saltmarsh

BSA/AML/CFT Boot Camp

1

saltmarsh

At Saltmarsh, we believe the way to ***achieve success is by contributing to the success of others***, which is why we thrive in genuine relationships. Our ***passion for people and excellence*** is more than a shared value; it's the foundation of our work.

What We Do

Advisory & Consulting | Audit & Assurance | Business Valuation | Client Accounting & Advisory | Employee Benefit Plan Administration | Wealth Management & Financial Planning | IT & Technology Services | Litigation & Dispute Advisory | Tax | Transaction Advisory / M&A | Trust & Estate Planning

Who We Serve

Construction & Real Estate Development | Financial Institutions | Government & Municipalities | Healthcare | High Net Worth Individuals | Hospitality | Manufacturing & Distribution | Nonprofit | Private Equity | Professional Services | Technology

accountingTODAY 2024 Best Firms to Work For

BEST of Accounting CLIENT SATISFACTION 2024

INSIDE public accounting TOP 200 FIRMS 2025

THE SALTMARSH WAY

saltmarshadvisors.com

2

Having worked for more than 20 years in the financial industry, I have seen compliance functions evolve from unknown, well-hidden departments deep inside banks to become a professional, complex and high-impact discipline.

The focus of the discipline has also shifted from primarily being about legal interpretations to many other areas such as risk assessments, project management, training, monitoring and data extractions as well as driving cultural change and communication. This implies that a career within compliance has become more exiting and meaningful today than ever before.

Anders Meinert Jørgensen · 1st
People leader with a strong commercial banking track record and deep experience within compliance and fighting financial crime

https://www.linkedin.com/pulse/why-compliance-banking-more-important-exciting-than-ever-j%C3%B8rgensen/

saltmarsh

3

Boot Camp Goals

Ask any question at any time

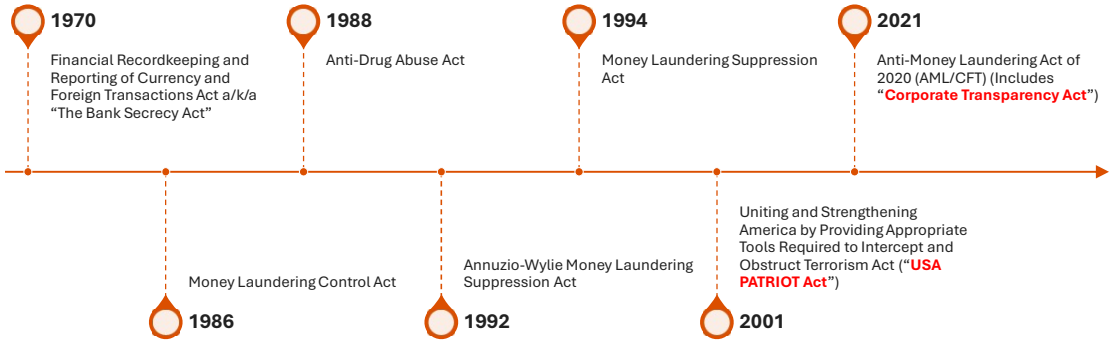
- ✓Introduce "money laundering" as the financial consequence of any crime
- ✓Understand the breadth of the Bank Secrecy Act's legal requirements
- ✓Introduce you to the Technical Reference Material – An assembly of lots of good BSA/AML/CFT information
- ✓Set the stage for a good BSA/AML experience

DISCLAIMER – This presentation and presenter intend to provide a broad-based explanation of the BSA's requirements and regulatory or independent testing interpretations over time. This is intended to educate and complement, but not to serve as a substitute for nor to override, competent legal advice, review of the statute or regulation, or regulatory guidance.

saltmarsh

4

How we got here



saltmarsh

5

What is "CFT"?

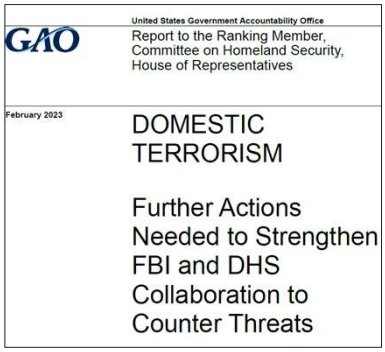
Consider updating policies & procedures to refer to AML/CFT, instead of BSA/AML

- Countering (or Combatting) the Financing of Terrorism
- FDIC: The Anti-Money Laundering Act of 2020 (the AML Act) modified subchapter II of chapter 53 of title 31 United States Code (the legislative framework commonly referred to as the BSA) and requires financial institutions to have reasonably designed risk-based programs to prevent money laundering and the financing of terrorism. By statute, individuals, banks, and other financial institutions are subject to the BSA recordkeeping requirements. *For purposes of consistency with the AML Act, the FDIC now uses the term "AML/CFT rather than "BSA/AML".*

saltmarsh

6

Combating the pernicious impact of illicit finance upon our financial system, economy, and society is integral to strengthening U.S. national security and prosperity. While there has been substantial progress in the United States and globally in addressing this challenge, the **U.S. anti-money laundering/countering the financing of terrorism (AML/CFT) regime** must adapt to an evolving threat environment, along with structural and technological changes in financial services and markets, for continued success in this critical fight.


United States Government Accountability Office

GAO

Report to the Ranking Member, Committee on Homeland Security, House of Representatives

February 2023

DOMESTIC TERRORISM

Further Actions Needed to Strengthen FBI and DHS Collaboration to Counter Threats


PRESS RELEASE

Three of the Highest-Ranking MS-13 Leaders in the World Arrested on Terrorism and Racketeering Charges

Thursday, February 23, 2023

Share

For Immediate Release

U.S. Attorney's Office, Eastern District of New York

saltmarsh

7

Global Perspective

- Financial Action Task Force / FATF

See page 24, 32, and 34 of reference material

saltmarsh

8

U.S. Money Laundering Statutes

18 USC 1956 – Conducting or attempting to conduct a financial transaction in a way that **conceals** or disguises the nature, location, source, ownership or control; **structuring** to avoid recordkeeping; or evading **taxes** on…the proceeds of "specified unlawful activity"

(aka the "predicate offenses")

20 years imprisonment; $500,000 fine or 2x; forfeiture

18 USC 1957 – Depositing, withdrawal, transfer or exchange of funds >$10,000 of the proceeds of SUA.

Knowledge is not relevant.

10 years imprisonment; forfeiture

31 USC 5324 – Prohibits structuring

5-10 years imprisonment; up to $1m fine; forfeiture

Those who **AID** or **ABET** have same punishment as if committed the crime

"**Willful Blindness**" - Deliberate avoidance of knowledge = knowledge

saltmarsh

9

What is money laundering

Concealing the origin or ownership of illegally obtained money.

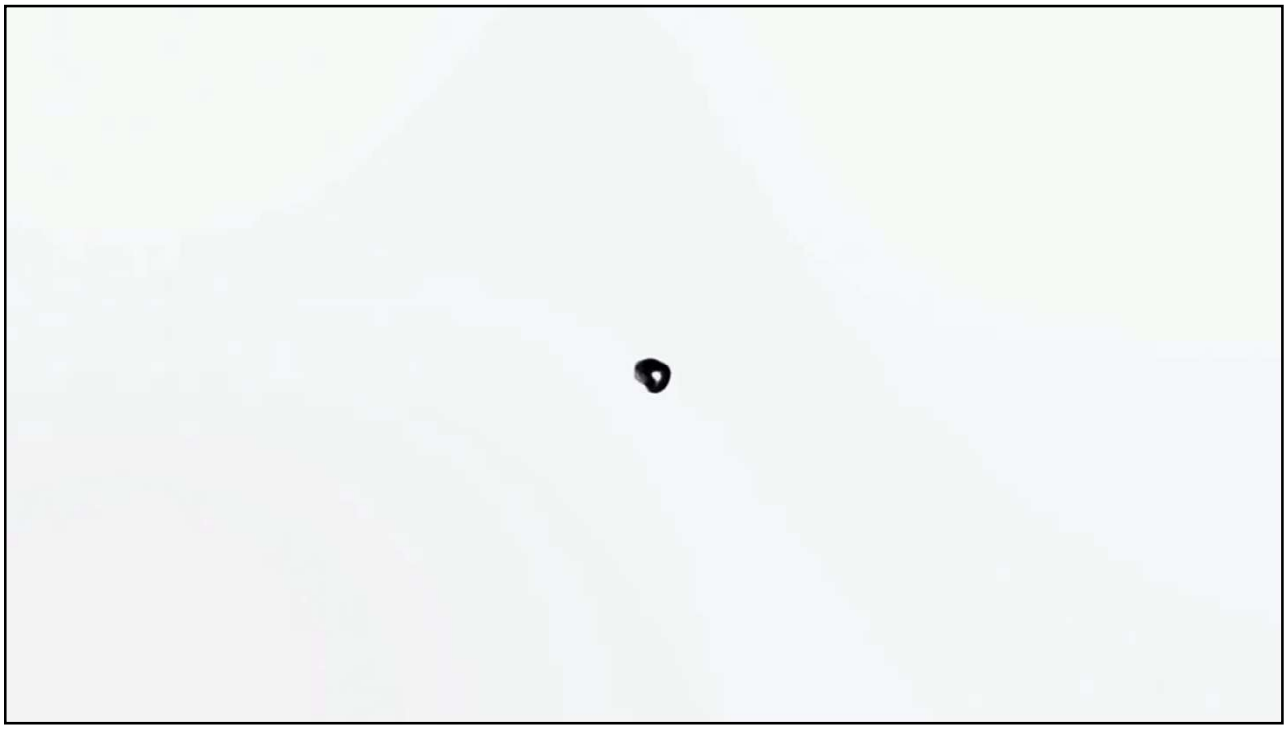
3 stages:

- **Placement/Filtering/Conversion/Transfer** of property derived from criminal activity into the financial system
- **Layer/Camouflage/Conceal/Disguise** the true nature, source, location, movement, ownership of property; move funds around to "muddy" the audit trail; add jurisdictional involvement & complexity
- **Integration/Investment/Acquisition/Possession** of property to look legitimate

To succeed, the criminal must **distance** himself or herself from the crime, the proceeds of crime, and the resultant property…Legal entities and arrangements are a great way to do that.

saltmarsh

10



11

Smurfs

- Third parties used to further the crime or assist in laundering proceeds
- Use multiple bank accounts, credit cards, shell companies
- Mix illegal gains with legitimate funds
- **Money Mules** - provide data or accounts to allow criminals to move money and go undetected - like opening a new bank account and giving someone else full access to it or processing certain transactions.
  - VERSUS social engineering scenario, where a person is victim of a scam. They get involved through psychological manipulation. These victims are usually unaware that their actions are breaking the law. They are being tricked into opening accounts, for example, through job advertisement.
  - LAW ENFORCEMENT is cracking down on ongoing offenders, through "knocks and talks" that advise the "victims" they are helping these people break the law
    - Could be convicted of unauthorized money transmission

saltmarsh

12

The BSA/AML/CFT Regulatory Environment

13

The BSA/AML/CFT Regulatory Environment

Statutes: 31 U.S.C. Chapter 53, Records & Reports on Monetary Instruments Transactions; 12 U.S.C. §§1951-1959

Regulations: 31 CFR Chapter X; Department of the Treasury, FinCEN/**Fin**ancial **C**rimes **E**nforcement **N**etwork

USA PATRIOT Act (31 U.S.C. 310) made FinCEN an official bureau of the Treasury, confirming its authority to implement, administer and enforce the BSA; make recommendations related to financial intelligence; and maintain, analyze and disseminate a government-wide data access service.

Each functional regulator also has specific BSA-related regulations

- Office of the Comptroller of the Currency (OCC): 12 CFR §21.11 and §21.21
- Federal Reserve Board (FRB): 12 CFR §208.62 and §208.63, 12 CFR §211.5(m), and 12 CFR §211.24(j)
- Federal Deposit Insurance Corporation (FDIC): 12 CFR §326.8; 12 CFR §353
- National Credit Union Administration: 12 CFR §748.1 and §748.2
- State banking or other business regulations

14

The AML/CFT Regulatory Environment

U.S. AML/CFT laws apply to **Financial Institutions (FIs):**

- "Banks" which includes Credit Unions and Trust Companies – FDIC, FRB, OCC, NCUA, FinCEN, and State banking departments
- "Non-Bank Financial Institutions" (NBFIs) *with* AML Requirements – SEC, IRS, TDFI
  - Money Service Business
    - check casher
    - money transmitter
    - currency dealer or exchanger
    - issuer or seller of traveler's checks or money orders
    - provider of prepaid access
  - Casino
  - Securities Broker/Dealer and Commodities Firm*
  - Insurance Company
  - Dealer in Precious Metals, Precious Stones, or Jewels*
  - Loan or Finance Company (Residential Mortgage Loan Originator; Housing GSE)
  - Persons involved in real estate closings and settlement*

https://bsaaml.ffiec.gov/manual/Appendices/05 List of "Financial Institutions"

*=Specifically mentioned in Treasury's 2024 National Money Laundering Assessment

saltmarsh

15

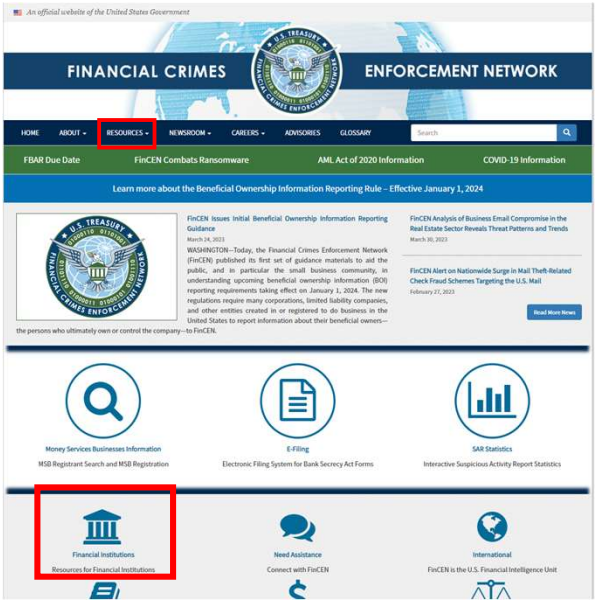
The AML/CFT Regulatory Environment

U.S. BSA laws applies to **Financial Institutions (FI):**

- "Banks" which includes Credit Unions and Trust Companies – FDIC, FRB, OCC, NCUA, FinCEN, and State banking departments
- Some "Non-Bank Financial Institutions" (NBFI) *with* AML Requirements – SEC, CTFC, IRS, OFR
- Some NBFIs *without* AML Requirements – IRS
  - Pawnbroker
  - Travel Agency
  - Automobile/boat/airplane sales
  - Person involved in real estate or closings * Proposed rule for title agents
  - Investment Advisor * Proposed rule

saltmarsh

16



www.fincen.gov

31 CFR Chapter X – Multiple sections could apply

CHAPTER X—FINANCIAL CRIMES ENFORCEMENT NETWORK, DEPARTMENT OF THE TREASURY

1000-1009		[RESERVED]
1010	1010.100 to 1010.980	GENERAL PROVISIONS
1011-1019		[RESERVED]
1020	1020.100 to 1020.670	RULE FOR BANKS
1021	1021.100 to 1021.670	RULES FOR CASINOS AND CARD CLUBS
1022	1022.100 to 1022.610-1022.670	RULES FOR MONEY SERVICES BUSINESSES
1023	1023.100 to 1023.670	RULES FOR BROKERS OR DEALERS IN SECURITIES
1024	1024.100 to 1024.640-1024.670	RULES FOR MUTUAL FUNDS
1025	1025.100 to 1025.600-1025.670	RULES FOR INSURANCE COMPANIES
1026	1026.100 to 1026.670	RULES FOR FUTURES COMMISSION MERCHANTS AND INTRODUCING BROKERS IN COMMODITIES
1027	1027.100 to 1027.600-1027.670	RULES FOR DEALERS IN PRECIOUS METALS, PRECIOUS STONES, OR JEWELS
1028	1028.100 to 1028.600-1028.670	RULES FOR OPERATORS OF CREDIT CARD SYSTEMS
1029	1029.100 to 1029.600-1029.670	RULES FOR LOAN OR FINANCE COMPANIES
1030	1030.100 to 1030.600-1030.670	RULES FOR HOUSING GOVERNMENT SPONSORED ENTERPRISES
1031-1059		[RESERVED]
1060	1060.100-1060.200 to 1060.800	PROVISIONS RELATING TO THE COMPREHENSIVE IRAN SANCTIONS, ACCOUNTABILITY, AND DIVESTMENT ACT OF 2010
1061-1099		[RESERVED]

PART 1010—GENERAL PROVISIONS

Contents

Subpart A—General Definitions

Subpart B—Programs

§1010.200 General.
§1010.205 Exempted anti-money laundering programs for certain financial institutions.
§1010.210 Anti-money laundering programs.
§1010.220 Customer identification program requirements.
§1010.230 Beneficial ownership requirements for legal entity customers.

Subpart C—Reports Required To Be Made

§1010.300 General.
§1010.301 Determination by the Secretary.
§1010.305 [Reserved]
§1010.306 Filing of reports.
§1010.310 Reports of transactions in currency.
§1010.311 Filing obligations for reports of transactions in currency.
§1010.312 Identification required.
§1010.313 Aggregation.
§1010.314 Structured transactions.
§1010.315 Exemptions for non-bank financial institutions.
§1010.320 Reports of suspicious transactions.
§1010.330 Reports relating to currency in excess of $10,000 received in a trade or business.
§1010.331 Reports relating to currency in excess of $10,000 received as bail by court clerks.
§1010.340 Reports of transportation of currency or monetary instruments.
§1010.350 Reports of foreign financial accounts.
§1010.360 Reports of transactions with foreign financial agencies.
§1010.370 Reports of certain domestic coin and currency transactions.

Subpart D—Records Required To Be Maintained

§1010.400 General.
§1010.401 Determination by the Secretary.
§1010.405 [Reserved]
§1010.410 Records to be made and retained by financial institutions.
§1010.415 Purchases of bank checks and drafts, cashier's checks, money orders and traveler's checks.
§1010.420 Records to be made and retained by persons having financial interests in foreign financial accou
§1010.430 Nature of records and retention period.
§1010.440 Person outside the United States.

Subpart E—Special Information Sharing Procedures To Deter Money Laundering and

PART 1020—RULE FOR BANKS

Contents

Subpart A—Definitions

§1020.100 Definitions.

Subpart B—Programs

§1020.200 General.
§1020.210 Anti-money laundering program requirements for financial institutions regulated only by a Federal functional regulator, including banks, savings associations, and credit unions.
§1020.220 Customer identification programs for banks, savings associations, credit unions, and certain non-Federally regulated banks.

Subpart C—Reports Required To Be Made By Banks

§1020.300 General.
§1020.310 Reports of transactions in currency.
§1020.311 Filing obligations.
§1020.312 Identification required.
§1020.313 Aggregation.
§1020.314 Structured transactions.
§1020.315 Transactions of exempt persons.
§1020.320 Reports by banks of suspicious transactions.

Subpart D—Records Required To Be Maintained By Banks

§1020.400 General.
§1020.410 Records to be made and retained by banks.

Subpart E—Special Information Sharing Procedures To Deter Money Laundering and Terrorist Activity

§1020.500 General.
§1020.520 Special information sharing procedures to deter money laundering and terrorist activity for banks.
§1020.530 [Reserved]
§1020.540 Voluntary information sharing among financial institutions.

Subpart F—Special Standards of Diligence; Prohibitions; and Special Measures

§1020.600 General.
§1020.610 Due diligence programs for correspondent accounts for foreign financial institutions.
§1020.620 Due diligence programs for private banking accounts.
§1020.630 Prohibition on correspondent accounts for foreign shell banks; records concerning owners of foreign banks and agents for service of legal process.
§1020.640 [Reserved]
§1020.670 Summons or subpoena of foreign bank records; termination of correspondent relationship.

AML/CFT Regulators

- **In addition to FinCEN's regulations and interpretations…..**
- **Federal Banking Agencies AML/CFT-related regulations:**
  - Office of the Comptroller of the Currency (OCC): 12 CFR §21.11 and §21.21
  - Federal Reserve Board (FRB): 12 CFR §208.62 and §208.63, 12 CFR §211.5(m), and 12 CFR §211.24(j)
  - Federal Deposit Insurance Corporation (FDIC): 12 CFR §326.8; 12 CFR §353
  - National Credit Union Administration: 12 CFR §748.1 and §748.2
- **State banking or other business regulations**
- **FFIEC Interagency Bank Exam manual/procedures:** https://bsaaml.ffiec.gov.manual

saltmarsh

19

Bank BSA Examinations

Examined at every Safety & Soundness Exam (generally every 12-18 months)

Part of CAMELS rating: Management

Interagency Exam Manual at www.ffiec.gov

- Consistency in Examination procedures
- Good guidance on risk factors and mitigation

saltmarsh

20

FFIEC Examination Manual

- Scoping and planning (2020)
- BSA/AML Risk Assessment (2020)
- Assessing the BSA/AML Compliance Program (2020)
  - Compliance Officer
  - Internal Controls
  - Independent Testing
  - Training
  - Customer Due Diligence (new 2018)

- Assessing Compliance with BSA Regulatory Requirements (2014-2021)
- Office of Foreign Asset Control (2014)
- Program Structures (2014)
- Risks Associated with Money Laundering and Terrorist Financing (2014-2021)

saltmarsh

21

The Five Pillars

1. BSA Officer

- Position is created by *law*
- Appointed by the Board of Directors (Board is ultimately responsible)
- Appropriate "authority, independence, and access to resources"

saltmarsh

22

The Five Pillars

2. A system of Internal Controls

- Reasonably designed to ensure compliance
- Must include a Customer Identification Program, and
- Effective 5/11/18, procedures that are reasonably designed to identify and verify beneficial owners of legal entity customers

saltmarsh

23

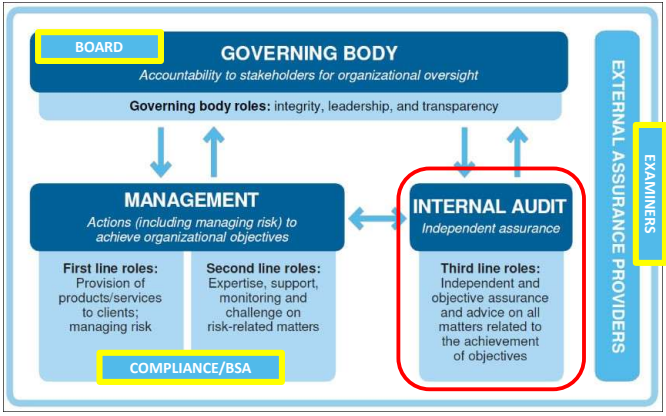
The Five Pillars

3. **Provide for Independent Testing of compliance**

saltmarsh

24

The "Three Lines" Model for Risk Management
(includes BSA/AML/CFT Risk)



- From the Institute of Internal Auditors *Revised July 2020*
- Not called Lines "of Defense" any more
- Recognizes "blurred lines" of controls in the Management portion
- Acknowledges Internal Audit's role in achieving objectives (value add)

saltmarsh

25

The Five Pillars

4. **Provide for Training for appropriate personnel**

(*Provide appropriate training for bank personnel*)

saltmarsh

26

The Five Pillars

(AML Program)

5. **Provide risk-based procedures for conducting ongoing customer due diligence (CDD) to:**

- Understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile;
- Conduct ongoing monitoring to identify and report suspicious transactions; and
- On a risk basis, maintain and update customer information
  - includes information regarding the beneficial owners of legal entity customers

saltmarsh

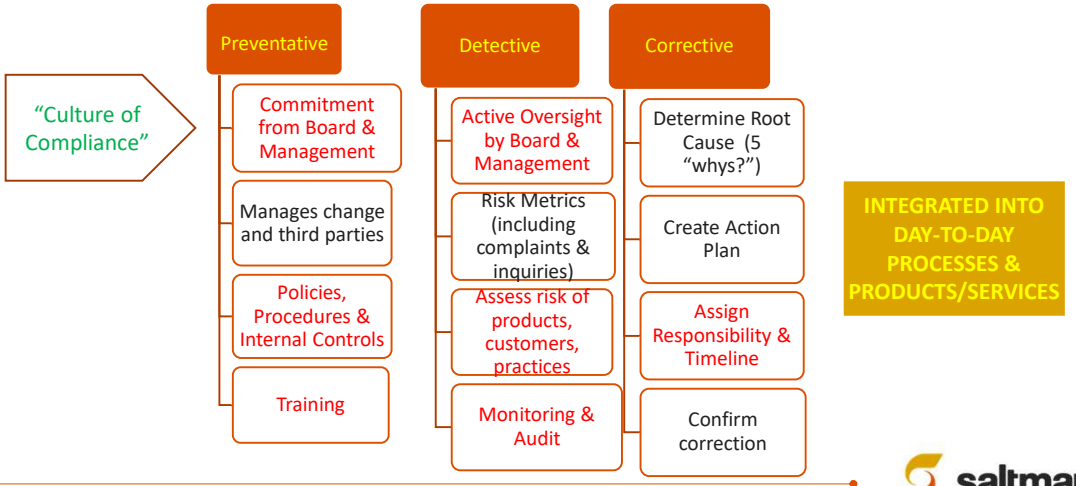
27

AML/CFT Framework

saltmarsh

28

Components of a Strong Compliance Management System (CMS)



saltmarsh

29

How can *you* identify and prevent money laundering?

Breaking Bad: Attorney Saul Goodman teaches Jesse Pinkman how to launder money from meth sales

ML doesn't exclusively involve cash, and it doesn't have to be illegal money coming IN to the financial system.

Money could already have been there to begin with and moved/transferred as part of the crime – for example, to purchase drugs, pay a bribe, embezzle funds. etc....

saltmarsh

30

BSA Requirements

1. Keep required records
2. Make required reports
3. Share information
4. Use risk-based processes to meet OFAC requirements
5. Use all the above to perform risk-based Customer Due Diligence and Enhanced Due Diligence to prevent and detect money laundering and terrorist financing (AML Program)
6. Assess risk on an ongoing basis to properly utilize resources and manage BSA/AML program, in light of your bank's risk appetite

saltmarsh

31

BSA Requirements

1. **Keep Required Records**
   - A. Customer Identification Program
   - B. Beneficial Owners of Legal Entity Customers
   - C. Funds Transfers
   - D. Monetary Instruments
   - E. Foreign Correspondent Banks
   - F. Other Bank Records

saltmarsh

32

Requirement #1 – Keep Records
A. Customer Identification Program – *page 1-3 in materials*

Prior to opening an account:

1. Obtain & Record 4 pieces of information *(name, birthday, address and ID number)* + any risk based enhancements as per your CIP Policy

2. Verify that Information – using **documentary** and/or **non-documentary** means
   - Documentary, such as (a) original unexpired government issued ID showing nationality or residence and bearing a photograph or similar safeguard; or (b) documents showing legal existence such as article of incorporation, business license, partnership agreement)

GOAL = Form a reasonable belief that you know the customer's true identity

saltmarsh

33

Requirement #1 – Keep Records
A. Customer Identification Program

"Account"

- *includes CD renewals and new relationships*
- *does not include participations or purchased accounts*

"Customer"

- *does not include existing customers that have met the "goal"*
- *does not include signers or guarantors (most banks "CIP" them though)*

saltmarsh

34

Requirement #1 – Keep Records
A. Customer Identification Program

Common areas of concern:

- Risk–based (layered) verification process – some accounts/customers require more
- Reliance on other parties – cannot, unless they are also a bank/regulated
- Need to provide "USA Patriot Act" notice, including for accounts opened not-in-branch
- Records created at account opening must be retained for 5 years from date account is closed
- Must have a process for fails, i.e., address discrepancies, SSN mismatch
- Others?

saltmarsh

35

Requirement #1 – Keep Records
B. Beneficial Owners of Legal Entity Customers – page 3-6 in materials

- Newly required 5/18/18 (why is this date important?)
- Establish and maintain written procedures that are reasonably designed to identify and verify beneficial owners of legal entity customers at the time a new account is opened
- Account is defined same as CIP rules
  - Existing customers are not exempt (but specific types of auto renewals are, per FIN 2018-R003)
  - You *can* document that you've verified with the existing customer that there are no changes to information already on file with the Bank.
- Legal entity customer is a general partnership or other entity that is created by filing a public document with the Secretary of State or similar office (e.g., corporation, LLC, Florida LLP)

saltmarsh

36

Requirement #1 – Keep Records
B. Beneficial Owners of Legal Entity Customers

Beneficial Owner:

Ownership Prong – Name and verify identify for EACH individual who, directly or indirectly, owns 25 percent or more of the equity interests of the legal entity; AND

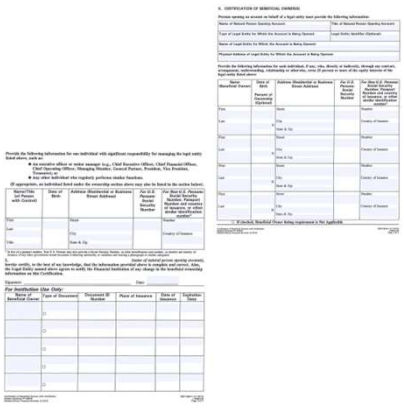
Control Prong – Name and verify identity of ONE individual with "significant responsibility to control, manage, or direct" the legal entity

saltmarsh

37

Requirement #1 – Keep Records
B. Beneficial Owners of Legal Entity Customers

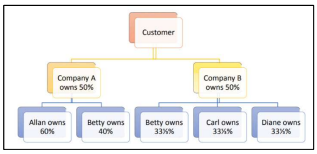
- FI must query the individual opening the account on behalf of the legal entity customer
  - Reg provides model certification form; other form(s) can be used so long as individual "certifies, to the best of the individual's knowledge, the accuracy of the information"
- FI must verify the identity of each beneficial, according to risk based procedures, to the extent reasonable and practicable
  - Same as under CIP Rules (*e.g.*, documentary/non-documentary; record retention; fails; reliance; AML program)



saltmarsh

38

Requirement #1 – Keep Records
B. Beneficial Owners of Legal Entity Customers



Common areas of concern:

- Complex ownerships – page 6
- Identify the events that trigger an update of beneficial owner information on *existing* customers (risk-based)
- Regulation requires update at new "relationships" and gives "cash management" as an example. *Does this include ACH origination? Online banking? Remote Deposit Capture?*
- No requirement to verify the ownership or control fact, unless you have "knowledge of facts that reasonably call into questions the accuracy of the information".
  - THIS IS WHY NO ONE (INCLUDING FINCEN) RECOMMENDS THAT BANKS ACCESS FINCEN's DATABASE UNDER THE CORPORATE TRANSPARENCY ACT
- Document what you did when information conflicts.

saltmarsh

39

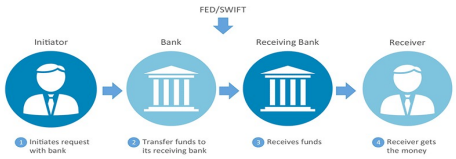
Requirement #1 – Keep Records
C. Funds Transfers – page 6-7 in materials

1

Verify ID & retain record of Originator's:

1) name
2) address
3) type & # of ID reviewed
4) SSN, EIN or "A" number; or passport country & #

- these records will already be on file for an *"established customer"*
- 5) method of Payment



2

Retain record of:

1) sender's name & address; amount;
2) execution date;
3) identity of receiving bank;
4) payment instructions;
5) If received with the order:
   - beneficiary name;
   - beneficiary address;
   - beneficiary account number;
   - other beneficiary identifier

3 4

Retain

1) "Payment Order" (instructions)
2) If not an *"established customer"* (i.e., for Payable Upon Proper ID/PUPID), verify ID* and document disposition of funds

*of person receiving funds, and, if different, of the beneficiary

saltmarsh

40

Requirement #1 – Keep Records
C. Funds Transfers

Common points of concern:

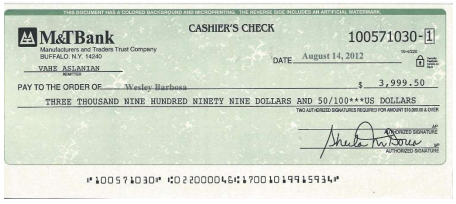
- Records must be retrievable for 5 years by originator's/beneficiary's name and account number
  - How to log joint owners or business name consistently
  - Have you sent/received on behalf of a "non-established customer"?
  - System conversions/mergers/acquisitions often involve retention within various systems
  - Internal transfers are also covered by recordkeeping
- *See reference material page 33 for sample log and AML/CFT "Red Flags"*

saltmarsh

41

Requirement #1 – Keep Records
D. Monetary Instruments – *page 7 in materials*

- Cashier's checks, money orders, travelers checks
- Purchased with $3,000-$10,000 in currency
  - Aggregated by business day if institution has knowledge



Common points of concern:

- Knowing who is "purchaser" (Authorized signer? Remitter?)
- "Log" of cash purchases is no longer required *by recordkeeping* regulation but can be very useful for due diligence and AML/CFT risk concerns.
- *See reference material page 34 for sample log and AML/CFT "Red Flags"*

saltmarsh

42

Requirement #1 – Keep Records
D. Monetary Instruments

RECORD:
- purchaser's name
- date of purchase
- type(s), serial number(s) and $ amount of each instrument(s) purchased

AND EITHER:
- verify the purchaser has a deposit account *(*where name and address have been previously verified and recorded)* OR
- verify identity and record purchaser's:
  - address;
  - date of birth,
  - SSN (or alien ID number);
  - document used to verify ID

saltmarsh

43

Requirement #1 – Keep Records
E. and F. Foreign Correspondent Accounts & Other Bank Records – page 8-9

Foreign Correspondent Bank Accounts – *not just clearing accounts*
- basic owner information
- (re)certification of compliance within 30 days and annual

Basic bank records, examples:
- loan purpose if > $10,000
- signature cards
- debits and checks issued on an account > $100
- deposit tickets showing the amount of cash involved
- list of each depositor which has not provided a taxpayer ID number despite reasonable efforts

Retain for five years; electronic records ok

saltmarsh

44

BSA Requirements

1. Keep required records
2. **Make required reports**
   A. Currency Transaction Reports
   B. Suspicious Activity Reports
   C. Foreign Institution and Financial Accounts
   D. International Transportation of Currency or Monetary Instruments
   E. Geographic Targeting Orders and other FinCEN requests

saltmarsh

45

Requirement #2 – Make Reports

- Discrete, or batch (requires approval) filing
- Status tracking
- Acknowledgement of each filing (DCN/ID#)
- For transmission only – you must save to your records (you can also print and retain in paper)

saltmarsh

46

Requirement #2 – Make Reports
A. Currency Transaction Reports – pages 9-15

Report on transaction(s) involving *more than* $10,000

- currency in (deposit, payment) OR currency out (withdrawal, cashed item)
- exchange of currency counts as BOTH

Aggregate multiple transactions if institution has knowledge they are BY (conductor) or ON BEHALF OF (beneficiary) any one person in any one business day

Must **verify identity** at time of the reportable transaction

saltmarsh

47

Requirement #2 – Make Reports
A. Currency Transaction Reports

- E-Filing is required within 15 calendar days of transaction
  - format revised regularly; not all fields are "required"
- FI can grant exemptions from CTR filing:

Improperly granted exemptions, like other "failure to files" can be subject to a **back-filing determination** from FinCEN.

	Who can be exempted:	Requirement for FI:
PHASE 1	domestic banks or governmental authority	• conduct initial due diligence • confirm eligibility annually
PHASE 1	publicly traded (listed) entities and their owned subsidiaries	• conduct initial due diligence • file initial designation form • confirm eligibility annually
PHASE 2	eligible non-listed businesses/payroll	• conduct initial due diligence • file initial designation form • monitor for suspicious activity • confirm eligibility annually • file revocation or begin filing CTRs

saltmarsh

48

Requirement #2 – Make Reports
B. Suspicious Activity Report – page 15-18

1. **Potential money laundering or BSA violations**

   $5,000 or more - Where FI knows, suspects, or has reason to suspect that the transaction(s):

   - ✓ was designed to evade any BSA requirements;
   - ✓ involves or hides funds or assets derived from illegal activities; or
   - ✓ has no business or apparent lawful purpose (or is not the sort in which the particular customer would normally be expected to engage), and the institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

saltmarsh

49

Requirement #2 – Make Reports
B. Suspicious Activity Report

2. **Known or suspected Federal criminal violation(s)**
   - committed or attempted against the FI
     - or involving transaction(s) through the FI
   - and FI believes it was an actual or potential victim
     - or was used to facilitate the criminal transaction

Filing threshold for Insider abuse is $0/any amount; otherwise, $5,000 if suspect can be identified and $25,000 if no suspect can be identified

saltmarsh

50

Requirement #2 – Make Reports
B. Suspicious Activity Report

- No loss is required (and the *attempt* at a transaction is SAR-worthy).
- **"Structuring" a CTR ($10,000) or other recordkeeping requirement ($3,000) is always SAR-worthy if thresholds met.**
- You get a Safe harbor for filing, even if the filing was not required.
- The SAR, or the existence of a SAR, is confidential. You may only share with law enforcement, examiners, and within your corporate organizational structure.
- You should Call law enforcement if activity is ongoing or is otherwise required (Adult Protective Services)

saltmarsh

51

Requirement #2 – Make Reports
B. Suspicious Activity Report

- Supporting documents should be identified in the narrative and are "deemed" filed with the SAR
  The SAR "narrative" should explain why the filer things the transaction(s) was suspicious
- e-file within 30 days of the initial detection of facts that constitute a basis for filing; delay for 30 additional days is allowed to identify the suspect
  **Time period begins when institution "determines" SAR-worthy
  FinCEN Guidance on AML System/investigation process – *Page 17-18 in reference materials*
- **Special rules for continuous filings on ongoing activity
- SAR Stats on FinCEN's site
  Top 3 reasons consistently are:
  1) Suspicion concerning the Source of Funds;
  2) Transaction(s) below CTR Threshold; and
  3) Check

saltmarsh

52

Requirement #2 – Make Reports
B. Suspicious Activity Report

- SAR filing is confidential,
  - But must notify the FI's board, or a committee thereof, of the SAR filing
  - Board MAY get SAR details if they want
  - WATCH for other Bank records that mention SAR filing

Issues to address in BSA Program:

- When is SAR determination actually made?
- Who has authority to file SAR?
- What if, after investigation, decision is made NOT to file SAR?
- How long to review on on-going activity?
- Whether/How long to keep an account open for SAR suspect?

saltmarsh

53

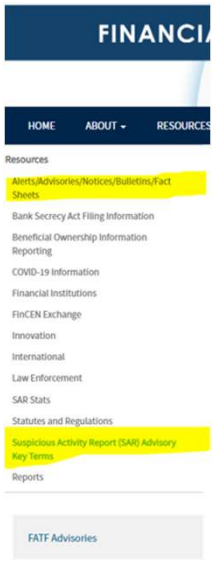
Requirement #2 – Make Reports
B. Suspicious Activity Report

- "Fraud, including financial crimes related to the COVID-19 pandemic,9 is the largest source of illicit proceeds in the United States, and represents one of the most significant money laundering threats to the United States, as highlighted in the U.S. Department of the Treasury's most recent National Money Laundering Risk Assessment,[10] National Strategy for Combatting Terrorist and other Illicit Financing,[11] and Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) National Priorities.[12]" (FinCEN Alert FIN 2023-007 regarding COVID Employee Retention Credit fraud)

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "**FIN-2023-ERC**" and select SAR field 34(z) (Fraud – other).

18 USC §1956 and §1957 list the underlying "specified unlawful activity" (SUA) but you can see the types of activity in the SAR form itself



saltmarsh

54

CONSUMER SENTINEL NETWORK DATA BOOK 2024

Report Type

Top 10 Fraud Categories

Rank	Category	# of Reports	% Reporting $ Loss	Total $ Loss	Median $ Loss
1	Imposter Scams	845,806	22%	$2,952M	$800
2	Online Shopping and Negative Reviews	383,441	76%	$432M	$130
3	Business and Job Opportunities	126,217	36%	$751M	$2,250
4	Investment Related	118,960	79%	$5,697M	$9,196
5	Internet Services	118,261	28%	$164M	$300
6	Prizes, Sweepstakes and Lotteries	97,350	22%	$351M	$1,000
7	Telephone and Mobile Services	92,520	39%	$56M	$240
8	Health Care	78,763	51%	$80M	$283
9	Travel, Vacations and Timeshare Plans	58,347	67%	$274M	$922
10	Mortgage Foreclosure Relief and Debt Management	34,159	21%	$82M	$1,500

Identity Theft Types

Rank	Theft Type	# of Reports
1	Credit Card	449,032
2	Other Identity Theft	358,993
3	Loan or Lease	176,400
4	Bank Account	114,608
5	Employment or Tax-Related	87,470
6	Phone or Utilities	82,626
7	Government Documents or Benefits	70,332

ftc.gov/data
March 2025

saltmarsh

55

Requirement #2 – Make Reports
C. FBAR and D. CMIR

C. Foreign Institution and Financial Accounts (FBAR)

- signer on account held in a foreign jurisdiction over $10,000 during prior calendar year
- e-file Foreign Bank and Financial Accounts Report (FBAR) annually

D. International Transportation of Currency or Monetary Instruments (CMIR)

- Person who physically transports, mails or ships >$10,000 into or out of the U.S. must file CMIR with Customs at time of entry or departure
- Person who receives must file within 15 days, unless already filed
- N/A for banks who ship by common carrier or postal service

saltmarsh

56

Requirement #2 – Make Reports
E. Geographic Targeting Order and other FinCEN Requests

Geographic Targeting Order: If reasonable grounds exist to conclude that additional recordkeeping and reporting are necessary…the Secretary may issue an order…in a geographic area…to obtain such information as Secretary may describe …concerning any transaction…for the payment, receipt, or transfer of funds…to maintain records…and to file a report in the manner specified in the Order. (*Page 25 in reference materials)*

Special Measures: Treasury Secretary can provide a broad range of orders involving jurisdictions, institutions, class of transactions, or type of account is a "primary money laundering concern"; includes reporting and recordkeeping, but also can include prohibitions.

saltmarsh

57

BSA Expectations – General Requirements

1. Keep required records
2. Make required reports
3. **Share information**
   - **A. 314(a)**
   - **B. 314(b)**

saltmarsh

58

Requirement #3 – Share Information
A. 314(a) – *page 19*

Special Information Sharing to Deter Money Laundering and Terrorist Activity

- FinCEN solicits information on law enforcement's behalf
- An entity or organization is engaged in (or is reasonably suspected, based on credible evidence, of engaging in) money laundering or terrorist financing
- Banks specify their contact and backup in the Call Report

saltmarsh

59

Requirement #3 – Share Information
A. 314(a)

Special Information Sharing to Deter Money Laundering and Terrorist Activity

- One-time search
- Generally search (although request may specify otherwise):
  - Current accounts of;
  - Accounts maintained for, during prior 12 months;
  - Transactions outside of an account conducted by, or for the benefit of, the named suspect, within the prior 6 months, records for which are required to be maintained, or that are recorded and maintained electronically

    Not just customers; refer to BSA recordkeeping rules
- Report to FinCEN within 15 days *only* if you have a match
- Confidential

saltmarsh

60

Requirement #3 – Share Information
B. 314(b) – *page 19-20*

Special Information Sharing to Deter Money Laundering and Terrorist Activity

- Encourages US Financial Institutions to share information in order to identify and report activities that may involve money laundering or terrorist financing
- Notify FinCEN of your intent to participate; and confirm that other side has also done so before sharing
- Establish and maintain procedures to protect the security and confidentiality of the information (we recommend keeping a log)
- Safe harbor from liability if requirements are followed

saltmarsh

61

Requirement #3 – Share Information
C. Non-Routine Sharing of Information

Non-routine subpoenas	Grand Jury subpoenas (GJS) National Security Letters (NSL)
120- hour rule - Requests for AML Records by Federal Regulator - Upon request, a bank must provide records related to its AML compliance, or one of its customers, within 120 hours	

saltmarsh

62

BSA Expectations – General Requirements

1. Keep required records
2. Make required reports
3. Share information

4. **Use risk-based processes to meet OFAC requirements – pages 20-22**

saltmarsh

63

Requirement #4 – Comply with OFAC
Regulatory Environment – OFAC

8 primary statutes with regulations at 31 CFR Title 31, Chapter 5 (§§501.101-598.901) – Applies to all US persons.

- Shares a common national security goal with BSA/AML/CFT and supervisory examinations are logically connected
- Prohibits doing business with, or transactions by or on behalf of, ***prohibited regions, countries, governments, regimes, businesses, individuals, vessels, digital currency wallet addresses, and others.***
  - Online search engine is available for individuals and entities but **not** for countries or other sanctions.
    - Ask your vendor(s) for coverage
    - Address "fuzzy logic"
    - Document the mitigating controls to close any gaps; follow OFAC's "Framework for Compliance Commitments" (essentially a Compliance Management System including a risk assessment)
- 50% rule – if prohibited person or entity directly or indirectly owns 50% of the property or entity, the property or entity is prohibited (note that "control" is not a factor here, but OFAC urges caution nonetheless).

saltmarsh

64

Requirement #4 – Comply with OFAC
Regulatory Environment – OFAC

- OFAC involves 35 different programs – FinCEN search includes Specially Designated Nationals and Blocked Persons list ("SDN List") PLUS FinCEN's Non-SDN "Consolidated Sanctions List"
- Generally, SDN transactions should be accepted, blocked, and reported to OFAC, while non-SDN should be rejected.
- Review specific sanction to see exactly what is required - Sanctions Programs and Country Information | Office of Foreign Assets Control (treasury.gov)
- Banks typically search all customers, beneficial owners, control persons, guarantors, official check payees, other side of wires/persons within the wire instructions, and people caching checks. NEW search concern is geolocation controls for prohibited countries in IP and email addresses (e.g., .sy for Syria, .ir for Iran). *See OFAC Enforcement action against daVinci Payments, issued 11/6/2023 and*
- OFAC In process wires: apps-treas.my.salesforce-sites.com/treasuryforms/Form?templateID=a1Qt0000002aSr6EAE
- OFAC Hotline 1-800-540-6322

saltmarsh

65

Requirement #4 – Comply with OFAC

- Significant sanctions for non-compliance
- Governance similar as for BSA: (*i.e.*, the Five Pillars)
  - Risk assess by products, customers and geographies
  - Maintain updated list(s); Test Software (Fuzzy Logic)
  - New accounts and one-time transactions (wires, monetary instruments,
  - Existing customer-base upon list changes
  - Report on Blocked Transactions

If you think you have a match, contact the OFAC "Hotline" at 1-800-540-6322 or email form (on website) for in-process wires

saltmarsh

66

BSA Expectations – General Requirements

1. Keep required records
2. Make required reports
3. Share information
4. Use risk-based processes to meet OFAC requirements
5. Use all the above to perform risk-based Customer Due Diligence and Enhanced Due Diligence to prevent and detect money laundering and terrorist financing (AML Program)

saltmarsh

67

Requirement #5 – AML Program *pages 23-24*

Customer Due Diligence (CDD)/Enhanced Due Diligence (EDD):

This requirement is specified throughout the FFIEC BSA/AML exam manual and calls for gaining an understanding of the customer at the time the relationship is established and throughout the life of the relationship.

Account due diligence pertains to the specific account of the customer

Enhanced due diligence is the additional level of review for those customers, accounts, products, services, or geographies that pose heightened/higher risk

Objective:

Predict with relative certainly the types of transactions in which a customer is likely to engage ("customer risk profile")

saltmarsh

68

Typical Customers and Transactions requiring Enhanced Due Diligence (EDD)

ID and Monitor *Potentially* Higher Risk Customers & Transactions

A. Shell companies
B. Non-resident aliens (special rules for private bank accounts)
C. Politically exposed persons/ Senior foreign political figure or close associate
D. Embassy or foreign consulate
E. Foreign Correspondent accounts
F. Trade Finance
G. Third party payment providers
H. Brokered deposits
I. Professional Service Providers*
J. Non-Bank Financial Institutions / Money Service Businesses*
K. Non-Governmental Organizations / Charities*
L. Cash-Intensive Businesses*
M. Privately Owned ATMs
N. Cannabis Related Businesses*
O. Cash, negotiable instruments, prepaid cards
P. Unverifiable sources and uses of funds
Q. Undisclosed beneficial owners
R. Wire transfers/e-banking
S. Structured transactions to avoid recordkeeping or reporting

You can reduce AML/CFT risk by choosing to not to bank these areas. As many states are enacting ESG-type statutes, you should perform CDD and document your ability/inability to mitigate risk and serve the client as a basis for deciding whether to bank the customer.

See pages 24-33 for things to look for in your EDD reviews.
**See LAST PAGE of reference material for more detailed list and NAICS codes for ID*

saltmarsh

69

From the FFIEC Exam manual…

- No specific customer type automatically presents a higher risk of ML/TF or other illicit financial activity
- There is no BSA/AML regulatory requirement or supervisory expectation for banks to have unique or additional CIP or CDD for any particular group or type of customer
- The level and type of CDD should be commensurate with the risks presented by the customer relationship
- The potential risk to a bank depends on the facts and circumstances specific to the customer relationship
- Banks must have appropriate risk-based procedures for conducting ongoing CDD to understand the nature and purpose of customer relationships, and to develop customer risk profiles
- Banks that operate in compliance with applicable BSA/AML regulatory requirements and reasonably manage and mitigate risks related to the unique characteristics of customer relationships are neither prohibited nor discouraged from providing banking services to any specific class or type of customer

saltmarsh

70

In accordance with the 5th pillar ---- Your policy and procedures should specify:

- The information you will obtain at new account opening for ALL customers (CDD) and for those with enhanced risk characteristics (EDD)
- Includes beneficial ownership forms
- Your risk rating algorithm, based on client, products and services, and geographies (usually different for business and consumers; usually based on occupation/nature of business and activity)
- How rating changes can be made
- What triggers an update of the beneficial Ownership form
- Reporting on risk position and changes
- How frequently customers of different risk profiles will be reviewed (Ongoing HDD or "High and Moderate Risk Reviews")
- What will be reviewed during the above reviews, which should vary based on type of risk presented

This is critical, whether you have an AML system or not

saltmarsh

71

CDD: Onboarding Customer Due Diligence

GOAL: Predict with relative certainly the types of transactions in which a customer is likely to engage ("customer risk profile")…."The foundation of a sound BSA/AML/CFT Program".

Basic CDD questions to ask **to establish profile & assign initial risk**:

- Have we done business with you before? Why are you here?
- What is your business structure? Is it complex? Newly formed? Why?
- Who are the Beneficial Owners and Control person? Are any of them foreign, politically exposed, or in the "news"?
- Where is your primary and additional addresses? Does google maps support? Is business international or far from branch?
- Is there an ATM on site at any of the locations? Who owns and funds the ATM?
- **What is your NAICS occupation/type of business**? Does business type require enhanced due diligence?
- **What is the purpose of the account?**
- **What are the sources of funds/wealth coming to the account?**
- **What are the Expected Transaction types, volumes, amounts, and geographic locations**
- **Will any funds come from (any type of service to) the marijuana, hemp, or CBD industry?**

If you have concerns at any time, you can review more information, such as prior banking references, licenses, a list of their major suppliers or customers, social media and review sites (facebook, Yelp, BBB), etc

saltmarsh

72

Enhanced Due Diligence/High Risk Reviews – Common Things

- Why is customer being reviewed?
- Who are they? What is their business? What is the entirety of their relationship with the Bank?
- What are you reviewing now? Has a site visit been performed? Is anything missing or outdated?
- What do you see?
  - Does this seem reasonable/commensurate with the expected, legitimate activities of their stated business/occupation and purpose of the account(s)?
- Is their rating appropriate?
- Is there any follow-up required?
  - At this point, a "case" or "investigation" can be opened, or the file can be "closed".

saltmarsh

73

Long-term EDD on products/services

including wire and cash-intensive peer reviews

Cashier's checks and Wire logs by purchaser (your customer), by remitter, by account, amount..

- On cashier's checks, is the remitter consistently the same as the purchaser? If not, why? Are they still "deposit accountholder" purchases?
- Are there unusual large or even dollar wires or checks that could be indicative of structuring?
- Are there multiple cashier's check issuances to the same purchaser in exchange for cash and other checks (e.g., using a proceed check like a bank account?)
- Are there unusual checks or wires to a payee, perhaps even from apparently unrelated customers, that do not make sense?
- Are there excessive "to-me", "from-me" checks or wires?
- Review check endorsements to see which account and bank took the check for deposit
- Review for customers that have incoming wires followed by outgoing wires?
- Are there unusual large or international wires without an apparent business purpose?
- "Google" the other side of transactions to determine whether they appear legitimate.
- Compare wire intensive customers to each other and to their unique businesses, looking for anomalies.

Review CTRs filed by customer and analyze dollar amounts.

- Compare to wire and cashier's check activity.
- For cash-intensive or exempt customers, determine whether activity has changed or remains consistent with peers and expected, legitimate business, and whether any suspicious activity is noted.

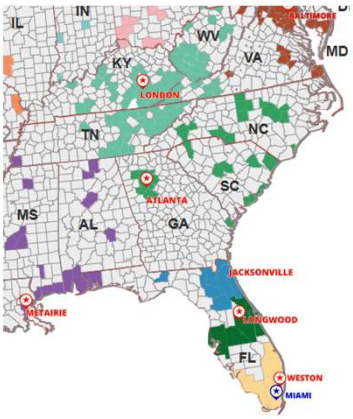
Review merchant-related ACH deposits and compare to peers to determine whether activity has changed or remains consistent with peers and expected, legitimate business, and whether any suspicious activity is noted.

saltmarsh

74

Requirement #5 – AML Program
Higher Risk Geographies *pages 24-25*

- **For example:**
- OFAC
- Special Measures (USA PATRIOT Act)
- Financial Action Task Force/FATF - High Risk and Non-Cooperative Countries and Territories (NCCTs)
- High Intensity Drug Trafficking Areas/HIDTA
  High Intensity Financial Crimes Areas/HIFCA
- FinCEN Advisories
- www.KnowYourCountry.com



HIGH INTENSITY DRUG TRAFFICKING AREAS (HIDTA)
PROGRAM COUNTIES MARCH 2025

saltmarsh

75

This is happening

saltmarsh

76

BSA Expectations – General Requirements

1. Keep required records
2. Make required reports
3. Share information
4. Use risk-based processes to meet OFAC requirements
5. Use all the above to perform risk-based Customer Due Diligence and Enhanced Due Diligence to prevent and detect money laundering and terrorist financing (AML Program)
6. Assess risk on an ongoing basis to properly utilize resources and manage BSA/AML program, in light of the Institution's risk appetite

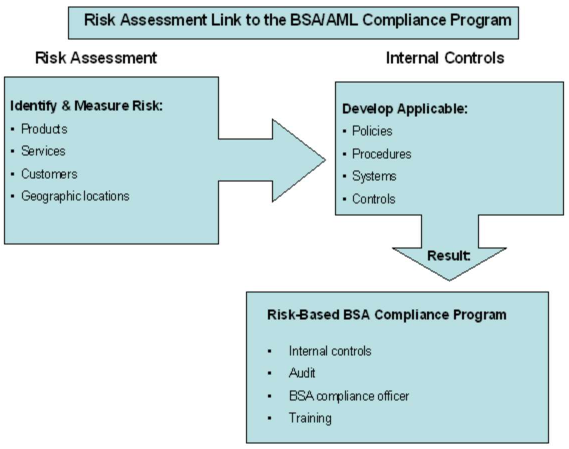
saltmarsh

77

Risk-Based Program

What does the Data say about the Quantity of Risk (Inherent) in your Customers, Products & Services, Geographies.

What is the Resultant Risk (and are there any gaps?) and which direction is the Risk going?



How Strong are your controls & How much Reliance do you Place on them?

saltmarsh

78

Risk Assessment – Better than obligatory

STEP 1. What does the Data say about the Quantity of Risk (Inherent) in your Customers, Products & Services, Geographies

STEP 2. How Strong are your controls/pillars? Have they been tested? How much reliance do you place on them?

Which direction are these trending?

Affects the bank's policies & procedures, level of monitoring and independent test procedures

saltmarsh

79

Suggested Factors for Assessing Strength of Controls/Pillars

Policy, Procedures, and Controls	Compliance Officer	Ongoing & Appropriate Training	Independent Testing	Customer & Enhanced Due Diligence
•High quality and current? Addresses regulatory changes, evolving risks, new products, and third parties? •Controls over recordkeeping, reporting, information sharing, OFAC, and ongoing customer due diligence? •Does risk assessment and individual client risk profiles consider customer, geographies, and products & services? •Do we routinely track, report, and assess governance over current and coming risk areas?	•Level of support from board & management? Reporting structure, time & resources (responsibilities)? •Knowledge of the bank and BSA requirements? •Works well with others (performance evaluations)? •Adequacy of staffing relative to risk/efficiencies? •Continuity plan?	•Recent, relevant, and specific (i.e., lending, IT)? •Measured for effectiveness and completion? •Includes one-on-one or group updates for critical areas?	•Truly independent? •Qualified and well-documented? •Are all "important" controls sufficiently tested? (e.g., CIP, CDD, OFAC, SAR, Training, AML System) •Do we determine root cause, and implement and verify real corrective action for exceptions or findings?	•Do we update and track geographic risk? •Do we determine sources of deposits and uses of withdrawals? •Do we apply enhanced verifications and documentation for prospective higher risk customers or accounts? •Has rating system been validated and proven? •Are our "profiles" independently validated or backed into by customer activity? •Do we respond to changes? •Have our AML alerting system(s) been validated to properly assist us in identifying suspicious or unusual transactions, accounts, geographies, and changes in customer behavior?

saltmarsh

80

Other important concepts for BSA/AML/CFT Compliance

81

Culture of (BSA) Compliance

FinCEN Advisory August 2014

- Leadership should be engaged
- Compliance should not be compromised by revenue interests
- Information should be shared throughout the organization
- Leadership should provide adequate human and technological resources
- The Program should be effective and tested by an independent and competent party
- Leadership and staff should understand how their BSA reports are used

82

AML System Model Validation

OCC & FRB 2011-12; FDIC FIL 22-2017

- Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance April 9, 2021
- BSA/AML Systems should be included in the model inventory:
  - Monitoring Systems; includes manual reports
  - Customer Risk Rating Tools
  - OFAC "Fuzzy Logic"
- Key Components:
  - Conceptual Soundness; gap analysis
  - Data Validation (inputs and outputs)
  - Rule or Parameter Validations (above- and below-the-line fine-tuning)

83

Third party BSA/compliance oversight

- An effective third party BSA/compliance risk management process will vary depending on the complexity and risk potential of the third-party relationship, but generally includes:
  - risk assessment
  - due diligence in selecting the third-party provider
  - appropriate contract structuring and review
    - Complaints, training, audit
  - sufficient oversight of third-party activities, including adequate quality control over products or services provided
- E.g., core service provider(s), AML system providers, auditors, appraisers, mortgage/loan brokers, etc.

84

Change Management

- The formality of change management process should be commensurate with the bank's size, complexity, and risk profile
- Anticipate and respond timely to changes in applicable laws and regulations, market conditions, and products and services offered by evaluating the change and implementing responses across affected lines of business
- The compliance & BSA functions should be involved in the due diligence and monitoring of new, modified, or expanded products or services
- Consider the entire lifecycle of a product or service in implementing change, and review the change after implementation to determine that actions taken have achieved planned results

saltmarsh

85

Thank you!

saltmarsh

86

Contact

Melba Moody

Manager, Financial Institutions

melba.moody@saltmarshadvisors.com

(800)477-7458

https://www.linkedin.com/in/melba-moody/

saltmarsh

87

Contact

Vicky Froehlich

Financial Institutions Consultant

vicky.froehlich@saltmarshadvisors.com

(800)477-7458

https://www.linkedin.com/in/victoria-m-740a2b187/

saltmarsh

88

saltmarsh

Thank You!

Receive Insights from Saltmarsh

saltmarshadvisors.com/subscribe

89