Card Tent's KYC & AML Compliance Policy

It is the policy of Card Tent to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. With this in mind we follow the guidelines as set out in the USA Patriot Act and additional regional acts.

US Patriot Act HERE

Our AML policies, procedures and internal controls will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

We will collect certain minimum customer identification information from each customer who opens an account; utilize risk-based measures to verify the identity of each customer who opens an account; and compare customer identification information with government-provided lists of suspected terrorists, once such lists have been issued by the government

Card Tent will collect the following information for all accounts, if applicable, for any person, entity or organization that is opening a new account and whose name is on the account:

1. full legal name;
2. date of birth (for an individual);
3. an address, which will be a residential or business street address (for an individual), or a principal place of business, local office, or other physical location (for a person other than an individual); and, for an increase in transactional limits,
4. an identification number, which will be a taxpayer identification number (for U.S. persons), or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard (for non-U.S. persons).
5. a linked and validated bank account

This information will be vetted using OFAC and for the US, the local secretary of state by company state of registration. It is then passed to our banking partners who will conduct their own due diligence as a secondary check to further eliminate risk.

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our firm will not open a new account and, after considering the risks involved, consider closing any existing account. We will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. We will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).

In verifying the information, we will consider whether the identifying information that we receive (if provided), such as the customer's name, street address, zip code, telephone number, date of birth and

taxpayer identification number, to allow us to determine that we have a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).

Appropriate documents for verifying the identity of customers include the following:

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- For a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument.

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity.

We will use the following non-documentary methods of verifying identity:

- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source.

We will verify the information within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions.

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (1) not open an account; (2) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (3) close or lock an account after attempts to verify customer's identity fail.

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

- Customers – Insufficient or Suspicious Information
    - Provides unusual or suspicious identification documents that cannot be readily verified.
    - Reluctant to provide complete information about nature and purpose of business, prior banking relationships, anticipated account activity, officers and directors or business location.
    - Refuses to identify a legitimate source for funds or information is false, misleading or substantially incorrect.
    - Background is questionable or differs from expectations based on business activities.
    - Customer with no discernible reason for using the firm's service.

- Efforts to Avoid Record keeping
    - “Structures” deposits or withdrawals below a certain amount to avoid reporting or record keeping requirements.
    - Unusual concern with compliance requirements and Card Tent’s AML policies.
- Certain Funds Transfer Activities
    - Wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent business reason.
    - Many small, incoming transfers or deposits being almost immediately withdrawn or wired out in manner inconsistent with customer’s business or history.
    - Activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.

Upon detection of any red flag, or other activity that may be suspicious, Card Tent will determine whether or not and how to further investigate the matter. Card Tent will monitor transaction and identity integrity through observance by designated person(s) and utilization of automated technological processes. These processes will assist in the detection of irregularities outside determined rules for identity qualifications as well as transactional values and frequency.

Outline of AML Integration

Automated technological processes

Account Profile

- **Basic Identity**
    - Collected information processed
        - Watchlist
        - Blacklist
        - Sanction
            - Any failure results in account lockout
            - Success permits Basic Transfer and Send AML
    - Merchant: Merchant Domain, Merchant Email
        - Merchant Email must match Merchant Domain
            - Failure results in account lockout
                - Upon reactivation request, additional identification is requested
                    - Merchant license
                    - Taxpayer Identification
                    - Valid government issued photo ID
                        - Failure continues account lockout
            - Success permits Basic Transfer and Send AML

- **Standard Identity**
    - Collected information processed
        - Watchlist
        - Blacklist
        - Sanction
            - Upon failure, additional identification is requested

                - Valid government issued photo ID
                    - Failure results in account lockout Success permits Standard Transfer and Send AML
    - **Advanced Identity**
        - Collected information processed
            - Watchlist
            - Blacklist
            - Sanction
                - Upon failure, additional identification is requested
                    - Valid government issued photo ID
                        - Failure results in account lockout
                - Success permits Advanced Transfer and Send AML
- **Send AML**
    - **Basic Velocity**
        - Qualify prerequisite profile/account information
            - If prerequisites are met the following is permitted
                - Highly restricted volume of transfers (wallet to wallet)
                - Highly restricted value amounts of transfers (wallet to wallet)
                - See Transfer AML for additional restrictions
    - **Standard Velocity**
        - Qualify prerequisite profile/account information
            - If prerequisites are met the following is permitted
                - Restricted volume of transfers (wallet to wallet)
                - Restricted value amounts of transfers (wallet to wallet)
                - See Transfer AML for additional restrictions
    - **Advanced Velocity**
        - Qualify prerequisite profile/account information
            - If prerequisites are met the following is permitted
                - Relaxed volume of transfers (wallet to wallet)
                - Relaxed value amounts of transfers (wallet to wallet)
                - See Transfer AML for additional restrictions
- **Transfer AML**
    - Basic Velocity
        - Qualify prerequisite profile/account information
            - If prerequisites are met the following is permitted
                - Highly restricted volume of transfers (All outside end-points)
                - Highly restricted value amounts of transfers (All outside end-points)
                - See Send AML for additional restrictions
    - Standard Velocity
        - Qualify prerequisite profile/account information
            - If prerequisites are met the following is permitted
                - Restricted volume of transfers (All outside end-points)
                - Restricted value amounts of transfers (All outside end-points)
                - See Send AML for additional restrictions
    - Advanced Velocity
        - Qualify prerequisite profile/account information
            - If prerequisites are met the following is permitted

- Relaxed volume of transfers (All outside end-points)
- Relaxed value amounts of transfers (All outside end-points)
- See Send AML for additional restriction

For more information, please email admin@cardtent.com.