Electronic Verification (EV) Policy

- **Southern Cross Partners Limited**
- **Loan Investment Trustees Limited**
- **Southern Cross Finance Limited**
- **SCFL Properties Limited**

June 2020

Version History

Version	Date	Amendments	Changes made by
1	26/06/2020	NEW POLICY	Johanna Bloemendal
2	17/08/2020	Review and Amendments	Tim Partington

Discussed at Board meeting (date)	
Approved (Signed)	

Part 1 - Introduction and Background

1.1 Introduction

This Electronic Verification Policy is dated 26 June 2020 and relates to the following reporting Groups:

- Southern Cross Partners Limited (FSP16281)
- Loan Investment Trustees Limited
- Southern Cross Finance Limited
- SCFL Properties Limited

This Policy is to be read in conjunction with the AML/CFT Risk Assessment, AML/CFT Programme and AML/CFT Procedures. This policy is how we have assessed the businesses needs and risk associated with using Electronic Verification.

1.2 Background

The business is seeing an increased need to verify investors non face-to-face. Historically, we have attempted to meet new investors in-person either via our BDM's, visits to the office or new investors have sent the original certified documents to the office. There is a greater need to allow investors to complete verification online, for ease of use to the investor, and to make this process more efficient.
We created a stakeholder group within the Southern Cross group to review online verification options. Those options were:

- RealMe
- Cloudcheck
- ApplyID

In reviewing the above options, we determined we did not have to limit our verification processes to a single option. We will always retain the choice of using RealMe and In-person, for medium/high risk persons. A Money Laundering Risk Assessment (MLRA) takes place for each potential investor, using the PEP screening results, where the potential investor resides and if they hold an at-risk passport. If the MLRA is LOW, we will have the option of using the Electronic Verification approach
Of the options above, we chose to use ApplyID. Please see IT details in appendix 1.

In June 2020, we commenced an in-house trial of ApplyID. This involved 9 staff members/Directors testing multiple factors including:

- Ease of use
- Time to complete
- Validation of ID / Proof of address
- Reporting for AML purposes

The testing results proved conclusive. The application is very easy to use, quick and reporting was comprehensive. (note: We will issue guidance to individuals being verified to remove phone covers for ease of use in taking photos.)

Part 2 – AML/CFT Obligations

Electronic Verification	
Our specific obligations under the AML/CFT Act are	
Section 11 – Customer due diligence	A reporting entity must conduct customer due diligence on: (a) A customer (b) Any beneficial owner of a customer (c) Any person acting on behalf of a customer
Section 12 – Reliance on risk assessment when establishing level of risk	When establishing the level of risk involved for the purposes of this subpart, a reposting entity must rely on its AML/CFT programme and its risk assessment undertaken in accordance with section 58.
Section 13 – Basis for verifying identity	Verification of identity must be done on: (a) The basis of documents, data or information issued by a reliable and independent source; or (b) Any other basis applying to a specified situation, customer, product, service, business relationship or transaction prescribed by regulations.
Section 14 – Circumstances when standard customer due diligence applies	A reporting entity must conduct standard customer due diligence in the following circumstances: (a) If the reporting entity establishes a business relationship with a new customer (b) If a customer seeks to conduct an occasional transaction or activity through the reporting entity; (c) If, in relation to an existing customer, and according to the level of risk involved – (i) There has been a material change in the nature or purpose of the business relationship; and (ii) The reporting entity considers that it has insufficient information about the customer (d) Any other circumstances specified in subsection (2) or in the regulations
Section 15 – Standard customer due diligence: identity requirements	A reporting entity must obtain the following identity informati0n in relation to the persons referred ti un section 11(1); (a) The person's full name; and (b) The person's date of birth; and (c) If the person is not the customer, the person's relationship to the customer; and (d) The person's address or registered offcie; and (e) The person's company identifier or registration number; and (f) Any information prescribed by the regulations

Section 16 – Standard customer due diligence; verification of identty requirements	A reporting entity must: (a) Take reasonable steps to satisfy itself that the information obtained under section 15 is correct; and (b) According to the level of risk involved, take reasonable steps to verify any beneficial owner's identity so that the reporting entity is satisfied that it knows who the beneficial owner is; and (c) If a person is acting on behalf of the customer, according to the level of risk involved, take reasonable steps to verify the person's identity and authority to act on behalf of the customer so that the reporting entity is satisfied it knows who the person is and that the person has authority to act on behalf of the customer; and (d) Verify any other information prescribed by regulations (i) Except as provided in subsection (3), a reporting entity must carry our verification of identity before establishing a business relationship or conducting an occasional transaction or activity.
Section 50 – Obligation to keep identity and verification records	1. In respect of each case in which a reporting entity is required, under subpart 1 of this Part, to identify and verify the identity of a person, the reporting entity must keep those records that are reasonably necessary to enable the nature of the evidence used for the purposes of that identification and verification to be readily identified at any time. 2. Without limiting subsection (1), those records may comprise: (a) a copy of the evidence so used; or (b) if it is not practicable to retain that evidence, any information as is reasonably necessary to enable that evidence to be obtained. 3. A reporting entity must retain the records kept by that reporting entity for: (a) in the case of records relating to the identity and verification of the identity of a person in relation to establishing a business relationship, a period of at least 5 years after the end of that business relationship; or (b) (b) in the case of records relating to the identity and verification of the identity of a person in relation to conducting an occasional transaction or activity, a period of at least 5 years after the completion of that occasional transaction or activity

Our obligations under the Amended Identity Verification Code of Practice 2013:	
Part 1: Documentary Identity Verification	1. One form of the following primary photographic identification: (a) New Zealand passport (b) New Zealand certificate of identity issued under the Passports Act 1992 (c) New Zealand certificate of identity issued under the Immigration New Zealand Operational Manual that is published under section 25 of the Immigration Act 2009 (d) New Zealand refugee travel document issued under the Passports Act 1992 (e) emergency travel document issued under the Passports Act 1992 (f) New Zealand firearms licence (g) overseas passport or a similar document issued for the purpose of international travel which: (i) contains the name, date of birth, a photograph and the signature of the person in whose name the document is issued; and (ii) is issued by a foreign government, the United Nations or an agency of the United Nations. (h) a national identity card issued for the purpose of identification, that: (i) contains the name, date of birth and a photograph of the person in whose name the document is issued, and their signature or other biometric measure included where relevant; and (ii) is issued by a foreign government, the United Nations or an agency of the United Nations. OR 2. One form of the following primary non-photographic identification: (a) New Zealand full birth certificate (b) certificate of New Zealand citizenship issued under the Citizenship Act 1977 (c) a citizenship certificate issued by a foreign government (d) a birth certificate issued by a foreign government, the United Nations or an agency of the United Nations in combination with a secondary or supporting form of photographic identification, for example: (e) New Zealand driver licence (f) 18+ Card (g) valid and current international driving permit as defined in rule 88(1)(b) of the Land Transport (Driver Licensing) Rule 1999 and a licence from another country with a translation. (h) Points 2 (e) – (g) above are not an exhaustive list of secondary or supporting forms of photographic identification that may be acceptable. Reporting entities must ensure they are satisfied that any secondary or supporting photographic identification they accept is independent and reliable. (i) Confirmation that the identity information presented in the secondary or supporting form of photographic identification is consistent with the records held by a reliable and independent

	source (for example the information that is recorded for the purposes of the Births, Deaths, Marriages, and Relationships Registration Act 1995 or the Citizenship Act 1977 by the Department of Internal Affairs can be substituted for the primary non-photographic identification required in points 2(a)-(d). OR 3. The New Zealand driver licence and, in addition, one of the following: (a) confirmation that the information presented on the driver licence is consistent with records held in the National Register of driver licences (b) confirmation that the identity information presented on the New Zealand driver licence is consistent with the records held by a reliable and independent source (for example the information that is recorded for the purposes of the Births, Deaths, Marriages, and Relationships Registration Act 1995, the Citizenship Act 1977, or the Passports Act 1992 by the Department of Internal Affairs) (c) a document issued by a registered bank that contains the person's name and signature, for example a credit card, debit card or eftpos card (d) a bank statement issued by a registered bank to the person in the 12 months immediately preceding the date of the application (e) a document issued by a government agency that contains the person's name and signature, for example a SuperGold Card as defined in the Social Security (SuperGold Card) Regulations 2007 (f) a statement issued by a government agency to the person in the 12 months immediately preceding the date of the application, for example a statement from the Inland Revenue Department. Note: Regulation 13(3) of the Health Entitlement Cards Regulations 1993 places strict restrictions on those who can legally demand or request a community services card as a form of identification. Reporting entities may accept a community services card under point 3(e) if the customer offers it; however, they cannot request it. 4. In order to comply with this code, the reporting entity must have appropriate exception handling procedures in place, for circumstances when a customer demonstrates that they are unable to satisfy the requirements in 1 to 3 above. 5. Reporting entities must have a process in place to check that no other person with the same or similar names has presented the same identity information or documents. 6. Where documents are provided in a language that is not understood by the person carrying out the verification, an English translation must be provided. 7. In all instances where *documentary* verification is being used a reporting entity should verify the identity of the customer: (a) face to face; or by

	(b) copies of documents provided that are certified by a trusted referee (see below for certification requirements).
Part 3: Electronic Identity Verification	An 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. 15. In order to conduct electronic identity verification of a customer's name and date of birth a reporting entity must; a) verify the customer's name from either: (a) a single independent electronic source that is able to verify an individual's identity to a high level of confidence; or (b) at least two independent and reliable matching electronic sources. (c) verify the customer's date of birth from at least one reliable and independent electronic source. 16. 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. 17. When determining what type of electronic sources will be considered reliable and independent, reporting entities must have regard to: (a) accuracy (how up to date is the information and what are the error rates and matching parameters); (b) security; (c) 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); (d) method of information collection; (e) whether the electronic source has incorporated a mechanism to determine the customer can be linked to the claimed identity (whether biometrically or otherwise); (f) whether the information is maintained by a government body or pursuant to legislation; and g) whether the information has been additionally verified from another reliable and independent source. 18. Reporting entities that use electronic identity verification methods must include information in their AML/CFT compliance programme that describes: (a) 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; (b) how the methods have regard to the matters described in clause 17; and

	(c) any additional methods that will be used to supplement electronic identity verification or otherwise mitigate any deficiencies in the verification process. Note: Nothing in this 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.

AplyID Verification	AplyID process is started by sending a link to a mobile phone number. Documents that can be used for Identity Verification are: • NZ Passport • NZ Drivers Licence NZ Passport is validated using the Department of Internal Affairs, and NZ Drivers Licence is validated using NZTA. As per our AML/CFT Programme, these are the only 2 documents that can be used for Identity Verification. If any customer has a MLRA of MED or HIGH, Identity Verification will not be completed using this method. APLYiD is built on a combination of OCR and Biometric technology in conjunction with Government trusted data sources. APLYiD partners with Centrix to utilise their vast array of government trusted data sources across New Zealand. APLYiD uses Centrix Smart ID, which is a customer identification data to support businesses to fulfil their AML compliance obligations for on-boarding new customers and Ongoing Customer Due Diligence (OCDD) obligations to regularly review, and if required, revalidate existing customer information. Smart ID validates the following data elements: 1. Personal Customers (PCs): • Full Name • Date of Birth • Physical Address • Government ID document verification Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT) New Zealand legislative requirements demand robust verification of consumer information. APLYiD works in partnership with Centrix Smart ID to provision a consumer identification service that can assist businesses with identity verification compliance under the AML/CFT legislation, providing a verification service of input data, including name, date of birth and address values. APLYiD can be utilised for either on-boarding new customers or for on-going customer due diligence. At the core, APLYiD leverage a bureau database to verify name, address and date of birth data. Centrix holds trusted source data on over 3 million NZ consumers, updated monthly by banks, finance, retail energy

	and telco providers. Changes to the Credit Reporting Privacy Code have enabled this data to be used for AML/CFT verification purposes. An important aspect of the Centrix service is the focus on the **trusted source** information. We consider this to be a very important aspect of our verification service and ensures that matched data is only confirmed based on the data being confirmed by a trusted source. This limits the opportunity for fraudulent applications passing the verification threshold. Smart ID can provide confirmation of the following personal information: • Surname • First Name • Middle Name • Date of Birth • Physical Address Smart ID interrogates several trusted data sources to verify personal customer information. We consider this to be a very important aspect of our verification service and ensures that matched data is only confirmed based on data provided by a trusted source. For AML compliance we do not consider files without a trusted source verification even though we may have matching data in the bureau database. This limits the opportunity for fraudulent applications passing the verification threshold. The following gives a brief overview of **each trusted database** that will be utilised: • Bureau Databases – Centrix (credit reporting, property ownership) • Comprehensive Credit Reporting • Retail Energy Database • External Database • NZTA – New Zealand Transport Authority • Department of Internal Affairs • International Watchlist / PEP status • Bureau File – Companies Office Additional measures applied by ALPYiD: • Tampering Checks of the ID provided • Biometric face matching (matching the photo on the ID to the person presenting) • Liveness test (ensuring the person presenting is 'live')

	More information can be found in the APLYiD Compliance Pack (Attached). PEP screening using AplyID At the time of completing the identity verification, AplyID will also complete a PEP screening / Watchlist check. This can also be done separately, for customers who a MED/HIGH or at time of KYC review. AplyiD use Membercheck to perform the PEP/Watchlist screening. Membercheck uses Acuris Risk Intelligence, links below. During our testing of the PEP/Wachlist screening, we have found AplyID produces a much more thorough, comprehensive report than our previous supplier, Cloudcheck. https://membercheck.net/ https://www.acurisriskintelligence.com/ Examples of the screening positive results are attached. All results will be saved to the relevant customer file.

Report for : Edmund Hillary
Generated by : Joy Li
Reference : EHIL17082020
Transaction id : i5k0iJ8k3k9UK6iY
Completed at : 17/08/2020, 03:33pm

Overview

PASS

PEPs and Sanctions Watchlist Clear

ID Document Data

First name:	Edmund
Middle name:	Percival
Last name:	Hillary
Date of birth:	20/07/1919