SMKG AML/ATF Policy Manual

OVERVIEW

This AML/ATF Manual (the "**Compliance Manual**") sets out the policies and procedures of Axepay Inc. (the "**Company**") for digital onboarding, underwriting and real-time AML screening and monitoring in order to detect and prevent money laundering and terrorist financing activities. The purpose is to assist the Company and its employees to comply with the most stringent anti-money laundering and anti-terrorist financing ("**AML/ATF**") requirements currently applied by first-tier regulatory jurisdictions including but not limited to the Bank Secrecy Act (BSA), the USA Patriot Act, and the Office of Foreign Assets Control (OFAC) regulations. It is also intended to act as a basis for ongoing review, development and documentation of the policies and procedures of the Company.

The Axepay Infrastructure is a fully automated payment and settlement infrastructure that processes data and sends instructions for multiple transaction payment types (B2B, B2C, C2B, B2B2C, P2P) and payment methods of the licensed financial services partners together with an ecosystem of licensed third-party financial services partners and solution providers (the Platform or Infrastructure") The Platform provides a registration onboarding/underwriting process for its Partners, Enterprise, Corporate (SME), Businesses, and Individuals, (the "Users"), digital management of the approval of documents, authentication and verifications, regulatory requirements (KYC/KYB/AML global verifications and screening), transaction screening and monitoring, reg-tech, biometrics, permission based blockchain with digital id-key access management, risk/fraud detection service and enterprise security.

Financial institutions (banks, credit, unions, trusts), money services businesses ("MSBs"), payment service providers ("PSPs") payment facilitators ("PFs"), other global licensed payment and FX providers and telecoms ("Financial Services Partners") have an important role in the Axepay Infrastructure. The Axepay Platform via its API allows access to the network of Financial Services Partners and processes the instructions of Users for financial transactions to the Financial Services Partners through the Platform. Axepay is not a Financial Services Partner and any funds transferred or payments made are completed by Axepay's Financial Services Partners.

Financial Services Partners operate in a heavily regulated financial space and hold the requisite licensing in the jurisdictions in which they operate their business. Fintechs that integrate financial transaction APIs of these regulated entities, like Axepay, need to implement procedures to comply with requirements of the Financial Services Partners and of first tier regulatory jurisdictions. Collecting and monitoring the right information is essential and fintechs that facilitate instructions on behalf of Users for financial transactions also need to embed infrastructure to manage effective Customer Due Diligence ("CDD"), Customer Identification Program ("CIP") and Enhanced Due Diligence ("EDD") programs to verify and authenticate User identities and assess the risk of Users sending instructions for financial transactions on the Platform to the Financial Services Partners.

To help in the fight against the funding of terrorism and money laundering activities, national and international Anti-Money Laundering/Anti-Terrorist Financing Laundering Laws (AML/ATF Laws)

require Axepay's Financial Services Partners to obtain, verify, and record information that identifies each person that the Financial Services Partner conducts business with including but not limited to a person who opens an account. The CDD review process includes CIP, being Know Your Customer ("KYC") and Know Your Business ("KYB") identification and verification criteria, and screening and monitoring for AML/ATF.

Axepay has built into the Platform the requisite regulatory requirements of first-tier regulatory jurisdictions including those of the Financial Services Partners. Axepay performs a first level of CDD including risk assessment and AML/ATF verification and screening in accordance with the Company's AML/ATF policies prior to submitting the User to our Financial Services Partners to complete their own CDD on Users including risk assessment and AML/ATF verification and screening in accordance with their respective AML/ATF policies and procedures. This model provides a double risk screening system review. In addition, the Company monitors all User transactions on the Platform on an ongoing real-time basis with AML/ATF screening and risk and fraud management tools independently from that of the Financial Services Partners.

This Compliance Manual represents the Company's recognition of its ongoing obligations to aspire to the highest standards of corporate governance and ethical conduct and maintain full compliance with the laws, rules, and regulations that govern the business of the Financial Services Partners. This obligation includes and it not limited to establishing and maintaining the most effective AML/ATF policies and procedures possible. To this end, the Company commits to continually update this Compliance Manual to ensure that it represents AML/ATF regulatory requirements being observed in the first-tier regulatory jurisdictions, including those of the Financial Services Partners, and to ensure that the policies and procedures set out herein are at all times supported by management and internal controls that are kept up-to-date and communicated to the employees and officers of the Company.

The primary compliance objectives of the Company will be implementing effective compliance policies and measures for combating money laundering/ terrorist financing using various measures like:

- Strict adherence to Know Your Customer ("KYC") and Verification regulatory requirements and Company policies and procedures.
- Ensuring implementation of systems for effective tracking, monitoring, and identification of unusual or suspicious transactions.
- Organizing training programs for the Company's Directors, Officers, and Employees on a continuous basis.
- Review and evaluation of AML/ATF policies and procedures at periodic intervals.
- Introducing new policies and procedures and withdrawal/modification of old policies and procedures wherever required.
- Keeping updated with changes in the Local, State, Federal, and/or International regulatory regulations.

Role of Compliance Officer

The Compliance Officer is responsible for all compliance functions and the overall administration of the Compliance Program, which includes the Anti-Money Laundering Program, the Company's day-to-day compliance with this Compliance Manual and any and all Directives in force in the jurisdictions in which Financial Services Partners, the Company's Users and the Company operates. The Compliance Officer will be instrumental in the development and conformity of the Company's compliance policies and procedures and in the development and maintenance of an ongoing compliance-training program for all directors, officers, and employees.

The Company has appointed a Compliance Officer whose primary duty is to ensure the effective implementation and enforcement of the policies and procedures set forth in this Compliance Manual. It is the Compliance Officer's responsibility to supervise all aspects of the Company's AML/ATF compliance and to further:

- The Compliance Officer is responsible for developing and implementing policies and procedures that ensure the MSB's compliance with relevant laws and regulations. These policies and procedures may cover areas such as anti-money laundering (AML) and counter-terrorist financing (CTF) compliance, customer due diligence (CDD), reporting requirements, and transaction monitoring.
- Conducting risk assessments: The Compliance Officer must conduct regular risk assessments to identify potential risks and vulnerabilities for the Company. Based on the results of the risk assessment, the Compliance Officer may recommend changes to policies, procedures, or internal controls to mitigate identified risks.
- Training employees: The Compliance Officer is responsible for providing training to employees on compliance policies, procedures, and regulations. This training may include identifying suspicious activities, reporting requirements, customer due diligence, and other relevant topics.
- Monitoring transactions: The Compliance Officer must monitor transactions to identify any suspicious activity or transactions that may indicate money laundering, terrorist financing, or other illegal activities. The Compliance Officer is responsible for reporting any suspicious activity to the relevant authorities.
- Conducting internal audits: The Compliance Officer must conduct regular internal audits to ensure that the Company is complying with relevant laws and regulations. The Compliance Officer must identify any deficiencies or weaknesses in the Company's compliance program and recommend corrective actions.
- Reporting to regulatory authorities: The Compliance Officer is responsible for filing reports with regulatory authorities as required by law. These reports may include suspicious activity reports (SARs), currency transaction reports (CTRs), or other reports required by the Financial Crimes Enforcement Network (FinCEN) or other regulatory authorities.

REG TECH

The Company has integrated a leading RegTech provider of regulatory updates that provides accurate, clean, vetted, daily regulatory data from regulators that is enriched by regulatory experts and delivered in a flexible format. This tool provides daily updates from 4000+ regulators via API. The RegTech provider uses proprietary technology to gather and structure regulatory data, which their regulatory experts further enrich.

MONEY LAUNDERING

The United Nations defines money laundering as "*any act or attempted act to disguise the source of money or assets derived from criminal activity*". Essentially, money laundering is the process whereby "dirty money" – produced through criminal activity – is transformed into "clean money", the criminal origin of which is difficult to trace.

Money Laundering is the process of concealing or disguising the existence, nature, or source of illegal funds in order to make them appear legitimate. In other words, money laundering is when a criminal attempts to transform the monetary proceeds from criminal activity into funds with an apparently legal source. Through a series of carefully arranged transactions the money launderer hopes to "wash away" all traces of the source of illegally obtained profit and make them appear legitimate. The money launder's goal is to deceive the authorities by making assets appear as if they have been obtained through legal means, with legally earned income, or to be owned by third parties who have no relationship to the true owner.

In order to successfully identify activities that could be indicative of money laundering, it is very important that employees understand how money laundering occurs. Money launderers use financial institutions and the services they offer to hide the source of criminal activity profits from law enforcement agencies. They do this by structuring their transactions in such a way to avoid the reporting requirements.

Money Laundering is not limited to cash or currency. Any type of funds can be laundered, including wire transfers, payments into or out of accounts, the receipt of bank cheques, personal cheques, money orders, traveler's checks, payments made by international drafts or stored value. Money is usually laundered through a complex series of transactions, and it typically includes three recognized stages: Placement, Layering, and Integration.

(i) **Placement,** the first stage of the money laundering process**,** involves placing the proceeds of crime in the financial system by the placement of bulk cash into the financial system without the appearance of being connected to any criminal activity. There are many ways in which cash can be placed into the financial system. Money launderers often place the money into circulation through financial institutions, such as banks, money service businesses, foreign currency exchange businesses, and casinos.

The Placement phase can involve transactions such as:

- Breaking up large amounts of cash into smaller sums and then deposit those directly into a bank account. This method is known as structuring;
- Shipping cash across borders for deposit in foreign financial institutions, or buying high-value goods, such as artwork, precious metals and stones, that can then be resold for payment by check or wire transfer;
- Using several individuals to place the illicit cash proceeds into several financial institutions in a single day. This process is known as smurfing;
- Exchanging cash for travelers' checks, food stamps, or other monetary instruments which can then be deposited into financial institutions;
- Purchasing goods and services such as a travel/vacation package, insurance policies, or jewelry. These purchases can be returned to the place of purchase in exchange for a refund check, which can then be negotiated at a financial institution or used to wire funds; and/or
- Smuggling cash out of a country and depositing that cash into a foreign financial institution.

(ii) **Layering,** the second stage of the money laundering process, involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds. At this stage the money launderer begins to move and manipulate funds to confuse their true origin as well as complicating or partially eliminating the paper trail. If the placement of funds has been undetected, money launderers' activities are more difficult to uncover. Layering may involve moving funds in various forms through multiple accounts at numerous financial institutions, both domestic and international, in a series of complex transactions. Sometimes there are many layers of activities and transactions, which make tracing funds extremely difficult.

The Layering phase can involve transactions such as:

- Transferring funds by check or monetary instrument;
- Wiring transfers of deposited cash from one account to another;
- Converting cash into monetary instruments such as traveler's checks;
- Reselling goods and monetary instruments;
- Investing in real estate and legitimate businesses, etc.;
- Exchanging monetary instruments for other monetary instruments, larger or smaller, possibly adding additional cash or other monetary instruments in the process;
- Performing wire transfers to accounts under various customer and business names at other financial institutions;
- Transferring funds outside and possibly back into the U.S. by various means such as wire transfers, particularly through "secrecy haven" countries; and/or

- Using shell banks and/or companies, which are typically registered in offshore havens.

(iii) **Integration,** the third and final stage in the money laundering process, involves placing the laundered proceeds back in the economy to create the perception of legitimacy. This stage typically follows the layering stage, however, it should be noted that integration can be accomplished simultaneously with the placement of funds. After the funds have been placed into the financial system and hidden through the layering process, the integration phase is used to create the appearance of legitimacy through additional transactions such as obtaining loans or purchasing property. These transactions provide the criminal with a plausible explanation as to where the funds came from to purchase assets as well as shield the criminal from any type of recorded connection to the illegal money. It becomes extremely difficult to distinguish legal and illegal wealth. The launderer can hide the true origin of the money by choosing to invest in real estate, buy luxury assets, enter business ventures, or any other activity that make them appear legitimate. During the integration phase, the funds are returned in a usable format to the criminal source.

The Integration phase can be achieved through various schemes such as:

- Inflating business receipts;
- Overvaluing and undervaluing invoices;
- Creating false invoices and shipping documents;
- Establishing a front company or phony charitable organization; and/or
- Using gold bullion schemes, i.e. buying gold bullion with illegal proceeds and then selling that gold bullion to retrieve the cash.

Other Methods of Money Laundering:

(i) Refining and Structuring: The exchange of small denomination bills for bills of larger denominations, usually carried out by several individuals who convert the bills at a number of different MSBs in order not to raise suspicion. The aim of refining is to decrease the bulk of large quantities of cash.

(ii) Currency Exchanges and Smurfing: Using MSBs to exchange foreign currency that can be easily transported out of the country or wired to accounts in other countries. For example, criminals could switch cash into other valuables such as trade goods, diamonds, gold bars or cheques. Large-denomination currency of one jurisdiction could also be divided into smaller sums to allow for easier transportation by couriers, with the exchange being carried out using multiple MSB locations to avoid suspicion.

(iii) Financial Institutions and Smurfing: when many inconspicuous individuals deposit cash, purchase money transfers, or buy bank drafts at various financial institutions. The cash is subsequently transferred to a central account or beneficiary. These individuals, commonly referred to as "smurfs", normally do not attract attention as they deal in funds that are below reporting thresholds and they appear to be conducting ordinary transactions.

(iv) Wire Transfers and Obscured Beneficiaries: The use of MSBs to wire funds from multiple locations to the same beneficiary in another country.

(v) Currency Smuggling: involves funds moved across borders to disguise their source and ownership and to avoid being subject to the record-keeping requirements. Funds are smuggled in various ways (such as concealing the funds in personal items or shipping containers either by mail, courier, and/or by vehicle, vessel, or aircraft) often to countries with strict bank secrecy laws.

(vi) Exchange Transactions: using proceeds of crime to buy foreign currency that can then be transferred to offshore bank accounts anywhere in the world.

(vii) Multiple invoicing of goods and services: By invoicing the same good or service more than once, a money launderer or terrorist financier is able to justify multiple payments for the same shipment of goods or delivery of services.

(viii) Over-shipments and under-shipments of goods and services: A money launderer can overstate or understate the quantity of goods being shipped or services being provided. In the extreme, an exporter may not ship any goods at all.

(ix) Falsely described goods and services: A money launder can falsely describe the goods or services being provided. For example, the launder could ship gold bars and charge them for silver bars.

(x) Gambling in Casinos: involves individuals who bring cash to casinos to buy gambling chips. After gaming and placing just a few bets, the gambler redeems the remainder of the chips and requests a casino check.

(xi) Nominees: using other people to conduct transactions on their behalf. Typically, nominees are family members, friends or associates who are trusted within the community and who will not attract attention. The use of nominees facilitates the concealment of the source and ownership of the funds involved.

(xii) Refining: Individuals change small bills into large bills. This is easily done by visiting a number of banks, casinos or money service businesses, so as not to arouse suspicion. The purpose of refining is to decrease the bulk of larger cash quantities

TERRORIST FINANCING

"The direct costs of mounting individual attacks have been low relative to the damage they can yield. However, maintaining a terrorist network, or a specific cell, to provide for recruitment, planning, and procurement between attacks represents a significant drain on resources. A significant infrastructure is required to sustain international terrorist networks and promote their goals over time. Organizations require significant funds to create and maintain an infrastructure of organizational support, to sustain an ideology of terrorism through propaganda, and to finance the ostensibly legitimate activities needed to provide a veil of legitimacy for terrorist organizations."

"Terrorists have shown adaptability and opportunism in meeting their funding requirements. Terrorist organizations raise funding from legitimate sources, including the abuse of charitable entities or legitimate businesses or self-financing by the terrorists themselves. Terrorists also derive funding from a variety of criminal activities ranging in scale and sophistication from low-level crime to organized fraud or narcotics smuggling, or from state sponsors and activities in failed states and other safe havens."

"Terrorists use a wide variety of methods to move money within and between organizations, including the financial sector, the physical movement of cash by couriers, and the movement of goods through the trade system. Charities and alternative remittance systems have also been used to disguise terrorist movement of funds. The adaptability and opportunism shown by terrorist organizations suggests that all the methods that exist to move money around the globe are to some extent at risk."
(From Financial Action Task Force, Terrorist Financing, February 29, 2008)

There are two primary sources of financing for terrorist activities:
(i) Obtaining financial support from countries, governments, organizations, or individuals;
(ii) Revenue-generating activities including criminal acts, legitimately earned income or donations to non-profit organizations involved in terrorist financing networks.

Terrorist financing provides funds for terrorist activity. The main purpose of terrorist activity is to intimidate a population or compel a government to do something. Terrorist activity is undertaken for political, religious or ideological purposes. This does not mean that an expression of political, religious or ideological beliefs alone is a terrorist activity, unless it is part of a larger conduit that meets the definition explained above. After the terrorist attacks of September 11, 2001, the United States and its allies launched a global war on terror focused on five fronts: diplomatic, financial, military, intelligence, and law enforcement. The United States and the global community quickly recognized the critical role that combating terrorist financing should play in the overall global effort against terrorism.
Terrorists need financial support to carry out terrorist activities and achieve their goals. In this respect, there is little difference between terrorists and other criminals in their use of the financial system. A successful terrorist group, much like a criminal organization, is one that is able to build and maintain an effective financial infrastructure. For this, it must develop sources of funding and means of obscuring the links between those sources and the activities the funds support. Terrorists need to find a way to make sure that funds are available and can be used to get whatever goods or services are needed to carry out terrorist acts.

Terrorist financing uses funds that are destined for a purpose rather than profits of crime. Terrorist funds are not necessarily derived through illegal methods. The fundamental aim of terrorist financing is to obtain resources to support terrorist activities. Although some of the funds are used for everyday items such as food, rent, bills, etc., the sums needed to mount terrorist attacks are not always large and the associated transactions are not necessarily complex. Because terrorist operations require relatively little money (for example, the attacks on the World Trade Center and the Pentagon are estimated to have cost approximately $500,000), terrorist financiers need to place relatively few funds into the hands of terrorist cells and their members in order to carry out their objectives. This is a significantly easier task than seeking to disguise the large amounts of proceeds generated by criminals and drug kingpins. Funds that support terrorist activity may come from illicit activity but are also generated through means such as fundraising through legal non-profit entities. In fact, a significant portion of terrorist funding comes from those who contribute to such non-profit organizations, some who know the intended purpose of their contributions and some who do not. Therefore, uncovering the root of terrorist financing can be a big challenge.

Funding Terrorism

Transnational organized crime groups have long relied on criminal proceeds to fund and expand their operations and are pioneers in using corporate structures to commingle funds to disguise their origin. It is the terrorists' use of social and religious organizations, and to a lesser extent, state sponsorship, that differentiates their funding sources from those of traditional organized criminal groups. While actual terrorist operations require only comparatively modest funding, international terrorist groups need significant amounts of money to organize, recruit, train and equip new adherents, and otherwise support their activities. Because of these larger organizational costs, terrorists often finance their terrorism efforts with a portion of the proceeds gained from traditional crimes such as kidnapping for ransom, narcotics trafficking, extortion, credit card fraud, counterfeiting and smuggling.

Like narcotics-related money launderers, terrorist groups also utilize front companies; that is, commercial enterprises that engage in legitimate enterprise, but which are also used to commingle illicit revenues with legitimate profits. Front companies are frequently established in offshore financial centers that provide anonymity, thereby insulating the beneficial owners from law enforcement. In addition to commingling the proceeds of crime, terrorist front companies also commingle donations from witting and unwitting sympathizers.

Movements of Criminal and Terrorist Funds

The methods used to move money to support terrorist activities are nearly identical to those used for moving and laundering money for general criminal purposes. In many cases, criminal organizations and terrorists employ the services of the same money professionals, accountants and lawyers, (also known as gatekeepers) to help move their funds.

In addition to the continued use of the formal financial sector, terrorists and traffickers alike employ informal methods to move their funds. One common method is smuggling cash, gems or precious metals across borders either in bulk or through the use of couriers. Likewise, both traffickers and terrorists rely on moneychangers. Moneychangers play a major role in transferring funds, especially in countries where currency or exchange rate controls exist and where cash is the traditionally accepted means of settling accounts. These systems are also commonly used by large numbers of expatriates to remit funds to families abroad. Both terrorists and traffickers have used alternative remittance systems, such as "hawala" or "hundi," and underground banking; these systems use trusted networks that move funds and settle accounts with little or no paper records. Such systems are prevalent throughout Asia and the Middle East as well as within expatriate communities in other regions.

Trade-based money laundering is used by organized crime groups and increasingly by terrorist financiers as well. This method involves the use of commodities, false invoicing, and other trade manipulation to move funds. Examples of this method include the Black Market Peso Exchange in the Western Hemisphere, the use of gold in the Middle East, and the use of precious gems in Africa. Some terrorist groups may also use Islamic banks to move funds. Islamic banks operate

within Islamic law, which prohibits the payment of interest and certain other activities. Since the mid-1970s, they have proliferated throughout Africa, Asia, the Middle East, and most recently Europe. Many of these banks are not subject to the anti-money laundering regulations and controls normally imposed on secular commercial banks. While they may voluntarily comply with banking regulations, and in particular, anti-money laundering guidelines, there is often no control mechanism to assure such compliance or the implementation of updated anti- money laundering policies.

Money Laundering and Terrorist Financing: Differences and Similarities

Most crime is committed for financial gain. However, the primary motivation for terrorism is not financial. Terrorist financing funds are used for a "purpose", to further a cause or send a message while money laundering crimes help conceal the profits of illicit activities. Money laundering crimes typically derive from criminal activity such as drug trafficking, fraud or arms smuggling. Terrorist funds are sometimes not derived through illegal means. Generally, they are used for mundane expenses such as food and rent. Hence, funds are not only for the terrorist act, themselves.

Often terrorists use legal enterprises to conduct their business. While the fundraising process may often be within legal limits, the use of charitable funds for terrorist purposes is something that is outside "traditional" money laundering scenarios. However, terrorists also covet secrecy of transactions and access to funds. Also, both terrorists and money launderers use the same methods to move their money, such as structuring payments to avoid reporting requirements, underground banking, such as the ancient system of Hawala.

The following gives a quick synopsis:

Motivation
Money Laundering: Profit
Terrorist Financing: Ideological

Funding Sources
Money Laundering: Internally from within criminal organizations
Terrorist Financing: Internally from self-funding cells (increasingly centered on criminal activity)
Externally from benefactors and fundraisers

Conduits
Money Laundering: Favors formal financial system
Terrorist Financing: Favors cash couriers or informal financial systems such as hawala and currency exchange firms

Detection Focus
Money Laundering: Suspicious transactions, such as deposits uncharacteristic of customer's wealth or the expected activity, which lead to relational links

Terrorist Financing: Suspicious relationships, such as wire transfers between seemingly unrelated parties, which lead to transactional links

Transaction Amounts
Money Laundering: Large amounts often structured to avoid reporting requirements
Terrorist Financing: Small amounts usually below reporting thresholds

Financial Activity
Money Laundering: Complex web of transactions often involving shell or front companies, bearer shares, and offshore secrecy havens
Terrorist Financing: No workable financial profile of operational terrorists exists, according to U.S. 9/11

Commission.
Money Trail
Money Laundering: Circular - money eventually ends up with person who generated it. Terrorist Financing: Linear – money generated is used to propagate terrorist group and activities.

Wilful Blindness

Wilful blindness is defined by the courts as the "deliberate avoidance of knowledge of the facts." This means that a person (employee) or entity may be convicted of money laundering if their suspicions about a transaction were raised but they nevertheless deliberately or consciously avoided knowledge of the truth, by not asking further questions. Where "red flags" or suspicions arise, they cannot be ignored.
Employees are required to notify the Compliance Department of any unusual/suspicious activity.

KNOW YOUR CUSTOMER (KYC) & CUSTOMER IDENTIFICATION PROGRAM (CIP)

The purpose of a Customer Identification Program (CIP) and Know Your Customer (KYC) procedures is to help ensure compliance with International Anti-Money Laundering and Anti-Terrorist Financing Laws and related regulations and interpretive rulings ("AML/ATF Laws"). CIP/KYC is closely associated with the fight against money laundering and terrorist activity which is why AML/ATF Laws require Financial Services Partners to take reasonable steps to ensure knowledge of their customers' normal and routine business activities. These procedures are intended to provide the necessary guidance to deter, detect, and prevent all forms of fraudulent and money laundering activity.

The objective of this policy is to attempt to ensure the immediate detection and identification of Users and/or any unusual/suspicious activity, and to prevent reputational (potential of adverse media publicity), operational (direct or indirect loss from inadequate or failed processes), and legal (lawsuits, adverse judgments, or contracts) risks. The elements included in this policy are the

following: User Acceptance procedure, User identification requirements, on- going screening, and monitoring; and risk management.
User Acceptance Policy

The Company's Platform provides data and transaction instructions to the Company's Financial Services Partners on behalf of its Users. Due diligence is required and performed on each User by the Company and by the Financial Services Partner. Each Financial Services Partner has its own Customer Acceptance Policy and CIP Program which the Financial Services Partner will undertake with respect to the User.

Before accepting any potential User and approving a User account, the Company will perform the following:

1. Verify the identity of any potential User using a risk-based approach;
2. Collect specific identifying information from each potential User;
3. If applicable, using a risk-based approach, collect specific identifying documentation from any or all potential User's ultimate beneficial owners or control persons;
4. Respond to circumstances and define actions to be taken when a potential User's identity cannot be appropriately verified with "reasonable belief";
5. Determine whether the potential User or its beneficial owners appears on any government watch lists, is a PEP, has any adverse media;
6. Obtain the purpose for opening the User account;
7. Obtain the anticipated monthly activity; and,
8. Maintain records of the information used to verify the identity of the User and, if applicable, the beneficial owners of the User.

Users that are Natural Person or Individuals

At a minimum, the following information will be collected for all individuals prior to being approved for a User account:

U.S. Individuals

- Name
- Date of birth
- Copy of a non-expired, government issued identification
- Social security number/Taxpayer identification number (U.S. Persons only)
- Physical address (P.O. Boxes are not acceptable)
- Telephone number

Non-U.S. Individuals

- The equivalent of the above information from the prospective country will be obtained for foreign persons seeking to open a User account. In addition, the User may be asked to provide a copy of his/her passport and visa if the individual resides in the United States on a temporary basis

Legal Entities
At a minimum, the following information will be collected for legal entities prior to being approved for User account:

U.S. Entities
- Legal name, including fictitious business name (DBA)
- Address
- Taxpayer identification number (TIN or EIN) if applicable
- Verification of registration of business name (Articles/Certificate of Incorporation, partnership agreement, etc.)
- Telephone number
- All information pertaining to the existence of the company must be government-issued and verifiable.

Non-U.S. Entities
- The equivalent of the above information from the perspective/originating country will be obtained for foreign persons seeking to open a User account.

User Verification-Electronic Know Your Customer (eKYC)

EKYC is a process of verifying the identity of a User electronically with non-face-to-face contact and information through a digital platform or app and involves:

- collecting User information: Collect the necessary customer information such as name, address, date of birth, and other relevant identification details.

- verifying User's identity: Use a reliable and secure method to verify the User's identity such as OTP (one-time password) verification, biometric verification, and facial recognition.
- Verifying the User's identity documents such as passport or driver's license using an electronic verification mechanism.

As the Company approves User accounts digitally, we receive copies of potential User identification by upload to the Platform and verify User identification documents, both individual and business, through an industry leading KYC/KYB ID Verification provider with global coverage. The third-party solution provider's AI powered digital identity verification technology validates identity document format and information and provides online address verification for individuals and businesses in over 230 countries and territories and provides a report on individuals and businesses with complete verification data and logs in a structured format for a thorough assessment.

Please refer to section "User Account Onboarding/Registration Procedures For Customer Due Diligence" and Schedule "A" CIP/KYC Information and Document Requirements for the detailed CDD documents and procedures required to be followed in the digital verification of a User.

Documentary Verification

As User accounts of the Company are approved digitally with non-face-to-face contact, information and corresponding documents provided by the prospective User will be verified with both documentary and non-documentary methods. Additional steps will be taken as diligence and prudence warrants. Should there be any doubt as to the identity of the person or the information provided, the User will not be approved for a User account. At a minimum, the following verification measures will be used:

Individuals.

- Passport
- State/Country Issued Driver's License or Identification Card-temporary and expired identification are not acceptable
- Armed Forces Identification Card
- Resident Alien Card

Legal Entities

- Articles/certificate of incorporation
- Articles of organization
- Fictitious business name/DBA registration
- Partnership agreement or certificate of partnership
- Registration of limited liability partnership
- Business license

Non-Documentary Verification

The following non-documentary measurements will be used:

Individuals

- Occupation
- Verification of social security number ("SSN"), if US
- Verification of address
- Verification of telephone number
- Verification of credit history through credit reporting agency, if applicable

Legal Entities:

- Verification of business address
- Verification of business telephone number
- Verification of business through credit reporting agency

Comparison of Users to Government Watch Lists

Every potential User that wishes to establish a User account with the Company will be compared to the various government watch lists, including the OFAC list, to determine if they are a match. The Company uses a third-party automated solution provider which verifies Users against a variety

of government issued lists and factors. This third-party automated solution provider is the world's most empowering AI risk technology tools with the most robust search engine, the largest database of its kind covering risk assessed, classified, unmatched global negative news coverage, PEP intelligence, and OFAC Sanctions Screening in over 240 countries and territories across the globe together with the largest daily addition of risk-relevant information plus daily monitoring of all accounts to assure quick delivery of material risk changes.

Names of potential Users that are an exact match to any entity under the Sanctions or Law Enforcement lists will not be opened.

Lack of Verification

If we are unable to determine within a reasonable belief that the identity of the User is known or the User is unable or unwilling to provide any of the requested information, the User account will not be opened. The following is a list of circumstances of when an account may not be opened:

- An individual is unable or unwilling to present an unexpired government-issued identification
- A beneficial owner of a business is unable or unwilling to present an unexpired government-issued identification
- Social security number belongs to someone else
- The Company is not familiar with the documents presented
- The Company is unable to verify the articles/certificate of incorporation
- Articles/Certificate of Incorporation are dissolved, suspended, or any status other than active
- Fictitious business name has expired
- Customer is required to file a fictitious business name but has not filed
- Customer name appears on OFAC list.

What is a Legal Entity?

Once an individual or a group of individuals decide to start a business, they must choose the organization of the business. The types of ownership explained in this section include:

- Sole Proprietorship
- Corporations
- Limited Liability Company (LLC)
- Partnerships

Sole Proprietorship

A sole proprietorship is an unincorporated business owned by one person. The owner operates the business under his or her name or a trade name. These businesses are sometimes referred to as a DBA/FBN (doing business as/fictitious business name). Technically, there is no legal distinction between the individual and the trade name. They are not separate legal entities.
Sole Proprietorships must provide the following information to open a User account:

- User Account Application-must be signed by the owner
- Non-expired and government issued identification of owner
- Social security number of owner, if applicable
- Taxpayer's identification number of business, if applicable
- Registration/license number
- Business license
- Fictitious Business Name Statement (DBA), if applicable
- Nature of business
- Services needed
- Expected volume
- Reason for international payments
- Currencies needed

Corporation

When a business decides to incorporate, the business will draw up Articles/Certificate of Incorporation describing the purpose of the business and the names of the shareholders. A corporation's Articles/Certificate of Incorporation states the purpose of the corporation and is filed by the founders of the corporation at a designated state office with the Secretary of State or the equivalent in other countries. It gives the corporation its legal existence.

A Corporation is a distinct legal entity that is separate from its shareholders. Its powers are limited to those within the scope of the powers granted to it under its Articles of Incorporation. The board of directors of a corporation, and not its shareholders, are responsible for the management of the corporation.
Corporate officers are elected and listed in the minutes of the board of directors meeting and can exercise only the authority delegated to them under the corporate charter or articles of incorporation and bylaws. They can bind the corporation only by their acts which are within the

scope of their actual or apparent authority; and they are answerable to the board of directors and must account to it.

Corporations must provide, at a minimum, the following information to open a User account:

- User Account Application must be signed by an officer or director of the company
- Taxpayer's identification number, if applicable
- Registration/license number, if applicable
- Articles of Incorporation unless they can be confirmed with the applicable Secretary of State
- Government issued identification of the signer
- Date and place of incorporation
- DBA registration if bank account is under the DBA of the business
- Name of beneficial owners owning 25% or more
- Government issued identification of beneficial owners owning 25% or more
- Name and residential address of all directors of the company and government issued ID
- Name and residential address of all officers of the company and government issued ID
- Nature of business
- Services needed
- Expected volume
- Reason for international payments
- Currencies needed

Limited Liability Company (LLC)

A domestic limited liability company generally offers liability protection similar to that of a corporation but is taxed differently. Domestic limited liability companies may be managed by one or more managers or one or more members. In addition to filing the applicable documents with the Secretary of State, an operating agreement among the members as to the affairs of the limited liability company and the conduct of its business is required.

To form an LLC, the organizers must file Articles of Organization and establish a written Operating Agreement entered into by the members of the LLC. The limited liability company does not file the operating agreement with the Secretary of State but maintains it at the office where the limited liability company's records are kept.

An LLC is a legal entity separate and distinct from its equity holders (known as "members"). Therefore, one of the advantages to an LLC is the limited liability of its members. In contrast to a limited partnership, there is no need for a "general member" who is liable for LLC obligations. The name of an LLC must end with the words "Limited Liability Company" or the abbreviation "LLC".

Limited Liability Companies must provide the following information to open a User account:

- User Account Application-must be signed by an authorized representative of the company

- Taxpayer's identification number
- Registration/license number
- Articles of organization may be required if unable to confirm the company information with the applicable Secretary of State
- Non-expired and government issued identification of the authorized representative
- Date and place of organization
- DBA registration if bank account is under the DBA of the business
- Nature of business
- Name of beneficial owners owning 25% or more
- Non-expired and government issued identification of beneficial owners owning 25% or more
- Name of all directors of the company
- Services needed
- Expected volume
- Reason for international payments
- Currencies needed

Partnership

A partnership is an unincorporated business organization in which two or more persons are associated as co-owners for the conduct of an ongoing business enterprise, and from which the partners share profits and losses. Partnerships are the most commonly used form of unincorporated business organization in which more than one individual or entity is involved. There are three types of partnerships being general, limited, and limited liability. Each one is described in the following paragraphs.

General Partnership:

All partners share in the profits and losses of the enterprise and in the management and operation of the partnership affairs. Each partner can, by his acts or conduct, bind the partnership and each is personally liable for the debts and obligations of the partnership, so that his individual assets can be subjected to execution to satisfy partnership debts when partnership assets are insufficient to pay those obligations.

Limited Partnership:

By contrast, there are one or more general partners who manage the partnership affairs and can bind the partnership, and one or more limited partners who are passive investors in the enterprise. The limited partners do not manage partnership affairs. They cannot, by their acts or conduct, bind the partnership. Limited partners are similar to shareholders in a corporation and generally do not have liability for the obligations of the limited partnership in excess of their capital contributions.

Limited Liability Partnership:

A limited liability partnership is a partnership that engages in the practice of public accountancy, the practice of law or the practice of architecture, or services related to accountancy or law. A limited liability partnership is required to maintain certain levels of insurance as required by law.

Partnerships must provide the following information to open a User account:

- User Account Application-must be signed by a partner of the company
- Taxpayer's identification number
- State of registration of partnership
- Partnership agreement may be required if unable to confirm the company information with the applicable Secretary of State
- Government issued identification of all partners
- Business license, if applicable
- Nature of business
- Name of beneficial owners owning 25% or more
- Services needed
- Expected volume
- Reason for international payments
- Currencies needed

Politically Exposed Persons (PEPs)

A politically exposed person is defined as a "senior political figure" who is a senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned corporation. In addition, a senior foreign political figure includes any corporation, business, or other entity that has been formed by, or for the benefit of, a senior foreign political figure.

The "immediate family" of a senior foreign political figure's parents, siblings, spouse, children, and in- laws are also considered to be PEPs. A "close associate" of a senior foreign political figure is a person who is widely and publicly known to maintain an unusually close relationship with the senior foreign political figure and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the senior foreign political figure. While close associates are more difficult to identify, they include individuals who due to the nature of their relationship with the PEP, are in a position to conduct significant domestic and international financial transactions on behalf of the PEP. Enhanced scrutiny of accounts and transactions involving senior foreign political figures, their families and associates is required in order to guard against laundering the proceeds of foreign corruption.

Illegal activities related to foreign corruption were brought under the definition of money laundering by Section 315 of USA Patriot Act. Abuses and corruption by political officials not only negatively impact their home country's finances, but can also undermine international government and working group efforts against money laundering. A financial institution or MSB doing business

with corrupt PEPs can be exposed to significant reputational risk, which could result in adverse financial impact through news articles, loss of customers, and even civil money penalties. Furthermore, a financial institution, its directors, officers, and employees can be exposed to criminal charges if they did know or should have known (willful blindness) that such funds stemmed from corruption or serious crimes.

An account that has a PEP as a beneficial owner must be approved by the applicable Financial Services Partner and the decision to do business with a PEP will be solely the decision of the Financial Services Partner. All User accounts, before approval, are screened for the purpose of determining if any of the beneficial owners and directors should be considered a PEP.

User Account Registration/Onboarding Process

The purpose of the KYC process is to verify the information the User has provided to the Company via the User account registration onboarding process to be a User of the Platform. All accounts must be AML compliant on the day the User account is opened.

Privately Held Company Accounts

The following verifications/reports must be performed/obtained on all private companies that apply for a Corporate User account:

- Third-party solution provider AML Report
- Ensure the owners/shareholders/directors/officers/company do not appear on any government watch lists
- Determine whether owners/shareholders/directors/officers/company are a PEP
- Ensure there is no negative media on the company
- Verify the type of address and whether it is a residence or business address
- Obtain the Articles of Incorporation if the business registration cannot be verified using the third-party solution provider KYC report
- Third-party solution provider KYC report on KYC/KYB documentation
- Risk-Rank the User

Publicly Held Company User Accounts

The following verifications/reports must be performed/obtained on all publicly owned Users registering for a Corporate account:

- Third-party solution provider AML Report
- Ensure the owners/shareholders/directors/officers/company do not appear on any government watch lists
- Determine whether owners/shareholders/directors/officers/company are a PEP
- Ensure there is no negative media on the company
- Third-party solution provider KYC report Report on verification of KYC/KYB documentation

- Verify the entity information using the ticker symbol provided
- Risk-Rank the User

Personal Accounts
The following verifications/reports must be performed/obtained on all Individual User accounts:

- Third-party solution provider AML Report
- Ensure the individual does not appear on any government watch lists
- Ensure the individual is not a PEP
- Ensure there is no negative media on the individual
- Verify the type of address and whether it is a residence or business address
- Third-party solution provider KYC report on verification of KYC/KYB documentation
- Risk-Rank the User

User Risk Ranking

In order to use the Company's Platform a User must be approved for a User account by each of the Company and the Financial Services Partner. The risk assessment of the User will be carried out when a potential User completes the User account registration process. The Company has integrated an automated state-of-the-art risk intelligence solution for its User on-boarding process-please refer to section "KYC Risk Management". In addition, as part of the User's risk assessment, the Company will take steps to "know its customers" at various times throughout the relationship with the User depending on the risk profile of the User.

The purpose of assessing User risk is to determine the level of risk a User may pose to the Company and its Financial Services Partners. The Financial Services Partners will perform their own independent User Risk Ranking on each User. It also assists in the determination of the amount of monitoring and due diligence to be performed with respect to the User. The Company will assign a risk rating of low, moderate, or high to each User account opened. Enhanced due diligence ("EDD") must be performed on all high-risk Users and high-risk Users will be flagged in the Company's Platform.

The Company's Risk Rating of a User involves the following steps:
Identify relevant risk factors: Identify the factors that are relevant to assessing the risk associated with the User. This includes things like

- risks associated with types of Users. Examples of the types of Users that may indicate a higher risk would include Politically Exposed Persons; Heads of International Organizations
- Geographic locations of the User
- User's country of origin, occupation, and transaction history
- User's type of business, business size, industry, its location, its customer base, and its transaction history
- User's credit history, payment behavior, purpose of transactions,

Define risk categories: Define risk categories or levels based on the severity of the risk and each risk category should be assigned a numerical score or rating.

Assign scores: Use a scoring model or algorithm to assign a numerical score to each User based on their data and the risk categories. The scoring model may weigh certain risk factors more heavily than others and may be adjusted over time based on the performance of previous scores.

Interpret scores: Assign a score to each User and interpret the score in the context of business and risk management objectives. This will involve setting thresholds, restrictions, or ongoing monitoring for different risk categories.

Risk Scoring: The Company assigns a numerical score to the User based on the level of risk identified during the risk assessment. The score may be based on a predetermined formula or algorithm that takes into account various risk factors, such as the User's transaction history, the country of origin, and the purpose of the transaction.

Ongoing Monitoring: The Company continues to monitor the User's transaction activity to ensure that it remains consistent with the risk score assigned. If the User's behavior changes or the level of risk increases, the Company may need to adjust the risk score and take additional measures to mitigate the risk.

Using a risk-based approach, the Company will conduct periodic risk assessments to determine where the money laundering and terrorist financing risks are greatest. The risk assessment takes into account the factors listed above and will apply the Company's risk rating methodology for its Users to assign a risk rating of "High", Moderate, or "Low" to each User.

Ongoing/Continuous User Screening and Monitoring

The Company will review, and if necessary, update User accounts on an ongoing basis. Whenever the User sends transaction instructions to a Financial Services Partner through the Platform, the User and the transaction data will be subject to screening and transaction monitoring by the Company's integrated automated state-of-the-art risk intelligence solution. Any negative responses will cancel the User's transaction instructions and the User's account will be updated accordingly.

KYC Risk Management

The Company has integrated a third-party automated state-of-the-art risk intelligence solution for its User on-boarding registration process. User identification documents, both individual and business, are verified through an industry leading KYC/KYB ID Verification provider with global coverage. The third-party solution provider's AI powered digital identity verification technology validates identity document format and information and provides online address verification for individuals and businesses in over 230 countries and territories and provides a report on individuals and businesses with complete verification data and logs in a structured format for a thorough assessment.

In addition, the Company uses a third-party automated solution provider which verifies Users against a variety of government issued lists and factors. This third-party automated solution provider is the world's most empowering AI risk technology tools with the most robust search engine, the largest database of its kind covering risk assessed, classified, unmatched global negative news coverage, PEP intelligence, and OFAC Sanctions Screening in over 240 countries and territories across the globe together with the largest daily addition of risk-relevant information plus daily monitoring of all accounts to assure quick delivery of material risk changes.

Video eKYC

The Platform has the capability built into the Platform to complete eKYC videos of individuals as required. The capabilities include live motion images to ensure the documents are captured in the live environment. Mobile phone, email, geo-tagging, biometric facial recognition, and IP is captured along with a ten (10) second video together with timestamped required CDD documents. All the documents captured are saved in our secured vault and authenticated by the support team.
With theses risk intelligence third party solution providers, the Company is able to obtain decision-ready due diligence detailed data on individuals and businesses across the globe together with intelligence in international negative news, PEPs and OFAC Sanctions screening including global financial sanctions, watch lists, politically exposed persons (PEP), global enhanced due-diligence services and news and media sources around the world. This allows the Company to identify banned or suspect entities, strengthen fraud protection, ensure regulatory compliance, and protect brand equity.

- Fosters regulatory compliance in the User account registration process and monitoring process
- Anti-Money Laundering, Know Your Customer and suspicious activity detection
- Government sanctions and PEP compliance
- Avoid headline risks

Transaction Monitoring Program

Transaction monitoring refers to the Company's ability to detect complex, suspicious, unusual transactions and unusual patterns of transactions, which have no apparent economic or lawful purpose. Any detection capability must provide meaningful outputs that can allow employees to scrutinize such occurrence to determine the appropriateness of the activity highlighted.

Appropriateness will be determined by comparing the highlighted activity to that of the User profile (KYC) to see if it makes sound rationale sense. If investigation into the appropriateness of the behavior does not provide sufficient clarity, then suspicion may be formed under relevant local suspicious reporting obligations.

The Platform monitors transactions by Client Profile and Data, including Beneficiary details, which means that each transaction instruction provided by a User is screened by the AML third- party solutions provider prior to being sent to the Financial Services Partner. The threshold and

frequency of each transaction type are screened for each transaction as well for each transaction instruction provided by a User.

Setting Limits:

- Payments limits for sending and receiving are set for Wire, ACH, Bank to Card, Card to Bank, Card to Card by each Financial Services Partner
- Payment partners, Rails and MSB's follow these instructions and set the limit on sending and receiving FX basis on the guidelines of each country regulator
- The limits may be based on the guidelines of each country regulator or self-imposed by the Financial Services Partner

Setting Restrictions:

- Each Financial Services Partner and payment type has region specific restrictions.
- These may include maximum and minimum transactions restrictions, restrictions on industry type, restrictions of acceptable currencies, frequency of transactions, and restrictions on the mode of payments.
- The restrictions may be based on the guidelines of each country regulator or self-imposed by the Financial Services Partner

The Platform monitors transaction instructions for:

- the transaction limit and frequencies set in the system as mandated by the Financial Services Partners and the frequency of the transactions following the compliance and protocol of each Country.
- the limits set by our Financial Services Partner Sponsors and Card Issuers.
- transactions which are recurring and the amount of these recurring transactions. A limit is set for each transaction beyond which there is a notification shared with the User.
- transactions which are beyond the threshold limit are flagged for additional documentation. Once the additional documents as defined by regions or countries are approved, the transaction instruction will be released to the Financial Services Partners. In the event the additional documentation is not provided in a stipulated time frame, the transaction instruction will be canceled.
- multiple address usage by same Corporate/Individual for transactions
- multiple Corporate/Individuals using same address for transactions
- multiple card usage by same Corporate/Individual for a transaction

User Profile and Recordkeeping

The Platform is end-to-end automated payment and settlement infrastructure including a fully integrated customer relationship management (CRM) system. The Platform provides the Company with the ability to create and maintain a clear view of Users including User CDD identification documentation, AML compliance and verification results both for the User and for the User's transactions, transaction details, transaction monitoring, Recipient details, any correspondence with the User and a complete history of records.

This is to ensure that:

(i) the audit trail for the account, the transaction instructions, and the transaction details transmitted to Financial Services Partners through the use of the Company's Platform that relate to any User and, where appropriate, the beneficial owner of the User, is clear and complete;
(ii) any User and, where appropriate, the beneficial owner of the User, can be properly identified and verified;
(iii) all User and transaction instruction and detail information are available on a timely basis; and
(iv) there are complete records of User risk assessment and suspicious transactions.

Retention Periods for Digital Documents

The Company maintains the digital documents of Active Accounts for a period of ten (10) years from date of the User Account being issued. The digital documents of non-active accounts that have the status of Suspended Account are maintained for a period of five (5) years from the date of the User account becoming a Suspended Account.

Risk Assessment Program Overview

The standards for AML prevention and detection recognize that money laundering is a risk that needs to be managed taking a proportionate approach. The Company has designed a risk assessment program that weighs a number of factors including regulatory, products/services, internal and external factors, customer type, industry, and geographic locations.
Risk assessment is a systematic process for identifying and evaluating events such as possible risks and opportunities that could affect the achievement of objectives, positively or negatively. Such events can be identified in the external environment (e.g., economic trends, regulatory landscape, and competition) and within an organization's internal environment (e.g., people, process, and infrastructure).

BSA/AML Compliance Risk Assessment

Given today's difficult regulatory environment, complex account monitoring requirements and demand for specialized expertise, the Company has established a goal of maintaining AML compliance program with "strong" monitoring processes. The Company is dedicated to achieving this goal and continuously monitors the various risks which could directly impact the quality of the Company's compliance program.
The development of the AML risk assessment involves three steps:

1. Identifying the specific risk categories unique to the Company;
2. Conducting a detailed analysis of all available data to assess the level of risk within each high risk category; and
3. Determining whether the BSA/AML compliance program is commensurate to the Company's risk profile and provides the necessary controls to mitigate the highest risks identified.

A Company's AML program must be commensurate with the risks posed by the location and size of the Company, its Financial Services Partners and by the nature and volume of the financial services the Financial Services Partners offer through the platform. The Company should identify and assess the money laundering and terrorist financing risks that may be associated with our unique combination of Financial Services Partners, products, services, Users and geographic locations and decide how to manage them. Since, a risk-based approach is one of the most effective ways to protect against money laundering and terrorist financing designing a risk-based system requires an assessment of our Users, products/services, and the geographical locations in which the Company and its Financial Services Partners operate and determine the risk they pose to us.

The BSA/AML risk assessment will help to mitigate the risks associated with the products and services we offer as well as the Users that use them. In addition, it will assist Company in recognizing and evaluating our compliance risks and the effectiveness of the controls in place to mitigate those risks. Lastly, it will ensure that the Company focuses its resources on the areas of our business that we believe pose the greatest risks. The risk assessment will be reviewed/ updated at on a regular basis or upon material risk changes.

OFAC Risk Assessment

The Company will conduct an OFAC Risk Assessment at least annually to best understand the residual risk and corresponding controls in place to control sanctions risk.

Country Risk Assessment

The purpose of assessing a country's risk is to determine the risk a country may pose based on anti-money laundering controls they may or may not have in place. The Company has developed a risk ranking process using public data as well as a subjectivity score for internal purposes and has incorporated country risk scores from a variety of different sources.

Industry Risk Ranking

The Company recognizes that some industries pose a higher risk than others. Most of these businesses conduct legitimate business; however, some aspects of these businesses may be susceptible to money laundering and/or terrorist financing. Each NAICS code is assigned to new Users and the NAICS code determines if it is a high or low risk industry based on the following categories:

- Terrorist type activities
- Cash Intensive
- Designated as High Risk by Regulators
- Layering/Integration Risk
- Internal Policy Restrictions

Cash Intensive Businesses

Cash intensive businesses and entities cover various industry sectors. These businesses are often utilized by money launderers to legitimize their illicit proceeds. It affords them the opportunity to move large amounts of funds embedded within a large number of similar transactions. These businesses are attractive to money launderers and/or terrorist financiers because they offer:

- Financial services that are less regulated which create more opportunities to conduct certain transactions without the hassle of the traditional bank;
- High ticket items that can be brought with little or no identification and later sold; and
- The ability to bring in high volume of cash allowing legitimate funds to be commingled with "dirty money".

Example: A criminal may own a cash-intensive business, such as a foreign currency dealer, and use it to launder currency from illicit criminal activities. The foreign currency sales do not, on the surface, appear unusual since the business is legitimately a cash-generating entity. However, the volume of foreign currency used to launder money will most likely be higher in comparison with similar foreign exchange businesses. The nature of cash-intensive businesses and the difficulty in identifying unusual activity may cause those businesses to be considered a high risk.

The following is a list of businesses which are deemed to pose a higher risk:

- Non-traditional financial entities, such as currency exchange houses, money transmitters, and check cashing facilities
- Casinos and card clubs
- Offshore corporations and banks located in tax and/or secrecy havens
- Leather goods stores
- Car, boat, and plane dealerships
- Used automobile or truck dealers and machine parts manufacturers
- Travel agencies
- Brokers/dealers
- Sellers of antiques, art, and furs
- Jewel, gem, and precious metal dealers
- Import/export companies
- Auctioneers
- Deposit brokers
- Pawn brokers
- Convenience stores
- Restaurants
- Night clubs
- Car washes
- Retail stores
- Parking garages, etc.

User Risk

The purpose of assessing User risk is to determine the level of risk a User may pose and the amount of monitoring and due diligence to be performed. The Company will assign a risk rating of Low, Moderate, or High to each User account opened on the Platform. Enhanced due diligence must be performed on all High-Risk Users.

Users are risk ranked during the User account registration process initially through the Company's User account onboarding procedures together with the information obtained by the third-party solution providers and the Company's Customer Risk Assessment tool to determine whether enhanced due diligence should be performed on the User. In addition, the Company performs transaction screening and monitoring on every transaction instruction sent by the User to the Financial Services Partners as well as requiring OTP verification. The Company may perform a mass-risk ranking on existing Users on a periodic basis to determine if the current risk rating is sufficient or should be updated.
Please refer to section "User Risk Ranking".

Enhanced Due Diligence (EDD)

If the risk assessment indicates a high level of risk, the Company will conduct enhanced due diligence ("EDD") measures. EDD is a more extensive and rigorous form of due diligence that is typically used for higher-risk customers or transactions and are designed to provide a more thorough assessment of the potential risks associated with a particular User or transaction. By conducting a more detailed analysis of the User's identity, background, and financial activities, the Company can better identify and mitigate any potential risks associated with doing business with that User and can implement an effective activity monitoring system.

The specific procedures used by the Company for EDD will depend on the circumstances and includes:

- completing an enhanced identity verification by obtaining additional information about the User's financial history and conducting a thorough background check on the customer, including any relevant public records, media reports, or other sources of information
- Additional 3rd party reports such as LexisNexis, DNBi, etc., if applicable
- conducting a telephone video conference
- enhanced documentation by reviewing additional documentation to verify the User's identity, such as passports, business licenses, tax returns
- confirming source of funds by identifying the source of the User's wealth and conducting an analysis of the legitimacy of the funds
- enhanced transaction monitoring by monitoring the User's transactions more closely by implementing additional automated alerts for the User and for unusual activity, including large transactions or transactions that are inconsistent with the User's known patterns of behavior
- conducting enhanced screening of Users who are classified as politically exposed persons (PEPs) to assess any potential risks associated with their political connections or influence
- Identification from beneficial owner(s) owing less than 25% of the business may be required
- full AML due diligence of the beneficial owners owing less than 25 % of the business

CHOOSING THE RIGHT FINANCIAL SERVICES PARTNER FOR A PARTNER CLIENT:

As a modern financial technology infrastructure supporting multiple payment options for global and local payments and provider of third-party solution ancillary services, we assess the needs of Users such as Partners and Corporates and their respective business flows. We then identify the specific Financial Services Partner for the Partners and Corporates, as the case may be, depending on the country and/or corridors of the Partner's/Corporate's operations and the type, method, timing, and cost of the payments. This simplifies the role of each Financial Services Partner and provides efficient and cost-effective transactions for Users.

USER ACCOUNT ONBOARDING/REGISTRATION PROCEDURES FOR CUSTOMER DUE DILIGENCE

Overview

Axepay employs industry best practices in our AML/ATF Program, including KYB/KYC. We have established standards for knowing who our Users are and the nature of the business that they are transacting with our Financial Services Partners. We have integrated with KYC and AML/ATF third-party solution providers that cover more than 230+ countries and territories for CDD review. The KYC/AML/ATF third-party solution providers verify and authenticate the User's CDD Documentation and provide screening and continuous monitoring of the global compliance watch list through fully automated, and comprehensive data collection for PEPs, Global Watch Lists / Sanctions, and Adverse Media together with a state-of-the-art, AI-driven system that examines specific criteria to deliver the most sophisticated name-matching that captures all critical and crucial data points.

Axepay performs CDD on potential Users through the User account registration process prior to a User being forwarded to the Finanical Services Partner for their independent CDD review and approval. CDD, including KYC/AML/ATF, is undertaken by Axepay once the potential User finishes the User account registration and uploads all required CDD Documentation. The User's identity and the User's CDD Documentation is verified, authenticated, and screened by AML/ATF third-party solution providers that are integrated with the Axepay Platform. Once approved by Axepay Admin, the CDD Documentation for the User is forwarded to the Financial Services Partner for their independent CDD review and approval.
In addition, after approval of a User by Axepay Admin and the Financial Services Partner, the AML/ATF third-party solution providers undertake continuous AML/ATF monitoring on Users including PEP, Global Watch Lists, Sanctions and Adverse Media. Users' transactions are continuously monitored on a 24x7 basis commencing with the financial transaction request on the Platform including AML/ATF screening, threshold dollar value limits, and frequency of payments to Recipients. Recipient's details are also screened and monitored by the AML/ATF third-party solution providers including Recipient's name, address, country, amounts, PEP, Global Watch Lists, Sanctions and Adverse Media.

DEFINITIONS:

Axepay Admin: Axepay or the Company and the infrastructure of the Platform.

Axepay Portal: the online User account registration process and Platform accessible via the Company's website.

Business: Businesses are B2B legal entities involved in a supply chain. May include individuals who are a legal entity, such as a sole proprietor or individual LLC. A Business is a Recipient, not a User, and does not have a User account on the Platform. A Business may only receive payments from a User account of a Partner, Corporate, or Individual. A Business needs to successfully complete the onboarding registration process for a User account in order to be a Corporate in the Platform.
Corporate(s): SME that are legal entities, including a Business, that has been approved for a User account in accordance with the onboarding registration process. May include individuals who are a legal entity, such as a sole proprietor or individual LLC.

Directors: Individuals that are a member of the Board of Directors of a company and are considered the governing body of the company. Directors are responsible for supervising the activities of the company and for making decisions regarding those activities.

Financial Services Partners: Financial institutions (banks, credit, unions, trusts), money services businesses ("MSBs"), payment service providers ("PSPs"), payment facilitators ("PFs"), other global licensed payment and FX providers and telecoms that provide any of the financial services via the Platform including but not limited to FX, funds transfer, payments, collections, payment processing.

Individuals: Natural persons that have been approved for a User account in accordance with the onboarding registration process.

Officers: Individuals that are responsible for the day-to-day operations of a company.

Partners: Large Enterprise organizations that have a network of Corporates and Individuals that need to be serviced for global cross-border and local payment services. They may require payment services locally in a specific Country or Countries, cross-border in specific corridor(s), and/or cross-border global payments generally. The Partner, and the Corporates and the Individuals of the Partner, all undertake the onboarding registration process to be approved by each of Axepay and the Financial Services Partner.

Beneficiary: Business or Individual that receives payments from a User account of a Partner, Corporate, or an Individual. A Beneficiary is required to be created and will be identified by specific data such as name, address, country, and payout location such as bank account routing data codes, bank address, card details.

Third-Party Solution Providers: We have partnered with KYB/KYC third-party solution providers for identity authentication and verification services including online identity, document, and

address verifications; and AML/ATF third-party solution providers for AML/ATF screening and monitoring of Global Watch Lists, Sanctions, PEPs, and Adverse Media. These third-party solution providers utilize automated and comprehensive data collection that captures all critical and crucial data points together with an AI-driven system that examines specific criteria to deliver the most sophisticated name-matching.

Ultimate Beneficial Owners: Individuals that own twenty-five percent (25%) or more of a legal entity, directly or indirectly.

Users: Partners, Corporates, Individuals that have completed the User account registration process, have been approved by each of Axepay Admin and the Financial Services Partner and have been issued a User account to use the Axepay Platform.

USER ACCOUNT REGISTRATION/ONBOARDING PROCESS AND CDD

To comply with AML/ATF Laws effective CDD needs to be implemented in the first stage of any business relationship which is onboarding a new customer that will become a User. Effective CDD involves knowing a User's identity, their financial activities and the risk they pose. KYC and AML/ATF procedures assist to establish a User's identity, understand the nature of the User's activities, satisfy the requirement that the source of the User's funds is legitimate and assess money laundering risks associated with the User. These procedures are a critical function to assess User risk and to prevent and identify money laundering, terrorism financing, other illegal corruption schemes and to limit fraud.

The following are key elements of Customer Due Diligence ("CDD"):

- Customer Identification Program (data collection, global identity verification and authentication, PEP, Global Watch Lists, Sanctions and Adverse Media
- Electronic Know Your Customer or eKYC is a process where the User's identity and address are verified electronically through authentication
- Verifying a User's identity through documents, including a national government issued ID document with a document reader and advanced document verification software;
- Risk assessment and management
- Ongoing monitoring and record-keeping of User documents and transactions
  The Axepay Platform provides a User account registration process for Partners, Corporates, and Individuals ("Users"). Potential Users are required to complete the online registration and upload the CDD information and documentation (the "CDD Documentation) in order that the Company may properly identify, verify, and review the potential User in accordance with AML/ATF Laws. The potential User will undergo CDD review and is required to be approved by each of Axepay Admin and independently by the Financial Services Partners prior to a User account being opened on the Axepay Platform. The CDD requirements of Financial Services Partners are included and built into the Platform.

The CDD process occurs at multiple levels on the Platform:

a. Level one CDD is completed by Axepay Admin on the Partner and each of the Corporates and the Individuals of the Partner.

b. Level two CDD occurs when a Financial Services Partner is assigned to the Partner and the CDD Documentation for the Partner is provided to the Financial Services Partner for independent review and approval.

c. Level three CDD occurs when each of the Corporates and the Individuals of the Partner are assigned to the same Financial Services Partner as the Partner and the CDD documentation for each of the Corporates and the Individuals are provided to the Financial Services Partner for independent review and approval.

d. Level four CDD occurs when a Recipient is created by the Partner, Corporate, or Individual. The information requirements of a Recipient will depend on the recipient type, country, and currency. The Recipient's details are also screened and monitored including name, address, country, amounts, and are subject to AML/ATF review including PEP, Global Watch Lists, Sanctions and Adverse Media.

GENERAL PROTOCOLS FOR ONBOARDING OF AXEPAY USER ACCOUNTS AND CDD

1. Identity and Document Verification:
   CDD Documentation for identity verification is sent via API to the third-party solution providers for identity and document verification to ensure the Partner, Corporate, or Individual is who they say they are and the CDD Documentation provided is authentic. A manual review may also be necessary, and the status of the registration will be identified as "Pending Account Registration Review" in the Platform.

2. The initial protocol for all Account Types is for Admin to authenticate the email and mobile number for the contact person of the potential User (Partner, Corporate, Individual) prior to providing login credentials to the Platform to complete the User account registration. The authentication of the Account Type is initially completed for the contact person who is an authorized signatory (the "Contact") of the potential User for security and fraud prevention purposes. Mobile phone and Email Verification: We do both mobile phone and email verification through OTP.

3. Businesses and Individuals are not permitted to register directly on the Axepay Platform and may only complete the User account registration when they receive an invite and a unique identifier key from an Approved Partner.

4. The CDD Documentation required for a User Account for a Partner, Corporate and Individual is set out in Schedule "A" which is subject to change depending on regulatory requirements or requirements of the Financial Services Partner.

5. All Beneficiaries created by a User are vetted on the platform for security reasons and must submit following documents as a proof for vetting process for smooth transactional flow:
    - Beneficiaries that are Individuals must provide government issued photo ID and address proof.
    - Beneficiaries that are Businesses must provide their business registrations government documents and the owners government issued photo ID and address proof.

6. All government issued documentation submitted for CDD purposes, including Passport, National ID, Driver's License, US SNN must have an expiry date exceeding six (6) months from date of submission of document. All other CDD Documentation submitted for User account registration purposes including bank account statements, utility bills must be recent and dated within three (3) months of date of submission.

7. All supporting documentation submitted and approved for User account registration purposes ("Approved Document") are tracked by expiry date. The Platform will flag an Approved Document one hundred and twenty days (120) days prior to the expiry date and notify Axepay Admin that the Approved Document needs to be updated with a Renewed Document. The User will be notified and requested to submit a Renewed Document within a stipulated time period. If the User does not comply with the request and submit a Renewed Document prior to the stipulated time period, the User's account will be deactivated and become a Suspended Account.

8. Document Renewal: The renewed document must be uploaded to the Platform and approved by each of Axepay Admin and the Financial Services Partner prior to the expiry date to be considered an Approved Document.

9. Suspended Account: Failure to upload the renewed document in the Platform and obtain approval by each of Axepay Admin and the Financial Services Partner in the required time-period will immediately result in the Active Account status being changed to Suspended Account. The Suspended Account status will not change to Active Account status until such time as a renewed document is uploaded to the Platform and approved by each of Axepay Admin and the Financial Services Partner.

10. User account registrations for all Account Types undergo CDD review by each of Axepay Admin and the Financial Services Partner. Upon approval of the User by the Financial Services Partner, the User is independently onboarded to each of Axepay and the Financial Services Partner. A User account is issued to the User including login credentials and a key to access the Axepay Platform to send instructions to the Financial Services Partner for financial transaction purposes.

11. User account registration on-boarding requirements, including requisite documents, for Account Types by Country, comply with Country jurisdiction requirements and are mandated by Financial Services Partners. With respect to certain jurisdictions, for example China, the Account Registration requirements also include submission of contractual documents representing the payment request, invoices, receipts, tracking information for

the delivery logistics, and bill of lading.

12. User account registration requirements including CDD Documentation are provided for reference purposes only, are not a finite list, and are subject to change at any time. Pending Account Registration Review may also result in additional document/information requests.

13. Inactive accounts: Users accounts with zero activity for a period of twelve (12) months, will receive a notification to the verified and authenticated email associated with the User account. This notification is sent every three (3) months to verify the User's response. In the event there is no response from the User subsequent to the second email, the User account will be deactivated and have the status of Suspended Account

14. The Company maintains the digital documents of Active Accounts for a period of ten (10) years from date of User Account being issued. The digital documents of non-active accounts that have the status of Suspended Account are maintained for a period of five (5) years from the date of the User account becoming a Suspended Account.

15. Video eKYC: The Platform has the capability built into the Platform to complete eKYC videos of individuals as required. The capabilities include live motion images to ensure the documents are captured in the live environment. Mobile phone, email, geo-tagging. Biometric facial recognition, and IP is captured along with a ten second video together with timestamped required CDD documents verification. All the documents captured are saved in our secured vault and authenticated by the support team. The video ekyc will occur during the User account registration process for CDD. Please refer to the section, "VIDEO EKYC PROCEDURES".

USER ACCOUNT REGISTRATION/ONBOARDING PROCEDURES

Financial Services Partners complete their own independent CDD review and approval process prior to onboarding the potential User and only Users approved by the Financial Services Partner will be issued a User account by Axepay Admin.

Please see Schedule" B" for Overview Diagram Flow for CDD and Continuous Screening and Monitoring.

1. PARTNER REGISTRATION (Enterprise)

1.1 Partner makes a request to receive the initial login credentials to complete the User account registration by completing a request with the required information on the Axepay Portal.

1.2 Upon manual review and a telephone conference with the Partner, Axepay Admin will approve or decline the request of the potential Partner to access the User account registration process.

1.3 If Axepay Admin approves the request for User Account Registration, the authorized representative of the Partner receives login credentials, via email, for access to User account registration. Partner completes the User account registration process and submits the required CDD Documentation for the legal entity type of the Partner.

1.4 Axepay Admin completes initial CDD Document review with the assistance of the Third- Party Solutions Providers by request to have the requisite CDD identity documents verified and authenticated and have the requisite searches undertaken to determine if the Partner appears on any government lists, has adverse media, or is a PEP, and will receive a KYC Report and an AML Report from the applicable Third-Party Solutions Providers.

1.5 If the User's CDD Documents have not been successfully verified and authenticated and the User is not able to be genuinely identified or the User appears on any government lists, has adverse media, or is a PEP, then Axepay Admin will decline the Partner at this stage of the User account registration process.

1.6 If Axepay Admin is satisfied that the CDD Documents have been successfully verified and authenticated and the Partner is genuinely identified and does not appear on any government lists, has no adverse media, and is not a PEP, then Axepay Admin will proceed to conduct a Risk Assessment of the Partner and assign a Risk Rating.

1.7 If Axepay determines the Risk Rating of the Partner is Moderate or Low, then the Partner will be approved and assigned to a Financial Services Partner. The CDD Documentation of the Partner will be sent to Financial Services Partner to complete its independent CDD review of the Partner and approve/decline Partner.

1.8 If Axepay Admin determines the Risk Rate of the Partner to be High, then the Partner will undergo Enhanced Due Diligence prior to being approved or declined. Please see the Enhanced

Due Diligence Procedures.

1.9 Upon completion of Enhanced Due Diligence, Axepay Admin will determine as to whether the Partner is approved or declined. If the Partner is declined, then the then Axepay Admin will decline the Partner at this stage of the User account registration process.

1.10 If the Partner is approved by Axepay Admin, the Partner will be flagged as High Risk and the CDD Documentation of the Partner will be sent to Financial Services Partner to complete its independent CDD review of the Partner and approve/decline Partner.

1.11 Upon CDD approval of Partner by each of Axepay Admin and the assigned Financial Services Partner, a User account is issued to Partner together with login credentials to access the Platform for transactions purposes and a key is generated by the Financial Services Partner for the Partner. If the Partner was identified as High Risk, the Partner, including its User account, will be subject to ongoing Enhanced Due Diligence Procedures.

1.12 If the Partner is not approved by the Financial Services Partner, the Partner will be declined and a User account will not be opened for the Partner.

2. CORPORATE REGISTRATION (SMEs) AS A CORPORATE VIA APPROVED PARTNER

2.1 The User account registration process for a Corporate may be completed indirectly through a Partner that has been approved for a User account (the "Approved Partner") or may be completed directly without an Approved Partner. While the CDD process for onboarding the Corporate without an Approved Partner remains same at the later stage, the initial process for registration of a User account for a Corporate will be different. Please see 3 below for the procedures for a direct Corporate registration without an Approved Partner.

2.2 All Corporates under the Approved Partner automatically get assigned to same Financial Services Partner as the Approved Partner.

2.3 The Approved Partner will email the Corporate a registration link together with a unique identifier key for the Approved Partner which is issued by the Platform. All Corporates associated with the Approved Partner will receive their own unique identifier key.

2.4 The Corporate commences the User account registration by accessing the link from the Approved Partner and completing the request which will include the unique identifier key which is required to submit the registration request for a User account for the Corporate.

2.5 An email and a SMS will be sent to the authorized representative of the Corporate to authenticate separately the email and the mobile number of the authorized representative of the Corporate.

2.6 As soon as each of the email and the mobile phone of the Corporate is authenticated, the authorized representative of the Corporate will be allowed to commence the User account registration process for a Corporate.

2.7 All required CDD Documentation for the legal entity type of the Corporate will be uploaded to the Axepay Platform by the Corporate during the User account registration process.

2.8 Axepay Admin completes initial CDD Document review with the assistance of the Third- Party Solutions Providers by request to have the requisite CDD identity documents verified and authenticated and also have the requisite searches undertaken to determine if the Corporate appears on any government lists, has adverse media, or is a PEP, and will receive a KYC Report and an AML Report from the applicable Third-Party Solutions Providers.

2.9 If the Corporate's CDD Documents have not been successfully verified and authenticated and the Corporate is not able to be genuinely identified or the Corporate appears on any government lists, has adverse media, or is a PEP, then Axepay Admin will decline the Corporate at this stage of the User account registration process.

2.10 If Axepay Admin is satisfied that the CDD Documents have been successfully verified and authenticated and the Corporate is genuinely identified and does not appear on any government lists, has no adverse media, and is not a PEP, then Axepay Admin will proceed to conduct a Risk Assessment of the Corporate and assign a Risk Rating.

2.11 If Axepay Admin determines the Risk Rating of the Corporate is Moderate or Low, then the Corporate will be approved and assigned to a Financial Services Partner. The CDD Documentation of the Corporate will be sent to Financial Services Partner to complete its independent CDD review of the Corporate and approve/decline Corporate.

2.12 If Axepay Admin determines the Risk Rate of the Corporate to be High, then the Corporate will undergo Enhanced Due Diligence prior to being approved or declined. Please see the Enhanced Due Diligence Procedures.

2.13 Upon completion of Enhanced Due Diligence, Axepay Admin will determine as to whether the Corporate is approved or declined. If the Corporate is declined, then the then Axepay Admin will decline the Corporate at this stage of the User account registration process.

2.14 If the Corporate is approved, the Corporate will be flagged as High Risk and the CDD Documentation of the Corporate will be sent to Financial Services Partner to complete its independent CDD review of the Corporate and to approve/decline Corporate.

2.15 The Corporate needs to be approved by each of Axepay Admin and the Financial Services Partner to be issued a User account for a Corporate. Upon approval by the Financial Services Partner, a User account will be issued to the Corporate with login credentials to access the Platform for transaction purposes and a key is generated by the Financial Services Partner for the Corporate. If the Corporate was identified as High Risk, the Corporate, including its User account, will be subject to ongoing Enhanced Due Diligence Procedures.

2.16 If CDD review of the Corporate results in a decline by the Financial Services Partner, a User account will not be issued to the Corporate.

3. REGISTRATION OF A CORPORATE (SMEs) WITHOUT AN APPROVED PARTNER

3.1 A Corporate that requests to register for a User account without a corresponding Approved Partner will be emailed a registration link together with a unique identifier key issued by the Platform by Axepay Admin.

3.2 The Corporate commences the User account registration by accessing the link from Axepay and completing the request which will include the unique identifier key which is required to submit the registration request for a User account for the Corporate. All required CDD Documentation will be uploaded to the Axepay Platform during the registration process.

3.3 An email and a SMS will be sent to the authorized representative of the Corporate to authenticate separately the email and the mobile number of the authorized representative of the Corporate.

3.4 As soon as each of the email and the mobile phone of the Corporate is authenticated, the authorized representative of the Corporate will be allowed to commence the User account registration process for a Corporate.

3.5 All required CDD Documentation for the legal entity type of the Corporate will be uploaded to the Axepay Platform by the Corporate during the User account registration process.

3.6 Axepay Admin completes initial CDD Document review with the assistance of the Third- Party Solutions Providers by request to have the requisite CDD identity documents verified and authenticated and also have the requisite searches undertaken to determine if the Corporate appears on any government lists, has adverse media, or is a PEP, and will receive a KYC Report and an AML Report from the applicable Third-Party Solutions Providers.

3.7 If the Corporate's CDD Documents have not been successfully verified and authenticated and the Corporate is not able to be genuinely identified or the Corporate appears on any government lists, has adverse media, or is a PEP, then Axepay Admin will decline the Corporate at this stage of the User account registration process.

3.8 If Axepay Admin is satisfied that the CDD Documents have been successfully verified and authenticated and the Corporate is genuinely identified and does not appear on any government lists, has no adverse media, and is not a PEP, then Axepay Admin will proceed to conduct a Risk Assessment of the Corporate and assign a Risk Rating.

3.9 If Axepay Admin determines the Risk Rating of the Corporate is Moderate or Low, then the Corporate will be approved and assigned to a Financial Services Partner. The CDD Documentation of the Corporate will be sent to Financial Services Partner to complete its

independent CDD review of the Corporate and approve/decline Corporate.

3.10 If Axepay Admin determines the Risk Rate of the Corporate to be High, then the Corporate will undergo Enhanced Due Diligence prior to being approved or declined. Please see the Enhanced Due Diligence Procedures.

3.11 Upon completion of Enhanced Due Diligence, Axepay Admin will determine as to whether the Corporate is approved or declined. If the Corporate is declined, then the then Axepay Admin will decline the Corporate at this stage of the User account registration process.

3.12 If the Corporate is approved, the Corporate will be flagged as High Risk and the CDD Documentation of the Corporate will be sent to Financial Services Partner to complete its independent CDD review of the Corporate and to approve/decline Corporate.

3.13 The Corporate needs to be approved by each of Axepay Admin and the Financial Services Partner to be issued a User account for a Corporate. Upon approval by the Financial Services Partner, a User account will be issued to the Corporate with login credentials to access the Platform for transaction purposes and a key is generated by the Financial Services Partner for the Corporate. If the Corporate was identified as High Risk, the Corporate, including its User account, will be subject to ongoing Enhanced Due Diligence Procedures.

3.14 If CDD review of the Corporate results in a decline by the Financial Services Partner, a User account will not be issued to the Corporate.

4. BUSINESS REGISTRATION (B2B) AS A CORPORATE VIA APPROVED PARTNER-A BUSINESS MAY NOT REGISTER DIRECTLY AT THIS TIME

4.1 The User account registration for a Business is completed indirectly through an Approved Partner. The Approved Partner will email the Business a link together with a unique identifier key issued by the Platform. All Businesses associated with the Approved Partner will each receive their own unique identifier key and will be assigned to the same Financial Services Partner as the Approved Partner.

4.2 The Business commences the User account registration by accessing the link from the Approved Partner and completing the request which will include the unique identifier key which is required to submit the registration request for a User account for the Corporate. All required CDD Documentation will be uploaded to the Axepay Platform during the registration process.

4.3 An email and a SMS will be sent to the authorized representative of the Business to authenticate separately the email and the mobile number of the authorized representative of the Business.

4.4 As soon as each of the email and the mobile phone of the Business is authenticated, the authorized representative of the Business will be allowed to commence the User account registration process for a Business.

4.5 All required CDD Documentation for the legal entity type of the Business will be uploaded to the Axepay Platform by the Business during the User account registration process.

4.6 Axepay Admin completes initial CDD Document review with the assistance of the Third- Party Solutions Providers by request to have the requisite CDD identity documents verified and authenticated and also have the requisite searches undertaken to determine if the Business appears on any government lists, has adverse media, or is a PEP, and will receive a KYC Report and an AML Report from the applicable Third-Party Solutions Providers.

4.7 If the CDD Documents of the Business have not been successfully verified and authenticated and the Business is not able to be genuinely identified or the Business appears on any government lists, has adverse media, or is a PEP, then Axepay Admin will decline the Business at this stage of the User account registration process.

4.8 If Axepay Admin is satisfied that the CDD Documents have been successfully verified and authenticated and the Business is genuinely identified and does not appear on any government lists, has no adverse media, and is not a PEP, then Axepay Admin will proceed to conduct a Risk Assessment of the Business and assign a Risk Rating.

4.9 If Axepay Admin determines the Risk Rating of the Business is Moderate or Low, then the Business will be approved and assigned to a Financial Services Partner. The CDD Documentation of the Business will be sent to Financial Services Partner to complete its independent CDD review of the Business and approve/decline the Business.

4.10 If Axepay Admin determines the Risk Rate of the Business to be High, then the Business will undergo Enhanced Due Diligence prior to being approved or declined. Please see the Enhanced Due Diligence Procedures.

4.11 Upon completion of Enhanced Due Diligence, Axepay Admin will determine as to whether the Business is approved or declined. If the Corporate is declined, then the then Axepay Admin will decline the Business at this stage of the User account registration process.

4.12 If the Business is approved, the Business will be flagged as High Risk and the CDD Documentation of the Business will be sent to Financial Services Partner to complete its independent CDD review of the Business and to approve/decline the Business.

4.13 The Business needs to be approved by each of Axepay Admin and the Financial Services Partner to be issued a User account for a Corporate. Upon approval by the Financial Services Partner, a User account will be issued to the Business as a Corporate with login credentials to access the Platform for transaction purposes and a key is generated by the Financial Services Partner for the Corporate. If the Corporate was identified as High Risk, the Corporate, including its User account, will be subject to ongoing Enhanced Due Diligence Procedures.
4.14 If CDD review of the Business results in a decline by the Financial Services Partner, a User account for a Corporate will not be issued to the Business.

5. INDIVIDUAL REGISTRATION VIA APPROVED PARTNER-INDIVIDUALS MAY NOT REGISTER DIRECTLY AT THIS TIME

5.1 The User account registration for an Individual is completed indirectly through an Approved Partner. The Approved Partner will email the Individual a link together with a unique identifier key issued by the Platform. All Individuals associated with the Approved Partner will each receive their own unique identifier key and will be assigned to the same Financial Services Partner as the Approved Partner.

5.2 The Individual commences the User account registration by accessing the link from the Approved Partner and completing the request which will include the unique identifier key which is required to submit the registration request for a User account for the Corporate.

5.3 An email and a SMS will be sent to the Individual to authenticate separately the email and the mobile number of the Individual.

5.4 As soon as each of the email and the mobile phone of the Individual is authenticated, the Individual will be allowed to commence the User account registration process.

5.5 All required CDD Documentation for the legal entity type of Individual will be uploaded to the Axepay Platform by the Individual during the User account registration process.

5.6 Axepay Admin completes initial CDD Document review with the assistance of the Third-Party Solutions Providers by request to have the requisite CDD identity documents verified and authenticated and have the requisite searches undertaken to determine if the Individual appears on any government lists, has adverse media, or is a PEP, and will receive a KYC Report and an AML Report from the applicable Third-Party Solutions Providers.

5.7 If the Individual's CDD Documents have not been successfully verified and authenticated and the Individual is not able to be genuinely identified or the Individual appears on any government lists, has adverse media, or is a PEP, then Axepay Admin will decline the Individual at this stage of the User account registration process.

5.8 If Axepay Admin is satisfied that the CDD Documents have been successfully verified and authenticated and the Individual is genuinely identified and does not appear on any government lists, has no adverse media, and is not a PEP, then Axepay Admin will proceed to conduct a Risk Assessment of the Individual and assign a Risk Rating.

5.9 If Axepay Admin determines the Risk Rating of the Individual is Moderate or Low, then the Individual will be approved and assigned to a Financial Services Partner. The CDD Documentation of the Individual will be sent to Financial Services Partner to complete its independent CDD review of the Individual and approve/decline Individual.

5.10 If Axepay Admin determines the Risk Rate of the Individual to be High, then the Individual will undergo Enhanced Due Diligence prior to being approved or declined. Please see the Enhanced Due Diligence Procedures.

5.11 Upon completion of Enhanced Due Diligence, Axepay Admin will determine as to whether the Individual is approved or declined. If the Individual is declined, then the then Axepay Admin will decline the Individual at this stage of the User account registration process.

5.12 If the Individual is approved, the Individual will be flagged as High Risk and the CDD Documentation of the Individual will be sent to Financial Services Partner to complete its independent CDD review of the Individual and to approve/decline Individual.

5.13 The Individual needs to be approved by each of Axepay Admin and the Financial Services Partner to be issued a User account for an Individual. Upon approval by the Financial Services Partner, a User account will be issued to the Individual with login credentials to access the Platform for transaction purposes and a key is generated by the Financial Services Partner for the Individual. If the Individual was identified as High Risk, will be subject to ongoing Enhanced Due Diligence Procedures.

5.14 If CDD review of the Individual results in a decline by the Financial Services Partner, a User account will not be issued to the Individual.

VIDEO EKYC PROCEDURES

The Platform has the capability built-in to complete eKYC videos of individuals as required. EKYC is be performed concurrently with the User account registration process for Individuals as well as the legal entity's owners, shareholders, directors, officers, and partners who are individuals. The capabilities include live motion images to ensure the documents are captured in the live environment. Mobile phone, email, geo-tagging, and IP is captured along with a ten (10) second video together with timestamped required CDD documents. All the documents captured are saved in our secured vault and authenticated by the support team.

1.1 Axepay Admin sends eKYC link to the individual to their business email ID and mobile number for first level of authentication and verification.

1.2 Individual receives eKYC link on their authenticated business email ID and mobile number.

1.3 Individual opens the link and fills in authenticated mobile phone number and/or email to receive OTP for eKYC process.

1.4 An OTP is sent to the individual on his registered email ID and/or mobile number

1.5 The individual enters the OTP and starts the process of eKYC. A message is displayed on the screen for individual stating the details of eKYC steps and terms to be accepted for eKYC.

1.6 Individual accepts the terms and moves to the eKYC video recording. A customized message is displayed to the individual stating what information is required to be

recorded on the ten (10) second video.

1.7 Individual is instructed on how to upload and/or scan either through the web dashboard or through their phone (plug-in utility embedded in the platform) the requisite CDD documents as set out in Schedule "A".

1.8 Individual records the video, previews it and submits it.

1.9 Individual 's geo-tagging, mobile number and email ID is captured during eKYC process.

1.10 Documents are captured and confirmation of document receipt is sent to individual via authenticated email/mobile phone.

1.11 Axepay Admin receives requisite CDD Documentation and video from individual for identity and document verification and authentication purposes. CDD review is completed in accordance with User Account Registration Procedures, including review and approval by the Financial Services Partners. An individual may be declined by Axepay Admin as a result of any missing/expired CDD Documents or in case of the clarity of the uploaded CDD Documents not being precise. In this case, Axepay Admin may request the individual to complete their eKYC process again.

Schedule "A"
CIP/KYC Information and Document Requirements

General Business Information

- Full Legal Company Name
- DBA/Fictitious Business
- Contact Name
  Business Telephone Number
- Mobile Telephone Number
- Business Website(s)
- Date of Business Formation or Incorporation
- Country or Jurisdiction of Formation or Incorporation
- Business ID type
- Federal Tax ID Number or Business Registration Number
- Description of Business
- Type of Business/ Legal Entity Structure
- Provide Constitutional Documents
- Are any of the entity's owners or Directors Politically Exposed Persons (PEPs)? Board Resolution or other proof regarding signatory authority
- Principal Place of Business
- Address, City, State/Province, Zip Code/Postal Code, Country
- Proof of Business Address-requested as needed
- Products and Services
- Purpose for sending or receiving payments
- Expected number of monthly payments
- Expected monthly trade volume
- Countries transacting with

Authorized Representative- General Information

- Eligible Account Signatory First Name, Middle Name, Last Name
- Job title
- Date of Birth
- Citizenship/Nationality
- Residential Street Address, City, State/Province, Zip Code/Postal Code, Country Email Address
  Business Phone Number
- Mobile Phone Number
- US: Social Security Number;
- Personal Identification ID Type (Passport, National ID, Driver's License, US SNN)
- ID Number
- ID Expiration
- Jurisdiction in which ID was issued
- ID Copy (Image)
- Personal identification verification

- Residence Certification Document: Proof of Residential Address: Acceptable documents: Valid national identity card; recent utility or telephone bill; bank statement or correspondence from a government agency.

Director(s)/Appointed Officer(s) - General Info: Must be completed for each Director and Appointed Officer

- First Name
- Middle Name
- Last Name
- Job title
- Date of Birth
- Citizenship/Nationality
- Residential Street Address, City, State/Province, Zip Code/Postal Code, Country Acceptable documents: Valid national identity card; recent utility or telephone bill; bank statement or correspondence from a government agency.
- Email Address
- Business Phone Number
- Mobile Phone Number
- Director/Appointed Officer Personal Identification (Passport, National ID, Driver's License, US SNN)
- ID Copy (Image)
- Proof of Residential Address Acceptable documents: Valid national identity card; recent utility or telephone bill; bank statement or correspondence from a government agency.
- ID Type
- ID Number
- ID Issuing Agency ID Issuing Country ID Issuing Region ID Expiration Date

Ultimate Beneficial Owner(s)

- Ultimate Beneficial Owner - Must be completed for each natural person who owns 25% or more of entity; if no natural persons own 25% or more, then complete for the natural person with the largest share
- First Name
- Middle Name
- Last Name
- Percentage of Ownership
- Job title
- Date of Birth
- Business Phone Number
- Mobile Phone Number
- Residential Street Address City State/Province Zip Code/Postal Country
- Proof of Residential Address: Acceptable documents: Valid national identity card; recent utility or telephone bill; bank statement or correspondence from a government agency. Citizenship/ Nationality
- Ultimate Beneficial Owner - Personal Identification (Passport, National ID, Driver's License, US SNN)
- ID Type

- ID Number
- ID Issuing Agency
- ID Issuing Country
- ID Issuing Region
- ID Expiration Date
- ID Copy (Image)
- Proof of Residential Address as above

Individual

- First Name Middle Name Last Name
- Job title
- Date of Birth Citizenship/Nationality
- Residential Street Address, City, State/Province, Zip Code/Postal Code, Country
- Proof of Residential Address: Acceptable documents: Valid national identity card; recent utility or telephone bill; bank statement or correspondence from a government agency.
- Email Address
- Business Phone Number
- Mobile Phone Number
- US: Social Security Number

Schedule "B"
Overview Diagram Flow for CDD and Continuous Screening and Monitoring