Sample AML and Sanctions Policy for Fintech Program Managers

The following is not legal advice and should only be used as starting precedents and operational best practices. Each product and company is unique, and you should consult with an experienced lawyer licensed in the relevant jurisdiction(s) to tailor the sample as needed.

Lithic does not assume responsibility for the contents of, or the consequence of using, any version of these documents or any other document found on our website. Lithic's legal team knows many fintech lawyers and we're happy to point Lithic customers to recommendations.

1. This sample policy is operations heavy by default, and portions of it are meant to also serve as basic procedures (e.g., the section on unusual activity reporting). You should feel free to excerpt the more operationally heavy sections into separate procedure documents as you see fit.
2. To help you fill out this sample policy, we've added some footnotes with considerations and yellow-highlighted brackets and prompts for you to fill in information. We've additionally orange-highlighted particular sections that depend on particular companies' practices.
3. All highlighted brackets should be accurately completed and all footnotes should be deleted before the sample is finalized. Consider searching for "[" and "]" to make sure you don't miss any.
4. The terms should be reviewed generally to ensure they accurately reflect your operations and practices (without removing any legally required sections).
5. Finally, delete this instructions page.

Other card program-related legal forms can be found in our documentation.

If you need more suggestions on how to build your compliance program, check out Lithic's Fintech Layer Cake podcast, available on major podcast and video streaming platforms.

* * * *

AML & Sanctions Policy

1. OVERVIEW & PURPOSE

[[your corporate name]], (the "**Company**") maintains a Bank Secrecy Act ("**BSA**"), anti-money laundering ("**AML**") and sanctions program (the "**Program"**). The purpose of this program is to support the Company's banking partners (each a **"Bank"**), and assist with their obligations arising from the the Bank Secrecy Act as amended by the USA PATRIOT Act and the Money Laundering Control Act of 1986 ("**MLCA**"), as well as various sanctions laws and regulations (collectively, the "**AML/CTF Laws**"). The Company also has direct obligations under U.S. sanctions laws, which are addressed in this policy.

The Company takes seriously its and the Banks' responsibility to comply with such laws, and it is committed to facilitating the Bank's compliance with AML/CTF Laws and all parties' compliance with sanctions requirements. Additionally, the Company strives to ensure that the Program is commensurate with the risks posed by the geographic locations, size, nature, and volume of the services provided by the Company to the Bank.

No part of this policy or the Program should be interpreted as contravening or superseding any other legal and regulatory requirements placed upon the Company or its Bank. Protective measures should not impede other legally mandated processes such as records retention or subpoenas. Any conflicts should be submitted immediately to the [[BSA Officer]][1] for further evaluation [[and/or subsequent submission to the Company's General Counsel]][2].

2. SCOPE

All Company employees are required to comply with this policy. The Company and its personnel, from entry level to senior management, are dedicated to BSA/AML/OFAC compliance. Responsibilities are effectively communicated, and compliance is integrated into the Company's overall culture.

All Company employees, including all levels of senior management are required to support the Company's total compliance with this policy order to protect the Banks from being used to facilitate money laundering, terrorist financing, and other criminal activities addressed by the AML/CTF Laws.

3. ROLES & RESPONSIBILITIES

3.1. Executive Risk and Compliance Committee[3]

The Company has established an "**Executive Risk and Compliance Committee**" or "**ERCC**", which is comprised of executive level members representing all areas of the business[4], and it is governed by a committee charter that has been approved by the Company's Board of Directors (the "**Board**"). The Board has delegated the authority to the ERCC, subject to the ERCC's charter, to carry out the purpose, responsibilities, and directives set forth in this policy. The ERCC may delegate the responsibility and authority for the day-to-day administration and oversight of this policy to the Compliance Officer or another qualified Company employee. Notwithstanding the foregoing, the ERCC has the ultimate responsibility and authority to oversee the administration and implementation of this policy.

Generally, the ERCC is responsible for the following:

- Establish and maintain this policy;

---

[1] Most banks will require you to have a board-appointed compliance officer that focuses on the Bank Secrecy Act. However, if you are a small team, you may want to ask your bank if you can have a senior business person or founder serve as the compliance officer. You might also ask your bank if you can wait for board-level governance, especially if your board only has one (or none!) outside board members. The reasoning is that early board members tend to be VC investors, and often do not provide the type of oversight banks envision boards do with more established companies. As a result, there's little difference if your board or if your C-level management acts as oversight for your program.

[2] Delete if you don't have an in-house general counsel, or if you prefer to keep your legal team out of the line for compliance escalations.

[3] We've drafted this section of the policy so that your board delegates oversight back to the company's management. If you prefer not to do this, or if your bank partner will not accept this structure, you can edit this section so these responsibilities fall to your Board of Directors.

[4] Typical areas to include are finance, operations, sales and your founders.

- Ensure adequate resources, tools, and technology are available and appropriately used to carry out the directives of this policy;
- Review and ratify any substantive changes to this policy, no less than annually; and
- Any other responsibilities delegated by the Board.

3.2. BSA Officer

The [[ERCC/Board]] has appointed [[NAME]] as the BSA Officer, and granted them the authority, subject to the supervision of the ERCC, to develop and administer a program that implements the required policies, procedures, monitoring, and training. The BSA Officer is required to:

(i) be knowledgeable of the AML/CTF Laws;

(ii) understand the Company's products, services, customers, and geographic locations;

(iii) understand the potential money laundering and terrorist financing risks associated with those activities; and

(iv) ensure the Program allows the Company to support its partner's obligations under the AML/CTF Laws.

The BSA Officer shall have direct access to the ERCC, which allows for the independence required to administer the Program appropriately. The BSA Officer will work with the ERCC and members of senior management to effectively integrate new products and services into the Company's operations while ensuring compliance with the applicable laws, regulations, and the Program. The ERCC, senior management, and the BSA Officer will ensure that strategic goals do not conflict with the directives of this policy to reduce or eliminate the amount of strategic risk associated with BSA/AML/OFAC compliance.

Given the compliance program may need to be adapted in between meetings of the [[ERCC/Board]], the BSA Officer is authorized to make changes to the Program, including policies and procedures, as necessary. Any such changes should be presented to and ratified by the [[ERCC/Board]] in its next regular meeting.

3.3. Senior Management

Company officers are responsible for the comprehension and implementation of the Program and ensuring employees understanding of their responsibilities. If at any time an employee is uncertain about the proper method of handling a situation or transaction, he or she should refer the issue to their immediate supervisor or contact the BSA Officer for further clarification.

It is also the responsibility of senior management to ensure their respective departments are adhering to the requirements of the Program.

4. PENALTIES

All employees must be aware of the penalties for money laundering. Substantial civil and criminal penalties are provided in the law for failure on the part of the Company or any employee to report or supply information, and for filing a false or fraudulent report, or for an employee to knowingly engage in a financial transaction which involves the proceeds of unlawful activities.

- Individuals, including the Company employees, convicted of aiding and assisting in money laundering face up to 20 years in prison for each money laundering transaction.
- Businesses, including individuals, face fines up to the greater of $500,000 or twice the value of the transaction.
- Any property involved in the transaction or traceable to the proceeds of the criminal activity, including loan collateral, personal property, under certain conditions, entire the Company accounts (even if some of the money in the account is legitimate) may be subject to forfeiture.

The Program is designed to avoid such violations and to assure compliance with the Bank's reporting responsibilities. Under no circumstances shall employees discuss these procedures with customers or provide customers with any advice as to the manner in which reporting requirements can be avoided.

5. BSA PROGRAM

5.1. BSA Risk Assessment[5]

The Company has developed a risk assessment that identifies the Company's BSA/AML and sanctions risk profile. The Company's risk assessment consists of the following:

- Assessment of new products, services, assessment of targeted customers, entities, and geographic locations.
- The risk assessment program is an ongoing process. It is the responsibility of the ERCC and senior management to ensure the Company's risk assessment is updated annually to identify changes in the Company's risk profile (e.g., when new products and services are introduced, existing products and services change, high-risk customers open and close accounts, or the Company expands through mergers and acquisitions).
- The Program was developed based on the risk assessment.
- The risk assessment process takes into consideration all risks highlighted by the regulators and auditors including compliance risk, reputational risk, operational risk, strategic risk, and risk to earnings.

Key risk indicators include:

- Products and Services
- Processes and Procedures
- Transaction volume and size within certain products and services
- Customer base
- Management experience
- Size and complexity of operations

Key performance indicators include:

- Fines or Penalties
- Regulatory Criticism - regulator or auditor
- Internal monitoring findings
- Reporting systems' outputs

5.2. System of Internal Controls

The Company will maintain an effective BSA, AML and OFAC internal control structure, including suspicious activity monitoring and referrals to any Banks.[6]

5.3. Independent Audit

It is the policy of the Company to conduct periodic[7] independent assessments by internal and/or external auditors to ensure complete adherence of the Bank Secrecy Act.[8] Results of this assessment

[5] Companies may want to copy and paste this section to use as a guide for developing your risk assessment. Risk assessments should be tailored to your product and operations, so each company's will be slightly different. Companies with more resources may consider hiring a consultant to help.

[6] For more information about regulator's expectations, you may want to review the Bank Secrecy Act/Anti Money Laundering Examination Manual (www.ffiec.gov/bsa_aml_infobase/default.htm)

[7] Regulated entities are required to conduct an annual independent assessment. Smaller companies are often able to conduct them on a less frequent basis. We suggest you consult with your banking partner or BaaS provider to understand their expectations.

[8] FinCEN regulations allow for a company insider, separate from day-to-day compliance operations, to prepare your independent assessment. Depending on company resources, you might ask your General Counsel or Controller to review the BSA and prepare an assessment of your program. But we generally recommend hiring an external consultant with prior compliance operations and management experience. Lithic can make recommendations upon request.

will be reported to the ERCC and the BSA Officer. Senior management and the BSA Officer will take appropriate action to correct any exceptions found as a result of the assessment.

In addition to annual independent assessments, the Company will maintain an ongoing monitoring program to ensure compliance with the policy and regulation. The BSA Officer is responsible for ongoing monitoring, and material findings will be reported to the ERCC. Corrective action will be tracked and reported in a manner similar to the process followed for the independent assessment. The purpose of ongoing monitoring is to implement a quality control function to ensure day-to-day compliance between full, comprehensive, assessments of the Program.

5.4. Training

It is the Company's policy that all Company personnel receive annual training on the directives of the Program no less than annually. Training will include regulatory requirements and the Company's internal BSA, AML, and OFAC policies, procedures, and processes. New hires will be provided BSA, AML, and OFAC training as set forth in the Company's Compliance Training Policy.

In the event any member of the ERCC is not an employee, that ERCC member will be provided with appropriate BSA training no less than annually. Documentation stating the ERCC Member's name who received the BSA training, the date of the training, and the training materials be retained by the Compliance Officer in accordance with the Company's Compliance Training Policy.

[[Certain key members of personnel will be cross trained in different areas of BSA compliance to ensure continuity in the event the BSA Officer is not able to fulfill duties due to absence or other unforeseen reasons. Daily BSA operations personnel will also be cross trained to ensure that duties can be filled in when persons are out of the office or in the event of staff turnover.]][9]

5.5. Reporting

Reporting to the ERCC will occur on an as needed basis, but no less than quarterly. Such reporting shall include (i) BSA testing and monitoring results, (ii) risk assessment results, (iii) audit and examination findings and recommendations, (iv) policy update recommendations, (v) summary of potentially suspicious activity reports sent to Bank(s), (vi) BSA compliance initiatives, and (vi) other reports requested by the ERCC or provided by the BSA Officer.

6. Internal Controls/Regulatory Requirements

6.1. Anti-Money Laundering Policy and Procedures

The Company's policy is to ensure proper adherence to the provisions and intent of the USA Patriot Act. The Bank Secrecy Act requires the Company to have procedures in place to assist in detecting and preventing money laundering activities and other illegal activities conducted at the Company.

One of the best methods for the Company staff to avoid being an unknowing accomplice to money launderers is to properly identify new customers when their account is opened. [[If a customer refuses or is unable to provide the requested information within 30 days of opening the account, the account is to be closed per the Company policy.]][10]

[[High Risk Customers[11] – One of the key aspects of an effective anti-money laundering program is the identification of customers that may pose a higher risk to the Company and may need additional monitoring. The Company's account opening process must include appropriate controls, procedures,

[9] Cross training may not be feasible for smaller fintech. Companies may consider cutting based on their staffing size.
[10] Companies may consider cutting or softening depending on their size. Smaller companies may have a hard time keeping track of the 30-day timeframe. **Companies offering lending products should note that closing accounts may also trigger adverse action notices under Regulation B** and/or have AML account closing procedures coincide with incomplete application notices.
[11] Many fintech companies will not offer products to high-risk customers. For example, your customers will be U.S. only, and often have primary checking or savings accounts with larger banks. As a result, you may want to cut or tailor this section of your policy.

and processes to identify high risk customers at account opening and/or throughout the account relationship. High-risk customers can be identified or classified based on their types of businesses and by the totality of the circumstances related to the customers' accounts. High Risk customers may include individuals, businesses, exempt customers, foreign customers, or any other type of customer. Many factors will be taken in consideration to determine if an account should be classified as a "high Risk" account and be closely monitored. High-risk account examples include:

- Politically Exposed Persons[12]
- Embassy and Foreign Consulate Accounts
- Professional Service Provider Accounts
- Nonresident aliens and foreign individuals
- Non-Bank Financial Institutions (MSBs)
- Non-Governmental Organization and Charity Accounts
- Business Entities (domestic and foreign)
- Cash Intensive Businesses
- Private Banking Customers

All high-risk accounts will be closely monitored by appropriately trained BSA personnel. Customers that create a higher risk will be placed on a high-risk customer list ("High-Risk List") maintained by the BSA Officer. The list will be updated as necessary. In addition, the line of business the customer is involved in may not necessarily place the account on the High-Risk List. A review will be performed periodically to determine if a customer shall remain under monitoring status.]]

6.2. Detecting Suspicious Activity – Red Flags

It is important to use the appropriate tools and to follow proper procedures to effectively monitor for, detect, and refer unusual activity to the Company's Banks.[13] The Banks may then file suspicious activity reports ("**SAR**") to fight money laundering and other illegal acts. The Company's employees should know the appropriate red flags for illegal activity associated with the products and services offered by the Company that would prompt them to notify their supervisor or the BSA Officer, who will decide whether to send an unusual activity report (**"UAR"**) to the appropriate Banks.

Suspicious financial transactions that the Company must report include those:

- Suspected by the Company to involve funds derived from illicit activities;
- Conducted for the purpose of hiding or disguising funds from illicit activity;
- Suspected of violating the federal money laundering statutes in any way;
- Potentially designed to evade the reporting or recordkeeping requirements of the Bank Secrecy Act; or
- Believed by the Company to be suspicious for any other reason.

If any Company employee becomes aware of or suspects criminal activity by either the Company, its employees, customers, vendors, or any other person or entity, that employee should promptly report the matter to the appropriate person, whether it be the BSA Officer, member of the ERCC, or a member of senior management.

[12] The U.S. does not have formal requirements for screening or monitoring PEPs, nor does the U.S. government maintain PEP lists. However, compliance is often tribalistic in nature and compliance professionals who are unaware of statutory and regulatory requirements will ask fintechs to do PEP screening. If you can, try to side step this. It is busy work and generally does not add any protections to a U.S. AML program.

[13] This section is written for card and banking fintechs, who are often directed to refer unusual activity to bank sponsors vs. filing SARs directly with FinCEN. Payment acceptance companies and those with their own regulatory licenses (e.g., money transmitters) will need to adapt this policy section to reference that the Company is the one filing SARs to FinCEN. Payment acceptance companies are often required by their acquiring banks to "voluntarily" file SARs on suspicious merchant account activity.

6.3. Customer Identification Policy and Procedures

All employees that are involved in opening new accounts and maintaining existing accounts must understand the Company's customer identification program ("**CIP**") requirements. The CIP rules require a financial institution to obtain certain information from potential customers. The information must be verified to form a reasonable belief that the customer's identity is known. The information may be verified using documents presented; this entails using a valid driver's license or passport. Non-documentary verification may also be used; this would be an independent means to confirm the customer's identity.

If it is believed that the customer is providing false information, the incident should be reported to the BSA Officer or immediate supervisor for further action. If the BSA Officer determines that the activity is potentially suspicious, the BSA Officer shall send a UAR to the appropriate Bank(s).

6.3.1. Customer Identification

At a minimum, the Company must obtain the following information to validate the true identity of an individual or entity seeking to open an account:

- Name
- For individuals, date of birth
- Address:
    - Individuals – residential or business street address
        - Individuals who do not have a residential or business street address – an Army Post Office or Fleet Post Office box number, or the residential or business street address of next of kin or another contact individual is acceptable
    - Entities - For persons other than individuals, (i.e., corporations, partnerships, and trusts) principal place of business and, if different, mailing address.
- Identification Number:
    - Individuals
        - U.S. Person[14] - a social security number; or
        - Non-U.S. Person - one or more of the following: A taxpayer identification number; Passport number and country of issuance; Alien identification card number; Number and country of issuance of any other government issued document evidencing nationality or residence and bearing a photograph or similar safeguard.
    - Entities - an Employer Identification Number issued by the IRS.

6.3.2. Verifying Identity / Documentation[15]

The Company shall develop and maintain procedures that will be used to verify applicants' identity prior to opening an account for that customer.

6.3.3. Lack of Verification

When the Company cannot form a reasonable belief that it knows the identity of a customer, the Company will take the following steps:

- Decline to open the account;
- Impose appropriate terms under which a customer may conduct transactions while the Company attempts to verify the customer' identity;

[14] U.S. Person in FinCEN's regulations refers to citizens, who are required to provide their SSN for bank-offered products like cards and demand deposit accounts. For non-citizen customers, see the "Non-U.S. Person" prong below.

[15] We recommend you document your operational workflow in a separate procedure. This can be where you identify your vendors and the steps employees take to use the vendors and action the CIP policy requirements. For more on how to build your KYC operations, check out Lithic's blog.

- Close the account after attempts to verify the customer's identity fail.

The account and the information that the Company has related to opening the account should be referred to the BSA Officer for investigation. The BSA Officer will determine if a UAR needs to be sent to the appropriate Bank(s).

6.3.4. OFAC Screening[16]

Prior to opening an account, all applicants shall be screened against the appropriate lists, but, at minimum, the Specially Designated Nationals (SDN) list provided by the Office of Foreign Assets Control ("**OFAC**") and the Consolidated Sanctions (non-SDN) list (collectively, the "**OFAC Screening**"). The Company shall ensure that it uses the most recent version of the lists when performing OFAC Screening. The Company shall develop and maintain OFAC Screening procedures that set forth the process, the lists in which the customers will be screened against, how to clear false positive alerts, and how alerts that cannot be cleared should be escalated to the BSA Officer. The Compliance department is responsible for reviewing the results. Any alerts that cannot be cleared according to the procedures should be promptly referred to the BSA Officer. The BSA Officer shall document the alert and notify the appropriate Bank(s) immediately.

6.3.5. US PATRIOT Act Notice

The Company will notify new customers of the Bank(s) requirement to verify the customers' identity prior to opening an account. The Company will use the following language to provide notice to customers:

"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 all financial institutions to obtain, verify, and record information that identifies each person who 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."

6.4. [[Beneficial Ownership Requirements for Legal Entity Customers[17]

The Company shall maintain written procedures that are reasonably designed to identify and verify beneficial owners of legal entity customers at account opening.

6.4.1. Certification Regarding Beneficial Owners of the Legal Entity Customer

The Company will obtain a Certification of Beneficial Owner(s) (see Appendix A below) ("**B/O Certification**") from the individual opening a new account on behalf of a legal entity customer. Legal entity includes a corporation, limited liability company (LLC), or other entity that is created by a filing of a public document with a Secretary of State or similar office, a general partnership, and any similar business entity formed in the United States or a foreign country. Legal entity does not include sole proprietorships, unincorporated associations, or natural persons opening accounts on their own behalf.

6.4.2. Information Collected

The Company must collect, at a minimum, the name, address, date of birth, and social security number (or passport number or other similar information, in the case of foreign persons) about the following individuals (see Section 6.3 above):

[16] You might consider wrapping your OFAC screening procedure into your KYC procedures, as the same staff can be used to tackle both operational needs at the same time.
[17] Companies that only have consumer customers can delete this section. Beneficial ownership requirements only apply to fintech with B2B offerings.

- Each individual who, directly or indirectly, owns 25 percent or more of the equity interest of the legal entity customer.
- Each individual who has significant authority to control, manage or direct the legal entity customer. Examples include: a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer. Even without a title, any individual who performs similar functions will be considered to have control.

The number of individuals that will be included under this requirement may be up to four ownership interest beneficial owners and one person with control. The Company will collect identifying information from other signers or members of a legal entity if it is necessary to meet customer due diligence requirements. The Company may also ask to see a copy of a valid driver's license or other valid identifying document for each beneficial owner listed on the form.

6.4.3. Beneficial Ownership Records to be Retained

At minimum the Company shall retain, for the beneficial ownership requirement, the following:

- For identification, any identifying information obtained, including, without limitation, the B/O Certification; and
- For verification, a description of any document relied on (noting the type, any identification number, place of issuance and, if any, date of issuance and expiration), or the results from any non-documentary methods used, including OFAC Screening results.

6.4.4. Exemptions and Exclusions from the Definition of Legal Entity Customer

The requirements to identify and verify do not extend to beneficial owners who are exempted from the definition of a "legal entity customer". Exclusions from the definition of a legal entity customer include:

- Financial institutions regulated by a Federal functional regulator or a bank regulated by a state bank regulator;
- Certain exempt persons for purposes of the currency transactions reporting obligations:
  - A department or agency of the United States, of any State, or of any political subdivision of a State; or any entity established under the laws of the United States, or any State, or of any political subdivision of any State, or under an interstate compact;
  - Any entity (other than a bank) whose common stock or analogous equity interests are listed on the New York, American, or NASDAQ stock exchange;
  - Any entity organized under the laws of the United States or of any State at least 51% of whose common stock or analogous equity interests are held by a listed entity;t
- Issuers of securities registered under section 12 of the Securities Exchange Act of 1934 (SEA) or that is required to file reports under 15(d) of that Act;
- An investment company, as defined in section 3 of the Investment Company Act of 1940, registered with the U.S. Securities and Exchange Commission (SEC);
- An SEC-registered investment adviser, as defined in section 202(a)(11) of the Investment Advisers Act of 1940;
- An exchange or clearing agency, as defined in section 3 of the SEA, registered under section 6 or 17A of that Act;
- Any other entity registered with the SEC under the SEA;

- A registered entity, commodity pool operator, commodity trading advisor, retail foreign exchange dealer, swap dealer, or major swap participant, defined in section 1a of the Commodity Exchange Act, registered with the Commodity Futures Trading Commission;
- A public accounting firm registered under section 102 of the Sarbanes-Oxley Act.

Additional regulated entities:

- A bank holding company, as defined in section 2 of Bank Holding Company Act of 1956 (12 USC 1841) or savings and loan holding company, as defined in section 10(n) of the Home Owners' Loan Act (12 USC 1467a(n));
- A pooled investment vehicle operated or advised by a financial institution excluded from the definition of legal entity customer under the final CDD rule;
- An insurance company regulated by a State;
- A financial market utility designated by the Financial Stability Oversight Council under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010;

Excluded Foreign Entities:

- A foreign financial institution established in a jurisdiction where the regulator of such institution maintains beneficial ownership information regarding such institution;
- A non-U.S. governmental department, agency or political subdivision that engages only in governmental rather than commercial activities; and
- Any legal entity only to the extent that it opens a private banking account subject to 31 CFR 1010.620.

6.4.5. Exemptions and limitations on exemptions

Subject to certain limitations, the Company is not required to identify and verify the identity of the beneficial owner(s) of a legal entity customer when the customer opens any of the following four categories of accounts:

- accounts established at the point-of-sale to provide credit products, solely for the purchase of retail goods and/or services at these retailers, up to a limit of $50,000;
- accounts established to finance the purchase of postage and for which payments are remitted directly by the financial institution to the provider of the postage products;
- accounts established to finance insurance premiums and for which payments are remitted directly by the financial institution to the insurance provider or broker; and
- accounts established to finance the purchase or lease of equipment and for which payments are remitted directly by the financial institution to the vendor or lessor of this equipment.

These exemptions will not apply under either of the following two circumstances:

- If the accounts are transaction accounts through which a legal entity customer can make payments to, or receive payments from, third parties.
- If there is the possibility of a cash refund for accounts opened to finance purchase of postage, insurance premium, or equipment leasing. If there's the possibility of a cash refund, the financial institution must identify and verify the identity of the beneficial owner(s) either at the initial remittance, or at the time such refund occurs.]]

6.5. Suspicious Activity Reporting[18]

If any Company employee becomes aware of or suspects criminal activity by either customers or Company employees, the Company employee should promptly report the matter to the BSA Officer, or a member of the ERCC. The BSA Officer will promptly investigate the matter to determine whether to refer it to the appropriate Bank(s). The investigation will be based on a review of the facts, as submitted by the employee, and a discussion with company officers in charge of the impacted areas.

If the circumstances warrant referring the matter to the applicable Bank(s), the BSA Officer will escalate a UAR to the appropriate Bank(s). It is the Banks' sole responsibility to determine if the UAR warrants the filing of a suspicious activity report ("**SAR**") with the Financial Crimes Enforcement Network ("**FinCEN**").

The BSA Officer, General Counsel, and any other employee aware of the matter will keep the information confidential. In addition, the Company will not place the referral in the personnel files of any Company directors, officers, or employees who might be party to the suspicious activity.

If the Company determines it necessary to report a suspected illegal activity to local law enforcement, the BSA Officer or ERCC will carefully review all known facts. The Company will refer the activity only when there is a reasonable basis for believing that a specific crime has occurred, is occurring, or may occur. The Company will notify the appropriate Bank(s) to determine whether to file such referrals with local agencies, other than the Banks' federal regulator, subject to the provisions of the Right to Financial Privacy Act.

"Known" or "suspected" illegal activity means any matter for which there is a reasonable basis to believe that a Federal criminal statute has or is suspected to have been violated, or an attempt is occurring, may occur, or had occurred, and there is a reasonable basis to believe that a financial institution was an actual or potential victim of the known or suspected criminal activity or was used to facilitate the criminal activity. The Company will refer suspicious activity to the appropriate Bank(s) in the following situations:

- The Company detects a known or suspected violation of a Federal criminal law and has a substantial basis to believe that one of its directors, officers, employees, agents, or other institution-affiliated parties committed or aided in the commission of the violation, regardless of the amount;
- The Company detects a known or suspected violation of Federal criminal law involving or aggregating to $5,000[19] or more (before reimbursement or recovery) and has substantial basis for identifying a possible suspect or group of suspects;
- The Company detects a known or suspected violation of Federal criminal law involving or aggregating to $25,000 or more (before reimbursement or recovery) and has no substantial basis for identifying a possible suspect or group of suspects; or
- The Company detects transactions aggregating to $5,000 or more that involves potential money laundering or violates the BSA. "Any transaction" means (i) a deposit withdrawal, (ii) a transfer between accounts, (iii) an exchange of currency; (iv) a loan; (v) an extension of credit; (vi) a purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security; (vii) or any other payment, transfer, or delivery by, through, or to a financial institution (by whatever means effected), conducted or attempted by, at, or through the Company and involving or aggregating to $5,000 or more in funds or other assets, if the Company knows, suspects, or has reason to suspect that:

[18] This section is operationally heavy and might be better placed into a separate procedure. If you are a smaller company, we suggest keeping it in this policy so your operational staff only have to look for one document when actioning cases.
[19] We recommend you consult with your BaaS sponsor or bank partner to confirm the thresholds they are looking for. MSBs and other fintechs that are directly regulated are likely to have lower limits due to anachronistic quirks in the BSA.

- The transaction involves funds derived from illegal activities or is intended or conducted to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any law or regulation or to avoid any transaction reporting requirement under Federal law;
- The transaction is designed to evade any regulations promulgated under the BSA. This includes an attempt at structuring the transaction; or
- The transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the Company knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

The BSA Officer will send UARs to the appropriate Bank(s) no later than 15 calendar days after the date of initial detection of an act described above (the relevant Bank(s) would then have 15 calendar days to determine whether to file a SAR). If the Company did not identify a suspect on the date that it detected an act triggering the filing, the relevant Bank(s) may delay filing a SAR for an additional 30 calendar days after the identification of a suspect. In no case will the Company delay reporting more than 60 calendar days after the date it detects a known or suspected violation warranting a UAR referral to the appropriate Bank(s). If situations involving violations require immediate attention, however, such as when a reportable violation is ongoing, the Company will immediately notify by telephone, or other expeditious means, the appropriate Bank(s) so the respective Bank(s) can determine whether notifying the appropriate law enforcement agency is warranted—in addition to filing a timely SAR report.

The following represents suspicious activity that should be reported to the appropriate Bank(s) through a UAR:[20]

- Any BSA violation, such as structuring or money laundering
- Bribery or gratuity
- Check fraud
- Commercial loan fraud
- Computer intrusion
- Consumer loan fraud
- Counterfeit check
- Counterfeit credit or debit card
- Counterfeit instrument
- Credit card fraud
- Debit card fraud
- Embezzlement
- False statement
- Identity theft
- Misuse of position or self-dealing
- Mysterious disappearance
- Terrorist financing
- Wire transfer fraud

6.6. Currency Transaction Reporting[21]

Currency Transaction Reporting ("CTR") requirements may be triggered based on ATM deposits, withdrawals and point-of-sale cash back transactions. [[The Company maintains appropriate controls so that customers are not able to obtain cash at or over the reporting limits via its products.]] [[The

[20] Fintechs may want to further tailor this list to account for their product offerings. For example, Privacy.com does not offer checks, so we would internally delete the reference to check fraud.
[21] Companies should tailor or cut this program depending on whether customers can deposit or obtain cash

Company maintains reporting so it can alert the relevant Banks about customers that require CTRs. Any such transactions are promptly reported to the relevant Bank, so that the Bank may complete a CTR to the appropriate authorities.]]

7. RECORD RETENTION

The Company will retain all records obtained and maintained in connection with the BSA and any related regulations for 5 years after the account is closed, or for a time specified in the BSA.

8. EXCEPTIONS, QUESTIONS, & INTERPRETATIONS OF THIS POLICY

Requests for exceptions to this policy may be submitted to the Company's BSA Officer, who may advise on, grant the request, or forward it to the ERCC.

Any questions regarding interpretation of this policy should be directed to the Company's Compliance department.

9. APPROVAL, REVIEW, & VERSION HISTORY[22]

Version	Changes By	Revision Notations	Date Reviewed
1		Policy drafted; effective date	

[22] It's an expected practice for companies to log version history of their AML policies. We've included a table here for your convenience.

Appendix A[23]

CERTIFICATION REGARDING BENEFICIAL OWNERS OF LEGAL ENTITY CUSTOMERS[24]

I. GENERAL INSTRUCTIONS

What is this form?

To help the government fight financial crime, Federal regulation requires certain financial institutions to obtain, verify, and record information about the beneficial owners of legal entity customers. Legal entities can be abused to disguise involvement in terrorist financing, money laundering, tax evasion, corruption, fraud, and other financial crimes. Requiring the disclosure of key individuals who own or control a legal entity (i.e., the beneficial owners) helps law enforcement investigate and prosecute these crimes.

Who has to complete this form?

This form must be completed by the person opening a new account on behalf of a legal entity with any of the following U.S. financial institutions: (i) a bank or credit union; (ii) a broker or dealer in securities; (iii) a mutual fund; (iv) a futures commission merchant; or (v) an introducing broker in commodities.

For the purposes of this form, a **legal entity** includes a corporation, limited liability company, or other entity that is created by a filing of a public document with a Secretary of State or similar office, a general partnership, and any similar business entity formed in the United States or a foreign country. **Legal entity** does not include sole proprietorships, unincorporated associations, or natural persons opening accounts on their own behalf.

What information do I have to provide?

This form requires you to provide the name, address, date of birth and Social Security number (or passport number or other similar information, in the case of Non-U.S.Persons) for the following individuals (i.e., the **beneficial owners**):

i. Each individual, if any, who owns, directly or indirectly, 25 percent or more of the equity interests of the legal entity customer (e.g., each natural person that owns 25 percent or more of the shares of a corporation); **and**

ii. An individual with significant responsibility for managing the legal entity customer (e.g., a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer).

The number of individuals that satisfy this definition of "beneficial owner" may vary. Under section (i), depending on the factual circumstances, up to four individuals (but as few as zero) may need to be identified. Regardless of the number of individuals identified under section (i), you must provide the identifying information of one individual under section (ii). It is possible that in some circumstances the same individual might be identified under both sections (e.g., the President of Acme, Inc. who also holds a 30% equity interest). Thus, a completed form will contain the identifying information of at least one individual (under section (ii)), and up to five individuals (i.e., one individual under section (ii) and four 25 percent equity holders under section (i)).

The financial institution may also ask to see a copy of a driver's license or other identifying document for each beneficial owner listed on this form.

[23] Cut if only offering consumer products. Beneficial Ownership screening only applies to privately held companies.
[24] This certification is a model form from FinCEN. Companies in the B2B space are generally free to adapt it and incorporate elements of the form into their onboarding flows. You'll want to have your bank partner approve your onboarding funnel designs before starting engineering work, to ensure they're willing to accept the way you've implemented the beneficial ownership information collection. If you and your bank partner are in disagreement on this topic, you may want to consult experienced fintech or AML counsel.

CERTIFICATION OF BENEFICIAL OWNER(S)

Persons opening an account on behalf of a Legal Entity must provide the following information:

a. Name and Title of Natural Person opening account: _____

b. Name, Type, and Address of Legal Entity for which the account is being opened: _____

c. The following information for **each** individual***,** if any, who directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise, owns 25% or more of the equity interests of the Legal Entity listed above:

Name	*Date of Birth*	*Address (Residential or Business Street Address)*	*For U.S. Persons: Social Security #*	*For Non-U.S. Persons: Social Security number, Passport number and Country of Issuance, or other similar identification number*[1]	*% of Ownership*

(If no individual meets this definition, please enter "Not Applicable")

d. The following information for **one** individual with significant responsibility for managing the Legal Entity listed above, such as:

☐ An executive officer or senior manager (e.g., Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, Treasurer); or

☐ Any other individual who regularly performs similar functions.

(If appropriate, an individual listed under section (c) above may also be listed in this section (d)).

Name/Title	*Date of Birth*	*Address (Residential or Business Street Address)*	*For U.S. Persons: Social Security #*	*For Non-U.S. Persons: Social Security number, Passport number and Country of Issuance, or other similar identification number*[1]

I,_____ (*name of natural person opening account*), hereby certify, to the best of my knowledge, that the information provided above is complete and correct.

Signature:_____ Date: _____

Legal Entity Identifier _____(Optional)

_____

[1] In lieu of a passport number, Non-U.S. persons may also provide a Social Security Number, an alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

BENEFICIAL OWNER VERIFICATION

Beneficial Owner #1

Driver's License Number, or Other Identifying Document: _____

State (or Country) of Issuance: _____; Issue Date: _____; Expire Date: _____

Secondary Form of Identification: _____

☐ **OFAC Check**; Comments (if applicable): _____

Beneficial Owner #2

Driver's License Number, or Other Identifying Document: _____

State (or Country) of Issuance: _____; Issue Date: _____; Expire Date: _____

Secondary Form of Identification: _____

☐ **OFAC Check**; Comments (if applicable): _____

Beneficial Owner #3

Driver's License Number, or Other Identifying Document: _____

State (or Country) of Issuance: _____; Issue Date: _____; Expire Date: _____

Secondary Form of Identification: _____

☐ **OFAC Check**; Comments (if applicable): _____

Beneficial Owner #4

Driver's License Number, or Other Identifying Document: _____

State (or Country) of Issuance: _____; Issue Date: _____; Expire Date: _____

Secondary Form of Identification: _____

☐ **OFAC Check**; Comments (if applicable): _____

Individual with Control

Driver's License Number, or Other Identifying Document: _____

State (or Country) of Issuance: _____; Issue Date: _____; Expire Date: _____

Secondary Form of Identification: _____

☐ **OFAC Check**; Comments (if applicable): _____

Comments:

_____

_____

_____

_____

_____

_____