force (FATF) guidance paper on Digital Identity, to provide the industry with a clear and informed outline of:

- The benefits of using an electronic AML/CFT provider;
- What needs to be considered when selecting a suitable provider; and
- A list of the providers currently in the New Zealand market.



The benefits of digitising CDD

The extent of the benefits gained from moving to a digital provider are determined by the solution adopted, the level of staff training provided and the overall level of digitisation within your business. However, in general terms, the benefits include:

Staff cost savings:

A digital provider may charge a fee per client or a flat annual licence fee, but in most cases, this will be far less than the cost of a staff member undertaking the work and the time taken to train and supervise this staff member. A digital solution also makes it quicker for the AML/CFT compliance officer to undertake checks.

Reduced audit costs:

Several AML/CFT digital providers have developed solutions which make it significantly faster for Strategi Compliance to complete the AML audit. This time saving translates to lower audit costs and the potential for larger sample sizes, enabling greater certainty of audit opinion.

Saving time and money:

Time is money for businesses and clients so the quicker you can transact the business, the cheaper it is. Depending on your business and the nature of your clients, the time saving per client could be anything from 10 minutes to one hour in some instances.

Improved client experience:

Clients are not subjected to having to provide copies of ID and proof of address. This enhances client relations and reduces a key 'pain point' of client onboarding.

Marketing advantage:

Currently, those reporting entities using digital CDD are in the minority so you can use 'painless CDD' as a marketing advantage. It provides a differentiator as to why a potential new client may choose your business over another.

Happier staff:

It is fair to say that most staff involved with CDD find it uncomfortable and laborious, especially when they need to ask long-standing clients for proof of identity and address. If this imposition can be easily removed, then staff can better spend their time building client relationships and solving client issues.

Improved compliance:

The single largest non-conformity issue we find when conducting AML audits relates to incorrectly conducting CDD. Selecting the right software provider can almost immediately remove this compliance issue and reduce the risk of non-compliance penalties.

Increased scalability:

If your business is growing, then often more staff are needed to service new and existing clients. Using a suitable AML digital solution will enable you to keep expanding without needing those additional staff to meet the regulatory obligations.

[AML/CFT digital providers can help reduce business costs and business risk, plus improve the client experience. Call Strategi Compliance on +64 9 414 1300 for more information.](#)

What does FATF think?

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global AML/CFT standard.

In March 2020, FATF issued a [guidance paper](#) on Digital Identity that outlines a risk-based

approach to help governments, supervisors and reporting entities use digital ID systems to comply with AML/CFT requirements. In summary, the guidance paper suggests that now is the time for reporting entities to be considering digitisation of CDD, but to take care to select a provider and digital services that are appropriate to the risks faced by the business.

The time is right for such a move, with regulatory authorities and the Financial Action Task Force now more supportive of digital solutions than they were previously.

David Greenslade

”



Complying with IVCOP

The Identity Verification Code of Practice (the code) was approved by the Ministers of Finance, Commerce, and Internal Affairs under section 64 of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act).

The IVCOP was subsequently amended to include a section (PART 3) on electronic identity verification. It states that electronic identity is a record kept in electronic form that contains authenticated core identity information about an individual. Electronic identity verification is using that record to verify an individual's identity when a reporting entity is conducting customer due diligence.

In order to conduct electronic identity verification of a customer's name and date of birth a reporting entity must;

- verify the customer's name from either:
 - (i) single independent electronic source that is able to verify an individual's identity to a high level of confidence; or
 - (ii) at least two independent and reliable matching electronic sources.
- verify the customer's date of birth from at least one reliable and independent electronic source.

Reporting entities must check the person's details against their customer records, to ensure that no other person has presented the same identity information or documents. When determining what type of electronic sources will be considered reliable and independent, reporting entities must have regard to:

- accuracy (how up-to-date is the information and what are the error rates and matching parameters);

- security;
- privacy (including whether the management and provision of the information is consistent with the Information Privacy Principles 5 to 11 in section 6 of the Privacy Act 1993);
- method of information collection;
- whether the electronic source has incorporated a mechanism to determine the customer can be linked to the claimed identity (whether biometrically or otherwise);
- whether the information is maintained by a government body or pursuant to legislation; and
- whether the information has been additionally verified from another reliable and independent source.

Reporting entities that use electronic identity verification methods must include information in their AML/CFT compliance programme that describes:

- the forms of electronic identity verification methods that are considered reliable and independent and in what circumstances they will be used for the purposes of identity verification;
- how the methods have regard to the matters described in clause 17 ([see IVCOP](#)); and
- any additional methods that will be used to supplement electronic identity verification or otherwise mitigate any deficiencies in the verification process.

Note: Nothing in the code of practice prevents a reporting entity from obtaining multisource verification from a single provider, so long as they are satisfied that the requirements in Part 3 are complied with.

How to choose an AML/CFT digital provider

There are several high-quality providers in the market, each with different services, support, and pricing on offer. One is not necessarily significantly better than the other. The key is to select a provider which can partner with your specific business to meet its current and foreseeable future, AML/CFT needs. Our checklist can help identify the right solution for you.

Checklist for selecting an AML/CFT digital provider

ITEM	TICK / CROSS
We have asked and received a satisfactory written response regarding how the provider enables compliance with IVCOP and in particular the steps set out in clauses 17 and 18 of the IVCOP (see note 1).	
We have identified the level of AML/CFT risk to the business and the level of assurance we need an IT system to provide to us.	
We have made a list of what a system MUST provide and what we would LIKE a system to provide (our needs and wants).	
Does the provider comply with our outsourcing policy?	
Does our business only have NZ clients, so that a limited sanctions list is acceptable?	
Can all CDD documents be stored electronically?	
Is access easy for the auditor?	
Is the system easy for staff to learn and use?	
How cost effective is it? (See note 2)	
Does the system conduct CDD and PEP checks?	
Does the system undertake prescribed transaction reporting?	
Are training registers provided or does the system link to Radar online AML/CFT training modules?	
Is transactional monitoring provided?	
Does the system provide the ability to store the AML/CFT programme and risk assessment?	

Note 1: Where reporting entities rely on third parties to perform elements of the CDD tasks, the ultimate responsibility for CDD remains with the reporting entity

Note 2: Cost effective does not necessarily mean cheap. The cost is relative to the effectiveness of the solution for meeting your business needs. An expensive solution may be the most cost effective if it does exactly what you want it to do and is robust, stable, dependable and easy to use.

AML/CFT digital providers list

We have undertaken market research to identify the AML/CFT digital providers listed alphabetically below. All have different features and benefits and it is a matter of selecting the provider most appropriate to where your business intends to be in coming years.

AMLHUB

AML Solutions
www.aml.co.nz

Andrew Freeman-Greene

E: andrew@amlsolutions.co.nz
T: +64 9 520 1144
M: +64 21 633575



APLY ID
www.aplyid.com

Manoj Patel

E: manoj@aplyid.com
T: 0800 555 219
M: +64 21 533712



Avid AML
www.avidaml.com

Daniel Rogers

E: daniel@avidaml.com
M: +64 21 737 535



Verifi
www.verifidentity.com

Vincent McCartney

E: sales@cloudcheck.co.nz
T: 0800 283 743
T: +64 9 953 8333



Connectworks
www.connectworks.com

Nigel Keats

E: enquire@connectworks.com
T: 0800 456 580



Dimension GRC
www.dimensiongrc.com

Jenine Colemore-Williams

E: info@dimensiongrc.io
T: 0800 863 463

AML/CFT digital providers

continued



Jade ThirdEye

www.jadethirdeye.com

Justin Mercer

E: jmercer@jadeworld.com
T: 0800 523 376



TIC

www.ticc.nz

Alice Tregunna

E: alice@ticc.nz
M: +64 22 389 6430



Vigilance

www.vigilance.co.nz

Sam MacGeorge

E: sales@vigl.biz
T: 0800 426 5238



2Shakes

www.2shakes.co.nz

Mike Kelly

E: mike@2shakes.co.nz
M: +64 21 069 9535

Our research has found there are a number of quality AML/CFT software solutions available now that can ease the pain, save time and money for the business and improve client relations.

David Greenslade

”

Next steps

Strategi Compliance is not in a position where it can, or should, recommend a specific software vendor.

However, we can:

- Arrange introductions to any of the providers listed;
- Help determine suitable selection criteria for your business; and
- Provide a generic guidance note outlining changes that would be required to AML/CFT Risk Assessments and Programmes once you have decided to proceed with a specific vendor.

Daniel Relf

Chief Executive Officer

+64 9 414 1300

daniel.relf@strategi.co.nz

Strategi is New Zealand's leading provider of independent AML/CFT services.





Strategi
Compliance

Disclaimer: While every care has been taken to supply accurate information, errors and omissions may occur. Accordingly, Strategi Limited and Strategi Institute Limited accept no responsibility for any loss caused as a result of reliance on the information supplied.

17 Corinthian Drive, Albany, Auckland 0632, PO Box 301426, Albany, Auckland 0752, New Zealand
Telephone +64 9 414 1300, Email info@strategi.co.nz | STRATEGI.CO.NZ

ADVICE YOU CAN
PROFIT FROM