RESERVE BANK
OF NEW ZEALAND
TE PŪTEA MATUA

AML/CFT Supervisor Workshop:
Reserve Bank of New Zealand

12th September 2017

Te Papa Museum, Wellington, New Zealand

RESERVE BANK
OF NEW ZEALAND
TE PŪTEA MATUA

Session 1:Transaction Monitoring

1. *Link to Risk Assessment*
2. *Reviewing and closing transaction monitoring alerts or notifications*
3. *Assurance-How do you actually know?*
    - *Systems*
    - *People*

Link to Risk Assessment

- There needs to be a clear link between your Risk Assessment and AML/CFT Programme, including transaction monitoring.
- Transaction monitoring (automated or manual) is a type of control.
- Transaction monitoring scenarios/rules should align to an identified money laundering or terrorist financing risk within your Risk Assessment.
- “Off the shelf” scenarios with no consideration of your Risk Assessment may result in some risks not being appropriately mitigated.

Reviewing and closing alerts or notifications

- Clear and documented rationale for **why** the alert/notification is not considered suspicious *i.e. no reasonable grounds to suspect money laundering or financing of terrorism.*

Some points to consider:

- Why has the alert triggered or been generated?
- Where have the funds come from/where are they going to?
- What is the customer's known source of usual income?
- What has subsequently happened to the funds?
- Use of clear and unambiguous language.

- Consider contacting the customer if further clarification is required.
- Do not need to prove beyond 'reasonable doubt' that the transaction is **not** suspicious.

System Assurance-How do you actually know?

A transaction monitoring system is a key money laundering/terrorist financing control, but how do you ensure it is operating effectively?

Some points to consider:

- Are all relevant products/services and transactions feeding into the TM system? New products?
- Have transaction codes been coded correctly? *i.e. 'Cash' is not 'Cash'!*
- Accuracy of country and jurisdictional codes?
- Thresholds or percentages correct for scenarios/rules?
- Ensure changes to other systems do not adversely impact the transaction monitoring system.
- Important to maintain a good working relationship with technology partners and/or vendors to ensure on-going assurance.

People Assurance

- People who review transaction monitoring alerts or notifications are also a key money laundering/financing of terrorism control.
- Some level of assurance or oversight of closed alerts/notifications.

Some points to consider:

- Has sufficient investigation been conducted?
- Is there a clear and documented rationale for closing the alert/notification?
- Is the documented rationale easily accessible and retrievable?
- Are results communicated to senior management or relevant committee?
- Is further training required?

Session 2: Verification of source of wealth

RESERVE BANK
OF NEW ZEALAND
TE PŪTEA MATUA

Verification of source of wealth

- Whenever source of wealth is required to be obtained, verification must also be conducted.
- The extent of the verification is dependent on the level of risk.
  - Source of wealth must be obtained and verified for all customers that are trusts.
  - For a higher risk trust *e.g. a trust established in a high risk jurisdiction* the level of verification should be greater.
- Reasonable steps to be taken *i.e. the source of the source of the source is* ***not*** *expected.*

Verification for Politically Exposed Persons

- Verification may be conducted via multiple sources.
  - Reliable and independent evidence obtained directly from the PEP
  - Open or public source
  - Asset disclosure registers or similar.

- What about a self-declaration of assets or income?
  - Yes, but to what extent can you validate the contents of the declaration?

- The level of verification able to be conducted may determine whether or not a business relationship is established or continued.

- Also useful for on-going monitoring and determining suspicious activity.

Current and future RBNZ activities

- Enhancing and embedding our relationship and outcomes focused model.
- Establishing Memoranda of Understanding with other international supervisory bodies.
- Continuation of 2017 on-site schedule and planning for 2018.
- Outreach Programme.
- Prescribed Transactions Reporting.
- Guidance for Phase Two entities.
- Preparation for 2020 Mutual Evaluation of New Zealand.

Contact us

- aml/cft@rbnz.govt.nz

Electronic Verification

RESERVE BANK
OF NEW ZEALAND
TE PŪTEA MATUA

Background

- New and emerging technologies and increasing customer demand to establish business relationships with reporting entities via digital or electronic means.

- Ensure that money laundering and terrorist financing risks are still appropriately mitigated.

- Greater clarity requested in relation to the Amended Identity Verification Code of Practice 2013.

- Balancing customer convenience and business development vs. compliance and money laundering/terrorist financing risks.

What have Supervisors being doing?

- Standing agenda item at Sector Supervisors' Forum.
- Electronic Verification Workshop held.
- Discussion and presentations by reporting entities and providers.
- Reviewing approaches adopted by other jurisdictions.
- Developing high level principles.

Outcomes:

1. To obtain a consistent view of electronic verification across all AML/CFT supervisors.
2. Provide greater clarity and guidance to reporting entities.
3. Mitigate the potential money laundering and terrorist financing risks associated with the use of electronic verification.

General principles

- Electronic verification is generally considered to be where a customer's identity is verified remotely or non-face-to-face.

- Electronic verification has two key components
  1. Confirmation of identity information via an electronic source(s).
  2. Matching the person you are dealing with to the identity that they are claiming *i.e. are they the same person*?

<u>Both components must be satisfied.</u>

General principles

- High level of confidence/Single independent electronic source.
  - Only an electronic source that can verify identity to a high level of confidence can be used as a single independent electronic source. To provide a high level of confidence, the electronic source must incorporate biometric information or information which provides a level of confidence **equal** to biometric information.
- Two matching reliable and independent electronic sources
  - A reporting entity must still have regard to whether the electronic sources include a mechanism to determine if the customer can be linked to the claimed identity (whether biometrically or otherwise).
  - If the electronic sources do not contain this mechanism, additional or supplementary measures **must be used** to ensure the person that the reporting entity is dealing with is the genuine holder of the identity they are claiming to be.

General principles

- Inclusion within AML/CFT Programme
  - Reporting entities that utilise electronic verification must clearly outline in their AML/CFT Programme how all the relevant criteria within the IVCOP is satisfied. This includes any additional methods that will be used to supplement electronic identity verification or otherwise mitigate any deficiencies in the verification process.

- Existing customers and use of electronic sources?
  - Electronic sources could also be used to verify information for a customer who established a business relationship with a reporting entity prior to 30 June 2013. Requirements in the IVCOP will still apply.

Proposed next steps….

Short term

- Review and publish a revised version of the Explanatory Note for the IVCOP by the end of 2017.
- Due to the various options available to verify a person's address no further prescription or guidance is recommended.
- Likely to include examples of "other additional methods".
- Any guidance will only contain good practice or affirmative examples.

Long term

- Consider amendments to the IVCOP?