AML Program Outline/Summary

The Department of Financial Institutions is providing this Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) program outline and summary to assist mortgage broker licensees with their required written AML program.

Nearly all of the content in this document comes from the Financial Crimes Enforcement Network (FinCEN) regulations contained in 31 CFR Parts 1010 and 1029 or FinCEN advisories. Use of this outline is not a substitute for reading and understanding all of 31 CFR Parts 1010 and 1029. This outline is not legal advice or interpretation. It gathers information contained in FinCEN's AML regulations and places it in a format that mortgage brokers may find useful to aid in their AML compliance programs.

The Bank Secrecy Act (BSA) defines the term "financial institution" to include, in part, a loan or finance company. Non-bank residential mortgage lenders and originators, generally known as "mortgage companies" and "mortgage brokers" in the residential mortgage business sector, are a significant subset of the "loan or finance company" category. FinCEN calls this subset Residential Mortgage Loan Originators (RMLOs). As of August 13, 2012, RMLOs are required to have a written AML program.

A mortgage broker's AML program may include, but not necessarily be limited to, the following sections:

I. *Introduction*
II. *Compliance Officer*
III. *Red Flags and Risk Assessment*
IV. *Customer Identification Program*
V. *Beneficial Ownership Requirement*
VI. *OFAC Compliance*
VII. *Required Reports*
VIII. *Recordkeeping*
IX. *Information Sharing with FinCEN*
X. *Voluntary Information Sharing with Other Financial Institutions*
XI. *AML Program Training*
XII. *Independent Testing*
XIII. *Approval by Senior Management*

I. **Introduction** *(Not a strict requirement of 31 CFR Parts 1010 and 1029, but present in most AML programs for stylistic considerations. The program should be read by all personnel, agents, and brokers as applicable, and used for training.)*

Within the introduction you may want to clearly *name your company* and state the purpose of the program, such as to:

1. Detect, prevent, and report loan fraud, identity theft, and other financial crimes;

2. Detect, prevent, and report money laundering;
3. Detect, prevent, and report terrorist financing.

II. Compliance Officer

The company must designate a Compliance Officer [required by 31 CFR § 1029.210(b)(2)].

You should list the Compliance Officer's BSA responsibilities, such as to ensure the AML program is implemented effectively, including monitoring compliance by the company's agents and brokers with their obligations under the program [required by 31 CFR § 1029.210(b)(2)(i)].

Responsibilities include ensuring required reporting and record keeping; ensuring the AML program is updated as necessary [required by 31 CFR § 1029.210(b)(2)(ii)]; and ensuring appropriate persons are educated and trained on their responsibilities under the AML program [required by 31 CFR § 1029.210(b)(2)(iii)].

III. Red Flags and Risk Assessment

You should consider and discuss risks of the company's products and services being used for mortgage fraud, money laundering, terrorist financing, or other financial crimes.

"FinCEN reports and other research underscore that mortgage fraud is one of the most significant operational risks facing RMLOs in the ordinary course of business."[1] FinCEN Advisory-- FIN-2012-A009 lists a non-exclusive list of 16 potential red flag indicators of illicit activity related to mortgage fraud. Fannie Mae has a Mortgage Fraud Prevention webpage containing recent and historical fraud alerts as well as an extensive list of more red flags for mortgage fraud.

The Federal Financial Institutions Examination Council's (FFIEC) BSA/AML Examination Manual, Appendix F, provides red flags for money laundering and terrorist financing activity.

You may want to list the red flag indicators of mortgage fraud, as well as money laundering and terrorist financing red flags that apply to your business model from the links above. (Appendix F is tailored to bank examiners, so not all red flags will apply to your business.) Add additional red flags you may know or become aware of as new scams develop. Some companies include the red flags on a checklist for MLOs to complete on each application.

Discuss the products and services your company provides and whether certain products are more likely to produce one or more red flags. Considerations may include, but should not be limited to:

- Does the company offer loans that do not verify income and/or assets?
    - Increased risk of mortgage fraud from borrower and loan originator; loan originator is prohibited from completing application for borrower or coaching borrower on amount of income and/or assets to state on application.

1. 77 FR 8148: AML & SAR for Non-Bank RMLOs p. 6

- Does the company accept cash deposits?
    - Most Washington state mortgage brokers do not accept cash deposits; those with trust accounts typically do not accept deposits large enough to facilitate money laundering.
- Do the company's products require legitimate sourcing of down payments?
    - If the company offers products that do not require down payments to come from seasoned funds in a financial institution, the risk is higher that the borrower may be laundering money through the down payment.
- Do borrowers send proceeds of cash-out transactions overseas?
    - Risk of recipients being on U.S. Department of State's list of Foreign Terrorist Organizations or U.S. Treasury Department's list of Specially Designated Nationals and Blocked Persons (SDN list).

Discuss the frequency your company sees one or more of the FinCEN, Fannie Mae, and FFIEC mortgage fraud, money laundering, or terrorist financing red flags. Determine your risks in relation to your products and services and frequency of observed red flags.

A good practice is for the AML program to state if any employee identifies one or more of the red flags, they are to report it to the AML program Compliance Officer for evaluation and possible SAR filing (including them on a checklist helps document the program and foster accountability from employees).

IV. **Customer Identification Program** (CIP), (31 CFR § 1010.220)

You should include your written CIP in the AML program.

- Explain how your company verifies it knows the true identity of each customer.
- List documentation and methods used to verify borrower identity.
    - U.S. National identity verification documents
    - Non-U.S. National identity verification documents
- Explain how your company determines if persons or businesses seeking to become your customer are on government lists of sanctioned entities, such as the SDN list.
- Detail how the borrowers are notified their identity is being verified subject to the Patriot Act.
- Ensure all CIP records are kept for a minimum of five years.

V. **Beneficial Ownership Requirements for Legal Entity Customers** (31 CFR § 1010.230)

- State the company will establish and maintain written procedures to verify the identity of each beneficial owner of legal entity customers (i.e. businesses) using Appendix A from 31 CFR § 1010.230 to document the identities and retain the documentation for five years.

VI. **OFAC Compliance** (not part of BSA, but CIP is, and checking SDN list is part of CIP)

Detail the company's procedures to comply with OFAC's prohibitions on dealing with certain countries, companies, and individuals and explain how the company ensures it isn't working with a company or individual on the SDN list. State the company will not work with persons on the SDN list and that the

company will report blocked transactions on OFAC's Reporting System within 10 business days of rejecting the transaction.

VII. **Required Reports** (31 CFR § 1029.320 & §1029.330)

Suspicious Activity Reports (SARS)

The company is required to and must report any transaction involving "funds or other assets of at least $5,000" when it "knows or suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part):"

a. "Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including without limitation the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation;"
b. "Is designed, whether through structuring or other means, to evade any requirements of this part or any other regulations promulgated under the Bank Secrecy Act…;"
c. Has no apparent business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the loan or finance company knows of no reasonable explanation for the transaction after examining the available facts, including background and possible purpose of the transaction; or"
d. "Involves the use of the loan or finance company to facilitate criminal activity."[2]

Name the individual at the company responsible for SAR filing (usually the AML Compliance Officer), and complete SARs according to the instructions on FinCEN's BSA E-Filing System within "30 calendar days after the date of the initial detection…of facts that may constitute a basis for filing a SAR…. If no suspect is identified on the date of such initial detection, a loan or finance company may delay filing a SAR for an additional 30 calendar days to identify a suspect, but in no case shall reporting be delayed more than 60 calendar days after the date of such initial detection."[3]

When more than one entity is required to file a SAR for the same transaction (e.g. mortgage broker and wholesale lender), only one SAR is required. The company is responsible, along with its joint filer, to ensure the SAR "contains all relevant facts, including the name of each financial institution involved in the transaction, the report complies with all instruction applicable to joint filings, and each institution maintains a copy of the report filed, along with any supporting documentation."[4]

Some suspicious activity requires mandatory notification to law enforcement. "In situations involving violations that require immediate attention, such as suspected terrorist financing or ongoing money

2. 31 CFR § 1029.320(a)(2)(i-iv)
3. 31 CFR § 1029.320(b)(3)
4. 31 CFR § 1029.320(a)(3)

laundering schemes" the company will "immediately notify by telephone an appropriate law enforcement authority in addition to filing timely a SAR."[5]

In addition to the mandatory SAR filing detailed above, a company may also voluntarily file a SAR any time it believes it has information "relevant to the possible violation of any law or regulation…" in accordance with the AML program's purpose to detect and prevent crime.[6] When filing a voluntary SAR the company will also notify FinCEN to "report suspicious transactions that may relate to terrorist activity" by calling FinCEN's Financial Institutions Hotline at 1-866-556-3974.[7]

Important note to include in written AML program – confidentiality of SARs [31 CFR §1029.320(d)]: The company, its employees, agents, and brokers (if applicable) must not disclose that a SAR is filed, or any information that reveals the existence of a SAR to anyone, including the person(s) involved in the suspicious transaction. The company should only disclose a filed SAR or the existence of a SAR, and/or provide the underlying facts, transactions, and documents when required by the following:

i. "FinCEN or any Federal, State, or local law enforcement agency, any Federal regulatory authority that examines the loan or finance company for compliance with the Bank Secrecy Act, or any State regulatory authority administering a State law that requires the loan or finance company to comply with the Bank Secrecy Act or otherwise authorizes the State authority to ensure the loan or finance company complies with the Bank Secrecy Act;"[8]
ii. Another financial institution when filing a joint SAR [31 CFR § 1029.320(d)(ii)(A)(2)];
iii. The company's corporate organizational structure for the purpose of complying with the Bank Secrecy Act [31 CFR § 1029.320(d)(ii)(B)].

Report of Cash Payments Over $10,000 Received in a Trade or Business (FinCEN Form 8300), (31 CFR §1010.330)

The company must file FinCEN form 8300 through FinCEN's BSA E-Filing System by the 15th calendar day after the date of receiving over $10,000 cash in one transaction, or two or more related transactions, if such an event were ever to occur. The confidentiality policies detailed above for SARs also apply to FinCEN Form 8300.

VIII. **Recordkeeping (**31 CFR § 1029.320(c), § 1029.400 & subpart D of § 1010)

The Company must retain all records produced pursuant to the AML program for a minimum of five years, including:

- SARs or Form 8300s including the original "or business record equivalent" of all underlying documentation of the entire transaction or transactions;
- All CIP information (as previously stated in CIP section).

5. 31 CFR § 1029.320(b)(4)
6. 31 CFR § 1029.320(a)
7. 31 CFR § 1029.320(b)(5)
8. 31 CFR §1029.320(d)(ii)(A)(1)

IX. **Information Sharing with FinCEN** (31 CFR § 1010.520)

FinCEN may request information from the company regarding whether it has current or past accounts, or any transactions, with any specified individual entity, or organization suspected of money laundering or terrorist activity.

If FinCEN requests information sharing from the company it will certify in writing that the subject(s) of the inquiry are engaged in, or reasonably suspected based on credible evidence of engaging in, terrorist activity or money laundering. It will also include enough specific identifiers "such as date of birth, address, and social security number" that would permit the company "to differentiate between common or similar names, and identify one person at FinCEN or the appropriate Treasury component who can be contacted with any questions relating to its request."[9]

"If a financial institution identifies an account or transaction identified with any individual, entity, or organization named in a request from FinCEN, it shall report to FinCEN, in the manner and in the time frame specified in FinCEN's request, the following information:"

a. "The name of such individual, entity, or organization;"
b. "The number of each such account, or in the case of a transaction, the date and type of each such transaction; and"
c. "Any Social Security number taxpayer identification number, passport number, date of birth, address, or other similar identifying information provided by the individual, entity, or organization when each such account was opened or each such transaction was conducted."[10]

The company must designate a contact person for FinCEN information sharing requests and provide FinCEN with "the name, title, mailing address, e-mail address, telephone number, and facsimile number of such person, in such manner as FinCEN may prescribe," and "promptly notify FinCEN of any changes to such information."[11]

The company must not use information from a FinCEN information sharing request for any purpose other than:

a. "Reporting to FinCEN";
b. "Determining whether to establish or maintain an account, or to engage in a transaction; or"
c. "Assisting the financial institution in complying with any requirement of this chapter."[12]

The company must "not disclose to any person, other than FinCEN or the requesting Treasury component, the law enforcement agency on whose behalf FinCEN is requesting information, or U.S.

9. 31 CFR § 1010.520(b)(2)
10. 31 CFR § 1010.520(b)(3)(ii)(A-C)
11. 31 CFR § 1010.520(b)(3)(iii)
12. 31 CFR § 1010.520(b)(4)(i)(A-C)

law enforcement attaché in the case of a request by a foreign law enforcement agency, which has been named in the information request, the fact that FinCEN has requested or has obtained information under this section, except to the extent necessary to comply with such an information request."[13]

The company must protect the security of FinCEN information requests in the same way it protects its customers' nonpublic personal information.

X. **Voluntary Information Sharing with Other Financial Institutions** (31 CFR § 1010.540)

The company may voluntarily share information with other financial institutions about individuals, entities, organizations, or countries "for purposes of identifying and, where appropriate, reporting activities" that it or the other financial institutions "suspects may involve possible terrorist activity or money laundering."[14]

Before voluntary information sharing with other financial institutions the company must notify FinCEN through *http://www.fincen.gov* and must renew the notification annually as long as the information sharing continues.

The company must also ensure the other financial institution(s) also notify FinCEN in the same manner, even if the other financial institution(s) are affiliates.

The company must not use information received from other financial institutions for any purpose other than:

a. "Identifying and, where appropriate, reporting on money laundering or terrorist activities;"
b. Determining whether to establish or maintain an account, or to engage in a transaction; or"
c. Assisting the financial institution in complying with any requirement of this chapter."[15]

The company must not disclose the information sharing with other financial institutions to any person or entity except FinCEN, and must keep the record of such sharing secure and confidential in the same way it protects its customers' nonpublic personal information.

Note: financial institutions that share information as discussed above "shall be protected from liability for such sharing, or for any failure to provide notice of such sharing, to an individual, entity, or organization that is identified in such sharing, to the full extend provided in subsection 314(b) of Public Law 107 – 56," provided the sharing is done according to the procedures discussed above.[16] (Not required to be put in the written AML program, but provided in this outline for informational purposes.)

13. 31 CFR § 1010.520(b)(3)(iv)(B)(1)
14. 31 CFR § 1010.540(b)(1)
15. 31 CFR § 1010.540(b)(4)(A-C)
16. 31 CFR § 1010.540(b)(5)

XI. AML Program Training [31 CFR § 1029.210(b)(3)]

All employees, agents, and brokers (as applicable) must be trained on their responsibilities under the AML program upon being hired, and all existing employees, agents, and brokers of the company will receive ongoing training of their responsibilities under the program.

You should specify the frequency of the ongoing training and state that training records will be maintained for a minimum period of five years from the date of the training.

XII. Independent Testing [31 CFR § 1029.210(b)(4)]

Independent testing must be conducted to monitor and maintain an adequate AML program. "The scope and frequency of the testing shall be commensurate with the risks posed by the company's products and services." "Such testing may be conducted by a third party or by any officer or employee of" the company, *except* the AML program Compliance Officer.[17] Records of independent testing must be kept for a minimum of five years.

XIII. Approval by Senior Management [31 CFR § 1029.210(a)]

The program must be approved by senior management. A best practice is to place a signature and date line on the document for senior management's approval. Alternative written documentation of senior management's approval is acceptable. Any future updates require documented new approval by senior management.

17. 31 CFR § 1029.210(b)(4)