Sass Society Inc d/b/a Wishes

Bank Secrecy Act, Anti-Money Laundering and

Office of Foreign Assets Control Compliance Program

Contents

1. Introduction and Policy Statement

Sass Society Inc d/b/a Wishes ("Wishes" or the "Company") was founded on April 17, 2020 in the State of California. The Wishes Services are offered as a platform to allow an individual, entity, or nonprofit organization (the "Organizer") to post a fundraiser ("Fundraiser") to the Platform to accept monetary donations ("Donations") from donors ("Donors") on behalf of the beneficiaries of the Fundraiser ("Wishers"). The company facilitates the Fundraiser of the Organizers and permits Donors to make donations to these Fundraisers. Wishes is not a payment processor and does not hold any funds. Instead, Wishes uses third-party payment processing partners to process Donations for a Fundraiser. The company is not a Financial Institution or Creditor.

All products/services offered by Wishes will only be provided digitally and the Company will not handle any cash, cash equivalents, checks, bank drafts or money orders as part of its operations.

This document describes the Company's Bank Secrecy Act ("BSA")/Anti-Money Laundering ("AML")/ Office of Foreign Assets Control ("OFAC") Compliance Program ("BSA/AML/OFAC Program" or "Program"), provides a comprehensive guide to its AML and government sanctions requirements, and describes how the Company will establish policies, procedure, and internal controls to meet its regulatory and contractual obligations.

For purposes of this Program, all of the products/services offered by Wishes will only be provided digitally and the Company will not handle any cash or cash equivalents as part of its operations. Thus, the Currency Transaction Reporting ("CTR") and the Currency and Monetary Instrument Report ("CMIR") reporting requirements are not included in this Program.

2. Policy Statement

It is the policy of Wishes to comply with all AML laws and regulations and to guard against the use of the Company's services for money laundering, terrorist financing, financial crime, or other illegal activity. BSA/AML/OFAC compliance is the responsibility of each staff member of the Company and the Board of Directors (the "Board" or "BOD").

The Company will make every reasonable effort to resist being associated with money laundering, terrorist financing, or any other type of criminal activity or transactions that may involve fraudulent activity or try to hide the actual purpose of the payments being processed. All directors, officers, and employees are required to immediately report all known attempts to launder money or create an evasive transaction as well as all suspicious activities to the Chief Compliance Officer ("CCO").

This Program will be reviewed, updated, and presented by the CO to the Board for formal approval at least annually but more often should significant operational or regulatory changes take place. The Company will formally approve this Program, the AML Risk Assessment, and the designation of the CO in written Board meeting minutes or written consents of the Board.

3. Guiding Laws, Regulations, Concepts

3.1. Bank Secrecy Act

Wishes is committed to compliance with the BSA and serves as guidance for the structure of this AML Compliance Program in terms of identifying the key elements of an effective AML compliance program. It requires written policies, procedures and internal controls reasonably designed to prevent and detect

money laundering and terrorist financing. The BSA outlines five pillars of an AML compliance program as follows:

- Designation of a Compliance Officer to ensure day-to-day compliance with the Program.
- Implementation of internal controls
- Provision for initial and ongoing training to appropriate personnel
- Facilitation of a periodic independent review of the AML Program
- Implementation of customer due diligence procedures, in particular for beneficial ownership

The Anti-Money Laundering Act ("AMLA"), passed by Congress in 2020, significantly expands the BSA through various measures. Namely, the AMLA formalizes the risk-based approach for financial institutions compliance programs; aligns regulatory supervision and examination priorities with the expanded purpose of the BSA; enhances whistleblower protections; and increases civil and criminal penalties for BSA violations. The AMLA also expanded the requirement for identified reporting companies to disclose beneficial ownership information to FinCEN, which will in turn maintain a nonpublic beneficial ownership database.

3.2. Office of Foreign Assets Control

OFAC administers a number of different sanctions programs. Sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals. U.S. persons must comply with OFAC regulations, including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. In the cases of certain programs, foreign subsidiaries owned or controlled by U.S. companies also must comply. Certain programs also require foreign persons in possession of U.S. origin goods to comply. OFAC publishes a list of Specially Designated Nationals ("SDN"s) which is a list of individuals, entities, vessels, and more recently IP addresses and blockchain addresses, with which no U.S. person or entity should transact.

3.3. Money Laundering ("ML") and Terrorist Financing ("TF") Description

Money laundering is the attempt to conceal or disguise the nature, location, source, ownership, or control of illegally obtained money. If illegally obtained money is successfully laundered, criminals maintain control over their funds and can establish a separate cover for their illicit source of income. The compliance regulations apply to any funds derived from illegal activities, such as funds held by terrorists, organized crime, tax evaders, and other groups and individuals seeking to transfer, spend, or invest money derived from any type of crime.

Money laundering is not limited to the use of cash. Money laundering can also be conducted via any type of transaction or group of transactions including, but not limited to, wire transfer, ACH, monetary instruments, prepaid cards, debit or credit cards, or cryptocurrency. Although money laundering is a diverse and often complex process, it basically involves three independent steps that can occur simultaneously.

3.3.1. Placement

The first and most vulnerable stage of laundering money is placement. The goal is to introduce the unlawful proceeds into the financial system without attracting the attention of financial institutions or law enforcement. Placement techniques include structuring currency deposits in amounts to evade reporting requirements or commingling currency deposits of legal and illegal enterprises.

3.3.2. Layering

The second stage of the money laundering process is layering, which involves moving funds around the financial system often in a complex series of transactions to create confusion and complicate the paper trail.

3.3.3. Integration

The ultimate goal of the money laundering process is integration. Once the funds are in the financial system and insulated by the layering stage, the integration stage is used to create the appearance of legality through additional transactions. These transactions further shield the criminal from a recorded connection to the funds by providing a plausible explanation for the source of the funds.

3.4. Terrorist Financing

Terrorist financing uses funds for illegal political purposes, but unlike with money laundering, money for the financing of terrorism is not necessarily derived from illicit proceeds. Most commonly, legitimate funds sources include charitable donations that may be sent to foreign government sponsors, international businesses, and personal employment services.

Although the motivation differs between traditional money laundering and terrorist financing, the methods used to fund terrorist operations can be the same as, or similar to, methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex. This is why it can be more difficult to detect terrorist financing and why it's so important to establish policies, procedures, and controls to monitor customer transactions to detect any potential suspicious activity that could be linked to terrorist financing.

3.5. Suspicious Activity

Activity conducted by a customer or non-customer using the financial institution where there are indications that the person engaging in the transaction may be doing so for fraudulent or illegal purposes. All money-laundering and terrorist financing activity is ideally uncovered as the result of observing suspicious activity.

Suspicious activity need not be proven to be illegal and is typically deemed suspicious on the observation of red flags and anomalies in activity that deviate from what the institution expects from its customers.

4. Corporate Governance and Roles and Responsibilities

4.1. Board of Directors

The Company's Board of Directors bears the ultimate responsibility for the Program, which includes understanding the policies, procedures, controls, and systems in place to effectively manage the Company's compliance risk and to ensure an effective compliance Program has been implemented to mitigate those risks. To accomplish this, the Board requires frequent and comprehensive reporting from the CO on topics such as:

- Volume data on customers, higher risk customers, transmissions, and geographic footprint;
- Compliance department staffing levels;
- Compliance training completion status;
- Notice of upcoming bank partner due diligence reviews or independent reviews;
- Statistical data on reports filed such as: Suspicious Activity Reports ("SARs") and reports to OFAC;

- Corrective actions or terminations of relationships with customers, vendors, and contract workers, etc.;
- Technology or other resource needs and ongoing projects to enhance compliance resources (e.g., monitoring, and due diligence systems);
- Potential significant third-party relationships (prior to signing contracts);
- Complaints received and resolution status;
- Confidentiality or privacy requirements;
- Proposed regulatory changes that potentially may impact the Company;
- Recent enforcement actions including penalties assessed; and
- Compliance Policy and Risk Assessment – initial versions and amendments – for formal Board approval.

The Board will also designate and reaffirm the CO annually, ensuring that the individual appointed has sufficient knowledge, authority, and resources to effectively meet the requirements of the BSA and OFAC. To further ensure and maintain a culture of compliance within the organization, the Board will also approve the Company's Program and Risk Assessment on an annual basis. Lastly, to ensure that the Board has the knowledge and understanding of its responsibilities under the Program, the CO will provide in-person compliance training to the Board at one of the periodic Board meetings on an annual basis. Board of Directors training will be documented.

4.2. Compliance Officer

While the Board accepts the ultimate responsibility for oversight of the Company's Program, the designated CO is responsible for coordinating and ensuring day to day BSA/AML/OFAC compliance efforts. The CO's role is critical to maintaining the effectiveness of the Company's Program. Responsibilities of the CO include, but are not limited to, the following:

- Developing and maintaining the BSA/AML Risk Assessment;
- Updating the Program policies and procedures to reflect current internal processes and, more importantly, state, and federal requirements and related guidance;
- Evaluating the adequacy and accuracy of management information systems and other processes used to generate information for reporting;
- Ensuring the validity of manual and automated systems / technology resources, including those systems used to identify potentially suspicious activity and reportable transactions;
- Monitoring and investigating transaction activity;
- Filing timely, complete, and accurate non-regulatory reports such as SARs and OFAC reports;
- Maintaining all records in accordance with the BSA for a minimum of five (5) years;
- Presenting periodic reporting to the Board of Directors/Senior Management ;
- Ensuring completion of initial and ongoing compliance training for all employees, including senior management and the Board;
- Providing for an independent compliance review on a periodic basis based on the Company's risk profile;
- Cooperating with bank partners, as appropriate, for regulatory examinations; and
- Coordinating responses to requests for information from law enforcement agencies.

The Company's CO may delegate specific duties but retains overall responsibility for daily compliance.

In addition, the CO will stay abreast of changes to laws and regulations as appropriate, being careful to implement changes to procedures and policies, and risk assessments as necessary. The CO will review the FinCEN and OFAC websites/notices to determine whether any new requirements are being issued

pertinent to the Company's operations. The CO may also subscribe to FinCEN or other relevant newsletter services.

The Board commits to allocating to the CO access to all necessary training, human resources, and technological support to meet their compliance responsibilities. The CO has direct access to the Board to ensure timely communication of all compliance issues.

4.3. Senior Management

Senior Management will support the Company's BSA/AML/OFAC efforts by creating an environment of compliance that provides avenues for all employees to detect, deter, and internally refer any incidents of unusual activity, including suspected money laundering and terrorist financing.

Senior Management takes an active role in compliance and pledges to:

- Establish a "culture of compliance" at Wishes
- Support the compliance function through proper resource allocation
- Maintain strict compliance with all applicable laws
- Create awareness of money laundering and terrorist financing risk applicable to all departments within the organization
- Assist with the assessment of risks and the application of appropriate risk-mitigating controls

Senior Management will also select a qualified CO, ensuring that the individual appointed has sufficient knowledge, authority, and resources to effectively run the BSA/AML & OFAC Program. To further ensure and maintain a culture of compliance within the organization, Senior Management will also ensure that the Company maintains a system of internal controls in compliance with BSA/AML & OFAC requirements. Internal controls are policies, procedures, and processes designed to mitigate ML/TF and other illicit financial activity risks and to ensure compliance with regulatory requirements.

Senior Management will also receive reporting from the CO for compliance metrics and/or issues on a periodic basis (at least monthly unless an issue must be addressed immediately). These reports will serve to relay vital information to management including statistics and happenings in the regulatory environment and the Company's operating environment. Senior Management will review and consider a wide array of risk and audit-related issues that could potentially affect the Company, its business operations and overall compliance risk and fraud exposure. These may include operations, information technology, human resources or any other departmental issue that could affect risk mitigation and compliance at the Company.

4.4. Company Staff

All employees of Wishes are responsible for supporting and adhering to the Company's Program efforts. Employees who fail to maintain the Company's high compliance standards and to meet their individual obligations for complying with this Program will be disciplined and employment may be terminated.

Employees are expected to:

- Be familiar with this manual and all applicable compliance policies and procedures related to their job functions;
- Complete all required compliance training and pass the exam;
- Protect customer information;
- Adhere to the Company's record retention schedules;

- Refer unusual or suspicious activity to the CO using the Incident Report form; and
- Cooperate with law enforcement and bank partners as directed by the CO.

4.5. Human Resources

The Company is committed to attracting, hiring, and retaining employees (including third-party vendors, contract employees, temporary workers, etc.) with the same integrity and dedication to compliance that is demonstrated by the Board and senior management. Management understands the risks associated with hiring individuals with prior legal offenses, particularly those related to money laundering and other financial crimes.

As a matter of course, Human Resources ("HR") conducts criminal background checks in advance of offering employment to any prospective employee. The HR Department will retain evidence of all screening results. If issues or discrepancies are identified during pre-employment screening, the resolution to such issues must be documented and HR must approve the hiring of such candidates in writing.

The company will not knowingly hire prospective employees with serious criminal backgrounds, especially those involving financial crimes. If the Company learns of a serious criminal incident involving any of its employees, that incident will be investigated, and appropriate actions will be taken (including termination of contract or employment).

All employees, prior to offer of employment, will also be subject to and required to clear sanctions screening including OFAC's Specially Designated Nationals ("SDN") List and other global sanctions lists as required by the Company.

5. Risk Management

5.1. BSA/AML/OFAC Risk Assessment

BSA requirements and best practices for an AML control framework indicate that the Company must maintain an effective Program commensurate with the risks posed by the location, size, nature, and volume of the services offered. To ensure that all relevant risk factors have been considered within its operation, the Company has developed a risk assessment process and risk based BSA/AML/OFAC compliance controls.

Further, the Company's banking partners may request to see the Company's risk assessment as a primary tool to verify that it has:

- Identified its applicable risks;
- Assessed the mitigating or exacerbating factors for each risk;
- Allocated the proper mix of resources to reduce risk exposure; and
- Determined a reasonable frequency for a periodic independent review of the Company's Program that is based on the present level of risk.

Typically, the risks assessed involve such considerations as the Company's products, services, customers, business model, OFAC and other watch list exposure, employee expertise, training, and turnover, technological resources, and geographic footprint.

Wishes management believes that the most effective way to build its risk-based AML Compliance Program is to first document all perceived inherent risks, all mitigating (or magnifying) factors to those

risks, and to assign residual risk levels and to take the appropriate actions to ensure the Company is at a risk level that is acceptable to senior management and the Board.

The Company's risk assessment is in writing, will be approved by the Board, updated at least annually or as necessary, and will always be considered PRIOR to implementing new products and services and/or operational changes.

6. AML and Sanctions Compliance Program

Wishe's written Program includes policies, procedures, and guides to assist staff in ensuring compliance with its obligations. As the Program evolves, written desktop procedures, forms, and job aids will continue to be developed and enhanced, as necessary. Management is fully committed to maintaining current policies and procedures and to revising these documents when appropriate to address regulatory changes and recommendations.

Guidance and best practices are to consider the "Five Pillars" of an effective AML compliance program, driven and developed by a risk assessment to identify where to apply resources and controls within those pillars.

7. First Pillar: AML Compliance Officer Designation

This Pillar is to designate a responsible individual to oversee daily compliance matters. The Company has designated Vick Ekizian, Chief Compliance Officer, as the CO who will be responsible for the Company's BSA/AML/OFAC compliance Program.

8. Second Pillar: System of Internal Controls

This Pillar is to establish a system of internal controls. Controls are the steps taken to identify and mitigate the risk of ML and AML violations. The level of sophistication of the internal controls should be appropriate for the size, structure, risks, and complexity of the business. As with the written program, the Company has established a system of internal controls and will leverage the controls put in place in other areas of the Company's group organizations as documented in this Program to ensure compliance with this requirement.

The Company incorporates a comprehensive approach to internal controls designed to mitigate identified risks. Examples of internal controls include:

- Know Your Customer ("KYC") program, including:
    - Customer identification and verification procedures;
    - Initial and ongoing due diligence and enhanced due diligence of all customer relationships;
    - Initial and ongoing due diligence and enhanced due diligence of third-party relationships;
    - Initial and ongoing OFAC/economic sanctions screening.
- Transaction monitoring;
- Report filing;
- Record keeping and record retention;
- Training;
- Periodic independent reviews; and
- Internal assessments, where applicable.

This document describes the controls that constitute this pillar.

8.1. Know Your Customer Program ("KYC") and Know Your Business ("KYB")

The Company offers its products and services to both individuals and entities. The Company has implemented a risk-based KYC program as a means of preventing and mitigating potential exposure to those customers who could use its services for illicit purposes. Further, to truly "know" its customers, the Company must develop and consistently apply and adhere to its Customer Due Diligence ("CDD") and Enhanced Due Diligence ("EDD") policies and procedures. The Company's due diligence policies and procedures are risk-based, whereby higher-risk customers and their transactions are reviewed more closely prior to establishing a customer relationship and periodically thereafter.

To meet regulatory requirements and expectations for confirming or verifying the identification of customers with whom the Company will provide its services to, Wishes may use either or both of documentary and non-documentary methods for verifying the customer.

Wishes will utilize a tiered approach to KYC and KYB based on the level of risk presented by the customer and will work with its KYC/KYB vendors and bank sponsor accordingly. This will include consumers and entities.

The level of due diligence on customers will be determine by risk factors that may include but are not limited to, duration of account, expected activity, transaction amounts and volumes, source of funds or wealth information, PEP exposure, geographical footprint, counterparties, products, and services utilized, negative or adverse media, potential fraud indicators, and customer device information.

Risk factors for entities include the above as applicable to the persons associated to the entity, along with the entity type, nature of business, government exposure, jurisdiction of incorporation, areas of operations and trade, third parties or agency involvement, length of time business was established, duration of account, negative or adverse media on entity, owners, or controllers, ownership or control structure, and market presence.

8.2. Customer Identification Program ("CIP") and Customer Onboarding

A customer must register at https://www.wishes.inc/ or the Wishes mobile app to use any of the Company's products or services. In order to successfully register for an account, the customer must provide the following information:

The minimum information required for individual customers is the following:

- Full name;
- Date of birth ("DOB");
- Address of residence or principal place of business
    - Post office boxes (P.O. Box) shall not be acceptable for purposes of customer onboarding/approval.
- Social Security Number or taxpayer identification number;
- Government issued document;
- Mobile phone number; and
- Email address.

Other information that will allow Wishes to identify the customer.

For organization customers that are legal entities, Wishes shall obtain the following identifying information from each legal entity customer before any account is approved/created and/or prior to the establishment of services:

a. Name— the full legal name of the entity, including any trading or doing business as ("DBA") names;
b. Principal place of Business Address
    i. the principal place of business or other physical location.
    i. Post office boxes shall not be acceptable for purposes of customer onboarding/approval.
c. Identification Number—A unique identification number, such as a
    i. tax identification number,
    ii. employer identification number, or
    iii. company registration number.
d. Further legal entity customers, including beneficial ownership information, shall be obtained (highlighting documentary and non documentary information as acceptable forms of verification).

Wishes will only onboard 501c3 entities.

Once this information is obtained, the Company uses a third-party vendor, Prove, to automatically identify and verify the customer using non-documentary methods, including public and non-public information databases. When the customer can be identified, the account is opened. Part of the automated verification process includes an OFAC sanctions screening.

Where the customer cannot be automatically verified using non-documentary methods and its third-party service provider's systems and resources, the Company will conduct additional due diligence ranging from manual research to asking the customer to upload a selfie holding a valid identification document (U.S. driver license, other official U.S. federal identification document, or a passport). Only once the customer can be identified and verified will the account be opened.

Where the above steps cannot identify and verify the customer, the account is not opened, and the customer is rejected.

Based upon the information and documentation provided, Wishes, will independently verify certain identification and verification information from its customers, utilizing a risk-based approach, in order to form a reasonable belief that it knows the true identity of the customer. Documentary and non-documentary verification methods may be utilized as part of the KYC process on customers. OFAC and PEP screening will also be conducted as part of the onboarding process as detailed later in this Program.

8.3. Politically Exposed Persons ("PEPs") Designation

Wishes will take all reasonable steps to ensure that it does not knowingly or unwittingly assist in hiding or moving the proceeds of corruption by senior foreign or domestic political figures and their associates. The Company understands that PEPs have used financial institutions as conduits for their illegal activities, including corruption, bribery, and money laundering. Thus, it has implemented this policy regarding PEPs as a best business practice to ensure compliance with U.S. AML laws and regulations.

The term "politically exposed person" generally includes a current or former senior political figure, their immediate family, and their close associates. PEPs can be foreign or domestic.

- A "senior foreign political figure" 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 typically includes the figure's parents, siblings, spouse, children, and in-laws.
- 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. The definition of senior official or executive must remain sufficiently flexible to capture the range of individuals who, by virtue of their office or position, potentially pose a risk that their funds may be the proceeds of foreign corruption. Titles alone may not provide sufficient information to determine if an individual is a PEP, since governments are organized differently from jurisdiction to jurisdiction.

Because the risks presented by PEPs vary, Wishes has implemented risk-based controls and monitoring related to customer accounts and transactions. Wishes will utilize Lexis Nexis to conduct PEP identification screening at customer onboarding. In determining the acceptability of PEPs relationships, Wishes will obtain sufficient information to determine whether an individual is or is not a PEP. For example, when conducting due diligence on a potential PEP, Wishes will review information identified by the third-party verification service provider and professional background. These factors would likely require some review of past and present employment as well as general references that may identify a customer's status as a PEP. PEPs are automatically classified as high-risk customers and are subject to enhanced due diligence and strict monitoring.

The above-noted items in the CIP and Customer Onboarding section are essential in meeting KYC obligations, and it is Wishes's responsibility to obtain accurate answers to all of them. All this information must be established and accurately recorded prior to any activity in the account. Customer information is instantly verified through the identity verification process.

If through information verification and account opening process, any information does not match with the available database, the account will be marked with a red flag and will go into a manual verification queue. All accounts in the manual verification queue will be reviewed by the CO or designee and depending on the information discovered through the review process, the account will be ether approved or rejected. Any manual review will be documented, and appropriate notes will be made on the customer's file recording any information discovered in the process and the reason behind the decision to approve or reject the account in question.

The CO or designee is responsible for reviewing all individual and business entity accounts with red flags and approving them prior to transacting. If the CO or designee is not available, the Chief Executive Officer ("CEO") will be responsible for account approval.

8.4. Customer Notification

In accordance with the USA PATRIOT Act, adequate notice of Wishes's CIP requirements must be provided to new customers from whom the Company is requesting identity information. Notice may be provided in various methods depending on how the account is opened or the service is provided. Wishes provides notice via its website, including in its terms of service.

The following language or comparable language will be used:

IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT

To help the government fight the funding of terrorism and money laundering activities, Federal law requires financial institutions to obtain, verify, and record information that identifies each individual or entity that opens an account.

What this means for you: When you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

9. Customer Due Diligence ("CDD")

The goal of conducting Customer Due Diligence ("CDD") is to help the Company develop an understanding of expected transactional behavior of its customer's transactions. Deciphering what is "normal" assists the Company in detecting what is unusual when monitoring activity.

Due diligence can be useful for all customers, but it is particularly useful when applied to higher risk customers. Company management understands that collecting and verifying customer data is the first critical step. In part to conduct its business, and in part to understand customer activity and be able to monitor for suspicious activity, the following data points are examples of what may be collected in addition to the customer identification and verification described above:

- Expected volume of donations to end-users
- Expected number of end-users who will be utilizing the Wishes app
- Expected frequency of donations made to entities or to other users
- Average transaction amount.

10. Enhanced Due Diligence ("EDD")

When a customer demonstrates risk that warrants further control, the Company may apply Enhanced Due Diligence ("EDD") to ensure it understands the higher risk customer and can thereby monitor effectively. EDD may also be executed, for example, where a discrepancy is observed on CIP; when transaction monitoring identifies an anomaly; on receipt of a subpoena or any other outside inquiry regarding a customer; or in any case where an employee or compliance team member determine that further due diligence is warranted based on the circumstances.

A basic EDD measure the Company may employ, for example, is requesting the customer provide proof of address and purpose of their transaction activity; or the same for a customer's counterparty; invoices or bills of lading; bank statements, tax returns, or financial statements, or any other document deemed acceptable by the CO that allows the Company to form a reasonable belief that it knows the identity of the customer and that their accompanying information is true and accurate, and that the activity being engaged in is legitimate and not associated with financial crime.

11. Beneficial Ownership

Beneficial owners are the actual individuals who are the directors, individuals with the authority over the account, trustees, and known beneficiaries and settlors of a trust, or significant shareholders, who directly or indirectly own 25% or more of a corporation or an entity or maintain significant control. When applicable, Wishes is required to obtain beneficial ownership information for two types of beneficial owners- those that satisfy the ownership prong and those that satisfy the control prong.

- The ownership prong refers to each individual who, directly or indirectly owns 25% or more of the equity interest of the legal entity customer.
- The beneficial owner within the control prong means a single individual with significant responsibility to control, manage, or direct the legal entity customer.

Beneficial owners cannot be other corporations, trusts, or other entities. They must be the individuals who are the owners or controllers of the entity. It is important to consider and review the names found on official documentation in order to confirm the accuracy of the beneficial ownership information. It may be necessary to search through many layers of information to confirm who are the beneficial owners, as the names found on official documentation may not always reflect the actual beneficial owners.

12. Ongoing CDD

The Company will update a customer's records at least annually for both individual and institutional customers. For those customers that have exceeded the above threshold limits, have been deemed high risk, or have been detected in the Company's transaction monitoring, the Company will require that they provide recent proof of address and proof of source of funds. In addition, the Company may request any other due diligence documentation deemed necessary to mitigate the risks associated with the customer.

12.1. Customer Risk Rating

Part of the purpose of collecting information from customers is to allow the Company to assign each customer or type of customer a Customer Risk Rating ("CRR"). The CRR assists the company in determining which customers warrant a higher level or greater frequency of review.

Once operations begin, the Company will create a risk assessment for its customer base and update it on an annual basis. Once it has selected and implemented a third-party transaction monitoring system, it will automate the customer risk assessment process accordingly. The goal is to perform the initial risk assessment as new customers establish their relationships with the Company. Data collected during the customer application process is used to determine the degree and frequency of due diligence and, as applicable, enhanced due diligence required. On a case-by-case basis, future due diligence review scopes and frequencies will be assigned and tracked based on the customer risk assessment established. For instance, a high-risk customer may require quarterly due diligence reviews while a low-risk customer may be assigned only annual due diligence reviews. The risk assessment will be maintained by the CO and shared with the Board periodically.

12.2. Customer Refusal to Provide Information

If a potential or existing customer refuses to provide the information as part of a due diligence or review process, fails to provide updated information when requested, is unable to provide required information, does not have required information or evidence or documents supporting required information, or appears to have intentionally provided misleading information, the Company will not conduct business with that person or entity.

Depending on the circumstance, the Company may bar or block the customer from opening accounts in the future, close currently existing accounts, or file or communicate any unusual activity to its partners as described elsewhere in this document.

12.3. Prohibited Customers

The Company will not establish or maintain relationships, or accept funds from, or on behalf of, any person or entity if they:

- Cannot be identified in accordance with Company's KYC program;
- Are unresponsive to information requested by the Company which is significant to their identification;
- Intentionally provide misleading information to the Company which is significant to their identification or activities;
- Are known sanctioned individuals or entities of relevant purview to the Company;
- Are identified as a known criminal and/or criminal associates;
- Are identified as a foreign shell bank or any other prohibited persons or entities as may be mandated by applicable law or regulation; and
- The person or entity is located outside of the Company's intended jurisdiction or is known and verified to be operating without required licensing and/or
- Are a prohibited customer or customer type according to the Company's bank or payments service provider's policies.

12.4. Prohibited Entities

The Company will not establish or maintain relationships, or accept funds from, or on behalf of, any entity that does not have a 501(c)(3) status, or, if they are involved in the following industries:

- Adult entertainment
- Counterfeit Goods/IP Infringement
- Illegal/controlled substance vendors
- Drug Paraphernalia
- Arms Weapons Manufacturing Suppliers, and
- Pseudo-Pharmaceuticals

In addition, the Company will terminate the relationship, if one already exists, and notify the relevant authorities about the person/entity/account/transactions, as necessary and applicable.

12.5. Prohibition on Shell Banks

A shell bank is a bank that has no physical presence in any country, or their presence is limited to a brass plaque or paperwork held in the offices of a company formation agent. Shell banks are high risk institutions for money laundering.

The Company will not enter into, maintain any relationships with, or conduct any transactions for or with banks it recognizes to be shell banks. The Company will not establish, maintain, administer, or manage a correspondent account in the U.S., or anywhere else, for, or on behalf of, a shell bank.

12.6. CIP Recordkeeping

Wishes will ensure compliance with recordkeeping requirements as applicable under the BSA and/or its bank partner's requirements. This includes transaction records regarding activation, loads, reloads, purchases, withdrawals, transfers, or other transactions that would reasonably provide law enforcement with a paper trail for any future investigations.

At a minimum, CIP records will include:

- All identifying information obtained
- A description of any document relied on as part of identification and verification, noting the type of document, any identification number contained in the document, place of issuance, and if any, the date of issuance and expiration
- A description of the methods and the results of any measures undertaken to verify the identity of the customer
- A description of the resolution of any discrepancy discovered when verifying the identifying information

Information obtained from the Company's customers will be retained for a period of five (5) years after the date the account with the customer is closed. Records are retained in a manner that permits their retrieval in accordance with regulatory, internal audit, and legal/compliance requirements.

13. Transaction Monitoring Program

The Company monitors for money laundering, terrorist financing, and other illegal activity associated with customers and their transactions on an ongoing basis, using a monitoring system and human review. The transaction monitoring ("TM") system is coded to run rules and employs machine techniques to detect irregular activity.

- Unusually high dollar amounts;
- Part of an unusual pattern of transactions;
- High rate of returns;
- Potential fraud; and
- Appear to have no apparent economic or visible lawful purpose.

Another element of the Company's internal control is watch list and database monitoring. The Company screens its database of customers and beneficiaries of transactions to:

- Identify prohibited customer types;
- Identify customers with higher risk characteristics; and/or,
- Establish/confirm expectations for customer behaviors.

Records and reports used in the monitoring of customer activity are notated to evidence review. These notations will indicate whether the activity appears to be:

- Normal for the customer;
- Can be explained for or by the customer; and/or
- Whether additional monitoring and/or research are warranted.

The TM is subject to independent validation should the risk profile of the Company significantly change, for example by a change in customer type, geographic exposure, or products/transactions.

14. Third Pillar: Compliance Training

The training Pillar is to provide periodic compliance training for appropriate employees. Thus, the Company has developed an AML training module that will be used to train new and existing employees. New hire training must be completed within 30 days of hire. In addition, all employees, including management, must complete ongoing training on an annual basis thereafter. All employees will be

required to take an exam to test their comprehension of the material presented and must obtain an 80% or passing grade to pass. If an employee is unable to take the training and pass the pass the exam, the event will be escalated to the employee's manager and HR for evaluation and action to determine what additional training is appropriate and explore options up to and including termination. The Board of Directors will also take the annual BSA/AML/OFAC training.

All training will be documented, including materials, attendance, test scores, and escalations, as described in the following sections.

14.1. Training Recipients

Relevant employees include the following categories:

a) Board of Directors

b) Senior Management

c) Customer-facing personnel

d) Compliance, Legal and Risk personnel

e) Any other personnel or group of personnel deemed relevant by the CO

14.2. Training Content

Initial and ongoing training materials address applicable laws, rules, and regulations as well as the Company policies and expectations.

Training materials will be reviewed and revised (as necessary) every year. At a minimum, content will include at a minimum:

- An overview of the AML laws that apply to the Company;
- The importance of a culture of compliance;
- The different layers of money laundering and how money laundering differs from terrorist financing;
- The controls that help prevent or identify money laundering such as KYC and suspicious activity monitoring;
- How to report suspicious activity to Compliance;
- Specific requirements, including, but not limited to, confidentiality and record keeping;
- An overview of OFAC requirements and responsibilities under OFAC; and
- The ramifications for non-compliance with the BSA and OFAC.

14.3. Training Documentation

The CO is responsible for ensuring:

- Training materials (including those produced by external firms or associations), attendance, and test records are documented and retained for a minimum of five (5) years;
- Successful completion is verified for all employees on a periodic basis; and
- The Board is periodically apprised of training completion status on a Company-wide basis.

14.4. Additional Training for Compliance Staff

Additional periodic internal or external professional development training is required for compliance staff, which may include webinars, conferences hosted by reputable compliance agencies or associations,

and professional certifications. All training provided to staff will be documented and retained as required.

15. Fourth Pillar: Independent Review

This pillar requirement of a comprehensive compliance program is to provide for the performance of an independent review of the Company's Program to assess its adequacy and effectiveness, including whether the business is operating in compliance with the requirements of the BSA and with its own policies and procedures.

The internal audit department, outside auditors, consultants, or other qualified independent parties may conduct the independent review. "Independent" means employees or outside parties who have not built nor have any role in the operation of the department. While the frequency of the review is not specifically defined in any statute, as a sound practice based on its AML risk profile, the Company will conduct an independent review every 12 to 18 months or more frequently as needed.

The independent reviewer will issue a report of findings and recommendations upon completion of testing. The CO will provide the results of the independent reviews to the Board of Directors and to the Company's bank partners as required. The CO will also track all exceptions noted in such review reports and will address the resulting recommendations or assign corrective action to other Company management.

16. Fifth Pillar: CDD Rule and Beneficial Ownership

The Fifth Pillar requires the creation of a risk based CDD program for conducting ongoing customer due diligence, to include, but not limited to:

- Understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile and assigning an AML Risk Rating
- Conducting ongoing monitoring to maintain and update customer information and to identify and report suspicious transactions.

In addition, the expectation is to conduct due diligence on businesses and non-individual customers at the 25% or greater ownership level, and also for those with "control" or reasonable access to the account. The Company's process for complying with the CDD Rule can be found in the Know our Customer Program section of this policy.

The Company will ensure that identification and verification steps for each beneficial owner are conducted to ensure compliance with this pillar.

17. Suspicious Activity Reporting

The Company will adhere to the following suspicious activity communications guidelines in its entirety. The Company will report potentially suspicious activities to the board and Bank partner for all observed suspicious activity.

Suspicious activity reporting is part of the Company's compliance monitoring and reporting responsibilities. Suspicious transactions are financial transactions that Wishes has reasonable grounds to suspect are related to conducting money laundering, terrorist financing, or other illegal activity, including fraud.

The Company monitors transactional activity to identify patterns of unusual size, volume, pattern or type of transactions, and geographic factors. The Company provides employee guidelines with examples of suspicious money laundering activity, red flags, that may warrant further scrutiny.

All Company employees are expected to be trained and required to be alert to potentially suspicious transactions and activities. Employees are to report information relevant to those transactions and activities using the Incident Report form on the same business day on which they become aware of unusual activity.

17.1. Red Flags

The CO or designee will review all internal referrals of suspicious activity provided by employees. The CO will examine and evaluate the background and purpose of all related activity to ascertain whether a reportable condition exists, document the findings and disposition of that examination and evaluation, and file any necessary report. The following serves as guidance for potential Red Flags in user/customer Due Diligence and Interactions with user/customers:

- The user/customer provides Wishes with unusual or suspicious identification documents that cannot be readily verified or are inconsistent with other statements or documents that the user/customer has provided, or the user/customer provides information that is inconsistent with other available information about the user/customer. This indicator may apply to account openings and to interactions after account openings.
- The user/customer is reluctant or refuses to provide Wishes with complete user/customer due diligence information as required by the Wishes procedures, which may include information regarding the nature and purpose of the user/customer's business, prior financial relationships, anticipated account activity, business location and, if applicable, the entity's officers and directors.
- The user/customer refuses to identify a legitimate source of funds or information is false, misleading, or substantially incorrect.
- The user/customer is domiciled in, doing business in or regularly transacting with counterparties in a jurisdiction that is known as a bank secrecy haven, tax shelter, high-risk geographic location (e.g., known as a narcotics-producing jurisdiction, known to have an ineffective anti-money laundering and counter-financing of terrorism (AML/CFT) systems or conflict zone, including those with an established threat of terrorism.
- The user/customer has no discernible reason for using Wishes' service.
- The user/customer has been rejected or has had its relationship terminated as a user/customer by another financial services firm.
- The user/customer's legal or mailing address is associated with multiple other accounts or businesses that do not appear related.
- The user/customer appears to be acting as an agent for an undisclosed principal but is reluctant to provide information.
- The user/customer is a trust, shell company or private investment company that is reluctant to provide information on controlling parties and underlying beneficiaries.
- The user/customer is publicly known or known to Wishes to have criminal, civil or regulatory proceedings against him or her for crime, corruption, or misuse of public funds, or is known to associate with such persons. Sources for this information could include news items, the Internet or commercial database searches.

- The user/customer's background is questionable or suspicious activities are reported where Criminal violations involving insider abuse in any amount and differ from expectations based on business activities.
- The user/customer exhibits unusual concern with Wishes' compliance with government reporting requirements and Wishes' AML policies.
- The user/customer tries to persuade an employee not to file required reports or not to maintain the required records.
- The user/customer is reluctant to provide the information needed to file reports to proceed with the transaction.
- Law enforcement has issued subpoenas or freeze letters regarding a user/customer or account at a securities firm.
- There is an unusual use of trust funds in business transactions or other financial activity.

When an employee of Wishes detects any red flag or other activity that may be suspicious, they will notify the AML Compliance Manager and CEO of Wishes for appropriate action. Under the direction of the AML Compliance Manager, Wishes will determine whether and how to further investigate the matter.

Where potentially suspicious activity must be reported to the Bank partner, it will be referred to the Bank partner using the "Incident Report". This may include gathering additional information internally or from third-party sources, contacting appropriate law enforcement or regulatory authorities (e.g. FinCEN, OFAC), freezing the account and/or filing an SAR. Wishes has contracted and integrated with an external/third-party Compliance Manager and System, including the engagement of providers to cover requisite regulatory compliance services. These integrations ensure global connectivity and coverage, redundancies to ensure access to global databases to support due diligence, monitoring and risk management/analytics purposes are appropriately backstopped for all Wishes and related customer-impacted AML/FCC activities, and to ensure best-in-class service ability to Wishes related to its AML/FCC needs.

17.2. Suspicious Activity Bank Referrals

Wishes will endeavor to refer all suspicious activity to its bank partner(s) in accordance with its contractual commitments to the bank(s). The Company will follow instructions provided by the bank(s) regarding their required timing and details and will cooperate in any follow-up investigation to support the banks' filing requirements.

The Company will maintain a log of referrals to its partner(s), including those investigations that may initially have been of concern though were later resolved to have a legitimate explanation or not be suspicious after the collection of all facts. There are a variety of legitimate transactions that could raise suspicion simply because they are inconsistent with a customer's historically "normal" activity.

17.3. Referral Quality

The Company will ensure that all referrals made to bank partner(s) are complete, accurate, and filed on a timely basis. The form will include all known suspect information, and care will be taken not to overstate or misrepresent information.

17.4. Emergency Notification to the Government

For violations requiring immediate attention, the CO or designee may determine that the event is significant enough to warrant contacting an appropriate law enforcement authority, which may be any of

the local offices of the IRS – Criminal Investigation Divisions, an appropriate local police department, or the U.S. Federal Bureau of Investigation ("FBI").

1. Confidentiality

Wishes directors, officers, and employees are prohibited from notifying any customer or person involved in any suspicious activity review or referral of the fact that an investigation or referral took place. Informing a customer that he or she is the subject of such is against Company policy.

In general, access to confidential information related to unusual or suspicious activity is limited to necessary employees and to those employees that are on a need-to-know basis.

In the United States, it is a crime to disclose SAR information to persons other than the proper authorities, except when such disclosure is requested by FinCEN or an appropriate law enforcement or federal banking agency. Should Wishes be subpoenaed or otherwise requested to disclose a SAR, it will not produce any information and will escalate the matter to the CO.

2. Reporting and Record keeping

2.1. CTRs and CMIRs and Money Orders

For the purposes of this Program, all the products/services offered by the Company will only be provided digitally and the Company will not handle any cash or cash equivalents as part of its operations. Wishes does not handle cash or monetary instruments or money orders or bank drafts or certified checks or postal money orders, either for funding accounts, disbursing funds, or exchanging value, in any way, shape or form, and has no intention of ever doing so. Thus, the Currency Transaction Reporting ("CTR") and the Currency and Monetary Instrument Report ("CMIR") AML reporting requirements are not included in this program.

3. Information Sharing

There are a number of circumstances in which the Company may share information with law enforcement, other financial institutions, its partners or others. The following are the ways and protocols in which the Company shares information.

3.1. Law Enforcement Inquiries and Requests for Information or Appearance

The Company is committed to cooperating with law enforcement as necessary to assist with the identification and apprehension of those who use its services and the Company network for illegal purposes.

The Company has established a process for identifying subjects of law enforcement ("LE") requests, responding to requests for information, documenting each request and the Company's responses, monitoring the transaction activity of those subjects, identifying unusual or suspicious activity related to those subjects, and filing SARs related to those subjects, if warranted. Law enforcement inquiries and requests can include subpoenas, grand jury subpoenas, National Security Letters ("NSLs") or other.

Should the Company receive a LE request, the request will be forwarded to the CO who will review the letter's contact information and confirm the requestor's identity. Any required response will be furnished within the deadline stipulated in the LE request, if specified. Compliance will maintain a log of

the LE requests received, and the responses provided to law enforcement, and document relevant dates to track timeliness.

The CO and their designees involved in any part of receiving and responding to any law enforcement requests will maintain the utmost confidentiality of all aspects of the case, involving individuals only on a need-to-know basis and only to the extent it is necessary to fulfill the request. We understand that none of our officers, employees or agents may directly or indirectly disclose to any person that the FBI or other federal government authority has sought or obtained access to any of our records.

3.2. 314(a) Information Sharing

314(a) does not currently apply to Wishes but the Company will cooperate with its bank partners to facilitate any 314(a) requests the banks receive. Section 314(a) of the PATRIOT Act establishes a mechanism for law enforcement agencies to communicate names of persons engaged in or suspected to be engaged in money laundering, financial crime, or terrorist financing in return for securing the ability to locate accounts and transactions involving those suspects promptly. Wishe's bank partner(s) will provide the Company with Section 314(a) lists on a periodic basis via a secure email system or other secure mechanism. The Compliance department will compare the names on that list to the full database of customers for the respective Bank Partner program. Wishes will compare its existing customers to the 314(a) list provided and search internal records for current accounts, accounts maintained during the preceding 12 months, and transactions conducted outside of an account by or on behalf of a named suspect during the preceding six months. If any matches are found, they are returned to the respective Partner Bank. If no matches are found, a confirmation email is sent to the respective Partner Bank confirming that there were no matches. Wishes will have 14 calendar days to respond to the 314(a) requests.

3.3. 314(b) Voluntary Information Sharing

Section 314(b) permits financial institutions, upon providing notice to the United States Department of the Treasury, to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity. The Partner Bank(s) may elect to share information under Section 314(b). If required, Wishes will register for 314(b) so that it is able to receive and send information under this section. Wishes will coordinate with the Partner Bank making the request to provide relevant information and vice versa.

3.4. Cooperation with Bank and Other Partners

The Company's bank and other partners may conduct periodic due diligence reviews of the Company's AML/OFAC Program and controls to ensure that the Company has developed an effective Program in accordance with the partner's own BSA requirements and best practices in the prevention of money laundering.

The Company will work closely with its partners to mitigate the risks associated with money laundering and terrorist financing. The Company will continue to maintain an effective compliance program that is periodically reviewed and enhanced according to regulatory guidance, auditor recommendations, and industry best practices.

4. Office of Foreign Assets Control ("OFAC")

4.1. OFAC Policy

The Office of Foreign Assets Control ("OFAC") of the U.S. Department of the Treasury administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction.

4.2. Corporate Governance

The Board of Directors is responsible for the review, approval, and maintenance of the OFAC Compliance Policy. To that end, the Board designated the CO as the dedicated OFAC sanctions compliance officer and ensures the compliance team has adequate resources and authority to operate.

4.3. OFAC Screening

Pursuant to regulatory guidance, Wishes utilizes a risk-based approach to OFAC sanctions screening and has implemented comprehensive policies and procedures to ensure compliance. The Company has contracted with a third-party sanctions screening provider, to screen against OFAC's SDN list in the following instances:

- At customer onboarding, the customer's name (individual and business names), business principals, and beneficial owners
- When a transaction is conducted, both the customer and beneficiary names are screened
- When employees are hired and periodically thereafter
- When conducting due diligence on critical vendors and third-party partners (such as banks and payment processors)

Wishes will not open a new account for any applicant appearing on any government watchlists and will close accounts for any persons or entities that are subsequently added to the OFAC list. At minimum the governmental lists used will include:

- OFAC Specially Designated Nationals and Blocked Persons List ("SDN" List)
- Non-SDN Palestinian Legislative Council ("NSPLC")
- FinCEN 311
- Foreign Sanctions Evaders
- Iran and Syria Non-proliferation Act
- Executive Order 13599 List

Additionally, there are several countries (including, in some cases, goods originating from those countries) that US persons are prohibited from dealing, transacting, or engaging with, and Wishes adheres to those provisions and will not engage in any transaction or dealing, or provide any service, involving the following countries:

- Cuba
- North Korea
- Lebanon
- South Sudan

- The Republic of Sudan
- Lybia
- Somalia
- Iran
- Syria
- Crimea region of Ukraine
- Russia

4.4. Controls Over the OFAC Filter

Since the OFAC list is updated frequently, the CO will subscribe to email notifications from OFAC to be alerted to changes in the list to ensure the Company's screening systems are up to date. As the Company's third-party vendor automatically links with OFAC to update and screen customers and transactions in real-time, the CO will test the system to ensure that updates are occurring in a timely fashion. The Company will also screen existing customers against these lists when they are updated and will document the results of any potential matches detected.

4.5. OFAC Reporting

In the event that the Company determines that a customer, or someone with or for whom the customer is transacting, is on the OFAC List or is from or engaging in transactions with a person or entity located in an embargoed country or region, the Company will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC. For match verifications, the Company may call the OFAC Hotline at 1-800-540-6322. If a true reportable match occurs, the Company will:

- Report the match to OFAC within ten (10) days of the occurrence
- Block the associated assets and hold the funds in a segregated interest-bearing account
- Report all blocked property to OFAC on an annual basis by September 30 for balances as of June 30
- Retain all related reporting and supporting documents for five (5) years

Wishes will also inform its bank partner of any block or rejected transactions reported to OFAC.

5. Special Measures

The Secretary of Treasury may require domestic financial institutions and financial agencies to take special measures against certain foreign jurisdictions, foreign financial institutions, classes of international transactions, or types of accounts of primary money laundering concern, as authorized by Section 311 of the USA PATRIOT Act.

The five special measures can be imposed, either individually, jointly, or in any combination:

- Record keeping and reporting of certain financial transactions
- Information relating to beneficial ownership
- Information relating to certain payable through accounts
- Information relating to certain correspondent accounts
- Prohibitions or conditions on opening or maintaining certain correspondent or payable through accounts

Wishes complies with the special measures. Special measures are not static, and the CO will continue to monitor special measures published by FinCEN.

The Financial Crimes Enforcement Network 311 Special Measures for jurisdictions, Financial Institutions, or Internal Transactions of Primary Money Laundering Concern can be found here: https://www.fincen.gov/resources/statutes-and-regulations/311-special-measures

6. Record Retention

BSA and OFAC regulations require that records and supporting documents be retained for potential review by regulatory agencies for a period of five (5) years, unless otherwise noted. This information must be maintained in a manner that permits it to be accessible within a reasonable period of time. It is the Company's policy to retain all required Program documentation including reporting, record keeping, and transaction records for at least five (5) years. The CO is responsible for ensuring that all applicable records are maintained securely.

Type of Record	Specific Information	Minimum Period
BSA Records	▪ Customers' Information including verification methods, results, and supporting documentation and Maintenance records related to changes in customer's information ▪ Identifications obtained ▪ Transaction Monitoring records ▪ UAR Records and supporting documentation. ▪ Incident Report escalations to CRB and supporting documentation. ▪ Decisions not to escalate unusual activity to CRB and supporting documentation.	5 Years
OFAC	● OFAC screening records and OFAC Reports including Annual Reports of Blocked Property, Reports of Blocked Transactions and Reports of Rejected Transactions. ● Incident Report escalations to CRB of true matches	5 Years
Information Sharing 314(a) Program	● FinCEN lists and respective reporting	5 Years
Government authorities' requests for information (i.e. Subpoenas) and supporting documentation	▪ Reponses to requests from federal authorities	Permanent

7. Employee Compliance Statement

Failure to comply with this Policy may subject an employee to a range of disciplinary actions, up to and including termination.

8. Board/Senior Manager Approval

The Board and Senior Management of Wishes approves this BSA/AML/OFAC Compliance Program and the AML & OFAC Risk Assessment. These are reasonably designed to achieve ongoing compliance with the requirements of the BSA and OFAC and the implementing regulations under these laws.

This approval is indicated by the signature(s) below:

Signature/Title Date_____

Signature/Title Date_____

Appendix A - Unusual Activity Report Form

The following form can be used to refer unusual activity to the AML Compliance Officer.

Unusual Activity Report

Unusual Financial Observation Report Mechanism*

Date: Month, Day, Year

Reporter's Name and Email Address: name@Company.com

To: [CompanyX] Compliance Officer

Subject: Report of unusual activity

What: Please describe your observation and why it is unusual.

Who: Please list the involved Users or Customers and counterparties and identify which are suspects or victims.

Where: Please identify where the activity is taking place include which platforms and other areas the activity appears to be taking place (e.g., [CompanyX] and BankX and CountryX).

Why: Why do you think the suspects are doing this – to perpetrate fraud, to launder money, to obtain assets, or other.

When: Please state the date range of activity.

How: Please describe how the unusual activity is happening – this may overlap with "What" or other sections of the Unusual Activity Report.

Other details: Any additional details that may help the CO investigate the issue.

*All names and contact information of reporters are kept strictly confidential. No retribution is allowed for reports made in good faith. Anonymous reports are allowed but reporting anonymously may inhibit further investigation.

For use by the CO:

Received date:

Received by:

Result of investigation:

Appendix B – Incident Report Template

INCIDENT REPORT	
Date Reported to CRB:	Name of Bank Partner:
Name and Address of Applicant:	**Account number and Date of Application:**
Dollar Amount Requested or Obtained:	**Amount of Financial Loss:** (If applicable)
Name of Suspect: (If identified)	**Are there any application(s) linked to this application? Yes: ___ or No___** **If yes, have you provided all relevant details for the linked application(s) below?** **Yes: ___ or No___**
PLEASE BE AS DETAILED AS POSSIBLE IN THE NARRATIVE AND ATTACH ALL SUPPORTING DOCUMENTATION.	
Submitted By: **Submitted Date:** **Telephone:**	X _____ Employee Signature
FOR BSA USE ONLY: **Approved By:** **Determination Date:**	X _____ Employee Signature