

California Lending Source

LO Contract & Office Policy Manual

Required Document Checklist:

- Please Fill, Sign, Date & Initial ALL PAGES in this packet
- Provide a complete, professional resume (NOTE: Resume must state FHA experience if any)

TABLE OF CONTENTS

Agent Information -	1
-ASSOCIATE-LICENSEE "LOAN OFFICER" COMMISSION AGREEMENT	2
-PURPOSE AND GENERAL DEFINITIONS + REQUIREMENTS/GENERAL STANDARDS	3
-LAW SUMMARY + FAIR LENDING & ANTI-DISCRIMINATION POLICY	4
-Background Check Policy and Procedure	5
-QUALITY CONTROL: OPERATIONS AND PERSONNEL	6
-Fraud & ANTI-MONEY LAUNDERING POLICIES-	10
-"Red Flags" Identity Theft Prevention Program	21
-RES/CLS POLICIES AND GUIDELINES+LO CONTRACT AGREEMENT	23
-Acknowledgement & Final Signature Page	27

AGENT INFORMATION

Date: _____

Name (as it appears on NMLS):

(First Name) (Last Name) "Nickname"

Cal DRE# NMLS#

Contact Info

Email: _____ Phone: _____

How did you hear about California Lending Source?

- Web Advertisement Phone Call Email

Preferred Payment Method for Commissions:

- Direct Deposit/Wire (\$10 fee) Check -Office Pickup
- Paid Directly from Escrow Check -Mail
- Transfer to BofA Account (free)

Note: Real Estate Source, Inc. / California Lending Source does not share any of this information with anyone outside of its organization. The information provided is used for bookkeeping records, transaction tracking, real estate activities and tax purposes only.

Initial _____

ASSOCIATE-LICENSEE “LOAN OFFICER” COMMISSION
AGREEMENT

(SENIOR LOAN OFFICERS)

A. Broker Fee

Real Estate Source, Inc. DBA “California Lending Source” (RES/CLS) will collect

A) \$795.00 BROKER FEE PER LOAN

B) 0.73% fee (from net commission) for state required insurance (see below)

Please note: E&O insurance is included in the per transaction broker fee

B. State Required Insurance

As of January 1st 2018, 0.73% will be deducted from all net commissions paid to Loan Officers in order to cover state required worker’s compensation insurance. [For example, assuming a gross \$10,795.00 Compensation; Deducting a broker fee of \$795.00 that gives a net commission of \$10,000.00, subtract 0.73% for worker’s comp insurance, (\$73.00 **OR** \$7.30/\$1,000) will leave \$9927.00 commission paid to agent] SEE BELOW VISUAL EXAMPLE:

\$10,795	←	Gross Commission
- \$795	←	CLS Broker Fee
<hr/>		
\$10,000	←	Net Commission
\$10,000	←	Net Commission
- \$73	←	Worker’s Comp Insurance (0.73% of Net Commission)
<hr/>		
\$9,927	←	Commission Paid to Agent

This will become effective January 1st 2018

Independent Contractor:

RES/CLS/ and LO agree that LO is not an employee of RES/CLS and may not be construed as such by reason thereof. Instead the LO is an independent contractor, and is hereby expressly prohibited from holding itself out as RES/CLS’s employee. LO shall have no authority to sign any writing on behalf of RES/CLS or to commit RES/CLS or its wholesale lenders in any manner whatsoever to fund loans. Broker shall not make express or implied representations or warranties to loan applicant(s) that conflict with the authority set forth herein.

I, the Loan Officer/Licensed Loan Originator signing below, understand the above terms of Real Estate Source, Inc’s/DBA “California Lending Source”(RES/CLS) compensation plan and I hereby agree to RES/CLS compensation terms. Real Estate Source, Inc.


Loan Officer (Print Name)

Signed

Date

Real Estate Source, Inc.
DBA “California Lending Source”

Brokerage

Broker  Tony Soheil Dini
NMLS#288511

NMLS#

PURPOSE AND GENERAL DEFINITIONS

DEFINITIONS

Hereafter, the employing broker Real Estate Source, Inc. DBA "California Lending Source" shall be referred to as "RES/CLS" . Also, the Loan Officer signing this contract and between whom RES/CLS and the Loan Officer are entering into an agreement, shall be referred to as "LO". "Lender" refers to any wholesale lender with which RES/CLS has a working relationship. With RES/CLS being the Loan Broker/Originator and these wholesale lenders being referred to hereafter as "Lender"

PURPOSE

The purpose of this document is to ensure that Real Estate Source, Inc. & it's agents and Loan Officers maintain compliance with HUD/FHA requirements and Wholesale Lender requirements for Sponsored Originators along with all federal and state real estate, banking, anti-money laundering, and lending regulations.

Effective Date:

The Effective Date of this Agreement shall be the date on which it is signed by Loan Officer.

Governing Law:

This Agreement shall be governed by and construed according to the laws of the State of California, without regard to its conflict of laws principles.

Captions and Section Headings:

Captions and section headings used herein are for convenience only and are not part of this Agreement and shall not be used in construing it.

Survival:

The covenants, indemnities, agreements, representations, and warranties made herein shall survive the termination of this Agreement, unless the context clearly provides otherwise.

Termination of this Agreement:

This agreement between RES/CLS and its agent/loan officer may be terminated by RES/CLS at any time for any reason. The Loan Officer may terminate this agreement and therefore leave the employ of RES/CLS at any time for any reason but must still comply with the terms set forth in this agreement in the event of termination of this agreement.

REQUIREMENTS/GENERAL STANDARDS:

- All LOs must use company provided email address and Google Drive when conducting business involving origination of mortgages.
- All LOs must use company provided copy of POINT to fill loan applications and submit to processor.
- All LOs must keep in good standing and maintain active, NMLS and RE licenses in the state of employment with RES/CLS.
- NMLS must be displayed on all marketing material and email signatures alongside CalDRE# as detailed on the compliance page on the following pages: morecommission.info and californialendingsource.com
 - <https://www.morecommission.info/compliance-announcements>
 - <https://www.californialendingsource.com/california-lending-source-lo-compliance>
- ABSOLUTELY NO RUNNING OF CREDIT without uploading a fully filled & signed copy of Borrower Sig authorization & Affiliated Business disclosure.
- ABSOLUTELY NO GIVING OF ANY REFERRALS, COMMISSION CREDITS, GIFT CARDS, OR ANY OTHER FORM OF COMPENSATION TO ANYONE, EVER.
- All files put in Google Drive and shared w/ broker & processor
- LO shall not have any affiliates, partner, director, principal manager, employee or 1099 contractor who is currently suspended under a limited denial of participation (LDP); under indictment for or has been convicted of an offense that reflects adversely upon the sponsored originators integrity, competence or fitness to meet responsibilities of a sponsored originator; will not engage in business practices that do not conform to generally accepted practices of prudent origination or that demonstrate irresponsibility; have been convicted of or who has pled guilty to a felony related to participation in the real estate or mortgage loan industry; or is in violation of provisions of the SAFE Mortgage Licensing Act of 2008 or any provision of State law.
- Operations are conducted in a professional, business-like environment;
- LO will be at all times in compliance with the provisions of the Real Estate Settlement Procedures Act (RESPA), including the distribution to mortgagors of the Special Information Booklet, Good Faith Estimates and disclosure of business relationships with a particular provider of services.

- The work of each LO & Loan Processor affiliated with RES/CLS can and will be audited by RES/CLS at any time during the course of, or after the close of any and all transactions that LO is/has participated in.
- Labelling Files: [<https://www.morecommission.info/compliance-announcements>]
- How to use Google Drive: [<https://www.morecommission.info/file-upload>]
- Physical documents must either be delivered to the office or kept in a locked and secured location.

LAW SUMMARY

Fair Housing Act (FHA)

The FHA prohibits discrimination in lending based on prohibited factors (race, color, religion, national origin, handicap, familial status, gender, and age). It also prohibits practices such as redlining, making excessively low appraisals, use of subjective or non-reviewable criteria, creating and exploiting a racially exclusive image, expressing intent to discriminate, and discriminating against women.

Equal Credit Opportunity Act (ECOA)

ECOA Prohibits discouraging applications and limits the manner in which lenders can inquire about marital status, spouses, former spouses, alimony and child support. Also establishes requirements for lenders such as providing copies of appraisals, providing appropriate disclosures and preserving records from the application/transaction.

Fair Credit Reporting

Fair Credit Reporting Act Regulates the activities of reporting agencies and the users of credit information and protects individuals from invasion of privacy and the dissemination of false or inaccurate information & requires disclosures when adverse action is taken.

Home Mortgage Disclosure Act (HMDA)

HMDA requires lenders to collect certain information about the loans they make so the government can track applications and ensure lenders are taking and approving applications equally for all groups of people.

Truth in Lending Act (TILA)

TILA requires the disclosure of information about the lender; amount financed, and finance charge, payments, security and interest rate. Also establishes that borrowers have a right to rescind most loans secured by their primary residence within three business days of loan closing.

Real Estate Settlement Procedures Act (RESPA)

RESPA requires lenders to provide advance disclosure information on loan settlement procedures and costs & also regulates the ways in which referrals between companies can be made and establishes parameters for the amount of money borrowers are required to place in an escrow account established for taxes and insurance.

Telemarketing Sales Rule

Telemarketing Sales Rule establishes parameters regarding the manner in which telemarketing can be conducted. Specifies times during which telemarketing is permitted, information that must be disclosed to consumers during telemarketing, and those records must be kept of telemarketing transactions.

Gramm Leach Bliley Act (GLB)

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and Pretexting Provisions.

FAIR LENDING & ANTI-DISCRIMINATION POLICY

It is against the policy of Real Estate Source, Inc. and its DBA "California Lending Source" (RES/CLS) TO DISCRIMINATE ON ANY BASIS, INCLUDING A LOAN APPLICANT'S RACE, NATIONAL ORIGIN, RELIGION, MARITAL STATUS, GENDER, OR AGE.

RES/CLS is committed to making high quality mortgage services available to diverse communities and customers on an equal opportunity basis. Loan products are available to all individuals who meet our lending criteria without regard to race, color, religion, national origin or ancestry, sex, marital status, handicap status, familial status, age (provided the applicant has the capacity to enter into a binding contract), receipt of public assistance, or the exercise of legal rights under the Consumer Credit Protection Act. RES/CLS does not tolerate discrimination of any kind and any act of discrimination violates RES/CLS's policy and its corporate commitment of providing homeownership opportunities to all qualified applicants. Our stand on nondiscrimination is absolute; there is a zero tolerance for any discriminatory act or behavior. Treating everyone fairly and making decisions based solely on creditworthiness is "Win/Win", plain and simple.

CONSISTENT AND FAIR TREATMENT

It is the policy of RES/CLS to treat all consumers consistently and fairly and in compliance with fair lending laws. Our LOs will offer assistance, encouragement and services in a fair, equitable and consistent manner during performance of their jobs. We will communicate our fair lending policy to all of our LOs and hold them accountable for treating all consumers consistently and fairly.

It is our policy and our practice to comply fully with the letter and spirit of fair lending statutes, including but not limited to, those cited below.

RES/CLS does not discriminate based on:

- | | | |
|-------------------|-------------------------------|--------------------------------|
| ◆ Race | ◆ Gender | ◆ Religion |
| ◆ Handicap | ◆ Exercise of Consumer Rights | ◆ Receipt of Public Assistance |
| ◆ National Origin | ◆ Age ◆ Marital Status | ◆ Family Status |
| ◆ Color | | |

Additionally, we commit to adherence to all state, municipal and local laws, regulations, statutes and all other laws regulating our industry. We expect all LOs to fully understand fair lending practices and to deal fairly and equally with all loan applicants. We insist that all negotiations be in good faith and without bias. We require that the letter and the spirit of fair lending practices, the following Federal laws, and all statutes governing lending and equal rights be complied with in each jurisdiction that the LO conducts business.

Background Check Policy and Procedure

All offers of employment at Real Estate Source, Inc. and its DBA California Lending Source (RES/CLS) are contingent upon clear results of a thorough background check. Background checks will be conducted on all final candidates and on all employees who are promoted, as deemed necessary.

Background checks will include:

- Social Security Verification: validates the applicant's Social Security number, date of birth and former addresses.
- Prior Employment Verification: confirms applicant's employment with the listed companies, including dates of employment, position held and additional information available pertaining to performance rating, reason for departure and eligibility for rehire. This verification will be run on the past two employers or the previous five years, whichever comes first.
- Personal and Professional References: calls will be placed to individuals listed as references by the applicant.
- Educational Verification: confirms the applicant's claimed educational institution, including the years attended and the degree/diploma received.
- Criminal History: includes review of criminal convictions and probation. The following factors will be considered for applicants with a criminal history:
 1. The nature of the crime and its relationship to the position.
 2. The time since the conviction.
 3. The number (if more than one) of convictions.
 4. Whether hiring, transferring or promoting the applicant would pose an unreasonable risk to the business, its employees or its customers and vendors.

The following additional background searches will be required if applicable to the position:

Motor Vehicle Records: provides a report on an individual's driving history in the state requested. This search will be run when driving is an essential requirement of the position.

Credit History: confirms candidate's credit history. This search will be run for positions that involve management of RES/CLS funds and/or handling of cash or credit cards.

Procedure

Final candidates must complete a background check authorization form and return it to Human Resources.

Human Resources will order the background check upon receipt of the signed release form, and either internal HR staff or an

employment screening service will conduct the checks. A designated HR representative will review all results.

The HR representative will notify the hiring manager regarding the results of the check. In instances where negative or incomplete information is obtained, the appropriate management and the director of Human Resources will assess the potential risks and liabilities

related to the job's requirements and determine whether the individual should be hired. If a decision not to hire or promote a candidate is made based on the results of a background check, there may be certain additional Fair Credit Reporting Act (FCRA) requirements that will be handled by Human Resources in conjunction with the employment screening service (if applicable). Background check information will be maintained in a file separate from employees' personnel files for a minimum of five years. Real Estate Source, Inc. reserves the right to modify this policy at any time without notice.

QUALITY CONTROL: OPERATIONS AND PERSONNEL:

I. PURPOSE

The purpose of the Quality Control Plan of Real Estate Source Inc/California Lending Source (RES/CLS) is to evaluate and monitor the overall quality of mortgage loan production for all types of loans, both conventional and government. The overriding controls of Quality Control are: to assure compliance with FHA's and RES/CLS own origination requirements throughout its operations; to protect RES/CLS, FHA and it's various Investors/ Lenders from unacceptable risk; to guard against errors, omissions and fraud; and to assure swift and appropriate corrective action. This Quality Control Plan is designed to be in compliance with Chapter 5 of HUD Handbook 4000.1.

RES/CLS will maintain manuals, which set forth the Company policy relative to all facets of RES/CLS's mortgage business. This includes, but is not limited to, all HUD notices and guidelines as they relate to HUD processing. HUD manuals will also be maintained as designated in HUD Handbook 4000.1.

II. PROGRAM INTEGRITY

The quality control monitoring and review function will be performed by designated personnel who do not perform the processing or loan origination functions. This review shall be performed on a monthly basis on files which have closed within the last 30 days. Records of reviews are to be maintained for a minimum of two years. Quality control review findings will be communicated to the appropriate production staff and actions taken to correct any deficiencies which are noted. Notification to investors and/or correspondents of problems and corrective actions taken will be made as appropriate.

III. PROCEDURES

Ensure that no participants in the mortgage transaction (excluding the seller of a principal residence) has been debarred or suspended, or is under an LDP for the program and jurisdiction. RES/CLS will periodically check employee list, at least semi-annually. RES/CLS will ensure that the mortgage applicant is not ineligible due to a delinquent federal debt.

Loans to receive review will be selected by random sample. The sample will be 10% of all loans closed by RES/CLS. Discretionary or problem reviews will be in addition to the random sample.

Review will include recertification of deposits (when needed), employment, and gifts, and a new credit report from a different reporting agency. These new exhibits will be in addition to the following review of existing exhibits relative to the analysis of mortgagor. The procedures will be revised periodically to reflect changes in FHA requirements. Employees responsible for the completion of the functions tested should be identified and failures or errors noted in this report.

EARLY PAYMENT DEFAULT

In addition to the loans selected for routine quality control reviews, mortgagees must review all loans going into default within the first six payments. As defined here, early payment defaults are loans that become 60 days past due.

HOME MORTGAGE DISCLOSURE ACT REPORTING

Verify that RES/CLS is in compliance with HMDA reporting requirements and HUD's requirements for reporting FHA-insured mortgages. Ensure that the reports are filed timely, that the information being reported is accurate and the information is being reported correctly.

PROCESSING

1. Ensure the processing of the file was performed by an authorized Company employee or an Authorized agent.
2. Review the Initial Application Disclosures, LE, TIL and compare with the application date to ensure compliance with RESPA.

ANALYSIS OF MORTGAGOR

For all files that have alternative documentation, other than that listed below, note the type of alternative documentation and determine the most efficient way to recertify the data.

1. Determine that a factual data credit report (in compliance with the credit report standards described in HUD Handbook 4155.1 as revised) has been obtained on all borrowers who will be responsible for the repayment of the mortgage.
 2. Make sure the credit report:
 - a. Identifies the subjects of the report.
 - b. Lists all accounts by name, location, and account number.
 - c. Lists employment for minimum of last two years.
 - d. Gives subject's current address and prior addresses for a minimum of two years.
 - e. Includes any pertinent information that contributes to a complete credit history of the borrower or borrowers.
 3. Ascertain that derogatory credit information is investigated and explained.
 4. If more than one credit report was ordered, then ensure all were submitted with the package to HUD/FHA or the Direct Endorsement Underwriter or the Investor.

 5. Review verifications of income and deposit to:
 - a. Ascertain that VOEs cover a two-year period or as required by Program/ Investor Guidelines and findings.
 - b. Assure that applicants' signatures are valid and consistent on any documents that require Borrower signatures and elsewhere in the file.
 - c. Confirm by checking dates sent and dates received that VOEs and VODs were emailed/ mailed and did not pass through the hands of the applicant or any other third party.
 - d. Ascertain that recent large deposits and/or derogatory information on the VODs are explained by the borrower, as required by Program guidelines/ findings.

 6. Review deposit receipt and/or preliminary title report to make sure all information regarding purchase or refinance transactions are properly reported on the application.
 7. Review accuracy of processing calculations on the application and on any worksheets.
 8. Review borrower rating to assure it is consistent with the Company and investor guidelines.
 9. If relevant documents were signed in blank by the mortgagor or the Company employee, ensure that all documents were initialed by mortgagor/employee.
 10. Ensure that the preliminary loan application lists each outstanding debt & asset and was used to qualify the mortgagor and that the information is consistent with the final application and all credit documents.

 11. Ensure any outstanding judgments on the Credit Report were on the HUD 92900, Mortgage Credit Analysis Worksheet (MCAW), and acceptably explained in accompanying documentation.
 12. Determine whether the loan file contains pertinent documentation of the mortgagor's source of funds for the required investment, the acceptability of that source, and that any obligation to repay the funds is included on the MCAW. This is especially important in cases where the source was other than the applicant's accounts at a financial institution.
 13. Ensure if mortgagor is self employed, the file has a financial statement, tax return and business credit report (if required) and/ or any other required documentation as set forth by Program/ Investor guidelines and findings.

 14. Ensure if there is a gift letter, it has the relationship of donor and no repayment and funds are both sourced and either deposited into mortgagor's account or sent directly to the Closing Agent, as required by Program/ Investor Guidelines and findings.
 15. Ensure the CD and HUD-1 (if applicable) is accurately prepared and properly certified. Assure that only FHA allowable fees and charges were paid by the mortgagor. The CD and HUD-1 should be compared with other relevant loan documents to determine whether the mortgagor made the required minimum investment and whether any credits resulted in over-insured mortgages.
 16. Determine whether the seller acquired the property at the time of or soon before closing, indicating a possible property "flip" and if so, that appropriate Investor/ Program guidelines are followed.

 17. If possible, determine whether the mortgagor transferred the property at the time of closing or soon after closing, indicating the possible use of a "straw buyer" in the transaction.
-

18. Ensure all conflicting information is resolved and properly documented in writing prior to submission of the loan to underwriting.
19. Determine whether there are sufficient and documented compensating factors if debt ratios exceed FHA limits.
20. Determine the accuracy and completeness of underwriting conclusions and mortgagee documentation.
21. Ensure the completed Underwriter's Mortgage Credit Analysis Worksheet, HUD 92900WS is retained in the file.
22. Determine all conditions were cleared prior to closing/ funding/ recording.
23. Determine whether the loan file contains all required loan processing, underwriting and legal documents.
24. If and when able, determine whether the loan was submitted for insurance within 60 days of closing or included a payment history showing the loan was current when it was submitted for mortgage insurance.
25. Analyze the overage obtained on the file and ensure compliance with Company guidelines.
26. Determine whether all items requiring documentation have been properly evidenced and retained in the file.

APPRAISAL REVIEW

1. Review all sections of the appraisal form and determine if they have been properly completed.
2. Review to determine that any title exceptions such as easements or encroachments disclosed in the title policy are considered by the appraiser.
3. Determine that flood insurance has been obtained if the property is located in a designated flood zone.
4. Determine that the estimate of value is properly supported by appropriate and timely cost, rental, and comparable sales data.
5. Review the appraiser's remarks to assure appropriate requirements were called for to effect needed repairs and eliminate deficiencies and that they meet minimum safety and soundness requirements.

SITE REVIEW

RES/CLS's offices, if engaged in origination or servicing of FHA-insured loans, must be reviewed to determine that they are in compliance with HUD's requirements. The review should be performed by qualified personnel not involved in the day-to-day processes they are reviewing or by an outside firm.

The review must include confirmation of the following:

1. The office is properly registered with FHA and the address is current;
2. Operations are conducted in a professional, business-like environment;
3. If located in a commercial space, the office is properly and clearly identified for any walk-in customers; has adequate office space and equipment; is in a location conducive to mortgage lending; and is separated from any other entity by walls or partitions (entrances and reception areas may be shared);
4. If located in noncommercial space, the office has adequate office space and equipment; displays fair housing poster if public is received; if it is open to receive the public, it must be accessible to persons with disabilities, including those with mobility impairments; if it is not open to the public, but used occasionally to meet with members of the public, alternate means of accommodations may be used to service persons with disabilities;
5. If Servicing, the servicing office provides toll-free lines or accepts collect calls from mortgagors.
6. The office is sufficiently staffed with trained personnel
7. Office personnel have access to relevant statutes, regulations, HUD issuances and Handbooks, either in hard copy or electronically.
8. Procedures are revised to reflect changes in HUD requirements and personnel are informed of the changes.
9. Personnel at the office are all employees of the mortgagee or contract employees performing functions that FHA allows to be outsourced; and
10. The office does not employ or have a contract with anyone currently under debarment or suspension, or a Limited Denial of Participation.

MIP REVIEW

For all FHA Loans, If and when able, assure that HUD-FHA Mortgage Insurance Premiums (MIP's) are remitted within 15 days from the date of loan closing and that late charges and interest and penalties (if any) are promptly submitted for single family mortgages.

REAL ESTATE SETTLEMENT PROCEDURES ACT - RES/CLS must verify compliance with the provisions of RESPA, including, but not limited to the following:

1. Distributing the Special Information Booklet to mortgage applicants;
2. Providing applicants with CFPB "Know before you Owe", LE and the settlement costs relating to obtaining a mortgage, any other required documents/ disclosures, no later than 3 business days after the application is received or prepared;
3. Providing applicants with their CD, HUD-1 if applicable, and any other required closing documents/ disclosures;
4. Disclosing transfer of servicing; and
5. Disclosing business relationships with affiliated entities.

REJECTED LOANS

Of all FHA loans rejected, RES/CLS will review a minimum of 10% concentrating on the following areas:

- Ensuring that the reasons given for rejection were valid;
- Ensuring that each rejection has the concurrence of an officer or senior staff person of RES/CLS, or a committee chaired by a senior staff person or officer;
- Ensuring that the requirements of the Equal Credit Opportunity Act are met and documented in each file;
- Ensuring that no Civil Rights violations are committed in rejection of applications; and
- Where possible discrimination is noted, RES/CLS will take immediate corrective action.

IV. RECONCILIATION

Upon completion of all phases of review, quality control management personnel will reconcile all of the information and determine if the actions taken and the ultimate products meet the standards for the program or investor involved with the individual loan.

V. CORRECTIVE ACTIONS

When discrepancies from original documents or exhibits are found, the file will immediately be analyzed for final disposition. Findings must be reported to RES/CLS's senior management within one month of completion of the initial report. Management must take prompt action to deal appropriately with any material findings. The final report or an addendum must identify actions being taken, the timetable for their completion, and any planned follow-up activities. If any patterns or trends are noted during these reviews, which are detrimental to RES/CLS, our investors or government agency, they will be promptly notified of such finding in writing.

Findings of fraud or other serious violations must be immediately referred, in writing to the Director of the Quality Assurance Division in the HUD Homeownership Center (HOC) having jurisdiction.

This should be done using the Lender Reporting feature in the Neighborhood Watch Early Warning System. Findings discovered by employees during the normal course of business and by quality control staff during reviews/audits of FHA loans are reported to HUD within 60 days of the initial discovery.

VI. PROCEDURAL COMPLIANCE

In addition to the review of case files, RES/CLS will comply with various Federal and State laws including, but not limited to, the following:

- Fair Housing Act
- Fair Lending Act
- ECOA
- RESPA
- TILA
- TRID
- Suspicious Activity Reporting

- Red Flags Rule
- Anti-Money Laundering Rules

Possible violations or incidences of discrimination must be reported to the Office of Fair Housing and Equal Opportunity in HUD's headquarters in a timely manner; any other incidences are to be reported to the appropriate Local/ State/ Government Agency or Regulatory Body.

VII. ADMINISTRATION OF THE PROGRAM

1. We are responsible for oversight, development, implementation and administration of this Quality Control Program and will hold its staff accountable for their part in its implementation. We will continually make changes to the program as necessary to address changing identity theft risks.
2. We have designated its president and lead processor as the individuals to implement this Program and provide staff training.
3. Appropriate review will be conducted by us to address the program material matters and evaluate the following:
 - The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with loan application requests
 - Service provider arrangements
 - Any significant incidents involving identity theft and management's response
 - Recommendations for material changes to the Program.

FRAUD & ANTI-MONEY LAUNDERING POLICIES

Compliance and Supervisory Procedures

1. Policy

It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the Bank Secrecy Act (BSA) and its implementing regulations.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment.

Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Our AML policies, procedures and internal controls are designed to ensure compliance with all applicable BSA regulations and FINRA rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

Rules: 31 C.F.R. § 103.120(c); FINRA Rule 3310.

2. AML Compliance Person Designation and Duties

The duties of the AML Compliance Person will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees, and review NASD Rules 1021 and 1031 for any applicable registration requirements. The AML Compliance Person will also ensure that the firm keeps and maintains all of the required AML records and will ensure that Suspicious Activity Reports (SAR-SFs) are filed with the Financial Crimes

Enforcement Network (FinCEN) when appropriate. The AML Compliance Person is vested with full responsibility and authority to enforce the firm's AML program.

The firm will provide FINRA with contact information for the AML Compliance Person, including: (1) name; (2) title; (3) mailing address; (4) email address; (5) telephone number; and (6) facsimile number through the FINRA Contact System (FCS). The firm will promptly notify FINRA of any change in this information through FCS and will review, and if necessary update, this information within 17 business days after the end of each calendar year. The annual review of FCS information will be conducted by Person's Name and will be completed with all necessary updates being provided no later than 17 business days following the end of each calendar year. In addition, if there is any change to the information, Person's Name will update the information promptly, but in any event not later than 30 days following the change.

Rules: 31 C.F.R. § 103.120; FINRA Rule 3310, NASD Rule 1160.

Resources: NTM 06-07; NTM 02-78. Firms can submit their AML Compliance Person information through FINRA's FCS Web page.

3. Giving AML Information to Federal Law Enforcement Agencies and Other Financial Institutions

a. FinCEN Requests under USA PATRIOT Act Section 314

We will respond to a Financial Crimes Enforcement Network (FinCEN) request concerning accounts and transactions (a 314(a) Request) by immediately searching our records to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity or organization named in the 314(a) Request as outlined in the Frequently Asked Questions (FAQ) located on FinCEN's secure Web site. We understand that we have 14 days (unless otherwise specified by FinCEN) from the transmission date of the request to respond to a 314(a) Request. We will designate through the FINRA Contact System (FCS) one or more persons to be the point of contact (POC) for 314(a) Requests and will promptly update the POC information following any change in such information. We will maintain documentation that we have performed the required search by maintaining a log showing the date of the request, the number of accounts searched, the name of the individual conducting the search and a notation of whether a match was found.

We will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. We will review, maintain and implement procedures to protect the security and confidentiality of requests from FinCEN similar to those procedures established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act with regard to the protection of customers' nonpublic information.

We will direct any questions we have about the 314(a) Request to the requesting federal law enforcement agency as designated in the request.

Unless otherwise stated in the 314(a) Request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the periodic 314(a) Requests as a government provided list of suspected terrorists for purposes of the customer identification and verification requirements.

b. National Security Letters

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. No broker-dealer, officer, employee or agent of the broker-dealer can disclose to any person that a government authority or the FBI has sought or obtained access to records. Firms that receive NSLs must have policies and procedures in place for processing and maintaining the confidentiality of NSLs. If you file a Suspicious Activity Report (SAR-SF) after receiving a NSL, the SAR-SF should not contain any reference to the receipt or existence of the NSL.

c. Grand Jury Subpoenas

Grand juries may issue subpoenas as part of their investigative proceedings. The receipt of a grand jury subpoena does not in itself require the filing of a Suspicious Activity Report (SAR-SF). However, broker-dealers should conduct a risk assessment of the customer who is the subject of the grand jury subpoena, as well as review the customer's account activity. If suspicious activity is uncovered during this review, broker-dealers should consider elevating the risk profile of the customer and file a SAR-SF in accordance with the SAR-SF filing requirements. Grand jury proceedings are confidential, and a broker-dealer that receives a subpoena is prohibited from directly or indirectly notifying the person who is the subject of the investigation about the existence of the grand jury subpoena, its contents or the information used to reply to it. If you file a SAR-SF after receiving a grand jury subpoena, the

SAR-SF should not contain any reference to the receipt or existence of it. The SAR-SF should provide detailed information about the facts and circumstances of the detected suspicious activity.

d. Voluntary Information Sharing With Other Financial Institutions Under USA PATRIOT Act Section 314(b)

We will share information with other financial institutions regarding individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering. We will ensure that the firm files with FinCEN an initial notice before any sharing occurs and annual notices thereafter. We will use the notice form found at [F i n C E N's Website](#) . Before we share information with another financial institution, we will take reasonable steps to verify that the other financial institution has submitted the requisite notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FinCEN will make available. We understand that this requirement applies even to financial institutions with which we are affiliated, and that we will obtain the requisite notices from affiliates and follow all required procedures.

We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, for example, by segregating it from the firm's other books and records.

We also will employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:

- identifying and, where appropriate, reporting on money laundering or terrorist activities;
- determining whether to establish or maintain an account, or to engage in a transaction; or
- assisting the financial institution in complying with performing such activities.

e. Joint Filing of SARs by Broker-Dealers and Other Financial Institutions

We will file joint SARs in the following circumstances. We will also share information about a particular suspicious transaction with any broker-dealer, as appropriate, involved in that particular transaction for purposes of determining whether we will file jointly a SAR-SF.

We will share information about particular suspicious transactions with our clearing broker for purposes of determining whether we and our clearing broker will file jointly a SAR-SF. In cases in which we file a joint SAR-SF for a transaction that has been handled both by us and by the clearing broker, we may share with the clearing broker a copy of the filed SAR-SF.

If we determine it is appropriate to jointly file a SAR-SF, we understand that we cannot disclose that we have filed a SAR-SF to any financial institution except the financial institution that is filing jointly. If we determine it is not appropriate to file jointly (e.g., because the SAR-SF concerns the other broker-dealer or one of its employees), we understand that we cannot disclose that we have filed a SAR-SF to any other financial institution or insurance company.

4. Checking the Office of Foreign Assets Control Listings

Before opening an account, and on an ongoing basis, we will check to ensure that a customer does not appear on the SDN list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC. Because the SDN list and listings of economic sanctions and embargoes are updated frequently, we will consult them on a regular basis and subscribe to receive any available updates when they occur. With respect to the SDN list, we may also access that list through various software programs to ensure speed and accuracy. See also [F I N R A' s O F A C Search Tool](#) that screens names against the SDN list. We will also review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated and he will document the review.

If we determine that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, we will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC within 10 days. We will also call the OFAC Hotline at (800) 540-6322 immediately.

Our review will include customer accounts, transactions involving customers (including activity that passes through the firm such as wires) and the review of customer transactions that involve physical security certificates or application-based investments (e.g., mutual funds).

5. Customer Identification Program

In addition to the information we must collect under FINRA Rule 2010 (Standards of Commercial Honor and Principles of Trade), NASD Rules 2310 (Recommendations to Customers - Suitability) and 3110 (Books and Records) and Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3(a)(9) (Beneficial Ownership regarding Cash and Margin Accounts) and 17a-3(a)(17) (Customer Accounts), we have established, documented and maintained a written Customer Identification Program (CIP). We will collect certain minimum customer identification information from each customer who opens an account; utilize risk-based measures to verify the identity of each customer who opens an account; record customer identification information and the verification methods and results; provide the required adequate CIP notice to customers that we will seek identification information to verify their identities; and compare customer identification information with government-provided lists of suspected terrorists, once such lists have been issued by the government. See Section 5.g. (Notice to Customers) for additional information. OR:

We will collect information to determine whether any entity opening an account would be excluded as a customer pursuant to the exceptions outlined in 31 CFR 103.122(a)(1)(i), in that we do not establish formal relationships with "customers" for the purpose of effecting transactions in securities. If in the future the firm elects to open customer accounts or to establish formal relationships with customers for the purpose of effecting transactions in securities, we will first establish, document and ensure the implementation of appropriate CIP procedures.

a. Required Customer Information

Prior to opening an account, a loan officer will collect the following information for all accounts, if applicable, for any person, entity or organization that is opening a new account and whose name is on the account:

- (1) the name;
- (2) date of birth (for an individual);
- (3) an address, which will be a residential or business street address (for an individual), an Army Post Office (APO) or Fleet Post Office (FPO) box number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address), or a principal place of business, local office, or other physical location (for a person other than an individual); and
- (4) an identification number, which will be a taxpayer identification number (for U.S. persons), or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard (for non-U.S. persons).

In the event that a customer has applied for, but has not received, a taxpayer identification number, we will [add procedures describing who, what, when and how] to confirm that the application was filed before the customer opens the account and to obtain the taxpayer identification number within a reasonable period of time after the account is opened.

b. Customers Who Refuse to Provide Information

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our firm will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, our

AML Compliance Person will be notified so that we can determine whether we should report the situation to FinCEN on a SAR-SF.

c. Verifying Information

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. A loan officer will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).

We will verify customer identity through documentary means, non-documentary means or both. We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. We may also use non-documentary means, if we are still uncertain about whether we know the true identity of the customer. In verifying the information, we will consider whether the identifying information that we receive, such as the customer's name, street address, zip

code, telephone number (if provided), date of birth and Social Security number, allow us to determine that we have a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).

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

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

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

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

- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source [identify reporting agency, database, etc.];
- Checking references with other financial institutions; or
- Obtaining a financial statement.

We will use non-documentary methods of verification when:

- (1) the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;
- (2) the firm is unfamiliar with the documents the customer presents for identification verification;
- (3) the customer and firm do not have face-to-face contact; and
- (4) there are other circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documentary means.

We will verify the information within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before

we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, we will, after internal consultation with the firm's AML Compliance Person, file a SAR-SF in accordance with applicable laws and regulations.

We recognize that the risk that we may not know the customer's true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated by the U.S. as a primary money laundering jurisdiction, a terrorist concern, or has been designated as a non-cooperative country or territory. We will identify customers that pose a heightened risk of not being properly identified. We will also take the following additional measures that may be used to obtain information about the identity of the individuals associated with the customer when standard documentary methods prove to be insufficient:

d. Lack of Verification

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (1) not open an account; (2) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (3) close an account after attempts to verify customer's identity fail; and (4) determine whether it is necessary to file a SAR-SF in accordance with applicable laws and regulations.

Rule: 31 C.F.R. §103.122(b)(2)(iii).

e. Record keeping

We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We will keep records containing a

description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We will retain records of all identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the record is made.

Rule: 31 C.F.R. §103.122(b)(3).

f. Comparison with Government-Provided Lists of Terrorists

At such time as we receive notice that a federal government agency has issued a list of known or suspected terrorists and identified the list as a list for CIP purposes, we will, within a reasonable period of time after an account is opened (or earlier, if required by another federal law or regulation or federal directive issued in connection with an applicable list), determine whether a customer appears on any such list of known or suspected terrorists or terrorist organizations issued by any federal government agency and designated as such by Treasury in consultation with the federal functional regulators. We will follow all federal directives issued in connection with such lists.

We will continue to comply separately with OFAC rules prohibiting transactions with certain foreign countries or their nationals.

Rule: 31 C.F.R. §103.122(b)(4).

Resources: NTM 02-21, page 6, n.24; 31 C.F.R. § 103.122.

g. Notice to Customers

We will provide notice to customers that the firm is requesting information from them to verify their identities, as required by federal law. We will inform them over the telephone that we will need identifying documents and will verify said documents in person when a new account is opened.

h. Reliance on Another Financial Institution for Identity Verification

We may, under the following circumstances, rely on the performance by another financial institution (including an affiliate) of some or all of the elements of our CIP with respect to any customer that is opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings or other financial transactions:

- when such reliance is reasonable under the circumstances;
- when the other financial institution is subject to a rule implementing the anti-money laundering compliance program requirements of 31 U.S.C. § 5318(h), and is regulated by a federal functional regulator; and
- when the other financial institution has entered into a contract with our firm requiring it to certify annually to us that it has implemented its anti-money laundering program and that it will perform (or its agent will perform) specified requirements of the customer identification program.

6. General Customer Due Diligence

It is important to our AML and SAR-SF reporting program that we obtain sufficient information about each customer to allow us to evaluate the risk presented by that customer and to detect and report suspicious activity. When we open an account for a customer, the due diligence we perform may be in addition to customer information obtained for purposes of our CIP.

For each account meeting the following criteria we will take steps to obtain sufficient customer information to comply with our suspicious activity reporting requirements. Such information should include

- the customer's business;
- the customer's anticipated account activity (both volume and type);
- the source of the customer's funds.

For accounts that we have deemed to be higher risk, we will obtain the following information

- the purpose of the account;
- the source of funds and wealth;
- the beneficial owners of the accounts;
- the customer's (or beneficial owner's) occupation or type of business;

- financial statements;
- banking references;
- domicile (where the customer's business is organized);
- description of customer's primary trade area and whether international transactions are expected to be routine;
- description of the business operations and anticipated volume of trading;
- explanations for any changes in account activity.

We will also ensure that the customer information remains accurate.

7. Correspondent Accounts for Foreign Shell Banks

Our firm does not establish, maintain, administer or manage correspondent accounts for foreign banks, we will not attempt to open a correspondent account. This includes our firm and our customers.

8. Due Diligence and Enhanced Due Diligence Requirements for Correspondent Accounts of Foreign Financial Institutions

Our firm does not do business with customers who want to compensate through or use foreign financial institutions

9. Due Diligence and Enhanced Due Diligence Requirements for Private Banking

Accounts/Senior Foreign Political Figures

Our firm does not open or maintain private banking accounts

10. Compliance with FinCEN's Issuance of Special Measures Against Foreign Jurisdictions

Financial Institutions or International Transactions of Primary Money Laundering Concern

We do not maintain any accounts with any foreign jurisdiction or financial institution. However, if FinCEN issues a final rule imposing a special measure against one or more foreign jurisdictions or financial institutions, classes of international transactions or types of accounts deeming them to be of primary money laundering concern, we understand that we must read FinCEN's final rule and follow any prescriptions or prohibitions contained in that rule.

11. Monitoring Accounts for Suspicious Activity

We will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business. (Red flags are identified in Section

11.b. below.) The AML Compliance Person or his or her designee will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

We will conduct the following reviews of activity that our monitoring system detects: We will document our monitoring and reviews as follows: The AML Compliance Person or his or her designee will conduct an appropriate investigation and review relevant information from internal or third-party sources before a SAR-SF is filed.

a. Emergency Notification to Law Enforcement by Telephone

In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, we will immediately call an appropriate law enforcement authority. If a customer or company appears on OFAC's SDN list, we will call the OFAC Hotline at (800) 540-6322. Other contact numbers we will use are: FinCEN's Financial Institutions Hotline ((866) 556-3974) (especially to report transactions relating to terrorist activity), local U.S. Attorney's office, local FBI office, and local SEC office, (to voluntarily report such violations to the SEC in addition to contacting the appropriate law enforcement authority). If we notify the appropriate law enforcement authority of any such activity, we must still file a timely SAR-SF.

Although we are not required to, in cases where we have filed a SAR-SF that may require immediate attention by the SEC, we may contact the SEC via the SEC SAR Alert Message Line at (202) 551-SARS (7277) to alert the SEC about the filing. We understand that calling the SEC SAR Alert Message Line does not alleviate our obligations to file a SAR-SF or notify an appropriate law enforcement authority.

b. Red Flags

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

Customers – Insufficient or Suspicious Information

- Provides unusual or suspicious identification documents that cannot be readily verified.
- Reluctant to provide complete information about nature and purpose of business, prior banking relationships, anticipated account activity, officers and directors or business location.
- Refuses to identify a legitimate source for funds or information is false, misleading or substantially incorrect.
- Background is questionable or differs from expectations based on business activities.

Efforts to Avoid Reporting and Recordkeeping

- Reluctant to provide information needed to file reports or fails to proceed with transaction.
- Tries to persuade an employee not to file required reports or not to maintain required records.
- “Structures” deposits, withdrawals or purchase of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements.
- Unusual concern with the firm’s compliance with government reporting requirements and firm’s AML policies.

Certain Funds Transfer Activities

- Wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent business reason.
- Many small, incoming wire transfers or deposits made using checks and money orders. Almost immediately withdrawn or wired out in manner inconsistent with customer’s business or history.
- Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.

Certain Deposits or Dispositions of Physical Certificates

- Physical certificate is titled differently than the account.
- Physical certificate does not bear a restrictive legend, but based on history of the stock and/or volume of shares trading, it should have such a legend.
- Customer’s explanation of how he or she acquired the certificate does not make sense or changes.
- Customer deposits the certificate with a request to journal the shares to multiple accounts, or to sell or otherwise transfer ownership of the shares.

Certain Securities Transactions

- Customer engages in prearranged or other non-competitive trading, including wash or cross trades of illiquid securities.
- Two or more accounts trade an illiquid stock suddenly and simultaneously.
- Customer journals securities between unrelated accounts for no apparent business reason.
- Customer has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason.
- Customer transactions include a pattern of receiving stock in physical form or the incoming transfer of shares, selling the position and wiring out proceeds.
- Customer’s trading patterns suggest that he or she may have inside information.

Transactions Involving Penny Stock Companies

- Company has no business, no revenues and no product.
- Company has experienced frequent or continuous changes in its business structure.
- Officers or insiders of the issuer are associated with multiple penny stock issuers.
- Company undergoes frequent material changes in business strategy or its line of business.
- Officers or insiders of the issuer have a history of securities violations.
- Company has not made disclosures in SEC or other regulatory filings.

Transactions Involving Insurance Products

- Cancels an insurance contract and directs funds to a third party.

- Structures withdrawals of funds following deposits of insurance annuity checks signaling an effort to avoid BSA reporting requirements.
- Rapidly withdraws funds shortly after a deposit of a large insurance check when the purpose of the fund withdrawal cannot be determined.
- Cancels annuity products within the free look period which, although could be legitimate, may signal a method of laundering funds if accompanied with other suspicious indicia.
- Opens and closes accounts with one insurance company then reopens a new account shortly thereafter with the same insurance company, each time with new ownership information.
- Purchases an insurance product with no concern for investment objective or performance.
- Purchases an insurance product with unknown or unverifiable sources of funds, such as cash, official checks or sequentially numbered money orders.

Activity Inconsistent With Business

- Transactions patterns show a sudden change inconsistent with normal activities.
- Unusual transfers of funds or journal entries among accounts without any apparent business purpose.
- Maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
- Appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.

Other Suspicious Customer Activity

- Unexplained high level of account activity with very low levels of securities transactions.
- Funds deposits for purchase of a long-term investment followed shortly by a request to liquidate the position and transfer the proceeds out of the account.
- Law enforcement subpoenas.
- Large numbers of securities transactions across a number of jurisdictions.
- Buying and selling securities with no purpose or in unusual circumstances (e.g., churning at customer's request).
- Payment by third-party check or money transfer without an apparent connection to the customer.
- Payments to third-party without apparent connection to customer.
- No concern regarding the cost of transactions or fees (i.e., surrender fees, higher than necessary commissions, etc.).

Responding to Red Flags and Suspicious Activity

When an employee of the firm detects any red flag, or other activity that may be suspicious, he or she will notify Compliance person. Under the direction of the AML Compliance Person, 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/or filing a SAR-SF.

12. Suspicious Transactions and BSA Reporting

We will file SAR-SFs with FinCEN for any transactions (including deposits and transfers) conducted or attempted by, at or through our firm involving \$5,000 or more of funds or assets (either individually or in the aggregate) where we know, suspect or have reason to suspect:

- (1) the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;
- (2) the transaction is designed, whether through structuring or otherwise, to evade any requirements of the BSA regulations;
- (3) the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or
- (4) the transaction involves the use of the firm to facilitate criminal activity.

We will also file a SAR-SF and notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes. In addition, although we are not required to, we may contact that SEC in cases where a SAR-SF we have filed may require immediate attention by the SEC. See Section 11 for contact numbers. We also understand that, even if we notify a regulator of a violation, unless it is specifically covered by one of the exceptions in the SAR rule, we must file a SAR-SF reporting the violation.

We may file a voluntary SAR-SF for any suspicious transaction that we believe is relevant to the possible violation of any law or regulation but that is not required to be reported by us under the SAR rule. It is our policy that all SAR-SFs will be reported regularly to the Board of Directors and appropriate senior management, with a clear reminder of the need to maintain the confidentiality of the SAR-SF.

We will report suspicious transactions by completing a SAR-SF, and we will collect and maintain supporting documentation as required by the BSA regulations. We will file a SAR-SF no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR-SF. If no suspect is identified on the date of initial detection, we may delay filing the SAR-SF for an additional 30 calendar days pending identification of a suspect, but in no case will the reporting be delayed more than 60 calendar days after the date of initial detection. The phrase “initial detection” does not mean the moment a transaction is highlighted for review. The 30-day (or 60-day) period begins when an appropriate review is conducted and a determination is made that the transaction under review is “suspicious” within the meaning of the SAR requirements. A review must be initiated promptly upon identification of unusual activity that warrants investigation.

We will retain copies of any SAR-SF filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR-SF. We will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, federal or state securities regulators or SROs upon request. We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations. We understand that anyone who is subpoenaed or required to disclose a SAR-SF or the information contained in the SAR-SF will, except where disclosure is requested by FinCEN, the SEC, or another appropriate law enforcement or regulatory agency, or an SRO registered with the SEC, decline to produce the SAR-SF or to provide any information that would disclose that a SAR-SF was prepared or filed. We will notify FinCEN of any such request and our response.

13. AML Recordkeeping

a. Responsibility for Required AML Records and SAR-SF Filing

Our AML Compliance Person and his or her designee will be responsible for ensuring that AML records are maintained properly and that SAR-SFs are filed as required.

In addition, as part of our AML program, our firm will create and maintain SAR-SFs, CTRs, CMIRs, FBARs, and relevant documentation on customer identity and verification and funds transmittals. We will maintain SAR-SFs and their accompanying documentation for at least five years. We will keep other documents according to existing BSA and other recordkeeping requirements, including certain SEC rules that require six-year retention periods (e.g., Exchange Act Rule 17a-4(a) requiring firms to preserve for a period of not less than six years, all records required to be retained by Exchange Act Rule 17a-3(a)(1)-(3), (a)(5), and (a)(21)-(22) and Exchange Act Rule 17a-4(e)(5) requiring firms to retain for six years account record information required pursuant to Exchange Act Rule 17a-3(a)(17)).

b. SAR-SF Maintenance and Confidentiality

We will hold SAR-SFs and any supporting documentation confidential. We will not inform anyone outside of FinCEN, the SEC, and SRO registered with the SEC or other appropriate law enforcement or regulatory agency about a SAR-SF. We will refuse any subpoena requests for SAR-SFs or for information that would disclose that a SAR-SF has been prepared or filed and immediately notify FinCEN of any such subpoena requests that we receive. We will segregate SAR-SF filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR-SF filings. Our AML Compliance Person will handle all subpoenas or other requests for SAR-SFs. We may share information with another financial institution about suspicious transactions in order to determine whether we will jointly file a SAR according to the provisions of Section 3.d. In cases in which we file a joint SAR for a transaction that has been handled both by us and another financial institution, both financial institutions will maintain a copy of the filed SAR.

c. Additional Records

We shall retain either the original or a microfilm or other copy or reproduction of each of the following

- A record of each extension of credit in an amount in excess of \$10,000, except an extension of credit secured by an interest in real property. The record shall contain the name and address of the person to whom the extension of credit is made, the amount thereof, the nature or purpose thereof and the date thereof;
- A record of each advice, request or instruction received or given regarding any transaction resulting (or intended to result and later canceled if such a record is normally made) in the transfer of currency or other monetary instruments, funds, checks, investment securities or credit, of more than \$10,000 to or from any person, account or place outside the U.S.;
- A record of each advice, request or instruction given to another financial institution (which includes broker-dealers) or other person located within or without the U.S., regarding a transaction intended to result in the transfer of funds, or of currency, other monetary instruments, checks, investment securities or credit, of more than \$10,000 to a person, account or place outside the U.S.;
- 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, from any person, account or place outside the U.S.

14. Clearing/Introducing Firm Relationships

We will work closely with our clearing firm to detect money laundering. We will exchange information, records, data and exception reports as necessary to comply with AML laws. Both our firm and our clearing firm have filed (and kept updated) the necessary annual certifications for such information sharing, which can be found on [FINCEN's Website](#). As a general matter, we will obtain and use the following exception reports offered by our clearing firm in order to monitor customer activity and we will provide our clearing firm with proper customer identification and due diligence information as required to successfully monitor customer transactions. We have discussed how each firm will apportion customer and transaction functions and how we will share information and set forth our understanding in a written document. We understand that the apportionment of functions will not relieve either of us from our independent obligation to comply with AML laws, except as specifically allowed under the BSA and its implementing regulations.

15. Training Programs

We will develop ongoing employee training under the leadership of the AML Compliance Person and senior management. Our training will occur on at least an annual basis. It will be based on our firm's size, its customer base, and its resources and be updated as necessary to reflect any new developments in the law.

Our training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of SAR-SFs); (3) what employees' roles are in the firm's compliance efforts and how to perform them; (4) the firm's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the BSA.

We will develop training in our firm, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos. We will maintain records to show the persons trained the dates of training and the subject matter of their training.

We will review our operations to see if certain employees, such as those in compliance, margin and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

16. Program to Independently Test AML Program

The testing of our AML program will be performed at least annually with an independent third party. We will evaluate the qualifications of the independent third party to ensure they have a working knowledge of applicable requirements under the BSA and its implementing regulations. Independent testing will be performed more frequently if circumstances warrant.

After we have completed the independent testing, staff will report its findings to senior management [or to an internal audit committee]. We will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved.

Rules: 31 C.F.R. § 103.120; FINRA Rule 3310.

17. Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the AML Compliance Person. We will also review the AML performance of supervisors, as part of their annual performance review. The AML Compliance Person's accounts will be reviewed by another member of senior management.

18. Confidential Reporting of AML Non-Compliance

Employees will promptly report any potential violations of the firm's AML compliance program to the AML Compliance Person, unless the violations implicate the AML Compliance Person, in which case the employee shall report to [the president/chairman of the board/audit committee chair]. Such reports will be confidential, and the employee will suffer no retaliation for making them.

19. Senior Manager Approval

Senior management has approved this AML compliance program in writing as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the BSA and the implementing regulations under it. This approval is indicated by signatures below.

“Red Flags” Identity Theft Prevention Program

Purpose

To establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

Definitions

Identify theft means fraud committed or attempted using the identifying information of another person without authority.

A covered account means:

1. An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts and savings accounts; and
2. Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

A red flag means a pattern, practice or specific activity that indicates the possible existence of identity theft.

The Program

RES/CLS establishes an Identity Theft Prevention Program to detect, prevent and mitigate identity theft. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the creditor from identity theft.

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Administration of Program

1. The organization's governing body, an appropriate committee of the governing body or a designated employee at the level of senior management) shall be responsible for the development, implementation, oversight and continued administration of the Program.

2. The Program shall train staff, as necessary, to effectively implement the Program; and
3. The Program shall exercise appropriate and effective oversight of service provider arrangements.

Identification of Relevant Red Flags

1. The Program shall include relevant red flags from the following categories as appropriate:

- a. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- b. The presentation of suspicious documents;
- c. The presentation of suspicious personal identifying information;
- d. The unusual use of, or other suspicious activity related to, a covered account; and
- e. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

2. The Program shall consider the following risk factors in identifying relevant red flags for covered accounts as appropriate:

- a. The types of covered accounts offered or maintained;
- b. The methods provided to open covered accounts;
- c. The methods provided to access covered accounts; and d. Its previous experience with identity theft.

3. The Program shall incorporate relevant red flags from sources such as:

- a. Incidents of identity theft previously experienced;
- b. Methods of identity theft that reflect changes in risk; and
- c. Applicable supervisory guidance.

Detection of Red Flags

The Program shall address the detection of red flags in connection with the opening of covered accounts and existing covered accounts, such as by:

1. Obtaining identifying information about, and verifying the identity of, a person opening a covered account; and
2. Authenticating customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing covered accounts.

Response

The Program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The response shall be commensurate with the degree of risk posed. Appropriate responses may include:

1. Monitor a covered account for evidence of identity theft;
2. Contact the customer;
3. Change any passwords, security codes or other security devices that permit access to a covered account;
4. Reopen a covered account with a new account number;
5. Not open a new covered account;
6. Close an existing covered account;
7. Notify law enforcement; or
8. Determine no response is warranted under the particular circumstances.

Updating the Program

The Program shall be updated periodically to reflect changes in risks to customers or to the safety and soundness of the organization from identity theft based on factors such as:

1. The experiences of the organization with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent and mitigate identity theft;

4. Changes in the types of accounts that the organization offers or maintains;
5. Changes in the business arrangements of the organization, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

Oversight of the Program

1. Oversight of the Program shall include:

- a. Assignment of specific responsibility for implementation of the Program;
- b. Review of reports prepared by staff regarding compliance; and
- c. Approval of material changes to the Program as necessary to address changing risks of identity theft.

2. Reports shall be prepared as follows:

- a. Staff responsible for development, implementation and administration of the Program shall report to

(the organization's governing body, an appropriate committee of the governing body or a designated employee at the level of senior management) at least annually on compliance by the organization with the Program.

- b. The report shall address material matters related to the Program and evaluate issues such as:

- i. The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
- ii. Service provider agreements;
- iii. Significant incidents involving identity theft and management's response; and
- iv. Recommendations for material changes to the Program.

Oversight of Service Provider Arrangements

The organization shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts.

Duties Regarding Address Discrepancies

The organization shall develop policies and procedures designed to enable the organization to form a reasonable belief that a credit report relates to the consumer for whom it was requested if the organization receives a notice of address discrepancy from a nationwide consumer reporting agency indicating the address given by the consumer differs from the address contained in the consumer report.

The organization may reasonably confirm that an address is accurate by any of the following means:

1. Verification of the address with the consumer;
2. Review of the organization's records;
3. Verification of the address through third-party sources; or
4. Other reasonable means.

If an accurate address is confirmed, the organization shall furnish the consumer's address to the nationwide consumer reporting agency from which it received the notice of address discrepancy if:

1. The organization establishes a continuing relationship with the consumer; and
2. The organization, regularly and in the ordinary course of business, furnishes information to the consumer reporting agency.

RES/CLS POLICIES & GUIDELINES + LO CONTRACT AGREEMENT

Application:

LO shall obtain from all applicants completed loan, credit, and similar applications, together with supporting verifications, approvals and related documentation, as required by law or as directed by RES/CLS along with its Lender(s) and in compliance with Applicable Law or any instructions of these authorities.

Nothing herein shall be construed as creating any obligation of RES/CLS or its lenders to accept the loan application packages and/or approve the loan application packages as prepared and presented by LO. LO agrees not to submit to any lender any loan application package for or on behalf of a loan applicant in connection with which any circumstances, conditions or events exist that, if known to Lender or RES/CLS, would cause Lender to deny approval of such loan application package(s).

In connection therewith, LO shall not withhold any information and shall promptly disclose to RES/CLS & Lender any material information that reasonably could be expected to be a relevant consideration in Lender's decision to close a loan, including, without limitation, discrepancies between information provided by the loan applicant and that obtained from other sources, factors bearing on the physical condition of the real property intended to secure Lender's lien, and any irregularities involving the purchase transaction covering said real property or the relationship or involvement of any other LOs, Mortgage Brokers, RE Brokers, RE Agents or escrows in connection therewith.

If at any time during the period between the original submission of the loan application package and the closing and funding of the loan applied for, LO learns or has reason to believe that any of the information or documentation submitted by LO either with the loan application package as originally submitted or as it may have been supplemented by LO, either in response(s) to Lender's request(s), if any, for additional information and/or documentation, or otherwise, or if any of LO's representations and/or warrants with regard thereto, either were when submitted or made, or thereafter have become, not true and/or not valid and/or not genuine, LO shall immediately give written notice thereof to RES/CLS & Lender.

The loans entered into pursuant to this agreement shall conform with all applicable provisions and requirements of:

- a) this Agreement;
- b) Lender's guidelines, underwriting requirements, bulletins or other requirements posted in Lender's loan matrixes & guidelines.

LO is not authorized to approve a loan application package on any Lender's behalf.

Licenses and Litigation:

RES/CLS & LO are required to have all licenses and permits to conduct mortgage business that are required by the applicable jurisdictions from which all mortgage loans originate and where the real property securing the mortgage loan is located. Additionally, RES/CLS & LO hold all applicable Federal, State, and other licenses, authorizations, endorsements, and approvals as deemed necessary to performance of obligations hereunder in compliance with Applicable Law and secondary market requirements, and is not in violation of any of the requirements of any such licenses, authorizations and/or approvals and there are no current, pending, or threatened investigations from any regulatory body, governmental or quasi governmental entity, and there is no litigation current, pending, or threatened that could impact the business of LO or RES/CLS. Broker shall promptly notify Lender and RES/CLS if any of the representations in this subsection change.

Compliance:

LO warrants that any loan it submits to Lender for approval will contain true and valid information and that LO shall, both in the conduct of its business generally, and, in particular, in its handling of each loan application, comply fully, completely, and in a timely manner with every requirement of all applicable Federal and State laws dealing with the origination of mortgage loans, including without limitation upon the generality of the foregoing, the Consumer Credit Protection Act, ("CCPA"); the Equal Credit Opportunity Act and Regulation B promulgated thereunder ("ECOA"); the Truth-in-Lending Act and Regulation Z promulgated thereunder ("TILA"); the Real Estate Settlement Procedures Act and Regulation X promulgated thereunder ("RESPA"); Gramm-Leach-Bliley Act, the related Interagency Guidelines Establishing Information Security Standards, and Regulation P and other applicable law regarding privacy; and all applicable State or Federal statutes, rules and regulations governing fraud, consumer credit transactions, predatory, and/or abusive lending, and mortgage banks and brokers in general, each as may be amended from time to time (together "Applicable Law"). In connection with ECOA, LO shall not discourage or pre-screen any applicant or in any other manner violate the terms of ECOA and Regulation B.

LO shall maintain, available for RES/CLS's inspection, and shall deliver to RES/CLS upon demand, evidence of compliance with all such requirements. Additionally, LO warrants that any loan it submits to Lender(s) shall, both in the conduct of its business generally,

and, in particular, in its handling of each loan application, comply fully, completely and in a timely manner with every requirement of all applicable RES/CLS policies and procedures then in effect.

Valid Information:

LO warrants that all signatures, names, addresses, social security numbers, amounts and other statements appearing on the credit application, mortgage notes, and all other documents relating to each mortgage loan are true and correct and do not omit any information which is necessary for Lender to make its credit decision with respect to such loan application.

LO Compensation/Fees:

The LO's compensation is set forth in the relevant ASSOCIATE-LICENSEE "LOAN OFFICER" COMMISSION AGREEMENT. LO shall be responsible for the payment of any fees set forth in the relevant program guides as published and as updated periodically by RES/CLS on the compliance page here:

<https://www.californialendingsource.com/california-lending-source-compliance-announcements>

Among other things, LO's duty of indemnification, or, at RES/CLS's sole option, repurchase, shall arise upon the occurrence of any of the following:

- 1) A breach by LO of any representation, warranty or covenant contained in this Agreement.
- 2) The failure of any loan to conform with the applicable investor guidelines or requirements for such loan, as determined by RES/CLS &/OR Lender, its successors and/or assigns and/or industry standards.
- 3) Any violation by the LO or any employee or agent of the LO of any Applicable Law.
- 4) The discovery by RES/CLS or Lender(s), any investor and/or any subsequent owner of a loan, of any defect with respect to the loan, including without limitation, the ability to include the loan in a GNMA/Fannie Mae/Freddie Mac Pool or otherwise sell the loan on the secondary market.
- 5) Any claim brought by a third party against RES/CLS based on facts or allegations against LO or the origination of any mortgage loan.
- 6) For the avoidance of doubt, LO is not required to indemnify RES/CLS for matters arising solely from the fraud, gross negligence, or intentional misconduct of RES/CLS. LO understands and agrees that in the event of a repurchase demand being made upon RES/CLS, LO may be required to submit further information to RES/CLS and/or to otherwise assist RES/CLS & Lender in responding to such repurchase request.

Submission of Transactions:

Upon entering a transaction into REC/CLS's or Lender's submission system and choosing to issue disclosures, LO is authorizing RES/CLS and its employees to request issuance of disclosures by the Lender on LO's behalf as LO's agent solely for the purpose of issuing disclosures.

Reimbursement of Broker:

In addition to the indemnity set forth herein, LO shall indemnify RES/CLS for all fees, costs, losses and expenses incurred, including reasonable attorney's fees, for claims made under Applicable Law.

Assignment:

Except as otherwise provided herein, neither this Agreement nor any right hereunder may be assigned by LO without the prior written consent of RES/CLS, and any such assignment shall be void and of no effect.

Records:

At all times during the term of this agreement, LO shall maintain a complete set of files and records of all business, activities, and operations conducted by LO as required by Federal and State lending guidelines and in accordance with RES/CLS's loan policies and procedures.

At all times during the term of this Agreement and at all times following the expiration or termination of this Agreement, RES/CLS, its regulators, internal auditors, or independent auditors, and its duly authorized agents, representatives, or employees have the right to audit, inspect, and copy any of the foregoing records, reports, and related materials of LO.

Confidentiality:

LO agrees to

(A) hold RES/CLS's Confidential Information in confidence, and to take precautions to protect such Confidential Information at least as strict as RES/CLS employs with respect to its own confidential materials, but in no case less than reasonable precautions LO uses to protect its own Confidential Information or as required by Applicable law. For purposes of this Agreement, "Confidential Information" shall mean:

- RES/CLS's network configuration, technical information, software, processes and methods, policies, procedures, contract terms, designs, financial information, pricing information, equipment configurations, specifications, customer and vendor lists, strategic alliances and partnerships, terms and conditions of any contracts or agreements between the parties, product and services development plans, forecasts, business and marketing plans and strategies, names and non-public information of employees and consultants, formulas, records, files, drawings, data and databases, interfaces, memoranda, know-how, patents, copyright, trade secrets, proprietary information, processes inventions, technology, and vendor lists and information, confidential information of RES/CLS's customers, affiliates, suppliers and partners,

(B) other non-public information which,

- I. if disclosed in a tangible or visual form, is clearly labeled as "Confidential";
- II. if disclosed in a non-tangible or non-visual form, is identified at the time of disclosure as Confidential Information; or
- III. given the circumstances of disclosure, and/or the nature of the information, Broker knew or reasonably should have known was Confidential Information, and (3) all 'non-public personal information' as defined in Title V of the Gramm-Leach Bliley Act and its implementing regulations (collectively, the "GLB Act"), as the same may be amended from time to time. LO's obligation to preserve the secrecy of Confidential Information shall survive the termination of this Agreement.

Records at Termination:

Upon termination of this Agreement, Broker agrees to return to RES/CLS all files, papers, and materials of any and every kind, regardless of form, which contain or relate to Confidential Information, except that LO may keep copies of any documents LO is legally required to retain under applicable record retention statutes or rules.

Integration:

This Agreement, including any and all other materials which are incorporated into this Agreement by reference as set forth throughout this Agreement is intended to, and does, set forth the entire understanding between the parties with regard to the subject matter of this Agreement and it is an add-on/addendum to the Real Estate Source, Inc. Office Policy Manual located here:

<https://www.morecommission.info/how-to-join>

Modifications:

With regard to modifications, amendments, or other changes made to the Agreement at RES/CLS's discretion made by posting at <https://www.californialendingsource.com/california-lending-source-compliance-announcements> RES/CLS intends to notify RE Agents & LOs of said changes by means of an email of general distribution to approved RES/CLS Agents & LOs brokers or other mass communication, which generally will also be posted to the RES/CLS Website. RES/CLS is not responsible for misdirected email, inaccurate or outdated email addresses, or otherwise mis-delivered, un-delivered or unsent notifications.

NOTWITHSTANDING THE FORGOING, MWF RESERVES THE RIGHT TO AMEND OR MODIFY THIS AGREEMENT FROM TIME TO TIME IN ITS SOLE AND ABSOLUTE DISCRETION AND SHALL PROVIDE THE BROKER WITH AMENDMENTS AND MODIFICATIONS BY POSTING SUCH TO

Severability:

If a court of competent jurisdiction finds any provision in this Agreement to be invalid, illegal, or otherwise unenforceable, that determination will not affect any other provision of this Agreement.

The invalid provision will be severed from this Agreement and all remaining provisions will continue to be enforceable by their terms and of full force and effect.

Attorney Fees:

In the event of a legal action between the LO and RES/CLS for breach of contract, the prevailing party in that action shall be entitled to an award of reasonable attorney’s fees and costs.

Terms of Agreement:

This Agreement shall commence on the Effective Date and shall be indefinite, with either party having the ability to terminate this Agreement, with or without cause by either party upon written notice. Upon termination of this Agreement, all terms, conditions, covenants, indemnities, agreements, representations and warranties shall continue to apply to all loans funded pursuant to this Agreement.

Construction:

This Agreement shall not be construed against the party preparing it, but shall be construed as if all parties jointly prepared this Amendment and any uncertainty or ambiguity shall not be interpreted against any one party.

Counterparts:

This Agreement may be executed and delivered by electronic transmission (facsimile or email), and in one or more counterparts, each of which shall be deemed to be an original and all of which taken together shall be deemed one and the same Agreement. In Witness Whereof, LO and RES/CLS each have caused their duly authorized representative to execute and enter into this Agreement as of the Effective Date.

I, the undersigned Loan Officer/Licensed Loan Originator, have read, understand and acknowledge the above contract I am entering into with RES/CLS and I hereby state that I will adhere to the terms of this contract and all policies and procedures of RES/CLS detailed above.


Loan Officer (Print Name)

Real Estate Source, Inc.
DBA “California Lending Source”

Brokerage

Signed

Date



Broker *Tony Soheil Dini*
NMLS#288511

Real Estate Source, Inc. CalDRE# 01869619 DBA “California Lending Source”
NMLS# 288738 1024 Iron Point Rd. Folsom, CA 95630
PH: 916-307-3444 EM:info@realestatesourceinc.com