Guidance: Complying with AML/CFT verification requirements during COVID-19 Alert Levels

This guidance is for reporting entities under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act) during COVID-19 Alert Levels.

While New Zealand is subject to COVID-19 Alert Levels, reporting entities will be changing the way in which they conduct their business. At COVID-19 Level 4, only those reporting entities providing essential services are able to continue to operate at their premises, and must operate in a way that limits the risk of the spread and transmission of COVID-19, with limited interactions with customers.

Undertaking activities and transactions for current customers

While the ongoing customer due diligence (CDD) and account monitoring requirements continue to apply, reporting entities should be aware of the challenges that their customers are currently facing.

The AML/CFT Act prescribes a risk-based approach to ongoing CDD and account monitoring. This means that for current customers, reporting entities have the discretion to not necessarily sight certain documents in certain circumstances, depending on the reporting entity's assessment of ML/FT risk.

The supervisors understand that, in the current situation, it may be more difficult for reporting entities to carry out ongoing CDD as per their usual processes. Instead, reporting entities should apply a risk-based approach. This may mean, for example, that reporting entities accept scanned copies of documents as an interim measure, with the originals to be sighted at a reasonable later time (upon lifting of alert levels).

New activities

It is anticipated that during the COVID-19 Alert Levels, reporting entities may still need to establish new business relationships or conduct occasional activities or transactions ('new activities') for new customers. However, we expect that the volume of new business relationships established during this period to be lower than normal. A core component of establishing new activities is verifying a person's identity.

Where a person's identity cannot be verified face-to-face because they cannot provide original identity documents, the AML/CFT Act contains various provisions:

A) Delayed verification provisions for new business relationships

The existing delayed verification provisions in sections 16(3) and 24(3) of the AML/CFT Act enable a reporting entity to establish a business relationship with a customer, but delay the verification component of CDD until later, subject to the following conditions:

1. it is essential not to interrupt normal business practice; and
2. money laundering and financing of terrorism risks are effectively managed through procedures of transaction limitations and account monitoring or (if the reporting entity is not a financial institution) through other appropriate risk management procedures; and
3. verification of identity is completed as soon as is practicable once the business relationship has been established.

This means a new business relationship with a customer could be established and funds credited into a facility, provided that verification is completed as soon as practicable after COVID-19 Alert Levels have been lifted.

Reporting entities need to consider how to effectively manage money laundering and financing of terrorism risks during this time. Supervisors expect reporting entities that are continuing to operate and establish new business relationships would implement transaction limitations, i.e. limited transfers or withdrawals until verification requirements were completed.

B) Amended Identity Verification Code of Practice 2013 (IVCOP)

The IVCOP does not restrict reporting entities to verifying a person's identity via face-to-face means only:

- Under Part 3 of IVCOP, reporting entities can offer electronic verification options. This requires no face-to-face contact with the customer.

  It is important to note that under IVCOP, additional measures, *e.g. requiring the first credit into the facility from a New Zealand registered bank in the same name as the new customer,* must be implemented where the electronic verification option does not contain a linking mechanism[1].

- Under Part 1 of IVCOP, a reporting entity must also have exception handling provisions for circumstances where a customer is unable to provide their original identity documents. With COVID Alert Levels in place, this is a time when exception handling measures would be suitable. Appropriate risk-based procedures must be adopted, this may include utilising the delayed verification provisions above if establishing a new business relationship.

It is also **important** to be aware that in this challenging environment, reporting entities should remain vigilant as criminals may try to target their products and services. Reporting entities must continue to effectively manage money laundering and financing of terrorism risks, and report suspicious activities where required to do so in accordance with the AML/CFT Act.

If any further assistance on specific scenarios is required, reporting entities should contact their AML/CFT Supervisor.

[1] The IVCOP provides that where an electronic source does not have a mechanism to link the customer to their claimed identity (whether biometrically or otherwise), a reporting entity must apply additional measures to ensure the person being dealt with online is the genuine holder of the identity they claim to be.