CHAINCE SECURITIES, LLC

ANTI-MONEY LAUNDERING (AML) PROGRAM

JULY 2025

[The Anti-Money Laundering Act of 2020: https://www.fincen.gov/anti-money-laundering-act-2020; FinCEN First National AML/CFT Priorities: https://www.fincen.gov/news/news-releases/fincen-issues-first-national-amlcft-priorities-and-accompanying-statements; FINRA Rule 3310; FINRA Regulatory Notice 21-36; NASD Notice to Members 02-21; FINRA web site AML page http://www.finra.org/RulesRegulation/IssueCenter/Anti-MoneyLaundering/index.htm; FINRA 2022 Report: https://www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program; Bank Secrecy Act; Office of Foreign Assets Control (OFAC) web site http://www.treas.gov/offices/enforcement/ofac; SEC web site AML page http://www.sec.gov/spotlight/moneylaundering.htm; SEC Anti-Money Laundering (AML) Source Tool: http://www.sec.gov/about/offices/ocie/amlsourcetool.htm; NASDAQ Rule 3011; SIFMA Anti-Money Laundering Resource Center: http://www.sifma.org/issues/legal-compliance-and-administration/anti-money-laundering-compliance/resources/; Regulatory Joint Statement on Digital Assets: https://www.sec.gov/news/public-statement/cftc-fincen-secjointstatementdigitalassets]

7.1 Introduction

This chapter explains CHAINCE SECURITIES LLC's Anti-Money Laundering (AML) Program. An explanation of money laundering and guidance for all employees to detect money laundering is included in the chapter *GENERAL EMPLOYEE POLICIES* in the section *Money Laundering*.

Money laundering laws and rules include digital assets regardless of whether they meet the definition of a security or commodity. These policies will be updated and appropriate procedures and action effected when new rules are adopted.

7.1.1 Definitions

[Bank Secrecy Act 31 CFR Chapter X Part 1023.100 Subpart A]

Monetary instruments:

1. Currency;
2. Traveler's checks in any form;
3. All negotiable instruments (including personal checks, business checks, official bank checks, cashier's checks, third-party checks, promissory notes (as that term is defined in the Uniform Commercial Code), and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee (for the purposes of Section 103.23), or otherwise in such form that title thereto passes upon delivery;
4. Incomplete instruments (including personal checks, business checks, official bank checks, cashier's checks, third-party checks, promissory notes (as that term is defined in the Uniform Commercial Code), and money orders) signed but with the payee's name omitted; and
5. Securities or stock in bearer form or otherwise in such form that title thereto passes upon delivery.
6. Monetary instruments do not include warehouse receipts or bills of lading.

Digital assets: Instruments that may qualify under applicable U.S. laws as securities, commodities, or security- or commodity-based instruments such as futures contracts or swaps. There is no uniform legal definition, and digital assets have different labels such as cryptocurrencies, digital tokens, digital currencies, virtual assets, and initial coin offerings.

7.2 AML Compliance Officer

[FINRA Rule 3310(d) and 3310.02]

Responsibility	• AML Compliance Officer
Resources	• Computer reports and other programs developed for the Program • Internal audits or outside audits of the Program • Regulations and rules for broker-dealer anti-money laundering programs • OFAC web site • Other sites and resources available

Frequency	• Annual - review policies and procedures and business lines
	• Annual and more frequently, as needed - develop and schedule AML education for employees
	• As needed - update program and provide revisions to senior management for review and approval
	• As required: revise delegation of AML responsibilities
	• Annually - review AML contact information on file with FINRA
	• Ongoing - review new regulations
	• Ongoing - monitor activity including:
	  ○ activity in micro-cap and penny stocks, particularly when transacted through omnibus accounts maintained for foreign financial institutions
	  ○ accounts for foreign customers that appear to have been opened solely to trade in IPOs and post-IPO trading in shares issued by companies based in restricted markets such as China
	  ○ due diligence with respect to SPAC sponsors and the appropriateness of disclosures in SPAC IPOs

Action	• Develop and update CHAINCE SECURITIES LLC's anti-money laundering program • Obtain senior management approval for the program and any changes to the program • Identify delegation of AML responsibilities among persons/departments and escalation of red flags to those persons • Monitor (or designate monitoring) the activity of CHAINCE , its associated persons, and customers to reasonably detect and prevent money laundering activities • Consider AML implications of new business lines and products • Develop AML education program for employees and schedule training • File required reports • Retain required records • Provide contact information to FINRA and update contact information if necessary • Review policies and procedures and new areas of business and update AML Program as needed
Record	• Designation of AML Compliance Officer • Delegation of AML responsibilities and escalation procedures

	• Current and past copies of anti-money laundering program with senior management approval • Records of AML education including who attended, date of training, and material covered • Reports filed • Reviews of the AML Program • Other records to be retained, as listed in the Program

CHAINCE SECURITIES LLChas designated an AML Compliance Officer who is responsible for developing policies, procedures, and internal controls reasonably designed to achieve compliance with AML rules and regulations.

7.3 Independent Testing

[FINRA Rule 3310.01]

Responsibility	• AML Compliance Officer
Resources	• Policies and procedures • Independent testing results
Frequency	• Annual - schedule, conduct, and follow up testing (unless the firm qualifies for testing every two years)
Action	• Identify person(s) to conduct testing • Conduct testing • Report results to CEO in annual compliance report • Revise policies and procedures as necessary • Conduct follow-up to determine corrective action has been taken
Record	• Independent testing results including who conducted and dates of review • Report to CEO • Record of changes to policies and procedures resulting from testing • Record of follow-up actions

The AML Compliance Officer will arrange for annual (on a calendar-year basis) independent testing of CHAINCE SECURITIES LLC's policies and procedures regarding money laundering and the effectiveness of the program. The review is conducted by member personnel or a qualified outside party. More frequent reviews will be conducted, if necessary, as determined by the AML Compliance Officer.

Independent testing must be conducted by someone with a working knowledge of the Bank Secrecy Act and implementing regulation requirements. Independent testing may not be conducted by:

- A person who performs the functions being tested;
- The designated AML Compliance Officer; or
- A person who reports to a person described in the above two items.

7.4 Training Program

All employees are provided with CHAINCE SECURITIES LLC's Money Laundering policy when they are hired. The policy is included in the chapter *GENERAL EMPLOYEE POLICIES*.

In addition, ongoing education will include the firm element continuing education program, periodic circulation of CHAINCE SECURITIES LLC's policy, and other educational programs directed at specific employees such as operations personnel. Training will be delivered at least annually by video, intranet systems, in-person lectures, and other methods including third parties who deliver AML training.

Training will include the following, as well as other subjects identified by the AML Compliance Officer:

- How to identify red flags and signs of money laundering
- What to do once the risk is identified (how, when and to whom to escalate unusual customer activity or other red flags)
- Employees' roles in CHAINCE SECURITIES LLC's compliance efforts and how to perform them
- CHAINCE SECURITIES LLC's record retention policy
- Disciplinary consequences (including civil and criminal penalties) for non-compliance

The AML Compliance Officer is responsible for retaining records of employees trained, the dates of training, and the subjects included in training.

7.5 Bank Secrecy Act (BSA) Filings

[BSA E-Filing System: http://bsaefiling.fincen.treas.gov/main.html; FinCEN web site for Adobe forms: https://www.fincen.gov/legal-reference-bank-secrecy-act-forms-and-filing-requirements]

The BSA E-Filing System web site provides a list of forms supported for electronic filing, and include the following (refer to the web site for the most current list of forms):

- Currency Transaction Report (FinCEN Form 112)
- Designation of Exempt Person (FinCEN Form 110)
- Suspicious Activity Report by the Securities and Futures Industries (FinCEN Form 111)
- Report of Foreign Bank and Financial Accounts (Form 114)

7.6 OFAC List And Blocked Property

[Dept. of Treasury, various statutes; OFAC web site http://www.treas.gov/offices/enforcement/ofac/; OFAC sanctions list search: https://sanctionssearch.ofac.treas.gov/; Sanctions search list FAQs: https://home.treasury.gov/policy-issues/financial-sanctions/faqs/search?faq-search=&field_topic_target_id=1636; Foreign Assets Control Regulations For The Securities Industry: https://www.treasury.gov/resource-center/sanctions/Documents/facbk.pdf]

The property of sanctioned persons or entities will be blocked and transfer of assets prevented for persons or entities included on the OFAC list of blocked persons or entities. In addition, securities issued by sanctioned countries and other sanctioned issuers will be blocked. OFAC (the Office of Foreign Assets Control of the U.S. Treasury Department) enforces the sanctions and publishes, on its web site (*www.treas.gov/ofac*), information about sanctions. The information is divided into several categories including:

- Persons and entities subject to sanctions, *Special Designated Nationals and Blocked Persons* (SDN list)
- Persons and entities engaged in drug trafficking, *Specially Designated Narcotics Traffickers* (SDNTKs)
- Terrorists and terrorist organizations, *Specially Designated Terrorists* (SDTs)

- Countries, governments, and other entities subject to sanctions

OFAC requirements apply to all persons and entities under U.S. jurisdiction, including foreign branches of U.S. institutions. This also includes foreign institutions that operate in the U.S.

The term "OFAC list" in this section includes all sanctions published by OFAC even though the information may appear in multiple lists. CHAINCE SECURITIES LLC relies on its AML support vendor, SEON,to monitor OFAC and other sanctions lists and the firm will block accounts and securities where appropriate and to file necessary reports.

7.6.1 Prohibited Transactions

CHAINCE SECURITIES LLC is prohibited from conducting transactions in any account on behalf of a sanctioned party or in certain blocked securities. Securities and funds may not be released and securities transactions may not be executed. Securities and funds may be deposited to a blocked account, but no securities or funds will be released until the account is no longer subject to sanctions. Funds or securities may not be transferred to sanctioned parties.

Because transactions are prohibited, all open orders for a blocked account will be cancelled.

7.6.2 Risk Factors

[https://www.treasury.gov/resource-center/sanctions/Documents/facbk.pdf]

Following are risk factors identified by OFAC that may warrant a heightened level of scrutiny.

International transactions, including wire transfers:

a) High number of international transactions, cross-border transactions, or investments in a foreign investment fund or on a foreign exchange;

b) Presence of overseas branches or multiple correspondent accounts with foreign financial institutions, including correspondent accounts subject to enhanced due diligence under Section 312 of the USA PATRIOT Act.

Foreign customers/accounts:

a) A large, fluctuating client base across a number of foreign jurisdictions involving a large number of security transactions;

b) Customers located in or having accounts in high-risk jurisdictions, such as countries found to be of "primary money laundering concern" pursuant to Section 311 of the USA PATRIOT Act;

c) Customers located in or having accounts in countries that are havens for money laundering or are inadequately regulated, including countries identified by the Financial Action Task Force as maintaining an inadequate AML/CFT regime;

d) Customers located in or having accounts in countries where local laws, regulations, or provisions (such as privacy laws) prevent or limit the collection of client identification information;

e) Customers located in an offshore financial center as identified by the U.S. Department of State;

f) Accounts for senior political or government officials ("politically exposed persons") of a foreign government;

g) Accounts of closely held corporations;

h) Accounts for unregistered or unregulated investment vehicles;

i) Accounts for non-resident aliens;

j) Accounts maintained at an offshore bank.

Foreign broker-dealers who are not subject to OFAC regulations:

a) Lack of information regarding beneficial owners of securities; and

b) Foreign broker-dealers that act as introducing brokers.

Risks of Investments in Foreign Securities:

Practical exposure increases when investing in a foreign investment fund or foreign exchange, because of the risk that the securities are issued by a sanctioned country or party or otherwise in violation of OFAC sanctions, *e.g.,* securities of an issuer that provides financing for a sanctions target. Other risk factors include:

a) Cross-border settlements involving the interaction of different settlement systems and laws in different countries;

b) Foreign securities that may be more prone to misidentification in the course of a trade, *e.g.,* similar names between two foreign issuers;

c) Foreign companies that issue shares in bearer form.

Personal Investment Corporations or Personal Holding Companies:

Beneficial ownership by a non-U.S. person that maintains a private banking account with a U.S. financial institution.

Very High Net Worth Institutional Accounts, Hedge Funds, Funds of Hedge Funds and Other Alternative Investment Funds (Private Equity, Venture Capital Funds) and Intermediary Relationships:

a) Lack of transparency regarding securities/investments and beneficial owners;

b) U.S. hedge fund with an offshore related fund where beneficial owners are offshore investors; and

c) Subscription funds that originate from or are routed through an account maintained at an offshore bank, or a bank organized or chartered in an inadequately supervised and poorly regulated jurisdiction, or a foreign shell bank.

Omnibus Accounts/Use of Intermediaries:

a) Potential for the use of code names to invest funds in the United States on behalf of sanctions targets, concealing the identities of the beneficial owners;

b) Accounts for intermediaries held in street name that trade on behalf of third parties, such as other broker-dealers, banks, and mutual funds; and

c) Cross-border trades executed for unregulated investment vehicles, *e.g.,* hedge funds, private equity funds, and other private pools of capital.

Third-Party Introduced Business:

Business introduced by an overseas bank, affiliate, or other investor based in high risk or inadequately regulated countries.

Confidential Accounts:

Private banking accounts established or maintained for non-U.S. persons or services, including financial and related services, to wealthy clients who use offshore accounts for tax avoidance purposes.

7.6.3 Blocking Requirements

Blocking requirements are generally triggered under the following circumstances:

- An account is opened for someone included on an OFAC list.
- The owner of an existing account is added to an OFAC list.
- A security is identified in a customer account where the issuer is the subject of sanctions.
- A request is made by a customer to pay or transfer funds or securities to a blocked person or entity.

While title to blocked property remains with the blocked person or entity, transactions affecting the property (including transfer of the assets) cannot be made without authorization from OFAC. Debits to blocked accounts are prohibited, but credits may be accepted. Cash balances in blocked accounts must earn interest at commercially reasonable rates. Blocked securities may not be paid, withdrawn, transferred (even in book transfer), endorsed, guaranteed, or otherwise dealt in.

It is not a violation to open an account for a blocked person. The violation occurs when the account is not frozen and assets are allowed to transfer out of the account. In addition, OFAC restrictions may vary depending on the blocked person or entity; details of blocking requirements are explained on the OFAC web site.

7.6.4 Monitoring Procedures

Monitoring is to be conducted as follows:

- Operations personnel and the firm’s AML support vendor, SEON, should be aware of the countries included on the OFAC list, to watch for new accounts to be opened for or requests to transfer funds or securities to residents of those countries.
- CHAINCE SECURITIES LLC (and its a clearing firm) has procedures to monitor new accounts, existing accounts, security positions, and potential disbursements of funds or securities.

7.6.5 Other Requests To Monitor Accounts

Regulators or law enforcement agencies may ask the industry's cooperation in identifying accounts for individuals or entities under investigation or suspected of criminal activities.

The AML Compliance Officer is responsible for responding to such requests; providing the necessary information; and retaining records of requests, reviews conducted pursuant to requests, and information provided to authorities.

7.6.6 Bank Affirmations

Banks are obligated to block property and comply with sanction requirements. Where CHAINCE SECURITIES LLChas bank accounts used to disburse funds to customers or to third parties at the

customer's request, CHAINCE SECURITIES LLCwill obtain a letter of affirmation that the bank has procedures in place to comply with federal requirements to block property.

7.6.7 Blocking Property And Disbursements

Any blocked account will not be permitted to engage in transactions other than the acceptance of deposits of funds or securities. Open orders of blocked accounts will be cancelled.

Disbursements of funds or securities may not be made to sanctioned parties. CHAINCE SECURITIES LLC(and its clearing firm) is responsible for monitoring requests for disbursements.

7.6.8 Reporting Blocked Property And Legal Actions

When an account or disbursement is blocked or a blocked security is identified, OFAC will be notified within 10 days of blocking. If CHAINCE SECURITIES LLC blocks an account or security, it will file the necessary report with OFAC. Reports filed by CHAINCE SECURITIES LLC will be retained in a file of blocked accounts or securities. Information to be reported includes:

- Owner or account party
- Property and property location
- Existing or new account number
- Actual or estimated value
- Date property was blocked
- Copy of the payment or transfer instructions
- Confirmation that funds have been deposited in a blocked account that is identified as blocked
- Name and phone number of contact person at CHAINCE

For rejected disbursements, the following information is to be filed:

- Name and address of the transferee financial institution
- Date and amount of the transfer
- Copy of the payment or transfer instructions
- Basis for rejection
- Name and phone number of contact person at CHAINCE

7.6.8.1 Annual Report Of Blocked Property

On an annual basis by September 30th, Form TDF 90-22.50 will be filed with OFAC for any blocked property held as of June 30.

7.6.8.2 Legal Actions Involving Blocked Property

U.S. persons involved in litigation, arbitration, or other binding alternative dispute resolution proceedings regarding blocked property must provide notice to OFAC. Copies of all documents associated with the proceedings will be submitted by Compliance to the OFAC Chief Counsel at the U.S. Treasury Department within 10 days of their filing. In addition, information about the scheduling of any hearing or status conference will be faxed to the Chief Counsel.

7.6.9 Role Of Operations Personnel

Operations personnel are an important first line of defense in preventing transactions with sanctioned parties. The following guidance is provided to assist Operations personnel in identifying blocked parties. Any questioned accounts or transactions should be referred to Compliance.

- Be familiar with countries included on the OFAC list. These are countries considered potential havens for money laundering, drug trafficking, or terrorist activities. Information is included on the OFAC web site at *www.treas.gov/ofac*.
- When processing the opening of accounts, question accounts for residents of countries included on the OFAC list.
- Question requests to transfer funds or securities to residents or entities domiciled in any country included on the OFAC list.

7.7 Currency Reporting Requirements

[SEC Securities Exchange Act of 1934 Rule 17a-8; Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart C]

The following summarizes the reporting requirements under the Bank Secrecy Act. CHAINCE SECURITIES LLC's designated supervisor of Operations is responsible for maintaining records of any currency reports required to be filed by CHAINCE SECURITIES LLCand retaining them for five years.

7.7.1 Transactions Involving Currency Over $10,000

If CHAINCE SECURITIES LLCaccepts a currency deposit exceeding $10,000, it is required to electronically file a Currency Transaction Report (CTR, Form 112) with the Financial Crimes Enforcement Network (FinCEN). Multiple transactions by the same person equaling over $10,000 in any one day must also be reported.

"Currency" is defined as the coin and paper money of the U.S. or legal tender of other countries. Currency also includes U.S. silver certificates, U.S. notes, federal reserve notes, and official foreign bank notes customarily used and accepted as a medium of exchange in a foreign country. CTRs must be filed by the 15^{th} calendar day after the day of the transaction and kept for 5 years.

7.7.2 Transactions Involving Currency Or Bearer Instruments Over $10,000 Transferred Into Or Outside The U.S.

Broker-dealers are required to file a Currency and Monetary Instrument Transportation Report (CMIR, Form 105) with the U.S. Customs Service to report transactions in currency and/or bearer instruments which alone or in combination exceed $10,000 and which are shipped or transported into or outside the U.S. This filing is not required for currency or other monetary instruments mailed or shipped through the postal service or by common carrier. CHAINCE SECURITIES LLC(and its clearing firm or other third party) is responsible for filing these reports and maintaining records of them. CMIRs must be filed within 15 days after the receipt of the currency or monetary instruments.

7.7.3 State Reporting Requirements

States have adopted various currency and suspicious activity reporting requirements. Most states have entered into an agreement with FinCEN to provide them with duplicate copies of forms filed by broker-dealers. Some states, however, require duplicate filing with the states themselves at the time the broker-dealer files with a federal agency. CHAINCE SECURITIES LLCwill file reports as required under state requirements.

7.8 Foreign Financial Account Reporting Requirements And Recordkeeping (FBAR)

[Bank Secrecy Act 31 CFR Chapter X Part 1010 Subpart C; FinCEN Notice 2012-1]

Certain "United States persons" that maintain accounts (including any account where the person has a financial interest in, or signature or other authority over) in foreign jurisdictions and with aggregate balances exceeding $10,000 are required to electronically file the Foreign Bank Account Report Form 114 with FinCEN on or before June 30th of each calendar year for accounts maintained during the previous calendar year. The FINOP is responsible for filing the annual report if it is required for CHAINCE .

The filing requirement applies to:

- Non-resident aliens and foreign entities "in and doing business" in the U.S.
- All forms of U.S. business entities, trusts, estates with foreign accounts.
- U.S. citizens and residents with signature or other authority over a foreign account.
- Trust beneficiaries with a greater than 50% beneficial interest in a trust with a foreign account.
- U.S. citizens and resident stockholders with greater than 50% of the value or vote of the shares of a corporation with foreign accounts.
- Entities that are disregarded for tax purposes, such as limited liability companies.

The filing requirement does not apply to certain entities or situations. The regulation should be consulted for specific exemptions or conditions of exemptions.

- If the account is maintained in the United States, it is not considered a foreign account even if it holds foreign assets.
- An omnibus account held by a custody bank that holds assets both in the U.S. and outside the U.S. is not considered a foreign account unless the customer has direct access to its foreign holdings maintained at the foreign institution.
- Certain entities are excluded including: foreign hedge funds, venture capital funds, or private equity funds; tax-exempt investors that own offshore "blocker corporations;" government pension funds; pension plan participants and IRA owners (provided the trustee files a FBAR); investment advisers and employees of such advisers that provide advice to SEC-registered entities; remainder interests in trusts and beneficiaries of discretionary trusts; employees of a U.S. or foreign entity that issued a class of foreign equity (including ADRs) registered with the SEC.

There also are exemptions for officers or employees with signature or other authority over certain foreign financial accounts but no financial interest in the reportable account. The regulation should be consulted for details regarding who is not required to notify FinCEN regarding signature or other authority over such an account.

7.9 Recordkeeping Requirements (Joint Rule and Travel Rule)

[Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart D]

In addition to maintaining records of reports filed with the IRS or other authorities, broker-dealers are obligated to maintain records of certain transactions, for potential inspection by regulators and other authorities. These records must be retained for five years.

7.9.1 Fund Transfers And Transmittals

[Bank Secrecy Act 31 CFR Chapter X Part 1010 Subpart D; FINRA Notice to Members 97-13, 96-67 and 95-69; SEC Q&As: http://www.sec.gov/about/offices/ocie/aml2007/fincen-advissu7.pdf; SEC Q&As: http://www.sec.gov/about/offices/ocie/aml2007/fincen-advsiii.pdf]

Broker-dealers are required to collect and retain information (such as name, address, account number of customer, date and amount of wire, payment instructions, name of recipient institution, and name and account information of wire payment recipient) and maintain records for domestic and international funds transfers (including wire fund transfers) of $3,000 or more, with certain exceptions.

CHAINCE SECURITIES LLC(and its clearing firm or other third party, if applicable) is responsible for complying with the requirements to record information regarding fund transfers and, when required, verifying information regarding transmitters and recipients who are not established customers. Examples of verification information include:

- Name and address
- ID reviewed (type and number on the ID)
- Taxpayer ID number (or alien ID or passport number including country of issuance)
- Copy or record of method of payment (*e.g.,* credit card, check)

7.9.2 Other Recordkeeping Requirements

[Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart D 1023.410]

The Bank Secrecy Act incorporates other records requirements that include records covered by *Books And Records* in the chapter *FINANCIAL AND OPERATIONS PROCEDURES*. CHAINCE SECURITIES LLCwill retain all of the following required records:

1. Trading authorizations which are addressed in the chapter *ACCOUNTS*
2. Records under 17a-3 which are addressed in the chapter *FINANCIAL AND OPERATIONS PROCEDURES*
3. A record of each receipt of currency, other monetary instruments, checks, or investment securities and of each transfer of funds or credit, of more than $10,000 received on any one occasion directly and not through a domestic financial institution, for any person, account or place outside the United States.

7.10 DVP/RVP Accounts

DVP/RVP accounts that use brokers to liquidate large volumes of low-priced securities may be a red flag for AML concerns. Such accounts should be the subject of reasonable inquiry to determine the source of the securities and to identify potential money laundering and registration issues. CHAINCE SECURITIES LLCis responsible for AML inquiries unless there is a formal undertaking by the customer's prime broker.

7.11 Omnibus Accounts And Transactions In Low-Priced Securities

[SEC Staff Bulletin: Risks Associated with Omnibus Accounts Transacting in Low-Priced Securities; FINRA Regulatory Notice 21-03; FINRA's 2022 Report: https://www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program]

Responsibility	• Designated Supervisor
Resources	• New accounts

	• Records of transactions
Frequency	• As required

Action	• Identify omnibus accounts with transactions in low-priced securities and new accounts intending to trade in those securities
	• Consider whether it is appropriate to obtain information about the ultimate beneficial owners
	• Determine whether the account should be subjected to heightened reviews and whether risks can be managed
	• If risks cannot be managed, consider:
	  ○ not opening, if a new account
	  ○ closing an existing account
	  ○ restricting or rejecting transactions in low-priced securities
	  ○ filing an SAR, if appropriate

Record	• New account records • Reviews of transactions and actions taken

There may be risks of illicit activities associated with transactions in low-priced securities through omnibus accounts maintained by foreign financial institutions (FFIs), particularly where the customer or beneficial owner is unknown. Such accounts may "nest" within omnibus accounts of financial institutions based in jurisdictions that are generally considered to be lower risk such as Canada or the UK. Such accounts may be subjected to added review and restrictions or a determination to not open or to close the account. Signs of potentially illicit trading activity in low-priced securities include:

- trading that coincides with a sudden increase in share price or trading volume, in the absence of legitimate news surrounding the company;
- investors depositing large blocks of shares of low-priced securities originating from convertible debt acquired from the issuer or a third party, immediately selling the shares and then transferring the proceeds out of the account;
- transactions in securities of issuers making questionable claims regarding their products or services related to a recent, major event (*e.g.,* the COVID-19 pandemic) or a new trend (*e.g.,* cryptocurrency or non-fungible tokens (NFTs)) or both; and
- increased trading that overlaps with a surge in relevant promotional activity on social media, investor chat rooms and message boards. Firms can find additional resources concerning potential warning signs of fraudulent activity.

7.12 Detecting Potential Money Laundering

Responsibility	• AML Compliance Officer • Other designated supervisor for review of AML Compliance Officer accounts • Reviewer of systems/procedures (*i.e.,* Internal Audit, Compliance)
Resources	• Internal reports of transactions, available exception reports
Frequency	• Daily and ongoing: review of transactions

	• Annual: test systems and data

Action	• For accounts that provide "banking-like services" (*i.e.,* wire transfers, check writing, ATM withdrawals) review for large movements of money with little or no securities trading
	• Monitor foreign currency-denominated wire transfers
	• Monitor customers' deposits and trades in penny stocks for potential suspicious activity
	• Review for red flags for IPOs in emerging markets
	• Monitor correspondent accounts maintained for foreign financial institutions
	• Supervisor(s):
	  ○ Review reports of transactions (cash and security transactions) to identify potential money laundering (including employee accounts)
	  ○ Another designated supervisor will review the AML Compliance Officer's accounts
	  ○ Report suspicious activity (see the policy in this chapter)
	  ○ Notify RRs, supervisors, and close accounts when necessary
	• Reviewer(s): Conduct reviews of systems and data sources to confirm potential suspicious activity will be identified and reported

Record	• Reviews including manual/electronic record of reviews of:
	  ○ banking-like services
	  ○ reports
	  ○ foreign currency wire transfers
	  ○ IPOs in emerging markets
	  ○ Correspondent accounts for foreign financial institutions
	• Action taken, when necessary
	• Suspicious activity reports
	• Reviews of systems and data and corrective action taken, if applicable

CHAINCE SECURITIES LLC has an ongoing program to identify potential money laundering. Monitoring will be conducted using available exception reports or review of a sufficient amount of account activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as "non-cooperative" are involved, or involve "red flags" (indicators of potential money laundering) which are included in the *Money Laundering* policy in the chapter *GENERAL EMPLOYEE POLICIES*. Items reviewed include trading and wire transfer transactions in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that customer. Among the information used to determine whether to file a suspicious activity report are exception or transaction reports that include transaction size, location, type, number, and nature of the activity.

Trading accounts will be identified and monitored where a series of financial transactions may help obscure the origins of the funds. This may include effecting securities transactions, closing the account, and transferring funds to a bank or other account, particularly to an offshore location. Trading penny stocks (which may involve unregistered distributions) or engaging in retail forex trading will, in particular, be monitored when they occur.

CHAINCE SECURITIES LLC has included an educational policy *(Money Laundering)* in the chapter *GENERAL EMPLOYEE POLICIES* to educate employees on money laundering and guidelines for detecting money laundering activities. Periodically detection of money laundering and the obligation to report suspicious activities will be included in continuing education and other educational programs for employees.

7.12.1 Clearing Firm AML Procedures

CHAINCE SECURITIES LLC will work with the clearing firm to exchange information, records, data and exception reports as necessary to comply with AML laws. Required certifications for information sharing are on file. As a general matter, the clearing firm will monitor CHAINCE SECURITIES LLC's customer activity as well as CHAINCE performing such monitoring , and the clearing firm will be provided with proper customer identification information as required to successfully monitor customer transactions. CHAINCE SECURITIES LLC's and the clearing firm's responsibilities are included in the clearing agreement and each firm is responsible for its own independent compliance with AML laws. CHAINCE SECURITIES LLC and the clearing firm cannot disclaim their respective responsibilities to comply with AML requirements.

7.12.2 Foreign Currency Transactions

Foreign financial institutions may purchase U.S.denominated bonds, generally issued by foreign governments, with the local currency, which are then transferred to a U.S. broker-dealer and sold, with proceeds then transferred offshore. U.S. broker-dealers act as intermediaries in these transactions and may receive foreign bonds or other securities worth millions of U. S. dollars without knowing who or how many underlying customers may be involved. RRs and CHAINCE SECURITIES LLC must be diligent about such transactions which may involve money laundering.

7.12.3 IPOs In Emerging Markets

[FINRA 2022 Report: https://www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program; SEC statement on emerging market investments: https://www.sec.gov/news/public-statement/emerging-market-investments-disclosure-reporting]

Emerging markets may pose an added risk of money laundering. Investors in IPOs in this market may be serving as nominees for an undisclosed control person or persons. These IPOs are typically smaller in size (*i.e.,* less than $100 million) and listed on the lower qualification tiers of U.S. stock exchanges. Red flags of potentially manipulative trading associated with how these investors open new accounts and trade these securities, after the IPO is completed, include:

- numerous unrelated accounts being opened at the same time, including with similar banking information, physical addresses, email address domains and current employer (which is often associated with the IPO issuer);
- documents investors provide in order to open an account or verify source of funds that may have been altered or could be fictitious;
- wire transfers received into these accounts that exceed the financial wherewithal of the investor as indicated on their new account documents, exceed the value of the shares purchased in the IPO and are either sent from similar banks, or bank accounts that share certain identifying information (*e.g.,* employer of account holder, email domain);
- investor accounts being accessed by a different Internet Protocol (IP) or Media Access Control (MAC) address than is known for the customer, granting login and trading capabilities to a third party or both;
- multiple orders with substantially similar terms being placed at or around the same time by seemingly unrelated investors in the same security that is indicative of "spoofing" or "layering"; and
- investors engaging in trading activity that does not make economic sense.

7.13 Information Sharing Between Financial Institutions

[USA PATRIOT Act Section 314(b); Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart E; Section 314(b) Fact Sheet: Section 314(b) Fact Sheet (fincen.gov)]

CHAINCE SECURITIES LLCdoes not share information with other financial institutions regarding accounts and account activity.

7.14 Suspicious Activities

[Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart B; USA PATRIOT Act Section 356; FINRA Notice to Members 02-47; FinCEN Guidance FIN-2008-G005; FinCEN FAQs: Answers to Frequently Asked Questions Regarding Suspicious Activity Reporting and Other Anti-Money Laundering Considerations https://www.fincen.gov/resources/statutes-regulations/guidance/answers-frequently-asked-questions-regarding-suspicious; 2022 FINRA Report: https://www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program]

Responsibility	• AML Compliance Officer
Resources	• Reports from employees of crimes or suspected crimes • Suspicious activities detected through ongoing reviews • Exception and other reports (internal and/or provided by a clearing firm) • FinCEN advisories • Other available information
Frequency	• As required

Action	• Maintain the confidentiality of SAR reviews and filings:
	  ○ Limit the sharing of information to those authorized and need to know
	  ○ Electronic files should be password-protected and use a file name that does not identify files as SARs-related
	  ○ Use a header on documents: CONFIDENTIAL
	  ○ In redaction markings or privilege logs, identify the redacted or privileged information as "nonpublic supervisory information"
	  ○ For production of documents, produce SAR documents separately from other documents and identify as confidential SAR information
	  ○ Destroy copies of SARs when retention periods have passed
	  ○ Confer with counsel or other outside expert regarding confidentiality questions
	• Include FinCEN red flags in suspicious activity identification
	• Respond to red flags associated with the movement or settlement of cash or securities (*e.g.*, wire and ACH transfers, debit card and ATM transactions, securities trading (including order entry), and journal transfers)
	• Respond to red flags regarding CHAINCE SECURITIES LLC's business operations including activity related to high-risk products and services (*e.g.*, cash management products and services; trading of low-priced, thinly traded securities; and suspicious activity introduced to CHAINCE SECURITIES LLC by other BDs)
	• Review and investigate suspicious transactions referred by employees or identified in review of surveillance reports
	• Review and investigate suspicious transactions referred by a clearing firm, if applicable

	• Review and investigate inquiries from law enforcement, regulators or other federal and state agencies that concern red flags of suspicious activity • Notify AML Officer of events that may require filing of an SAR, including cybersecurity events, account compromise or takeovers or fraudulent wire or ACH transfers. • Periodically review reports to confirm integrity of captured data and adjust reports as necessary • Determine whether CHAINCE SECURITIES LLC(or its clearing firm, if applicable) will file a SAR • If appropriate, file Form SAR with FinCEN and state authorities • Notify senior management, as appropriate, of forms filed • Provide copy to parent company, if applicable • File SARs jointly with other financial institutions, if applicable
Record	• Notes and other documented reviews including record of manual/electronic review and actions taken, if applicable • Review of reports for integrity and adjustments made • Copies of SARs filed by CHAINCE SECURITIES LLCare retained in the SAR file with notation of when and to whom sent

CHAINCE SECURITIES LLC has an obligation to identify suspicious activities and file Suspicious Activity Reports (SARs) for transactions that may be indicative of money laundering activity. Suspicious activities include a wide range of questionable activities; examples include trading that constitutes a substantial portion of all trading for the day in a particular security; trading or journaling between/among accounts, particularly between related owners; late day trading; heavy trading in low-priced securities; unexplained wire transfers, including those to known tax havens; unusually large deposits of funds or securities. For business introduced to a clearing firm, CHAINCE SECURITIES LLC will have access to transaction data from the clearing firm and will supply this to CHAINCE SECURITIES LLC's transaction monitoring vendor for exception reporting. Exceptions will be reviewed by CHAINCE compliance personnel in connection with relevant KYC information on the client to determine whether exceptions can be resolved or should be regarded as suspicious activity subject to potential suspicious activity reporting.

7.14.1 Identifying Potential Suspicious Activity

CHAINCE SECURITIES LLC uses a number of tools to identify potential suspicious activity including:

- Transaction information including disbursement of funds or securities
- Education of firm personnel, particularly supervisors in Operations areas
- Employee reports of potential suspicious activity forwarded to the AML Compliance Officer
- Internal reports or reports provided by a clearing firm

- Reports from CHAINCE's transaction monitoring and KYC support vendor, SEON

7.14.1.1 SAR Escalation

When a member of the firm detects any red flag or other activity that may be suspicious, he or she will notify the AMLCO. Under the direction of the AMLCO and in conjunction with Senior Management and outside legal counsel, the Firm will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third party sources, contacting the government, freezing the account, and filing a SAR.

7.14.2 When A Report Must Be Filed

A SAR must be filed for any transaction that, alone or in aggregate, involves at least $5,000 in funds or other assets, if CHAINCE SECURITIES LLC knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is part) falls into one of the following categories:

- Transactions involving funds derived from illegal activity or intended or conducted to hide or disguise funds or assets derived from illegal activity.
- Transactions designed, whether through structuring or other means, to evade the requirements of the Bank Secrecy Act (BSA).
- Transactions that appear to serve no business or apparent lawful purpose or are not the sort of transactions in which a particular customer would be expected to engage, and for which CHAINCE SECURITIES LLCknows of no reasonable explanation after examining the available facts.
- Transactions that involve the use of CHAINCE SECURITIES LLC to facilitate criminal activity.

Excluded from the filing requirement are violations otherwise reported to law enforcement authorities such as:

- a robbery or burglary that is reported to law enforcement authorities
- lost, missing, counterfeit, or stolen securities reported pursuant to 17f-1
- a violation of federal securities laws or SRO rules by CHAINCE , its officers, directors, employees, or RRs that are reported to the SEC or SRO, except for violations of Rule17a-8 (filing of Currency and Transaction Reports) which must be reported on a SAR

7.14.3 Filing A Report And Emergency Notification

If CHAINCE SECURITIES LLC determines to file a SAR with FinCEN, the AML Compliance Officer will file:

- within 30 days of becoming aware of the suspicious transaction; or
- if no suspect has been identified within 30 calendar days of detection, reporting may be delayed an additional 30 calendar days or until a suspect has been identified, but no later than 60 days from date of initial detection.

In situations involving violations that require immediate attention (such as terrorist financing or ongoing money laundering schemes), the AML Compliance Officer will immediately notify by telephone an appropriate law enforcement agency. Suspicious transactions that may relate to terrorist activity may also be reported to FinCEN's Financial Institutions Hotline. In either event, a SAR will be filed.

7.14.3.1 Emergency Notification

[FINRA Notice to Members 02-21]

When conducting due diligence or opening an account, Federal authorities will be notified immediately by the AML Compliance Officer, when necessary, in the following situations:

- A legal or beneficial account holder or person is engaged in a transaction listed on or located in a country or region listed on the OFAC list.
- An account is held by an entity that is owned or controlled by a person or entity listed on the OFAC list.
- A customer tries to use bribery, coercion, or similar means to open an account or carry out a suspicious activity.

- There is reason to believe a customer is trying to move illicit cash out of the government's reach.
- There is reason to believe the customer is about to use funds to further an act of terrorism.

Emergency contacts include:

- OFAC Hotline (1-800-540-6322)
- Financial Institutions Hotline (1-866-556-3974)
- Local U.S. Attorney's office
- Local FBI office
- Local SEC office

7.14.4 Retention Of Records

The AML Compliance Officer maintains a file of copies of SARs filed with FinCEN and all related documents for a period of 5 years from the filing date.

7.14.5 Providing SARs Information To SROs

[SEC letter to CEOs: http://www.sec.gov/about/offices/ocie/brokerdealerletter.htm]

While SARs are to be treated as confidential, CHAINCE SECURITIES LLC will provide SARs and supporting documentation available to any self-regulatory organization (SRO) that examines CHAINCE SECURITIES LLC for compliance with the SAR Rule, upon request of the SEC. The request may be part of a routine examination, an investigation, or part of the SRO's risk assessment effort within its examination program.

7.14.6 Prohibition Against Disclosure

By statute and regulation, CHAINCE SECURITIES LLC may not inform customers or third parties that a transaction has been reported as suspicious. U.S. Treasury and Federal Reserve Board regulations also require CHAINCE SECURITIES LLC to decline to produce SARs in response to subpoenas and to report to FinCEN and the Federal Reserve Board the receipt of such requests and CHAINCE SECURITIES LLC’s response. Failure to maintain the confidentiality of SARs may subject an employee to civil and criminal penalties under Federal law. Violations may be enforced through civil penalties of up to $100,000 for each violation and criminal penalties of up to $250,000 and/or imprisonment not to exceed five years. CHAINCE SECURITIES LLC may also be liable for civil money penalties resulting from AML deficiencies that led to improper SAR disclosure up to $25,000 per day for each day the violation continues.

Procedures to protect the confidentiality of SARs include the following:

- Access to SARs is limited to employees on a "need-to-know" basis
- SARs will be maintained in locked physical or electronic files
- SARs may not be left on desks or on open computer files and must be viewed without access by unauthorized persons
- SARs shared with others will be clearly marked "Confidential"

Compliance (or CHAINCE SECURITIES LLC’s counsel) is responsible for responding to subpoena requests and Compliance will notify FinCEN and the Federal Reserve Bank of any subpoenas for SARs.

7.14.7 Politically Exposed Persons (PEP)

[FinCEN Advisory FIN-2018-A003]

FinCEN has highlighted how corrupt foreign PEPs' activity may trigger suspicious activities requiring reporting. FinCEN's advisory lists red flags which are incorporated into CHAINCE SECURITIES LLC's suspicious activity identification and reporting process.

7.15 Requests And Written Notices From Regulators, Enforcement Agencies, And Other Authorized Persons

Under the Bank Secrecy Act, financial institutions are required to respond to federal banking agency requests for information relating to anti-money laundering compliance. The Rule requires provision of information and account documentation for any account opened, maintained, administered or managed in the U.S. The AML Compliance Officer maintains records of information provided in response to regulators' requests including the request, date of response, and information provided.

7.15.1 Federal Banking Agency Requests -- 120-Hour Rule

[USA PATRIOT Act Section 319(b)]

Upon receiving a request from a Federal banking agency, the AML Compliance Officer will provide the requested information within 5 days (120 hours) of receiving the request or will make available the information for inspection by the banking agency.

7.15.2 Information Sharing With Enforcement Agencies

[Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart E; USA PATRIOT Act Section 314]

Responsibility	• AML Compliance Officer
Resources	• Deposit records, purchase/sale records, account records, other records as required, FinCEN Secure Information Sharing System (SSIS)
Frequency	• Upon request • Bi-weekly: review SSIS
Action	• Conduct bi-weekly review of SSIS and print confirmation page • If a match is found, submit the information as required
Record	• Documentation of reviews including a confirmation page from SSIS and records of positive search results

Enforcement agencies (FinCEN, state, local, and certain foreign law enforcement agencies eligible to make requests) send requests to FinCEN's Secure Information Sharing System (SSIS). CHAINCE SECURITIES LLCis required to review the SSIS bi-weekly to identify requests for information and to send required information within required timeframes.

Enforcement agency requests are confidential and may not be disclosed to the subject of the request. CHAINCE SECURITIES LLCwill not use information provided to enforcement agencies for any purpose

other than (1) to report to an agency as required under Section 314; (2) to determine whether to establish or maintain an account, or to engage in a transaction; or (3) to assist CHAINCE SECURITIES LLCin complying with any requirement of Section 314.

7.15.3 National Security Letters

[FinCEN SAR Activity Review, Trends, Tips & Issues, Issue 8 (National Security Letters and Suspicious Activity Reporting) (4/2005)]

National Security Letters (NSLs) are written investigative demands that may be issued by the local Federal Bureau of Investigation and other federal government authorities conducting counterintelligence and counterterrorism investigations to obtain, among other things, financial records of broker-dealers. **NSLs are highly confidential. CHAINCE SECURITIES LLC and its employees are barred from disclosing to any person that a government authority or the FBI has sought or obtained access to records.**

The AML Compliance Officer is responsible for responding to an NSL and maintaining the confidentiality of the letter and the response. If an SAR-SF is filed after receiving an NSL, the SAR-SF cannot make reference to the receipt or existence of an NSL. The SAR-SF will only contain detailed information about the facts and circumstances of the detected suspicious activity.

7.15.4 Grand Jury Subpoenas

[FinCEN SAR Activity Review, Trends, Tips & Issues, Issue 10 (Grand Jury Subpoenas and Suspicious Activity Reporting) (5/2006)]

The receipt of a grand jury subpoena concerning a customer does not in itself require the filing of a Suspicious Activity Report (SAR-SF). When a grand jury subpoena is received, the AML Compliance Officer will:

- Conduct a risk assessment of the customer subject to the subpoena as well as review the customer's account activity.
- If suspicious activity is identified during the risk assessment and review, the risk assessment will be elevated and an SAR-SF will be filed. The SAR-SF will not contain any reference to the receipt or existence of the subpoena. The SAR-SF will only contain detailed information about the facts and circumstances of the detected suspicious activity.

The existence of a subpoena and any response are confidential and may not be disclosed directly or indirectly to the person who is the subject of the subpoena. The AML Compliance Officer will maintain the subpoena and any response in a confidential file and will only share information with those authorized.

7.15.5 Foreign Bank Correspondent Accounts

[USA PATRIOT Act Section 313]

Upon receipt of a written request from a Federal law enforcement officer for information about a foreign bank correspondent account, the AML Compliance Officer will provide the requested information no later than 7 days after receipt of the request.

Compliance will terminate any correspondent relationship with a foreign bank within 10 business days of receiving a notice from the Treasury Dept. or the U.S. Attorney General that the foreign bank failed either to comply with a summons or subpoena or to contest it in a U.S. court.

7.15.6 Requests By Law Enforcement To Maintain Accounts

Law enforcement agencies may have an interest in having accounts remain open in spite of suspicious or potential criminal activity in connection with the account. The AML Compliance Officer will consider such requests and, if the account will remain open, require the federal law enforcement agency to provide a written request issued by a supervisory agent or by an attorney within the U.S. Attorney's Office or another office of the Department of Justice. If requested by a state or local law enforcement agency, the letter must be issued by a supervisor or local prosecutor's office.

The written request must include:

- the agency's request that the account remain open;
- the purpose of the request; and
- the duration of the request (not to exceed 6 months).

The request will be retained for 5 years.

If CHAINCE SECURITIES LLC is aware the account is under investigation (because of a subpoena, 314[a] request, National Security Letter, or similar communication), the requesting law enforcement agency will be advised before making a decision about the status of the account.

7.16 Accounts Requiring Approval By The AML Compliance Officer

The following accounts require review and approval by the AML Compliance Officer at the time of opening. The AML Compliance Officer may require additional information for these accounts.

- **Numbered accounts** (accounts designating a number rather than a name as the account name). The firm does not permit numbered accounts.
- **Any account requesting confidential handling** of its name, mailing of confirmation and statements, *etc.*
- **Accounts domiciled in high risk countries.** Accounts domiciled in countries identified by OFAC or the Financial Action Task Force on Money Laundering (FATF) as having inadequate anti-money laundering standards or representing high risk for crime and corruption.
- **Foreign public officials.** Includes individuals in high offices of foreign governments, political party officials and their families and close associates (if known and/or readily identifiable).
- **Correspondent and Private Banking accounts.** See the section *Due Diligence For Correspondent And Private Banking Accounts*.

7.17 Customer Identification Program (CIP)

[USA PATRIOT Act Section 326; Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart B; FINRA Notice to Members 03-34; FinCEN Frequently Asked Questions: https://www.fincen.gov/resources/statutes-regulations/guidance/interagency-interpretive-guidance-customer-identification; FinCEN No-Action position on CIP requirements under clearing arrangements: FIN-2008-G002; Guidance on Obtaining and Retaining Beneficial Ownership Information, FinCEN Guidance, FIN-2010-G001 March 5, 2010]

The opening of customer accounts is subject to customer identity verification requirements under CHAINCE SECURITIES LLC's Customer Identification Program (CIP). Requirements for employees opening accounts as explained in the chapter *ACCOUNTS* are duplicated in this section to consolidate all AML requirements within this chapter.

7.17.1 Definition Of Customer Under CIP Rule

The definition of "customer" under the CIP rule is different than definitions under other rules. Who is a "customer" under this Rule affects CHAINCE SECURITIES LLC's obligations.

Under the CIP rule and for purposes of this section, "customer" is defined as:

- A person that opens a new account.
- An individual who opens a new account for:
    - An individual who lacks legal capacity; or
    - An entity that is not a legal person.

"Customer" does not include a financial institution regulated by a Federal regulator; a bank regulated by a state bank regulator; those exempted under Federal rule include municipalities; or a person with an existing account at CHAINCE SECURITIES LLC, providing there is reasonable belief that the true identity of the person is known.

7.17.2 Accounts Opened By Other Financial Institutions

Responsibility	• AML Compliance Officer
Resources	• Other financial institution's CIP • Contract with other financial institution
Frequency	• Initially when an institution opens accounts and updated as needed - evaluate institution's CIP • Annual - obtain certification

Action	• Where required:
	  ○ Confirm institution is subject to AML rules/requirements
	  ○ Evaluate other institution's CIP
	  ○ Contract with other institution regarding compliance with CHAINCE SECURITIES LLC's CIP requirements
	  ○ Obtain annual certification

Record	• Evaluation of other institution's CIP • Contract with other financial institution • Annual certifications from the financial institution

7.17.2.1 Financial Intermediaries As Customers Vs. Beneficial Owners

[Guidance from Dept. of Treasury and SEC regarding broker-dealer CIP rule: http://www.sec.gov/divisions/marketreg/qa-bdidprogram.htm]

Financial institutions (such as banks, clearing firms, investment advisers, *etc.*) act as intermediaries opening accounts including master and omnibus accounts. The SEC has stated that the underlying beneficial owners are **not** "customers" subject to CIP requirements under the following circumstances outlined in the SEC's guidance:

1. the omnibus account or relationship is established by or on behalf of a financial intermediary for the purpose of executing transactions that will clear or settle at another financial institution, or the omnibus account holder provides limited information to CHAINCE SECURITIES LLC solely for

the purpose of delivering assets to the custody account of the beneficial owner at another financial institution;
2. the limited information given to CHAINCE SECURITIES LLC about the beneficial owner is used primarily to assist the financial intermediary with recordkeeping or to establish sub-accounts that hold positions for a limited duration to facilitate the transfer of assets to another financial institution;
3. all transactions in the omnibus account or sub-accounts at CHAINCE SECURITIES LLC are initiated by the financial intermediary; and
4. the beneficial owner has no direct control over the omnibus account or sub-accounts at the broker-dealer.

CHAINCE SECURITIES LLC is not obligated to look through the intermediary financial institution to the underlying beneficial owners if the intermediary identifies itself as the accountholder. Even if CHAINCE SECURITIES LLChas some information about beneficial owners, the intermediary (not the beneficial owner) is treated as the customer for purposes of the CIP rule under these circumstances.

7.17.2.2 Reserved

7.17.2.3 Registered Investment Adviser Accounts

[SEC Division of Market Regulation No-Action Letter to SIFMA dated January 9, 2015: http://www.sec.gov/divisions/marketreg/mr-noaction/2015/sifma-010915-17a8.pdf]

Responsibility	• AML Compliance Officer
Resources	• New investment adviser accounts
Frequency	• As required
Action	• For each SEC-registered adviser opening accounts with CHAINCE SECURITIES LLC where CHAINCE SECURITIES LLCwill rely on the adviser for CIP compliance: ○ Conduct due diligence to review adviser including confirming adviser's SEC registration and update as needed ○ Obtain the adviser's written agreement to comply with CIP requirements ○ Obtain annual certification
Record	• Due diligence review • Written agreement of CIP compliance • Annual certifications

CHAINCE SECURITIES LLC may rely on an SEC-registered investment adviser to perform some or all of the CIP obligations related to customers where CHAINCE SECURITIES LLC and the investment adviser have a customer relationship, under the following conditions.

- it is reasonable to rely on the adviser's assurances;
- the investment adviser is a U.S. investment adviser registered with the SEC under the Investment Advisers Act of 1940; and
- the adviser enters into a written agreement with CHAINCE SECURITIES LLC in which the adviser agrees that:

- it has implemented its own AML Program consistent with the requirements of 31 U.S.C. 5318(h) and will update such AML Program as necessary to implement changes in applicable laws and guidance;
- it (or its agent) will perform the specified requirements of CHAINCE SECURITIES LLC's CIP in a manner consistent with Section 326 of the PATRIOT Act;
- it will promptly disclose to the broker-dealer potentially suspicious or unusual activity detected as part of the CIP being performed on the broker-dealer's behalf in order to enable CHAINCE SECURITIES LLC to file a Suspicious Activity Report, as appropriate based on CHAINCE SECURITIES LLC's judgment;
- it will promptly provide its books and records relating to its performance of CIP to the Commission, to an SRO that has jurisdiction over CHAINCE , or to authorized law enforcement agencies, either directly or through CHAINCE , at the request of (i) CHAINCE, (ii) the SEC, (iii) an SRO that has jurisdiction over the broker-dealer or (iv) an authorized law enforcement agency.

7.17.3 Master Accounts And Sub-Accounts

[FINRA Regulatory Notice 10-18; SEC National Exam Risk Alert "Master/Sub-accounts:" http://www.sec.gov/about/offices/ocie/riskalert-mastersubaccounts.pdf]

Responsibility	• Designated Supervisor
Resources	• New master/sub-accounts
Frequency	• As required when master/sub-accounts are established
Action	• Except for those accounts meeting the requirements of the prior subsections regarding financial institution intermediaries, determine, where possible, sub-account ownership including whether persons associated with the master account customers are not themselves customers. Where sub-account holders directly effect transactions, subject the holders to CIP verification. • Conduct CIP reviews • Include master/sub-accounts in reviews of transactions to identify potential insider trading
Record	• Records of master and sub-account ownership (where applicable) • AML/CIP reviews • Review of transactions including record of action taken, if any

Accounts are sometimes established as "master accounts" that represent multiple sub-accounts. Depending on facts and circumstances (discussed below), master/sub-accounts may be recognized as separate customer accounts subject to CIP reviews.

7.17.3.1 Description Of Master/Sub-Accounts

A master account may have multiple underlying accounts on behalf of underlying investors; sub-advisers may be authorized to effect transactions without the intermediation of the master account owner. Also, an individual or entity may set up sub-accounts for separate trading strategies or algorithms. Sub-accounts may be used by individual traders or groups of traders. The master account may be another broker-dealer or a partnership that provides its individual partners trading authority over separate sub-accounts.

7.17.3.2 Obligations To Conduct CIP Reviews

Except for accounts opened by investment advisers and financial institutions discussed under *Accounts Opened By Other Financial Institutions* and meeting the conditions of that section, when there are separate owners of the sub-accounts, CHAINCE SECURITIES LLC has an obligation to identify the beneficial owners. Indicators that there may be separate owners requiring CIP review of the sub-accounts include:

- The sub-account owner is entering orders for itself.
- CHAINCE SECURITIES LLC has actual notice the sub-accounts have different owners.
- The sub-accounts are separately documented and/or receive separate reports.
- The sub-accounts are addressed separately in terms of transaction, tax or other reporting.
- The services provided to the sub-accounts engender separate surveillance and supervision of the sub-accounts for compliance with rules or for risk management purposes consistent with the review of separately owned accounts.*
- There are financial arrangements or transactions with the sub-accounts, or separate account terms, that reasonably raise questions concerning whether such accounts represent separate beneficial owners.*
- The sub-accounts incur charges for commissions, clearance and similar expenses, separately, based upon the activity only of that subject sub-account.*
- There is evidence of financial transactions or transfers of assets or cash balances that would reasonably evidence separate beneficial ownership of the sub-accounts.*
- CHAINCE SECURITIES LLC (or RR) is aware of or has access to a master account or like agreement that evidences that the sub-accounts have different beneficial owners.
- There is evidence that a party maintaining a master/sub-account arrangement has interposed sub-accounts that have or are intended to have the effect of hiding the beneficial ownership interest.*
- The number of sub-accounts maintained is so numerous as to reasonably raise questions concerning whether such accounts represent separate beneficial owners.*

*Items above would not apply in the case of accounts opened by a registered BD or a bona fide investment adviser.

7.17.4 Customer Due Diligence (CDD)

[USA PATRIOT Act Section 326; Bank Secrecy Act 31 CFR Chapter X Part 1010, Part 1020, Part 1023, Part 1024 and Part 1026; FinCEN 2016 FAQs: https://www.ffiec.gov/press/pdf/Customer%20Due%20Diligence%20-%20Overview%20and%20Exam%20Procedures-FINAL.pdf; FinCEN 2018 FAQs: https://www.fincen.gov/resources/statutes-regulations/guidance/frequently-asked-questions-regarding-customer-due-0; FINRA Rule 3310; FINRA Regulatory Notice 18-19 and 17-40]

This section is duplicated from the chapter *ACCOUNTS*.

Responsibility	• Designated Supervisor
Resources	• New account application and other customer ID information
Frequency	• When accounts are opened

Action	• Before approving an account, determine by manual inspection that customer identification (ID) verification information is included with the new account application and meets CHAINCE SECURITIES LLC's requirements
	• For legal entity customers:
	  ○ Obtain beneficial ownership certifications
	  ○ Determine whether a threshold lower than 25% ownership is warranted depending on the customer's risk for potential enhanced monitoring or to collect additional information including expected account activity
	• For non-documentary verification, check the information included with the new account application for completeness and consistency with other customer-provided information (name, address, phone number, taxpayer ID number, *etc.*) The firm may also compare customer provide information to publicly available data, such as Social Security/Tax ID number registries.
	• For unacceptable verification information (incomplete, inconsistent), return the application to the RR for further information or disapprove the account
	• Obtain annual certification from other financial institutions
	• Include beneficial owners in AML transaction monitoring

Record	• New account records include customer ID verification as well as the supervisor's approval and customer certifications • Annual certifications from other financial institutions • Certifications from legal entity customers or documentation of oral certification, where applicable

When opening new accounts, the customer's identity must be verified, as required by federal law. Customer identification (ID) information must be completed on the new account application. This includes, under FinCEN's requirements:

1. customer identification and verification;
2. beneficial ownership identification and certification;
3. understanding the nature and purpose of customer relationships; and
4. ongoing monitoring for reporting suspicious transactions and, on a risk basis maintaining and updating customer information.

Customer ID verification does NOT apply to accounts for:

- persons with an existing account at CHAINCE SECURITIES LLC(unless the account requires approval by the AML Compliance Officer)
- banks
- governmental entities
- issuers of listed equity securities
- other financial institutions subject to regulation by the SEC, CFTC, Federal Reserve Board, OCC, FDIC, Office of Thrift Supervision, or the National Credit Union Administration
- persons opening accounts to participate in an ERISA plan

In addition, for accounts defined as "legal entity customers" (defined below), information must be obtained about beneficial owners. This requirement applies to accounts established May 11, 2018 or later. If CHAINCE SECURITIES LLC becomes aware of a change of beneficial ownership after May 11 for accounts established before that date, the customer's records must be updated under CDD requirements.

7.17.4.1 Definitions

[Exchange Act Rule 17a-3(a)(17)(i)(A); FINRA Rule 4512]

The regulations should be consulted for more complete definitions.

Legal entity customer: corporation; limited liability company; another entity created by a public filing with a Secretary of State or equivalent; general partnership; limited partnership; business trust created through a state filing; or any similar entity formed under federal law. Does not include sole proprietorships, unincorporated associations, and natural persons opening their own account. Other exclusions are a federal- or state-regulated financial institution; political departments and agencies of the U.S. or a State; various different types of entities registered with the CFTC or SEC; and other entities included in the regulation. [Questions 22-28, 2018 FAQs]

Beneficial owner:

- each individual, if any, who, directly or indirectly, owns 25% or more of the equity interests of a legal entity customer (*i.e.,* the ownership prong); and
- a single individual with significant responsibility to control, manage, or direct a legal entity customer, including an executive officer or senior manager (*e.g.,* a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer); or any other individual who regularly performs similar functions (*i.e.,* the control prong).

Ownership and control prongs: The CDD rule utilizes a two-pronged approach to defining a beneficial owner - an ownership prong and a control prong. Under the ownership prong, a beneficial owner is defined as each individual, if any, who, directly or indirectly, owns 25 percent or more of the equity interests of a legal entity customer. However, the rule recognizes that there may be instances when no single individual owns 25 percent or more of the equity interest of the legal entity; in such instances, CHAINCE SECURITIES LLCis still required to collect the required information for one individual who controls, manages or directs the legal entity customer. Under the control prong, a beneficial owner is defined as a single individual with significant responsibility to control, manage or direct a legal entity customer, including an executive officer or senior manager (*e.g.,* a chief executive officer, chief financial officer, chief operating officer, managing member, general partner, president, vice president or treasurer) or any other individual who regularly performs similar functions. The ownership and control prongs, although related, are independent requirements. Thus, satisfaction of, or exclusion from, regulatory obligations under one prong does not mean CHAINCE SECURITIES LLC's obligations under the other prong are also satisfied or excluded. [Question 9, 2016 FAQs]

7.17.4.2 Required Customer Information

[Exchange Act Rule 17a-3(a)(17)(i)(A); FINRA Rule 4512]

Basic information required **prior to opening the account** includes:

- **Name**
- **Date of birth,** for an individual
- **Address:**
    - for an individual, residential or business street address. If no street address exists or is available, an APO or FPO box number or the residential or business street address of a next of kin or another contact individual
    - for a non-individual (corporation, trust, *etc.*) a principal place of business, local office, or other physical location.
- **Telephone number**

- **Employment status** (including occupation and whether the person is associated with a broker dealer)
- **Annual income**
- **Net worth** (excluding value of primary residence)
- Account's investment objectives
- For joint accounts, information on each joint owner (financial information may be combined)
- **Taxpayer identification number** for a U.S. person (U.S. citizen or non-individual established or organized under U.S. or state laws).
- **Identification number for non-U.S. person** which may include a taxpayer ID number; passport number and country of issuance; alien identification card number; or the number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photo or similar safeguard.
- **Beneficial owners** (see the section that follows) including information about the following:
    - the nature and purpose of customer relationships to develop a customer risk profile
    - information sufficient at the time of account opening so customer activity may be assessed for SAR requirements (may include type of customer requesting services; type of account being opened; services or products being used)

In the case of a customer who has applied for a taxpayer identification number but has not yet received it, notation must be made on the new account application that the taxpayer ID has been applied for. The account will be restricted to liquidating transactions if the taxpayer ID number is not received within 30 days of opening the account.

In addition, under FINRA Rule 4512 CHAINCE SECURITIES LLC will retain the name of the RR responsible for the account and, if multiple RRs are assigned to the account, a record indicating the scope of their responsibilities with respect to the account. This requirement does not apply to an institutional account.

7.17.4.3 Accounts For Individuals

When opening an account for an individual, the following information is required:

- An unexpired government-issued identification including a photo and nationality or residence such as a driver's license or passport and record information from it on the new account application, **OR**
- A copy of the photo ID with the new account application. (The photo ID [original or copy] must be seen by the employee opening the account to record the information. This information may NOT be taken from the customer over the phone.)
- If the photo ID is not available at the time the new account application is being completed, the RR is to indicate on the new account application whether the customer will provide a copy of photo ID within 30 days of account opening **OR,** if the customer cannot provide a photo ID, the reason why not.
- If the photo ID is not received within 30 days, the account will be restricted to liquidating transactions only until the ID is received.

If the customer has not appeared in person at CHAINCE SECURITIES LLC’s office, "non-documentary" information will ALSO be required, as explained in a section that follows.

If the customer cannot produce the required photo ID, an explanation must be included on the new account application AND non-documentary information will be required to open the account.

7.17.4.4 Accounts For Legal Entity Customers

For legal entity customers, information must be obtained and verified regarding beneficial owners [Question 4, 2018 FAQs]. Obligations when opening accounts that include underlying owners or beneficiaries include the following:

- Determine whether the customer is acting as an agent for or on behalf of another, and if so, obtaining information regarding the capacity in which and on whose behalf the customer is acting.
- Where the customer is a legal entity that is not publicly traded in the United States, such as an unincorporated association, a private investment company (PIC), trust or foundation, obtain information about the structure or ownership of the entity so as to allow CHAINCE SECURITIES LLC to determine whether the account poses heightened risk.
- Where the customer is a trustee, obtain information about the trust structure to allow CHAINCE SECURITIES LLC to establish a reasonable understanding of the trust structure and to determine the provider of funds and any persons or entities that have control over the funds or have the power to remove the trustees.
- Obtain the identities of individuals who satisfy the definition as beneficial owners, either directly or indirectly through multiple corporate structures (complex ownership structures). [Question 3, 2018 FAQs]
- Obtain from the legal entity customer's representative a completed certification form identifying beneficial owners; updating information may require re-certification. [Questions 6 & 16, 2018 FAQs] [https://www.fincen.gov/resources/filing-information]
- Determine the nature and purpose of the customer relationship to determine risk profiles and identify the need for additional monitoring. [Questions 35-37, 2018 FAQs]

If CHAINCE SECURITIES LLC has affiliates with customers, information may be shared across the enterprise to cross-check beneficial ownership information.

7.17.4.4.1 Customer Representations

CHAINCE SECURITIES LLC may reasonably rely on information provided by customers if it has no knowledge of facts that would call into question the reliability of the information.

- There is no requirement to independently investigate a legal entity customer's ownership structure.
- CHAINCE SECURITIES LLC may rely on information provided by the customer to determine if the legal entity is excluded from the definition of legal entity customer.

7.17.4.4.2 Retention Of Beneficial Ownership Information

Identifying information will be maintained for a period of five years after the legal entity's account is closed. Verification records must be maintained for a period of five years after the record is made. CHAINCE SECURITIES LLC will also retain a description of each document relied on for verification, any non-documentary methods and results of measures undertaken for verification and the resolution of substantive discrepancies discovered in identifying and verifying the identification information for five years after the record is made. [Questions 9 & 10, 2018 FAQs]

7.17.4.4.3 Specific Account Requirements

Existing customers: For existing customers subject to CIP, CHAINCE SECURITIES LLC may rely on information obtained through the CIP to fulfill CDD requirements, providing that a representative of the customer certifies or confirms (orally or in writing) the accuracy of pre-existing CIP information. This also

applies to the opening of multiple accounts, simultaneously or not. Oral confirmation must be documented in account records, and written confirmation will be retained with account information. [Questions 7 & 13, 2018 FAQs]

Foreign customers: Companies traded on foreign exchanges are subject to CDD requirements (while companies traded on U.S. exchanges are exempt). A "risk-based" approach may NOT be taken for these foreign customers, but CHAINCE SECURITIES LLC may rely on their public disclosures as are available for other legal entity customers (whether listed or not). A foreign financial institution (FFI) is excluded from the definition of a legal entity customer if its foreign regulator collects and maintains beneficial ownership information about the FFI. CHAINCE SECURITIES LLC may rely on representations of the FFI as to whether the exclusion applies.

Internal recordkeeping and operational accounts: When CHAINCE SECURITIES LLC opens an account or subaccount (*e.g.,* to accommodate trading strategies) relating to an existing legal entity customer, the account is not considered a new account and is not subject to CDD beneficial ownership requirements. [Question 11, 2018 FAQs]

Trusts as beneficial owners: If a trust owns 25% or more of the equity interests of a legal entity customer, the beneficial owner is the trustee, regardless of whether the trustee is a natural person or a legal entity. If there are multiple co-trustees of a trust that is a 25% or greater owner of equity interests of a legal entity customer, CHAINCE SECURITIES LLC is not required to identify and verify the identity of all co-trustees. It must collect and verify the identity of, at minimum, one co-trustee of such a multi-trustee trust. [Questions 19 & 20, 2018 FAQs]

Pooled investment vehicles (PIV): For a PIV whose operators or advisers are not excluded from the definition of a legal entity customer, CHAINCE SECURITIES LLC is not required to look through the PIV to identify and verify individuals who own 25% or more of its equity interests. However, CHAINCE SECURITIES LLC is required to collect beneficial ownership information. [Question 18, 2018 FAQs]

Lower-risk customers: For certain lower-risk customers, the nature and purpose of the relationship can be developed by inherent or self-evident information.

7.17.4.4.4 Anti-Money Laundering Requirements

Beneficial owners are subject to AML requirements. See other requirements in this chapter.

7.17.4.4.5 Currency Transaction Reporting (CTR) Requirements

CDD requirements do not change existing CTR requirements. CHAINCE SECURITIES LLC will presume different businesses that share a common owner are operated separately and independently from each other and from the common owner. Transactions across commonly owned legal entity customers will not be aggregated absent indications the businesses are not operating independently (*i.e.,* same staff or location, accounts of one business are repeatedly used to pay the expenses of another business). Beneficial owners of a trust or estate account are not required when completing a CTR. Beneficial owner listing is only required if CHAINCE SECURITIES LLC knows that the transaction(s) requiring filing is made on behalf of a beneficial owner and results in either cash in or cash out totaling more than $10,000 during any one business day. [Questions 32 & 33, 2018 FAQs]

7.17.4.4.6 OFAC

Beneficial owners are subject to OFAC reviews outlined in this AML chapter.

7.17.4.5 Enhanced Due Diligence (EDD)

Some types of accounts, because of the potential risk for hiding the identity of underlying beneficial owners or money laundering activities, are subject to enhanced due diligence. The AML Compliance Officer will determine which accounts are subject to EDD and what reviews are necessary. Procedures for correspondent and private banking accounts are included in a separate section of this AML program. Certain trusts, corporate entities, shell entities, and private investment companies are examples of customers that may pose heightened risk.

EDD may include steps, in accordance with the level of risk presented, to identify and verify beneficial owners, to reasonably understand the sources and uses of funds in the account, and to reasonably understand the relationship between the customer and the beneficial owner. EDD information may be used for monitoring purposes and to determine whether there are discrepancies between information obtained regarding the account's intended purpose and expected account activity and the actual sources of funds and uses of the account.

7.17.4.6 Third Party Accounts

Customer ID required for third party accounts includes the following:

On behalf of an incompetent person: Obtain customer ID of the person holding power of attorney.

With power of attorney or trading authorization held by a third party: Obtain customer ID of the owner of the account. Customer ID is not necessary for the individual with authority over the account unless that person is unfamiliar to the RR or the circumstances regarding the opening of the account raises questions (customer requires wiring funds to an offshore address; third party is a foreign citizen; *etc.*).

7.17.4.7 Reserved

7.17.4.8 Intermediated Account Relationships

[Various guidance from the U.S. Treasury and SEC regarding mutual fund CIP rule, BD CIP rule, FAQs regarding FCMs and introducing brokers, and foreign accounts]

If an intermediary is the customer and CHAINCE SECURITIES LLC has no CIP obligation regarding the intermediary's underlying customers under existing guidance, CHAINCE SECURITIES LLC will treat the intermediary as its legal entity customer. For example, the intermediary may be treated as the customer for transactions through omnibus accounts if:

- the omnibus account was established to execute transactions for settlement at another institution or the intermediary provides limited customer information to CHAINCE;
- the limited information provided is used primarily for recordkeeping purposes or to establish sub-accounts that hold positions for limited durations;
- all transactions in the omnibus account are initiated by the intermediary; and
- the beneficial ownership has no direct control over the omnibus account.

7.17.4.9 Accounts For Non-Individuals

Account documents usually obtained for non-individual accounts (trust instruments, articles of incorporation, partnership agreements, government-issued business license, *etc.*) will usually satisfy customer ID requirements. In the case of corporations, a certified copy of the articles of incorporation is

required. These documents must be obtained within 30 days of account opening to satisfy the requirement.

7.17.4.10 Non-Documentary Methods Of Verifying Customer Identification

Non-documentary methods of verifying customer ID involve other procedures. Non-documentary methods must be used in the following circumstances:

- An individual is unable to present acceptable photo ID.
- The documents presented are unfamiliar.
- The account is opened without obtaining documents.
- The customer opens the account without appearing in person at CHAINCE.
- Other circumstances, at the discretion of the RR's supervisor, New Accounts, and/or the AML Compliance Officer, where CHAINCE SECURITIES LLC is unable to verify the customer's identity.

In these circumstances, a non-documentary method must be indicated by the RR on the new account application:

- Direct customer contact information
- Information from a consumer reporting agency or other database
- References from another financial institution
- Obtained a financial statement

7.17.4.11 Additional Verification For Certain Customers

For the following types of customers, a minimum of TWO forms of customer ID are required in addition to review and approval by the AML Compliance Officer **prior to** opening the account:

- Numbered accounts
- Accounts domiciled in high-risk countries included on the Treasury Dept. OFAC list (check with Operations personnel for a list of those countries or go to *http://www.treas.gov/offices/enforcement/lists/*)
- Accounts for foreign public officials (individuals in high office in other countries, their families and close associates, political party officials)

7.17.4.12 Lack Of Customer ID Verification

When CHAINCE SECURITIES LLC cannot form a reasonable belief that it knows the true identity of a customer, CHAINCE SECURITIES LLC will:

- not open an account
- impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity
- close an account after attempts to verify customer's identity fail

For **customers who fail to provide required ID or documents within 30 days of account opening,** the account will be restricted to liquidating transactions only until satisfactory ID verification is received.

For **accounts where non-documentary verification results in substantive, unresolved discrepancies** (information that is inconsistent such as name, address, taxpayer ID number, *etc.*), either the account will not be opened or will be immediately closed.

Where inability to verify raises questions about the customer, filing a Suspicious Activity Report will be considered (see the section *Suspicious Activity Reports*).

Questions regarding accounts that do not comply with requirements to verify customer ID should be referred to the AML Compliance Officer.

7.17.4.13 Customer Notice

Customers are provided notice, prior to opening an account, that their identification will be verified. This notice may be on CHAINCE SECURITIES LLC's web site, on new account applications, or in other disclosures provided at the time of account opening.

7.17.5 CIP Records

Customer identification verification records are retained with new account application records in accordance with rule recordkeeping requirements and the terms of the other financial institution's CIP including:

- all identifying information recorded on the new account application
- documentary verification including information from or copies of government-issued IDs or passports
- non-documentary verification
- account approval or disapproval
- resolution of discrepancies
- referral of the account to the AML Compliance Officer
- closing of an account that fails to meet CIP requirements
- other records as may be required

Records are retained for at least 5 years after the account is closed.

7.17.6 Comparison With Government Lists

As required by law, CHAINCE SECURITIES LLC compares customer information against government lists. The section *OFAC List And Blocked Property* in this Anti-Money Laundering Program describes comparison of accounts with lists published by the Treasury Dept and other sanctions lists

Approved:

Wilfred Daye

_____

Wilfred Daye

Chief Executive Officer

Date:8/11/2025