2 Audiences // 1 Takeaway

1. Decide if this will be a priority
2. Clarify the definition of correct behavior
3. Decide how you’re going to communicate your expectations
The Four Pillars

1. Development of internal policies, procedures, and related controls
2. Designation of a compliance officer
3. Independent review for compliance
4. Thorough and ongoing training program
The Crumbling Pillar of Training

We must reframe our attitude toward compliance training.
Record This:

Training is not a business problem, it is not a nice-to-have, it is an insurance activity against employee errors.
MMC - Common Exam
Finding

Most common weaknesses identified pertain to record keeping (e.g. training logs) and lapses in actually training employees.
(3) Provide for on-going training of appropriate persons concerning their responsibilities under the program. A loan or finance company may satisfy this requirement with respect to its employees, agents, and brokers by directly training such persons or verifying that such persons have received training by a competent third party with respect to the products and services offered by the loan or finance company.
<table>
<thead>
<tr>
<th>Step</th>
<th>Examination Procedure</th>
<th>Assigned to:</th>
<th>Date Completed:</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>I1</td>
<td>Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Determine that the institution has the appropriate BSA/AML policies and procedures in place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Determine the frequency that management reviews and updates the BSA/AML policies and procedures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Determine who is responsible for implementing the BSA/AML policies and procedures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I2</td>
<td>Training</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Determine who receives training regarding BSA/AML and how often training is required for current employees</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Determine when new hires receive training regarding BSA/AML</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Does the institution have tracking in place to ensure all employees have BSA/AML training</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I3</td>
<td>Reporting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Determine if the institution files the appropriate reports with FinCEN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Determine if reports are filed within the time-frame required by FinCEN (within 30 days after the date of the initial detection)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Determine if reports are maintained as required regarding security and privacy</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

https://www.csbs.org/mortgage-examination-supplements
Looking For…
Examiners should determine if the following elements are addressed in the training program and materials:

- Training frequency is specified
- Attendance records and training material are documented
- Employees are accountable for ensuring BSA compliance

https://www.csbs.org/mortgage-examination-supplements

MMC Exam Manual//BSA/AML Module
Looking For...

• Internal policies, procedures, and new rules and regulations are covered
• Different forms of money laundering and terrorist financing as it relates to identification is covered
• Examples of suspicious activity is covered.
• Competency of staff (testing and test scores)

https://www.csbs.org/mortgage-examination-supplements

MMC Exam Manual//BSA/AML Module
What We Are All Looking For…

FRAUD
Looking Back

What would have happened in 2000’s if AEs had to submit SARs?

What would happen if LOs had submitted SARs with changed income amounts in loan origination scenarios?
We Find Fraud by Training How to Look For It
There Is A Connection

Who’s behind the breaches?

75% perpetrated by outsiders.

25% involved internal actors.

There Is A Connection

What tactics do they use?

62% of breaches featured hacking.

51% over half of breaches included malware.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.
There Is A Connection

Who are the victims?

24% of breaches affected financial organizations.

15% of breaches involved healthcare organizations.

12% Public sector entities were the third most prevalent breach victim at 12%.
There Is A Connection

What else is common?

66% of malware was installed via malicious email attachments.

73% of breaches were financially motivated.
An Internal Issue

- Training must be more timely
- Training must be more topical
- Training must be more memorable
Now Let’s Solve the Issue

“Maybe stories are just data with a soul.”

~Brené Brown
REDEFINE & SHOW

What is Money Laundering outside of origination and underwriting activities.
Money Laundering

• Process where people engage in a series of transactions to exchange their “dirty” funds for “clean” money.

• Using transactions to cover up the source of the funds.
STAGES OF MONEY LAUNDERING

**PLACEMENT**
Putting illicit funds into a licit business or activity. Moving cash across borders, pushing deposits, and buying and selling goods with cash.

**LAYERING**
Complex financial transactions are completed to make it difficult to identify the trail of fund originations.

**INTEGRATION**
The re-entering of illegal funds into the economy under the guise of legit earnings through real estate.
**SOME FAVORITE MORTGAGE RED FLAGS**

1. The submission of invalid documents in order to cancel mortgage obligations or pay off a loan balance.

2. The same notary public and/or “authorized representative” working with an unusually large number of borrowers.

3. Past misrepresentations made by borrowers in previous attempts to secure funding.

4. The resubmission of a rejected loan application with the key borrower replaced by a company/corporation.

5. When public and personal documents indicate that borrowers reside at a different location than the address listed on the loan application.

6. Improper/incomplete file documentation and reluctance on the part of the borrower to provide more information or broken promises to provide information.
COMBINE

Because of Cyber Security risks BSA/AML is even MORE IMPORTANT!
“Do you have anything between 10 am and 12 pm?”

https://youtu.be/D5VN56jQMWM
BEFORE THE DIRECTOR OF THE DEPARTMENT OF FINANCE
OF THE STATE OF IDAHO

STATE OF IDAHO, DEPARTMENT OF
FINANCE, CONSUMER FINANCE
BUREAU,

Complainant,

vs.

ALEJANDRO FLORES, dba
FULL SPECTRUM LOANS

Respondent.

Docket No. 2018-8-03

ORDER TO CEASE AND DESIST
FINDINGS OF FACT

6. In June 2018, a Vice President of Compliance for Nationstar Mortgage, LLC (Nationstar), contacted the Conference of State Bank Supervisors (CSBS) regarding an incident whereby someone from an entity called Full Spectrum Loans (FSL) had contacted a consumer about a debt consolidation loan. FSL’s representative identified himself as a loan officer named “Jonathan McGrail” and utilized an identifying NMLS number. This NMLS number did belong to one of Nationstar’s loan officers, Jonathan McGrail, who had no affiliation with Respondent nor with FSL.
8. Since the consumer was a resident of Idaho, the CSBS passed the information/complaint on to the Department. The Department contacted the consumer, R.M., who then filed a formal written complaint. The complaint was substantially similar to the information provided by Nationstar. R.M. indicated that he received a phone call from a person identifying himself as “Jonathan McGrail,” of FSL. R.M. stated that the person also represented himself as a loan officer specializing in helping veterans refinance their homes. R.M. further stated that he and “Mr. McGrail” spoke several times over the phone and since R.M. was unable to make his house payments, they discussed a refinancing agreement. “Mr. McGrail” sent a “Second-Chance Mortgage Refinance Approval” document to R.M., who signed it and sent it back to FSL along with a check for $3,200.00.
9. An examiner for the Department determined that the host for the domain name “fullspectrumloans.com” was GoDaddy. Through a subpoena issued to GoDaddy, the examiner identified Respondent as the registrant for the domain name “fullspectrumloans.com.” Upon information and belief, Alejandro Flores was the person who represented to R.M. that he was “Jonathon McGrail.”
Transactional Laundering

John Doe transfers $9,000.00 to Jane Doe via PayPal for the purchase of a car. However, no car is sold, no physical cash exchanges hand, and Jane subsequently uses the funds to purchase counterfeit goods, which will later be sold in the black market.

These type of transactions can be very elusive and easily fly below the radar of a financial institution’s AML alerting system. Once a consistent pattern of activity is formed these transactions may be mistakenly viewed as normal transaction activity.

Criminals Are Using *Fortnite* to Launder Money

By TAMARA EVDOKIMOVA

JAN 24, 2019 • 3:14 PM
How microtransactions and in-game currencies can be used to launder money

By Steven Messner  April 13, 2018

We speak with a cyber security expert about new ways of laundering money online.
Phishers Target Anti-Money Laundering Officers at U.S. Credit Unions

A highly targeted, malware-laced phishing campaign landed in the inboxes of multiple credit unions last week. The missives are raising eyebrows because they were sent only to specific anti-money laundering contacts at credit unions, and many credit union sources say they suspect the non-public data may have been somehow obtained from the National Credit Union Administration (NCUA), an independent federal agency that insures deposits at federally insured credit unions.
Money Laundering Via Author Impersonation on Amazon?

Patrick Reames had no idea why Amazon.com sent him a 1099 form saying he’d made almost $24,000 selling books via Createspace, the company’s on-demand publishing arm. That is, until he searched the site for his name and discovered someone has been using it to peddle a $555 book that’s full of nothing but gibberish.
‘White Label’ Money Laundering Services

Laundering the spoils from cybercrime can be a dicey affair, fraught with unreliable middlemen and dodgy, high-priced services that take a huge cut of the action. But large-scale cybercrime operations can avoid these snares and become much more profitable when they’re able to disguise their operations as legitimate businesses operating in the United States, and increasingly they are doing just that.
What we're worried about is Alexa listening in and Too-Smart AI issues (clip of Sawyer)

https://youtu.be/OlfQ93VAQnQ
The Final Action

What to do when they see Suspicious Activity?

Do they know how to file a SAR?
Make It Snappy//
Make It Memorable

• Take aways should only be 1 or 2 per training
• Train frequently and with simplicity in mind
• “Tell Up and Shut Up”
Knowledge Coop
Training That Your People Want to Watch

f: The Knowledge Coop
in: NathanKnottingham
t: Knowledgecooper

nathan@knowledgecoop.com