ON314

AML/CFT Policy

22 April 2022

Version 1.0

Contents

Money Laundering Controls

We have a strong customer focus and take the protection of the company, its officers and employees, and that of our customers extremely seriously.
ON314 monitored all the transactions over the ON314 platform for risk-assessment and suspicious activity detection. These advanced establishments ensure that we prevent wash trading as customer identification is handled by our expert who is a well-trained specialist in doing KYC identification.
Suspicious activity can include more than just suspected money laundering attempts. For the purpose of the Policies, a "Suspicious Transaction" means a transaction or attempted transaction, which to a person acting in good faith:

- Gives rise to a reasonable ground of suspicion that it may involve proceeds of criminal or other illicit activity, regardless of the value involved;
- Appears to be made in circumstances of unusual or unjustified complexity ;
- Appears to have no economic rationale or bona fide purpose; and
- Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

When such suspicious activity is detected, the Compliance Officer will determine whether a filing with any law enforcement authority is necessary.

A summary of the Applicant's proposed money laundering controls in relation to the key money laundering requirements is set out below:

Customer due diligence at outset

'ON314' will undertake customer due diligence checks for all new customers. The Applicant has carried out a risk assessment to identify those circumstances where enhanced due diligence will be required taking into consideration:

- The jurisdiction;
- The type of service provided;
- Whether the transaction is instigated on a face to face or non-face to face basis;
- The size of the transaction;
- Whether the customer is an individual or business;
- Whether the transaction forms part of an ongoing relationship with the customer or is a single transaction;
- The type of identification presented by the customer; and
- Whether there are any other characteristics which should be taken into consideration.

Where it is identified that enhanced due diligence must be undertaken further information will be requested. Should the customer be unable to provide further details or provide information which gives rise to a suspicion the Compliance Officer in charge of overseeing Money Laundering functions will freeze the transaction and make a report to BCSTP.

Business relationship

The Money Laundering Regulations require a firm to undertake customer due diligence measures in the following circumstances:

- Where a business relationship is established;
- Where it carries out an occasional transaction amounting to S$1,000 or more;
- Where there is a suspicion of money laundering or terrorist financing; or
- Where there is doubt around the veracity of the documentation provided.

A business relationship is defined as a relationship between a firm and a customer which is expected to have some element of duration. The Applicant has determined that a business relationship will exist in the following circumstances:

- Where a unique customer number is allocated, and a customer registration form completed;
- Where a payment card is issued;
- Where customers are able to undertake transactions by telephone or over the internet.

We anticipate that a significant percentage of the transactions undertaken will be with relationship customers to which the requirements of the Money Laundering Regulations apply. We therefore intend to undertake a base level of checks for all customers regardless of whether or not they constitute a business relationship to ensure any associated risks are mitigated and compliance requirements satisfied.

Once a business relationship has been established with the customer, we will undertake full customer due diligence checks and apply enhanced due diligence procedures where we deem it necessary.

Customer due diligence requirements

All transactions in relation to payment services are expected to be predominantly on a non-face to face basis because the customer will be required to open an account before undertaking any transactions. Customers will only be able to open an account through the website or by phone. Non-face to face transactions are considered to be higher risk and additional checks will be completed before the transaction is undertaken. This will include at least one of the following:

- Requesting certified identification and proof of address;
- Verification of the customers details against an external database such as ComplyAdvantage / Worldcheck (in our case, Qgengroup)
- Telephone contact via a land line to the customer's home and verification of the personal identity information already provided;
- Sending a letter to the customer's home followed up by a telephone call; or
- Requiring that the funds be sent from an account in the customer's name.

Business customers

All business customers are deemed to have established a business relationship with the Applicant and will be subject to an appropriate level of customer due diligence checks. A business customer must provide the following information prior to undertaking any transactions:

- Full name, registered number and registered address;
- Business address;
- Nature of the business;
- Names of all directors;
- Confirmation of the names of all directors and beneficial owners;
- Written confirmation that the named individual has authority to act on behalf of the company;
- Identification and address verification documents for all of those who are authorised to act on behalf of the company;
- The turnover of the business and the number of employees;

- Length of time trading.

This information must be supported by:
- An extract from the register;
- A certificate of incorporation;
- The memorandum and articles of association; and/or
- A company structure chart.

Linked transactions

The Applicant is required to identify where a customer transacts S$1,000 or more either through a single transaction or for a series of linked transactions because this acts as a standard trigger point for the application of the enhanced customer due diligence requirements. We have determined that a series of transactions will be deemed as being linked in the following circumstances:

- Where the same sending customer has sent S$1,000 or more in the last three months to the same receiving customer in a number of individual transactions (or S$1,000 within one month);
- Where three sending customers or more are sending to the same receiving customer and the receiving customer has received more than S$1,000 in the last three months (or S$1,000 within one month);
- Where a sending customer is sending funds on behalf of more than one individual.

Our IT systems will identify the risk for a potential series of linked transactions and will produce regular reports. The Compliance Team is responsible for actioning any such report and will carry out any investigation required to determine whether or not there are any suspicious circumstances.

Source of funds

Where a customer wishes to undertake a transaction for S$1,000 or more they will also be required to provide written proof of the source of funds. Where the customer is unable to provide an acceptable source of funds the transaction will be undertaken and a report made to the BCSTP.

Sanctions check

We will scan all transactions against the BCSTP Sanctions List. Where a match is identified the transaction will be held (frozen) and a report will be made to BCSTP by the Compliance team. In addition, transactions from Senders and to beneficiaries in USD will be verified against the relevant BCSTP Foreign Asset Control list(s).

Politically exposed persons (“PEP”)

All customers will be required to indicate whether they or any member of their family has previously worked in a non-SG country at any time during the previous 12 months. Where an answer is positive, we are required to make enquiries to establish whether the customer may meet the criteria for a PEP. In cases where a PEP is identified the approval of the Compliance Team will be required, the source of funds must be established and the relationship will be subject to enhanced monitoring.

Monitoring on-going relationships

We will monitor the number and volume of transactions on a real-time basis. The management information produced will be reviewed by the Compliance Team with specific reference to the following:

- Whether the volume of transactions which are being processed for the customer is consistent with what was anticipated at the start of the relationship;
- Whether there are any sudden increases in transactions from an existing customer;
- Whether there are any uncharacteristic transactions which are not in keeping with the customer's known level of activity;
- Whether there are any peaks of activity at particular locations or at particular times;
- Whether there are any unfamiliar or untypical types of transaction or customer; and
- Whether there are any transactions matched to a PEP or against a sanctions list.

Correspondent Financial Institutions

'ON314' understands the importance of having a full understanding of the partner institutions it works with and who are involved in the end to end payment processes and will maintain a register of all Correspondent Institutions.

This will include details of all key persons/directors and the Bank will regularly cross check this to the appropriate sanctions and PEP lists.

Suspicious Transactions Reporting

The Applicant will have in place multiple systems which identify when a customer or transaction falls outside of the prescribed parameters. In addition, all staff will be trained to be vigilant and to report any suspicions to the Compliance Team. Examples of suspicious activity include, but are not limited to:

- Where the transaction is for a higher amount than would be expected based on the given employment status;
- Where the customer is sending money on behalf of a group of other people;
- Where the customer attempts to split the transaction into several smaller transactions to avoid the obligation to provide proof of the source of funds;
- Customers who do not appear to be the legitimate owners of the funds such as a student undertaking a transaction for a large amount;
- Transactions which appear to be linked to transactions processed by other customers;
- Customers who cannot provide adequate identification;
- Where the source of funds cannot be identified;
- Where their customer is not local to the business;
- Where the customer pays in used notes or smaller denominations;
- Transactions where the customer is accompanied by another individual who tells him what to do;
- Transactions which involve large numbers of high denomination notes;
- A customer whose business operates on a cash basis;
- Customers who are not native to the country they are sending the funds to; and
- Customers who process large volumes of cash transactions.

Where appropriate the Compliance Team will report the matter to relevant external bodies including the BCSTP and will be the liaison with those external agencies should the matter require further investigation.

Risk assessment

'ON314' has a comprehensive risk assessment framework which identifies those customers and scenarios which present a higher risk and therefore require a higher level of due diligence.

The framework will be kept under regular review by the Compliance Team and will be updated in response to information from a variety of sources including internal and external intelligence, management information and changes to company strategy. In addition, the risk assessment framework will be reviewed on at least a bi-annual basis.

Compliance monitoring

A number of the application procedures and transaction monitoring processes are automated and regular management information is produced for review by the Compliance Officer.

Where deficiencies are identified, these will be reported to the Executive Committee and a management action plan will be put in place to mitigate any potential risk.

Internal communication and training

Training will be provided to all members of staff at the commencement of their employment with a refresher provided at least annually thereafter. In addition, all staff will be required to undertake and pass an AML training module provided by an external supplier. The Compliance Team will maintain a training record detailing the training provided and completed for all members of staff.

On an ongoing basis, the Head Compliance Officer will make available to staff relevant materials to heighten the awareness of anti- financial crime issues.

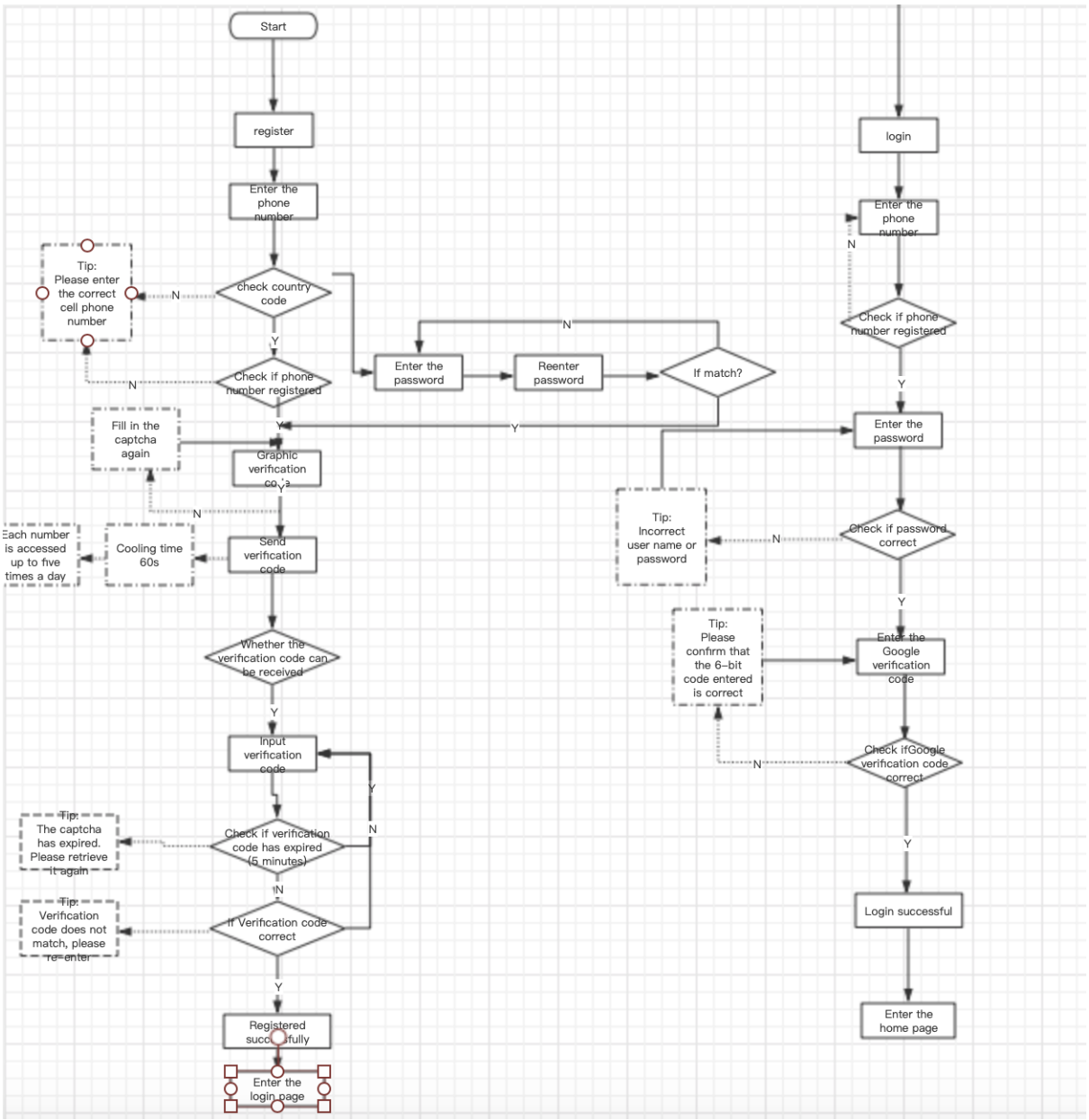
Appendix 1 Process Diagrams

E-Wallet or Customer Records (account) has been specifically built for the purpose of keeping records of activity and linking transactions and documentation under a unique identifier.

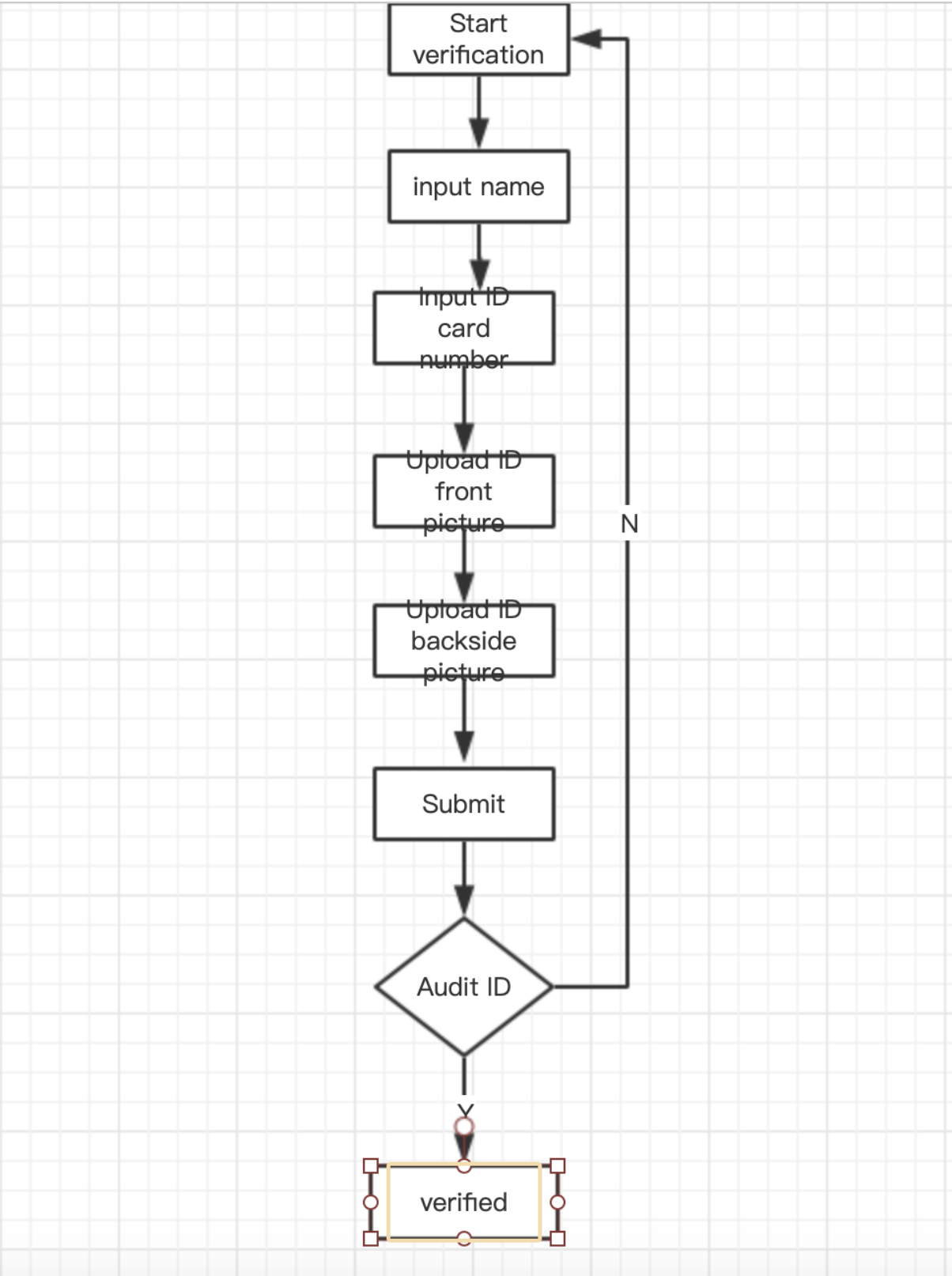
A 2-step customer registration and verification process requires customers to register and complete our Enhanced Due Diligence (EDD), which includes compliant automated identity verification, AML checks, PEP & sanction list screening (attached Qgengroup compliance report), before customer can access the services, provided by ON314 and its potential partners. Each registered account is constantly AML monitored.

After the individual registration is completed, the customer has the opportunity to upgrade the account to a business account, which requires to process a separate KYB, before the account can be upgraded.

Registration Process



Validation Process



Customer that fail the validation stages will have their details added to the Internal Watchlist to prevent fraudulent attempts where Complete Information on Payer (CIP) might be recycled during a future attempt to make a new account application after the rejection is issued. In case a customer did not receive the Email or SMS for validation, the customer can contact support.

To be able to upgrade customer account to a business account, the KYC needs to be completed first