DENTONS

Financial Crime Prevention

A UK/US Comparison

March 2015

Agenda

- The Laws
- The Regulatory Requirements
- The Enforcement Actions
- Prevention of Money Laundering and Terrorist Finance
- Trends in Financial and Trade Sanctions
- Trends in the Prevention of Bribery and Corruption

AML

DENTONS

AML - Key Concepts 

- Criminal property
- Criminal conduct
- CDD/EDD
- Systems and controls
- What FCA wants

AML - Key Concepts

- Source of the asset is a critical factor.
- The laws are based on the type of organization and/or nature of the business conduct.
- KYC-CDD (due diligence)
- Effective systems and controls
- The legal and practical benefits of conduct consistent with government guidance.

AML: The Laws 1

The Law	The Offence	The Punishment
Proceeds of Crime Act 2002 (Part 7) s327	Concealing etc	Max 14 years/unlimited fine
POCA s 328	Arrangements	Max 14 years/unlimited fine
POCA s 329	Acquisition, possession and use	Max 14 years/unlimited fine
POCA s 330	Failure to disclose: regulated sector	Max 5 years/unlimited fine
POCA s 331	Failure to disclose: nominated officer in RS	Max 5 years/unlimited fine
POCA s 332	Failure to disclose: other nominated officers	Max 5 years/unlimited fine
POCA s 333A	Tipping off: regulated sector	Max 2 years/unlimited fine
POCA s 339	Disclosure in wrong form	Fine

AML: The Laws 2

The Law	The Offence	The Punishment
Terrorism Act 2000 s18	In relation to terrorist property: concealing, removing, transferring to nominees, or in any other way.	Max 14 years/unlimited fine
TA s19/21A	Failure to disclose - unregulated/regulated sector	Max 5 year/unlimited fine
TAs21D	Tipping off - regulated sector	Max 2 years/unlimited fine
Counter-Terrorism Act 2008		
Sched VII	Failure to comply with direction	Max 2 years/unlimited fine

AML: The Laws 3

The Law	The Offence	The Punishment
Money Laundering Regulations 2007: Reg 20 (referring to many other Regs)	Failure to have in place (a) CDD measures and ongoing monitoring; (b) reporting; (c) record-keeping; (d) internal control; (e) risk assessment and management; (f) monitoring and management of compliance with, and internal communication of, such policies and procedures, **in order to prevent activities related to money laundering and terrorist financing.**	Max 2 years/unlimited fine
JMLSG Guidance Notes	**No offence, but endorsed by Treasury, and taken into account by FCA**	

AML: The History of US AML Laws

The Law	The Offence	The Punishment
Bank Secrecy Act (1970) **(BSA)** **12 USC 1829b, 12 USC 1951–1959, and 31 USC 5311, et seq.**	Established requirements for recordkeeping and reporting by private individuals, banks and other financial institutions Designed to help identify the source, volume, and movement of currency and other monetary instruments transported or transmitted into or out of the United States or deposited in financial institutions Required banks to (1) report cash transactions over $10,000 using the Currency Transaction Report; (2) properly identify persons conducting transactions; and (3) maintain a paper trail by keeping appropriate records of financial transactions.	

AML: The History of US AML Laws

The Law	The Offence	The Punishment
The Money Laundering Control Act of 1986 (P.L. 99-57)	•Established money laundering as a federal crime •Prohibited structuring transactions to evade CTR filings •Directed banks to establish and maintain procedures to ensure and monitor compliance with the reporting and recordkeeping requirements of the BSA	Introduced civil and criminal forfeiture for BSA violations

AML: The History of US AML Laws

The Law	The Offence
The Anti-Drug Abuse Act of 1988 (P.L. 100-690)	Expanded the definition of financial institution to include businesses such as car dealers and real estate closing personnel and required them to file reports on large currency transactions Required the verification of identity of purchasers of monetary instruments over $3,000

AML: The History of US AML Laws

The Law	The Offence
Annunzio-Wylie Anti-Money Laundering Act of 1992 (P.L. 102-550)	• Strengthened the sanctions for BSA violations • Required Suspicious Activity Reports and eliminated previously used Criminal Referral Forms • Required verification and recordkeeping for wire transfers • Established the Bank Secrecy Act Advisory Group (BSAAG) • Required banking agencies to review and enhance training, and develop anti-money laundering examination procedures • Required banking agencies to review and enhance procedures for referring cases to appropriate law enforcement agencies • Streamlined CTR exemption process • Required each Money Services Business (MSB) to be registered by an owner or controlling person of the MSB • Required every MSB to maintain a list of businesses authorized to act as agents in connection with the financial services offered by the MSB • Made operating an unregistered MSB a federal crime

AML: The History of US AML Laws

The Law	The Offence
Money Laundering Suppression Act of 1994 (P. L. 103-310)	• Required banking agencies to review and enhance training, and develop anti-money laundering examination procedures • Required banking agencies to review and enhance procedures for referring cases to appropriate law enforcement agencies • Streamlined CTR exemption process • Required each Money Services Business (MSB) to be registered by an owner or controlling person of the MSB • Required every MSB to maintain a list of businesses authorized to act as agents in connection with the financial services offered by the MSB • Made operating an unregistered MSB a federal crime • Recommended that states adopt uniform laws applicable to MSBs.

AML: The History of US AML Laws

The Law	The Offence
USA Patriot Act of 2001 (P.L. 107-56)	• Criminalized the financing of terrorism and augmented the existing BSA framework by strengthening customer identification procedures • Prohibited financial institutions from engaging in business with foreign shell banks • Required financial institutions to have due diligence procedures (and enhanced due diligence procedures for foreign correspondent and private banking accounts) • Improved information sharing between financial institutions and the U.S. government by requiring government-institution information sharing and voluntary information sharing among financial institutions

AML: The History of US AML Laws

The Law	The Offence
USA Patriot Act of 2001 (P.L. 107-56)	• Prohibited financial institutions from engaging in business with foreign shell banks. • Expanded the anti-money laundering program requirements to all financial institutions • Increased civil and criminal penalties for money laundering • Provided the Secretary of the Treasury with the authority to impose "special measures" on jurisdictions, institutions, or transactions that are of "primary money laundering concern" • Facilitated records access and required banks to respond to regulatory requests for information within 120 hours • Required federal banking agencies to consider a bank's AML record when reviewing bank mergers, acquisitions, and other applications for business combinations. • Required federal banking agencies to consider a bank's AML record when reviewing bank mergers, acquisitions, and other applications for business combinations.

AML: The History of US AML Laws

The Law	The Offence
USA Patriot Act of 2001 (P.L. 107-56)	• Required financial institutions to have due diligence procedures (and enhanced due diligence procedures for foreign correspondent and private banking accounts) • Improved information sharing between financial institutions and the U.S. government by requiring government-institution information sharing and voluntary information sharing among financial institutions • Expanded the anti-money laundering program requirements to all financial institutions • Increased civil and criminal penalties for money laundering • Provided the Secretary of the Treasury with the authority to impose "special measures" on jurisdictions, institutions, or transactions that are of "primary money laundering concern" • Facilitated records access and required banks to respond to regulatory requests for information within 120 hours

AML: BSA Laws and Regulations Statutes

12 USC 1818(s) — "Compliance with Monetary Recordkeeping and Report Requirements" Requires that the appropriate federal banking agencies shall prescribe regulations requiring insured depository institutions to establish and maintain procedures reasonably designed to assure and monitor the compliance of such depository institutions with the requirements of the BSA.

See Additional Information for list and description of regulations

In addition, this section requires that each examination of an insured depository institution by the appropriate federal banking agency shall include a review of the procedures, and that the report of examination shall describe any problem with the procedures maintained by the insured depository institution.

See "*Red Flags*" for some of the examiners' key issues

AML: Failure to comply with BSA Laws and Regulations and Statutes

12 USC 1818(s) — Cease and Desist for Failure to Comply with Monetary Recordkeeping and Report Requirements

If the appropriate federal banking agency determines that an insured depository institution has either 1) failed to establish and maintain procedures that are reasonably designed to assure and monitor the institution's compliance with the BSA; or 2) failed to correct any problem with the procedures that a report of examination or other written supervisory communication identifies as requiring communication to the institution's board of directors or senior management as a matter that must be corrected, the agency shall issue an order requiring such depository institution to cease and desist from the violation of the statute and the regulations prescribed thereunder. Sections 1818(b)(3) and (b)(4) of Title 12 of the USC extend section 1818(s) beyond insured depository institutions.

AML: Failure to comply with BSA Laws and Regulations and Statutes

The government will typically allege in a criminal proceeding:

- **Willfully failing to establish and maintain an effective AML program in violation of 31 USC 5318(h).**
- **Willfully failing to conduct and maintain due diligence on correspondent bank accounts held on behalf of foreign person in violation of 31 USC 5318(i).**
- **They may allege violations of 18 U.S.C. 1956 (laundering of monetary instruments) or 1957 (engaging in monetary transactions in property derived from specified unlawful activity).**
- **These provide for criminal exposure for the illegal act and/or using the proceeds of an illegal act.**
- **.Statutory sentences up to 20 years.**
- **Fines up to the greater of $500,000 or twice the value of the property involved.**
- **The government's fallback position may be to seek civil and criminal penalties for regulatory violations.**

AML: What the Regulator Wants 

FCA Rule	Requirement	Example
Principle 3	A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.	If your systems and controls are not good enough you can get fined even if there is no evidence of criminal offence

AML: What the Regulator Wants 

FCA Rule	Requirement	Example
SYSC (3 or 6)	• Take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulator system and for countering the risk that the firm might be used to further financial crime. • ensure systems and controls: (1) enable it to identify, assess, monitor and manage money laundering risk; and (2) are comprehensive and proportionate to nature, scale and complexity of activities.	See PRIN 3
FC	A lot!	

FCA - AML 1

- *Governance*:
  - senior management involvement with MLRO report, getting right MI, ensure independent challenge of high risk relationships
  - staff reward structures that take into account AML compliance failings
- *MLRO*
  - independent, knowledgeable, robust and well-resourced, and poses effective challenge to the business where warranted
  - has a direct reporting line to executive management or the board
  - escalates where appropriate
  - awareness of high risk areas
- *Assessment of risks of ML*
  - systems and controls in place to identify, assess and monitor risk.
  - risk assessment informs processes
  - consideration of risk to include political connections, country risk, source of funds, sector risk, involvement in public contracts.
  - manage risk of relationship manager closeness to clients

FC - AML 2

- *CDD checks*
  - understanding limitations of electronic sources and not relying entirely on a single source of information.
  - understanding of purpose of transaction and ownership structures
- *Ongoing Monitoring*
  - understanding limits of automated programmes
  - challenging and dealing with the unexpected
  - feeding results into customer risk profile
- *Higher-risk situations: enhanced DD and monitoring*
  - all high risk relationships checked by the MLRO, use of independent internal or external intelligence reports.
  - how CDD is different for high risk customers and how EDD information is treated and stored
  - involvement of senior management in approving high risk customers
  - correspondent banks address risks

FCA - AML 3

- *Liaison with Law Enforcement*
  - clear, and understood by staff
  - SARs through nominated officer
  - policy on what is reportable
  - dealing with production orders
- *Reliance and record keeping*
  - retrievability of documents for production order
  - sample records where rely on others
- *CTF*
  - have risks been assessed and how
  - who is responsible for liaison with authorities
- *Payments*
  - checking payer information
  - checking respondent information and SWIFT cover messages
  - sampling inward payments

AML: The Bank Examiner's "Red Flags"

Customers Who Provide Insufficient or Suspicious Information

- A customer uses unusual or suspicious identification documents that cannot be readily verified.
- A customer provides an individual tax identification number after having previously used a Social Security number.
- A customer uses different tax identification numbers with variations of his or her name.
- A business is reluctant, when establishing a new account, to provide complete information about the nature and purpose of its business, anticipated account activity, prior banking relationships, the names of its officers and directors, or information on its business location.
- A customer’s home or business telephone is disconnected.
- The customer’s background differs from that which would be expected on the basis of his or her business activities.

AML: The Bank Examiner's "Red Flags"

Customers Who Provide Insufficient or Suspicious Information con't

- A customer makes frequent or large transactions and has no record of past or present employment experience.
- A customer is a trust, shell company, or Private Investment Company that is reluctant to provide information on controlling parties and underlying beneficiaries. Beneficial owners may hire nominee incorporation services to establish shell companies and open bank accounts for those shell companies while shielding the owner’s identity.

AML: The Bank Examiner's "Red Flags"

Efforts to Avoid Reporting or Recordkeeping Requirement

- A customer or group tries to persuade a bank employee not to file required reports or maintain required records.
- A customer is reluctant to provide information needed to file a mandatory report, to have the report filed, or to proceed with a transaction after being informed that the report must be filed.
- A customer is reluctant to furnish identification when purchasing negotiable instruments in recordable amounts.
- A business or customer asks to be exempted from reporting or recordkeeping requirements.
- A person customarily uses the automated teller machine to make several bank deposits below a specified threshold.

AML: The Bank Examiner's "Red Flags"

Efforts to Avoid Reporting or Recordkeeping Requirement

- A customer deposits funds into several accounts, usually in amounts of less than $3,000, which are subsequently consolidated into a master account and transferred outside of the country, particularly to or through a location of specific concern (e.g., countries designated by national authorities and Financial Action Task Force on Money Laundering (FATF) as non-cooperative countries and territories).
- A customer accesses a safe deposit box after completing a transaction involving a large withdrawal of currency, or accesses a safe deposit box before making currency deposits structured at or just under $10,000, to evade Currency Transaction Report (CTR) filing requirements.

AML: The Bank Examiner's "Red Flags"

Funds Transfers

- Many funds transfers are sent in large, round dollar, hundred dollar, or thousand dollar amounts.
- Funds transfer activity occurs to or from a financial secrecy haven, or to or from a high-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer's business or history.
- Many small, incoming transfers of funds are received, or deposits are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer's business or history.
- Large, incoming funds transfers are received on behalf of a foreign client, with little or no explicit reason.

AML: The Bank Examiner's "Red Flags"

Funds Transfers con't

- Funds transfer activity is unexplained, repetitive, or shows unusual patterns.
- Payments or receipts with no apparent links to legitimate contracts, goods, or services are received.
- Funds transfers are sent or received from the same person to or from different accounts.
- Funds transfers contain limited content and lack related party information.

AML: The Bank Examiner's "Red Flags"

Automated Clearing House Transactions

- Large-value, automated clearing house (ACH) transactions are frequently initiated through third-party service providers (TPSP) by originators that are not bank customers and for which the bank has no or insufficient due diligence.
- TPSPs have a history of violating ACH network rules or generating illegal transactions, or processing manipulated or fraudulent transactions on behalf of their customers.
- Multiple layers of TPSPs that appear to be unnecessarily involved in transactions.
- Unusually high level of transactions initiated over the Internet or by telephone.
- National Automated Clearing House Association (NACHA) information requests indicate potential concerns with the bank’s usage of the ACH system.

AML: The Bank Examiner's "Red Flags"

Activity Inconsistent with the Customer's Business

- The currency transaction patterns of a business show a sudden change inconsistent with normal activities.
- A large volume of cashier's checks, money orders, or funds transfers is deposited into, or purchased through, an account when the nature of the accountholder's business would not appear to justify such activity.
- A retail business has dramatically different patterns of currency deposits from similar businesses in the same general location.
- Unusual transfers of funds occur among related accounts or among accounts that involve the same or related principals.
- The owner of both a retail business and a check-cashing service does not ask for currency when depositing checks, possibly indicating the availability of another source of currency.
- Goods or services purchased by the business do not match the customer's stated line of business.
- Payments for goods or services are made by checks, money orders, or bank drafts not drawn from the account of the entity that made the purchase.

AML: The Bank Examiner's "Red Flags"

Lending Activity

- Loans secured by pledged assets held by third parties unrelated to the borrower.
- Loan secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties.
- Borrower defaults on a cash-secured loan or any loan that is secured by assets which are readily convertible into currency.
- Loans are made for, or are paid on behalf of, a third party with no reasonable explanation.
- To secure a loan, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via currency or multiple monetary instruments.
- Loans that lack a legitimate business purpose, provide the bank with significant fees for assuming little or no risk, or tend to obscure the movement of funds (e.g., loans made to a borrower and immediately sold to an entity related to the borrower).

AML: The Bank Examiner's "Red Flags"

Changes in Bank-to-Bank Transactions

- The size and frequency of currency deposits increases rapidly with no corresponding increase in non-currency deposits.
- A bank is unable to track the true accountholder of correspondent or concentration account transactions.
- The turnover in large-denomination bills is significant and appears uncharacteristic, given the bank’s location.
- Changes in currency-shipment patterns between correspondent banks are significant.

AML: The Bank Examiner's "Red Flags"

Cross-Border Financial Institution Transactions

- U.S. bank increases sales or exchanges of large denomination U.S. bank notes to Mexican financial institution(s).
- Large volumes of small denomination U.S. banknotes being sent from Mexican casas de cambio to their U.S. accounts via armored transport or sold directly to U.S. banks. These sales or exchanges may involve jurisdictions outside of Mexico.
- Casas de cambio direct the remittance of funds via multiple funds transfers to jurisdictions outside of Mexico that bear no apparent business relationship with the casas de cambio. Funds transfer recipients may include individuals, businesses, and other entities in free trade zones.
- Casas de cambio deposit numerous third-party items, including sequentially numbered monetary instruments, to their accounts at U.S. banks.
- Casas de cambio direct the remittance of funds transfers from their accounts at Mexican financial institutions to accounts at U.S. banks. These funds transfers follow the deposit of currency and third-party items by the casas de cambio into their Mexican financial institution.

AML: The Bank Examiner's "Red Flags"

Trade Finance

- Items shipped that are inconsistent with the nature of the customer's business (e.g., a steel company that starts dealing in paper products, or an information technology company that starts dealing in bulk pharmaceuticals).
- Customers conducting business in high-risk jurisdictions.
- Customers shipping items through high-risk jurisdictions, including transit through non-cooperative countries.
- Customers involved in potentially high-risk activities, including activities that may be subject to export/import restrictions (e.g., equipment for military or police organizations of foreign governments, weapons, ammunition, chemical mixtures, classified defense articles, sensitive technical data, nuclear materials, precious gems, or certain natural resources such as metals, ore, and crude oil).
- Obvious over- or under-pricing of goods and services.

AML: The Bank Examiner's "Red Flags"

Trade Finance con't

- Obvious misrepresentation of quantity or type of goods imported or exported.
- Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
- Customer requests payment of proceeds to an unrelated third party.
- Shipment locations or description of goods not consistent with letter of credit.
- Documentation showing a higher or lower value or cost of merchandise than that which was declared to customs or paid by the importer.
- Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment. Any changes in the names of parties should prompt additional OFAC review.

AML: The Bank Examiner's "Red Flags"

Insurance

- A customer purchases products with termination features without concern for the product's investment performance.
- A customer purchases insurance products using a single, large premium payment, particularly when payment is made through unusual methods such as currency or currency equivalents.
- A customer purchases product that appears outside the customer's normal range of financial wealth or estate planning needs.
- A customer borrows against the cash surrender value of permanent life insurance policies, particularly when payments are made to apparently unrelated third parties.
- Policies are purchased that allow for the transfer of beneficial ownership interests without the knowledge and consent of the insurance issuer. This would include secondhand endowment and bearer insurance policies.
- A customer is known to purchase several insurance products and uses the proceeds from an early policy surrender to purchase other financial assets.

AML: The Bank Examiner's "Red Flags"

Shell Company Activity

- A bank is unable to obtain sufficient information or information is unavailable to positively identify originators or beneficiaries of accounts or other banking activity (using Internet, commercial database searches, or direct inquiries to a respondent bank).
- Payments to or from the company have no stated purpose, do not reference goods or services, or identify only a contract or invoice number.
- Goods or services, if identified, do not match profile of company provided by respondent bank or character of the financial activity; a company references remarkably dissimilar goods and services in related funds transfers; explanation given by foreign respondent bank is inconsistent with observed funds transfer activity.
- Transacting businesses share the same address, provide only a registered agent's address, or have other address inconsistencies.

AML: The Bank Examiner's "Red Flags"

Shell Company Activity con't

- Unusually large number and variety of beneficiaries are receiving funds transfers from one company.
- Frequent involvement of multiple jurisdictions or beneficiaries located in high-risk offshore financial centers.
- A foreign correspondent bank exceeds the expected volume in its client profile for funds transfers, or an individual company exhibits a high volume and pattern of funds transfers that is inconsistent with its normal business activity.
- Multiple high-value payments or transfers between shell companies with no apparent legitimate business purpose.
- Purpose of the shell company is unknown or unclear.

AML: The Bank Examiner's "Red Flags"

Embassy and Foreign Consulate Accounts

- Official embassy business is conducted through personal accounts.
- Account activity is not consistent with the purpose of the account, such as pouch activity or payable upon proper identification transactions.
- Accounts are funded through substantial currency transactions.
- Accounts directly fund personal expenses of foreign nationals without appropriate controls, including, but not limited to, expenses for college students.

AML: The Bank Examiner's "Red Flags"

Employees

- Employee exhibits a lavish lifestyle that cannot be supported by his or her salary.
- Employee fails to conform to recognized policies, procedures, and processes, particularly in private banking.
- Employee is reluctant to take a vacation.

AML: The Bank Examiner's "Red Flags"

Other Unusual or Suspicious Customer Activity Customer frequently exchanges small-dollar denominations for large-dollar denominations.

- Customer frequently deposits currency wrapped in currency straps or currency wrapped in rubber bands that is disorganized and does not balance when counted.
- Customer purchases a number of cashier's checks, money orders, or traveler's checks for large amounts under a specified threshold.
- Customer purchases a number of open-end stored value cards for large amounts. Purchases of stored value cards are not commensurate with normal business activities.
- Customer receives large and frequent deposits from on-line payments systems yet has no apparent on-line or auction business.
- Monetary instruments deposited by mail are numbered sequentially or have unusual symbols or stamps on them.

AML: The Bank Examiner's "Red Flags"

Other Unusual or Suspicious Customer Activity Customer frequently exchanges small-dollar denominations for large-dollar denominations con't

- Suspicious movements of funds occur from one bank to another, and then funds are moved back to the first bank.
- Deposits are structured through multiple branches of the same bank or by groups of people who enter a single branch at the same time.
- Currency is deposited or withdrawn in amounts just below identification or reporting thresholds.
- Customer visits a safe deposit box or uses a safe custody account on an unusually frequent basis.
- Safe deposit boxes or safe custody accounts opened by individuals who do not reside or work in the institution’s service area, despite the availability of such services at an institution closer to them.

AML: The Bank Examiner's "Red Flags"

Other Unusual or Suspicious Customer Activity Customer frequently exchanges small-dollar denominations for large-dollar denominations con't

- Customer repeatedly uses a bank or branch location that is geographically distant from the customer’s home or office without sufficient business purpose.
- Customer exhibits unusual traffic patterns in the safe deposit box area or unusual use of safe custody accounts. For example, several individuals arrive together, enter frequently, or carry bags or other containers that could conceal large amounts of currency, monetary instruments, or small valuable items.
- Customer rents multiple safe deposit boxes to store large amounts of currency, monetary instruments, or high-value assets awaiting conversion to currency, for placement into the banking system.

AML: The Bank Examiner's "Red Flags"

Other Unusual or Suspicious Customer Activity Customer frequently exchanges small-dollar denominations for large-dollar denominations con't

- A customer establishes multiple safe custody accounts to park large amounts of securities awaiting sale and conversion into currency, monetary instruments, outgoing funds transfers, or a combination thereof, for placement into the banking system.
- Unusual use of trust funds in business transactions or other financial activity.
- Customer uses a personal account for business purposes.
- Customer has established multiple accounts in various corporate or individual names that lack sufficient business purpose for the account complexities or appear to be an effort to hide the beneficial ownership from the bank.

AML: The Bank Examiner's "Red Flags"

Other Unusual or Suspicious Customer Activity Customer frequently exchanges small-dollar denominations for large-dollar denominations con't

- Customer makes multiple and frequent currency deposits to various accounts that are purportedly unrelated.
- Customer conducts large deposits and withdrawals during a short time period after opening and then subsequently closes the account or the account becomes dormant. Conversely, an account with little activity may suddenly experience large deposit and withdrawal activity.
- Customer makes high-value transactions not commensurate with the customer’s known incomes.

AML: The Bank Examiner's "Red Flags"

Potentially Suspicious Activity that May Indicate Terrorist Financing

- Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from high-risk countries (e.g., countries designated by national authorities and FATF as non-cooperative countries and territories).
- The stated occupation of the customer is not commensurate with the type or level of activity.
- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).
- Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

AML: The Bank Examiner's "Red Flags"

Potentially Suspicious Activity that May Indicate Terrorist Financing

Funds Transfers

- A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves high-risk locations.
- Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
- Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to high-risk countries.

AML: The Bank Examiner's "Red Flags"

Other Transactions That Appear Unusual or Suspicious

- Transactions involving foreign currency exchanges are followed within a short time by funds transfers to high-risk locations.
- Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in high-risk locations.
- A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from high-risk locations when there appear to be no logical business reasons for dealing with those locations.
- Banks from high-risk locations open accounts.
- Funds are sent or received via international transfers from or to high-risk locations.
- Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.

AML: The most common issues

Exhibit 4: Number of Filings by Type of Suspicious Activity by Depository Institutions*
March 1, 2012 through December 31, 2014

Rank	Supicious Activity Type	Filings (Overall)	Percentage (Overall)
1	Multiple transactions below CTR threshold	464,135	11.06%
2	Suspicion concerning the source of funds	441,764	10.52%
3	Transaction with no apparent economic, business, or lawful purpose	256,727	6.12%
4	Transaction out of pattern for customer(s)	240,334	5.73%
5	Suspicious use of multiple locations	240,317	5.73%
6	Check	183,879	4.38%
7	Suspicious EFT/wire transfers	180,802	4.31%
8	Two or more individuals working together	167,631	3.99%
9	Identity theft	166,895	3.98%
10	Other suspicious activities-Other	161,927	3.86%
11	Provided questionable or false documentation	156,759	3.73%
12	Consumer Loan	152,525	3.63%
13	Credit/Debit Card	130,109	3.10%
14	Fraud-Other	103,520	2.47%
15	Suspicious use of multiple accounts	90,795	2.16%
16	Identification documentation-Other	85,590	2.04%
17	Multiple transactions below BSA recordkeeping threshold	78,911	1.88%
18	Counterfeit Instrument (other)	74,877	1.78%
19	Alters transactions to avoid CTR requirement	70,078	1.67%
20	Mortgage fraud-Other	65,615	1.56%

AML: The most common issues con't

21	Money laundering-Other	65,515	**1.56%**
22	Multiple individuals with same or similar identities	62,734	**1.49%**
23	Refused or avoided request for documentation	53,076	**1.26%**
24	Suspicious use of noncash monetary instruments	51,826	**1.23%**
25	ACH	43,549	**1.04%**
26	Wire transfer	41,700	**Less than 1%**
27	Forgeries	35,226	**Less than 1%**
28	Suspicious inquiry by customer regarding BSA reporting or recordkeeping requirements	31,773	**Less than 1%**
29	Account takeover	31,423	**Less than 1%**
30	Elder financial exploitation	27,312	**Less than 1%**
31	Structuring-Other	25,502	**Less than 1%**
32	Single individual with multiple identities	23,271	**Less than 1%**
33	Embezzlement/theft/disappearance of funds	21,792	**Less than 1%**
34	Alters transaction to avoid BSA recordkeeping requirement	19,506	**Less than 1%**
35	Suspicious use of third-party transactors (straw-man)	15,242	**Less than 1%**
36	Customer cancels transaction to avoid BSA reporting and recordkeeping requirements	11,599	**Less than 1%**
37	Exchanges small bills for large bills or vice versa	11,093	**Less than 1%**
38	Suspicion concerning the physical condition of funds	11,078	**Less than 1%**
39	Appraisal fraud	9,818	**Less than 1%**
40	Suspicious receipt of government payments/benefits	9,789	**Less than 1%**

AML: The most common issues con't

41	Misuse of position or self-dealing	8,362	**Less than 1%**
42	Mail	8,045	**Less than 1%**
43	Unauthorized electronic intrusion	7,943	**Less than 1%**
44	Unlicensed or unregistered MSB	7,695	**Less than 1%**
45	Suspicious designation of beneficiaries, assignees or joint owners	7,608	**Less than 1%**
46	Loan Modification fraud	6,252	**Less than 1%**
47	Suspicious exchange of currencies	5,814	**Less than 1%**
48	Foreclosure fraud	4,131	**Less than 1%**
49	Business loan	3,372	**Less than 1%**
50	Suspicious use of informal value transfer system	3,118	**Less than 1%**
51	Trade Based Money Laundering/Black Market Peso Exchange	3,017	**Less than 1%**
52	Little or no concern for product performance penalites, fees, or tax consequences	2,890	**Less than 1%**
53	Changes spelling or arrangement of name	2,801	**Less than 1%**
54	Healthcare	1,809	**Less than 1%**
55	Mass-marketing	1,442	**Less than 1%**
56	Suspected public/private corruption (foreign)	937	**Less than 1%**
57	Suspected public/private corruption (domestic)	898	**Less than 1%**
58	Pyramid scheme	746	**Less than 1%**
59	Bribery or gratuity	736	**Less than 1%**
60	Terrorist financing-Other	677	**Less than 1%**
61	Known or suspected terrorist/terrorist organization	515	**Less than 1%**

AML: The "who" we need to focus on

Exhibit 7: Filings by Affiliation or Relationship by Depository Institutions*
March 1, 2012 through December 31, 2014

Relationship	2012	2013	2014
Accountant	6	266	232
Agent	18	453	415
Appraiser	86	4,101	738
Attorney	16	150	190
Borrower	5,044	66,842	51,329
Customer	31,349	788,103	997,610
Director	30	228	221
Employee	1,355	12,615	14,462
No relationship to institution	6,238	212,958	357,695
Officer	79	451	444
Owner or Controlling Shareholder	65	381	301
Other	14,940	156,083	188,598
Unknown/Blank	3,142	141,495	210,978

*Some Suspicious Activity Reports may list a subject (or multiple subjects) with multiple relationships to the financial institution.

AML: What are the "manner and means"?

Exhibit 9: Number of Filings by instrument type(s)/payment mechanism(s) involved in the suspicious activity by Depository institutions*
March 1, 2012 through December 31, 2014

Type of Instrument Type(s)/ Payment Mechanism(s)	2012	2013	2014
Bank/Cashier's check	2,074	39,649	53,495
Foreign currency	38	2,265	2,168
Funds transfer	4,244	98,780	144,122
Gaming instruments	11	178	196
Government payment	271	8,848	8,497
Money orders	357	6,032	11,107
Personal/Business check	6,941	116,309	154,179
Travelers checks	58	979	1,001
U.S. Currency	10,459	306,189	418,574
Other	1,034	18,254	29,685

*Some SAR filings may list multiple instrument type(s)/payment mechanism(s).

AML: Key Enforcement Actions

Year	Firm	Breach	Sanction
2003	Abbey	Branch CDD failings, SAR delays	£2m
2008	Syndicatum (and its MLR0)	Poor risk assessment and lack of CDD	£49K (£17.5K on MLRO) - financial difficulties
2010	Alpari (and MLR0)	Poor CDD, sanctions, PEP screening and training	£140K (£14K on MLR0)
2012	Coutts	Poor EDD procedures on PEPs	£8.75m
2012	Habib	Reliance on head office, poor EDD	£525K (£17,500 on MLRO)
2012	Turkish Bank	Correspondent banking	£294K
2013	EFG	EDD - good policy on paper, poor in practice	£4.2m
2013	Guaranty Trust	Poor PEP DD, risk assessments, sanctions, source of funds	£525K
2014	Standard Bank	Civil penalty for MLR breach - EDD on PEPs	£7.6m

AML: Key U.S. Enforcement Actions

Year	Firm	Sanction	Conduct
1/27/15	Oppenheimer & Co., Inc.	$20m	Inadequate policies, procedures, and internal controls reasonably designed to detect and report suspicious securities trading activity.
1/07/14	JP Morgan	$2.05b fine and forfeiture	BSA/AML/Failure to report Madoff's conduct
2012	HSBC	$1.9b fine	AML/Sanctions

Financial and Trade Sanctions

DENTONS

Financial and Trade Sanctions - the Law

The Law	The Offence	The Punishment
Sanctions SIs	Providing financial or economic resources, directly or indirectly, to designated person without licence, or facilitating this	Max 7 years/ unlimited fine
	Failing to freeze funds	max 7 years/ unlimited fine
	Misleading form/failure to comply with licence or co-operate with Treasury	Max 2 yrs/unlimited fine
Terrorist Asset Freezing etc Act	Similar to SIs	Similar to SIs
MLRs Reg 20	Includes terrorist finance	As AML
Export Credit Order 2008	Trade sanctions - embargoed goods/jurisdictions, dual use goods	Various up to 10 years/ unlimited fine
JMLSG	No offence, not endorsed, but guidance published	

Financial and Trade Sanctions

Office of Foreign Assets Control (OFAC)

U.S. Treasury office that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security interests against foreign countries, international narcotics traffickers and those engaged in the proliferation of weapons of mass destruction.

Actions can be brought against all U.S. persons, banks, bank holding companies and non-bank subsidiaries that must comply with OFAC regulations including foreign bank branches and many of their overseas offices and subsidiaries.

Regulations require:

- Block accounts and other property of specified countries, entities and individuals.
- Prohibit or reject unlicensed trade and financial transactions with specified countries, entities and individuals.

Sanctions - what the regulator expects

- *Governance*
  - individual of sufficient authority responsible for sanctions compliance
  - clarity on when to screen with appropriate escalation procedures
- *Risk assessment*
  - assess which areas of business present most risk, with up to date assessment
  - understand all local financial sanctions regimes in relevant jurisdictions
- *Screening customers against sanctions lists*
  - effective, up-to-date and appropriate screening systems
  - appropriate mixture of manual and automated screening
  - checking of customers' directors and beneficial owners
  - rely on others only where confident it is appropriate
- *Matches and escalation*
  - how to determine whether a name match is "real"
  - procedures on notifying FCA, or submitting SAR, as well as notifying HMT
- *Weapons proliferation* – checks built in to sanctions process

The examiner's handbook is a good resource

Page 146 of http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2007.pdf

Examination Procedures

Office of Foreign Assets Control

Objective. *Assess the bank's risk-based Office of Foreign Assets Control (OFAC) compliance program to evaluate whether it is appropriate for the bank's OFAC risk, taking into consideration its products, services, customers, entities, transactions, and geographic locations.*

1. Determine whether the board of directors and senior management of the bank have developed policies, procedures, and processes based on their risk assessment to ensure compliance with OFAC laws and regulations.

2. Regarding the risk assessment, review the bank's OFAC compliance program. Consider the following:

   - The extent of, and method for, conducting OFAC searches of each relevant department or business line (e.g., automated clearing house (ACH) transactions, monetary instrument sales, check cashing, trusts, loans, deposits, and investments) as the process may vary from one department or business line to another.

   - The extent of, and method for, conducting OFAC searches of account parties other than accountholders, which may include beneficiaries, guarantors, principals, beneficial owners, nominee shareholders, directors, signatories, and

Consider using the examiner's handbook to spot-check your risk analysis

Page 358 of http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2007.pdf

Appendix M: Quantity of Risk Matrix — OFAC Procedures

Examiners should use the following matrix, as appropriate, when assessing a bank's risk of encountering an OFAC issue.

Low	Moderate	High
Stable, well-known customer base in a localized environment.	Customer base changing due to branching, merger, or acquisition in the domestic market.	A large, fluctuating client base in an international environment.
Few high-risk customers; these may include nonresident aliens, foreign individuals (including accounts with U.S. powers of attorney), and foreign commercial customers.	A moderate number of high-risk customers.	A large number of high-risk customers.
No overseas branches and no correspondent accounts with foreign banks.	Overseas branches or correspondent accounts with foreign banks.	Overseas branches or multiple correspondent accounts with foreign banks.
No electronic banking (e-banking) services offered, or products available are purely informational or non-transactional.	The bank offers limited e-banking products and services.	The bank offers a wide array of e-banking products and services (i.e., account transfers, e-bill payment, or accounts opened via the Internet).

An example of a designation for blocking

U.S. DEPARTMENT OF THE TREASURY

Contact Us | Press Center | Blog | Accessibility | Google Privacy | Español | Languages

Advanced Search

Home | Treasury For... | About | Resource Center | Services | Initiatives | Careers | Connect with Us

- Consumer Policy
- Economic Policy
- Financial Markets, Financial Institutions, and Fiscal Service
- Financial Sanctions
  - Specially Designated Nationals List (SDN List)
  - Consolidated Sanctions List
  - Search OFAC's Sanctions Lists
  - Additional Sanctions Lists
  - **OFAC Recent Actions**
  - Complete List of Sanctions Programs and Country Information
  - Frequently Asked Questions
  - OFAC Civil Penalties and

Resource Center

Home » Resource Center » Financial Sanctions » OFAC Recent Actions » Counter Terrorism Designations

Counter Terrorism Designations

1/14/2015

OFFICE OF FOREIGN ASSETS CONTROL

Specially Designated Nationals List Update

The following individual has been added to OFAC's SDN List:

AL-ASHQAR, 'Abdallah (a.k.a. AL ASHQAR, Abdullah Jihad; a.k.a. AL MAQDISI, Abu al Muhtasib; a.k.a. AL-ASHQAR, Abdallah; a.k.a. AL-'ASHQAR, 'Abdallah; a.k.a. AL-ASHQAR, 'Abdallah Jihad Musa; a.k.a. AL-ASHQAR, Abdullah; a.k.a. AL-ASHQAR, Abdullah Jihad; a.k.a. AL-MAQDISI, Abu-al-Muhtasib; a.k.a. AL-TAWHID, Muhandes; a.k.a. AL-TAWHID, Muhandis; a.k.a. ASHKAR, Abdallah; a.k.a. "ABU-HAJIR"; a.k.a. "AL MUHTASIB, Abu"), Region: Gaza; DOB 1986; nationality Palestinian (individual) [SDGT].

PRESS CENTER

Press Releases

02/19/2015

Remarks by Under Secretary for International Affairs Nathan Sheets at The Peterson Institute for International Economic...

View All Press Releases

Featured Photo

April 14, 2014 - Secretary Lew and Ukrainian Finance Minister O...

View All Photos

Daily Press Guidance

02/20/2015

Daily Treasury Guidance for Friday, February 20, 2015

View All

Sanctions: Key Enforcement Actions

Year	Firm	Breach	Sanction
2010	RBS	Inadequate sanctions systems and controls	£6.5m (first fine under MLR)
2010	Alpari (and MLR0)	Poor CDD, sanctions, PEP screening and training	£140K (£14K on MLR0)
2013	Guaranty Trust	No recording of sanctions checks unless match, often started relationship without checking	£525K

Bribery and Corruption

DENTONS

Bribery And Corruption - Comparison 1

	 ANTI-BRIBERY PROVISIONS	 BRIBERY ACT
Prohibited Conduct:	Prohibits direct and indirect bribery of non-US officials, including officers and employees of state-owned enterprises, for purposes of obtaining or retaining business.	Prohibits bribery of any person (not limited to foreign officials or other public sector) to induce them to act "improperly."
Bribe Recipients:	Prohibits only payment of/offer to pay a bribe; requesting/ accepting a bribe is not a violation.	Prohibits payment of/offer to pay a bribe, as well as requesting/ accepting a bribe.

Bribery And Corruption - comparison 2

	 ANTI-BRIBERY PROVISIONS	 BRIBERY ACT
Jurisdiction	• US companies (public or private) • Most non-US subsidiaries of US companies • Foreign companies listed on a US stock exchange • US citizens and residents • Third parties and employees of any nationality acting for a US company • Third parties and employees of any nationality who commit an act in furtherance of a violation in the US (including by using US mails or wires)	• UK companies • Foreign companies that operate in the UK • UK nationals and residents • Any person acting while in the UK • Any person acting overseas with a "close connection" to the UK

Bribery And Corruption - comparison 3

	 ANTI-BRIBERY PPROVISIONS	 BRIBERY ACT
Knowledge Requirement:	Requires corrupt intent.	For bribing foreign public officials no requirement for dishonest intent. In other cases of giving bribes must intend or know of acting "improperly." Companies face strict liability for failure to prevent acts of bribery.
Reasonable and bona fide promotional expenditures:	Permissible	No exception or defence (but reasonable, proportionate and bona fide expenditure unlikely to amount to bribery under the Act).
"Facilitating" payments to expedite routine governmental action:	Permissible	No exception or defence. In practice, prosecutors may decide that prosecuting some small payments is not in the public interest.

Bribery and Corruption - what the regulator expects

- *Governance*
  - senior management able to demonstrate a good understanding of the requirements and to lead by example and get good MI.
  - clear, audited, policies and procedures, under control of senior individual
- *Risk assessment*
  - consider ABC associated with products and services offered, customers and jurisdictions dealt with and business practices (e.g. corporate hospitality).
  - consider what might lead to downplaying of risk
- *Policies and procedures*
  - behaviour expected clearly set out and documented with unambiguous consequences for breach. Availability of whistle-blowing procedure for suspicions.
- *Dealing with third parties*
  - carry out thorough due diligence on third parties, monitor payments made to them and record rationale behind them.
  - anti-corruption clauses in contracts.

Bribery and Corruption Trends

- Average settlement in 2014 was $157m.
- Alstom, SA -$772m to settle allegations that it bribed Indonesian officials.
- Alcoa, Inc.-$384m to settle allegations that it paid bribes to secure work in Bahrain.
- Number of actions decreased from 2010 high water mark of 48 to 26.
- Now requiring post-settlement in most settlements
- Hot geography for matters is Nigeria, China and Iraq.
- Energy and natural resource sectors led the way.
- Pharmaceutical, Life Sciences and Health Care (medical devices) to follow?
- Department of Justice still largest player with SEC in second place.
- *FBI shifting personnel (30) to full-time positions.

Bribery and Corruption: Key Enforcement Actions

Year	Firm	Breach	Sanction
2006	Aon	Insufficient due diligence on third parties; Insufficient monitoring of third parties; Insufficient training; Insufficient MI	£5.95m
2011	Willis	No recording of commercial rationale; inadequate due diligence was carried out on overseas third parties; inadequate review of relationships; poor staff monitoring ad MI	£6.895m
2013	JLT Speciality	Poor checks over third parties, lack of DD,response to warnings	£1.8m
2014	Besso	Poor controls over 3rd party relationships	£315,000

The Regulators and Enforcers

DENTONS

Do you know who they are?

The main players on the U.S. side

The Takeaway

DENTONS

The Takeaways

1.The enforcement investigation "tipping point" is how you handle your most lucrative relationship.

2. Appreciate the government's inability to find, much less reach entities outside the U.S. may heighten your legal risk because they can find and reach you ("*Gatekeeper Strategy*").

3. The balancing act between privacy and transparency of financial activity may be moving toward the later consideration because of HSBC leaks, change of course with Swiss bank accounts and terrorist attacks/architecture discoveries in Europe.

4. U.S. and U.K. (primary actors) enforcement actions will lead to follow-on activity in secondary countries.

The Takeaways con't

5. Primary actors' legal authority and resources, including technology, has led to a disproportionate extraterritorial impact outside of the primary geography that should be considered when responding to a legal issue or performing legal risk analysis.

6. Cross border due diligence must appreciate more than just the differences in personnel, language and experience.

- What is the enforcement culture for the reporting entity?
- Are the standards used for analysis the same across regions (i.e. are we using the same red flags to identify risk)?
- How do the laws of the various venues compare?
- How do the legal privileges of the various venues compare?

The moral from the UK

- You will be OK if
  - You know the law
  - You know your business
  - You know your products
  - You know your customers
  - Your policies are practical
  - Your staff are trained
  - Your management is involved
  - Your audits are thorough
  - Your concerns are documented
  - **You take compliance seriously**
  - **You make it clear that you do**

The Moral from the US

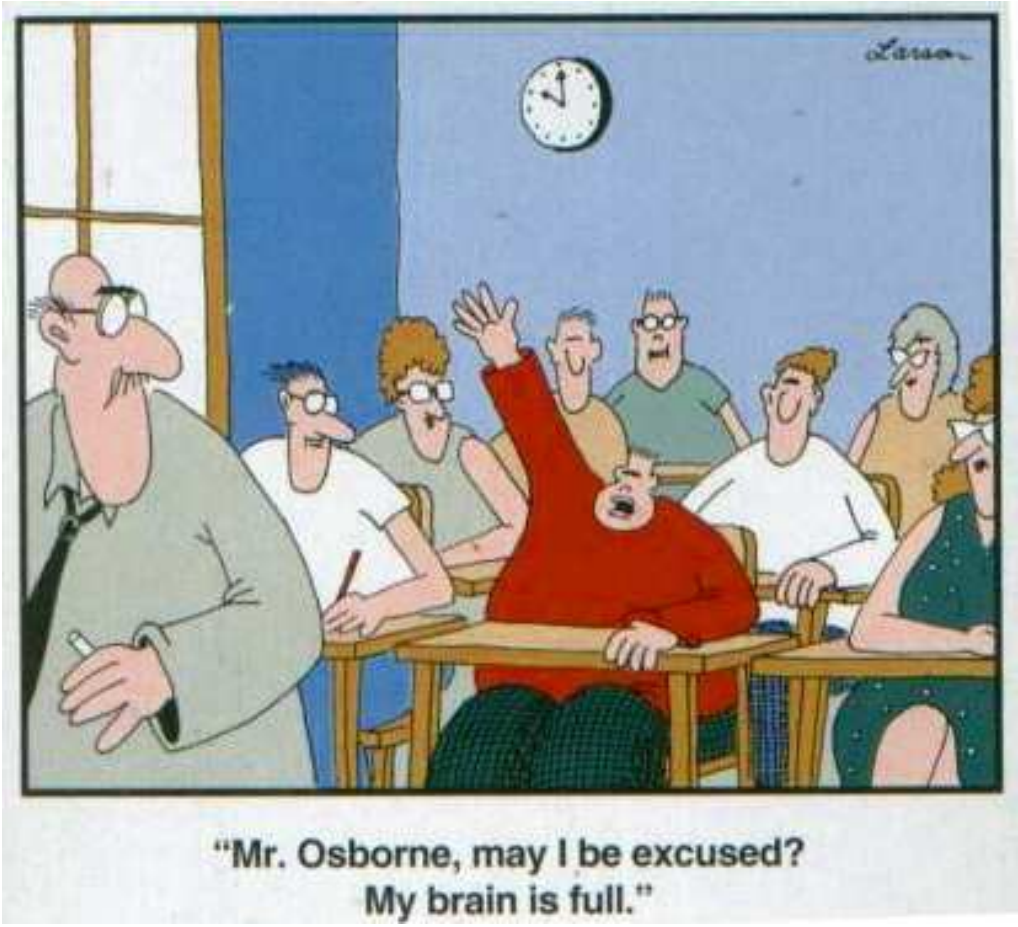
- Same song as before, second verse:

  Can you find the problem?

  Can you fix the problem?

  Can you demonstrate it will not happen again?

Questions?



DENTONS

Thank you

Dentons UKMEA LLP
One Fleet Place
London
EC4M 7WS
United Kingdom

DENTONS

Additional Information/Legal References

AML: BSA Regulations

Regulations\U.S. Treasury/FinCEN

- 31 CFR 103 — “Financial Recordkeeping and Reporting of Currency and Foreign Transactions” Sets forth FinCEN regulations that promulgate the BSA. Select provisions are described below.
- 31 CFR 103.11 — “Meaning of Terms” Sets forth the definitions used throughout 31 CFR Part 103.
- 31 CFR 103.16 — “Reports by Insurance Companies of Suspicious Transactions” Sets forth the requirements for insurance companies to report suspicious transactions of$5,000 or more.
- 31 CFR 103.18 — “Reports by Banks of Suspicious Transactions” Sets forth the requirements for banks to report suspicious transactions of $5,000 or more.
- 31 CFR 103.22 — “Reports of Transactions in Currency” Sets forth the requirements for financial institutions to report currency transactions in excess of $10,000. Includes 31 CFR 103.22(d) — “Transactions of Exempt Persons,” which sets forth the requirements for financial institutions to exempt transactions ofcertain persons from currency transaction reporting requirements.

AML: BSA Regulations

Regulations\U.S. Treasury/FinCEN

31 CFR 103.23 — “Reports of Transportation of Currency or Monetary Instruments” Sets forth the requirements for filing a Currency or Monetary Instruments Report.

- 31 CFR 103.24 — “Reports of Foreign Financial Accounts” Sets forth the requirement that each person having a financial account in a foreign country must file a report with the Internal Revenue Service annually.
- 31 CFR 103.27 — “Filing of Reports” Filing and recordkeeping requirements for Currency Transaction Reports (CTRs), Report of International Transportation of Currency or Monetary Instruments (CMIR), and Report of Foreign Bank and Financial Accounts (FBAR).
- 31 CFR 103.28 — “Identification Required” Sets forth the requirement that financial institutions verify the identity of persons conducting currency transactions in excess of $10,000.

AML: BSA Regulations

Regulations\U.S. Treasury/FinCEN

- 31 CFR 103.29 — “Purchases of Bank Checks and Drafts, Cashier’s Checks, Money Orders, and Traveler’s Checks” Sets forth the requirements that financial institutions maintain records relating to purchases of monetary instruments with currency in amounts between $3,000 and $10,000.
- 31 CFR 103.32 — “Records to Be Made and Retained by Persons Having Financial Interests in Foreign Financial Accounts” Sets forth the requirement that persons having a financial account in a foreign country maintain records relating to foreign financial bank accounts reported on an FBAR.
- 31 CFR 103.33 — “Records to Be Made and Retained by Financial Institutions” Sets forth recordkeeping and retrieval requirements for financial institutions, including funds transfer recordkeeping and transmittal requirements.
- 31 CFR 103.34 — “Additional Records to Be Made and Retained by Banks” Sets forth additional recordkeeping requirements for banks.

AML: BSA Regulations

Regulations\U.S. Treasury/FinCEN

- 31 CFR 103.38 — “Nature of Records and Retention Period” Sets forth acceptable forms of records required to be kept and establishes a five-year record-retention requirement.
- 31 CFR 103.41 — “Registration of Money Services Businesses” Requirements for money services businesses to register with the U.S. Treasury/FinCEN.
- **31 CFR 103.57 — “Civil Penalty” Sets forth potential civil penalties for willful or negligent violations of 31 CFR Part 103.**
- **31 CFR 103.59 — “Criminal Penalty” Sets forth potential criminal penalties for willful violations of 31 CFR Part 103.**
- 31 CFR 103.63 — “Structured Transactions” Prohibits the structuring of transactions to avoid the currency reporting requirement.
- 31 CFR 103.100 — “Information Sharing Between Federal Law Enforcement Agencies and Financial Institutions” Establishes procedures and information sharing between federal law enforcement and financial institutions to deter money laundering and terrorist activity.

AML: BSA Regulations

Regulations\U.S. Treasury/FinCEN

- 31 CFR 103.110 — “Voluntary Information Sharing Among Financial Institutions” Establishes procedures for voluntary information sharing among financial institutions to deter money laundering and terrorist activity.
- 31 CFR 103.120 — “Anti-Money Laundering Program Requirements for Financial Institutions Regulated by a Federal Functional Regulator or a Self-Regulatory Organization, and Casinos” Establishes, in part, the standard that a financial institution regulated only by a federal functional regulator satisfies statutory requirements to establish an AML program if the financial institution complies with the regulations of its federal functional regulator governing such programs.
- 31 CFR 103.121 — “Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks” Sets forth the requirement for banks, savings associations, credit unions, and certain non-federally regulated banks to implement a written Customer Identification Program.

AML: BSA Regulations

Regulations\U.S. Treasury/FinCEN

- 31 CFR 103.137 — “Anti-Money Laundering Programs for Insurance Companies” Sets forth the requirement for insurance companies that issue or underwrite “covered products” to develop and implement a written AML program that is reasonably designed to prevent the insurance company from being used to facilitate money laundering or financing of terrorist activities.
- 31 CFR 103.176 — “Due Diligence Programs for Correspondent Accounts for Foreign Financial Institutions” Sets forth the requirement for certain financial institutions to establish and apply a due diligence program that includes appropriate, specific, risk-based, and, where necessary, enhanced policies and procedures that are reasonably designed to enable the institution to detect and report known or suspected money laundering activity involving any correspondent account for a foreign financial institution.
- 31 CFR 103.177 — “Prohibition on Correspondent Accounts for Foreign Shell Banks; Records Concerning Owners of Foreign Banks and Agents for Service of Legal Process” Prohibits a covered financial institution from establishing a correspondent account with a foreign shell bank and requires the financial institution to maintain records identifying the owners of foreign financial institutions.

AML: BSA Regulations

Regulations\U.S. Treasury/FinCEN

- Sets forth the requirement for certain financial institutions to establish and maintain a due diligence program that includes policies, procedures, and controls that are reasonably designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving any private banking account that is established, maintained, administered, or managed in the United States for a non-U.S. person.
- 31 CFR 103.185 — “Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationship” Requires a financial institution to provide foreign financial institution records upon the request of an appropriate law enforcement official and to terminate a correspondent relationship with a foreign financial institution.
- 31 CFR 103, Subpart I, Appendix A — “Certification Regarding Correspondent Accounts for Foreign Banks” Voluntary certification forms to be completed by a foreign bank that maintains a correspondent account with a U.S. bank.
- 31 CFR 103, Subpart I, Appendix B — “Recertification Regarding Correspondent Accounts for Foreign Banks” A voluntary re-certification form to be completed by a foreign bank.

AML: BSA Regulations

Board of Governors of the Federal Reserve System

- Regulation H — 12 CFR 208.62 — “Suspicious Activity Reports” Sets forth the requirements for state member banks for filing a SAR with the appropriate federal law enforcement agencies and the U.S. Treasury.
- Regulation H — 12 CFR 208.63 — “Procedures for Monitoring Bank Secrecy Act Compliance” Sets forth the requirements for state member banks to establish and maintain procedures to ensure and monitor their compliance with the BSA.
- Regulation K — 12 CFR 211.5(k) — “Reports by Edge and Agreement Corporations of Crimes and Suspected Crimes” Sets forth the requirements for an Edge and agreement corporation, or any branch or subsidiary thereof, to file a SAR with the appropriate federal law enforcement agencies and the U.S. Treasury.
- Regulation K — 12 CFR 211.5(m) — “Procedures for Monitoring Bank Secrecy Act Compliance” Sets forth the requirements for an Edge and agreement corporation to establish and maintain procedures reasonably designed to ensure and monitor compliance with the BSA and related regulations.

AML: BSA Regulations

Board of Governors of the Federal Reserve System

- Regulation K — 12 CFR 211.24(f) — “Reports of Crimes and Suspected Crimes” Sets forth the requirements for an uninsured branch, an agency, or a representative office of a foreign financial institution operating in the United States to file a SAR with the appropriate federal law enforcement agencies and the U.S. Treasury.
- Regulation K — 12 CFR 211.24(j) — “Procedures for Monitoring Bank Secrecy Act Compliance” Sets forth the requirements for an uninsured branch, an agency, or a representative office of a foreign financial institution operating in the United States to establish and maintain procedures reasonably designed to ensure and monitor compliance with the BSA and related regulations.
- Regulation Y — 12 CFR 225.4(f) — “Suspicious Activity Report” Sets forth the requirements for a bank holding company or any non-bank subsidiary thereof, or a foreign bank that is subject to the Bank Holding Company Act or any nonbank subsidiary of such a foreign bank operating in the United States to file a SAR with the appropriate federal law enforcement agencies and the U.S. Treasury.

AML: BSA Regulations

Federal Deposit Insurance Corporation

- 12 CFR 326 Subpart B — “Procedures for Monitoring Bank Secrecy Act Compliance” Sets forth requirements for state nonmember banks to establish and maintain procedures to ensure and monitor their compliance with the BSA.
- 12 CFR 353 — “Suspicious Activity Reports” Establishes requirements for state nonmember banks to file a SAR when they detect a known or suspected violation of federal law, a suspicious transaction relating to a money laundering activity, or a violation of the BSA.

AML: BSA Regulations

National Credit Union Administration

- 12 CFR 748 — “Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance” Requires federally insured credit unions to maintain security programs and comply with the BSA.
- 12 CFR 748.1 — “Filing of Reports” Requires federally insured credit unions to file compliance and Suspicious Activity Reports.
- 12 CFR 748.2 — “Procedures for Monitoring Bank Secrecy Act (BSA) Compliance” Ensures that all federally insured credit unions establish and maintain procedures reasonably designed to assure and monitor compliance with the recordkeeping and reporting requirements in the BSA.

AML: BSA Regulations

Office of the Comptroller of the Currency

- 12 CFR 21.11 — “Suspicious Activity Report” Ensures that national banks file a Suspicious Activity Report when they detect a known or suspected violation of federal law or a suspicious transaction relating to a money laundering activity or a violation of the BSA. This section applies to all national banks as well as any federal branches and agencies of foreign financial institutions licensed or chartered by the OCC.
- 12 CFR 21.21 — “Procedures for Monitoring Bank Secrecy Act (BSA) Compliance” Requires all national banks to establish and maintain procedures to ensure and monitor their compliance with the BSA.

AML: BSA Regulations

Office of Thrift Supervision

- 12 CFR 563.177 — “Procedures for Monitoring Bank Secrecy Act (BSA) Compliance” Requires savings associations to implement a program to comply with the recordkeeping and reporting requirements in the BSA.
- 12 CFR 563.180 — “Suspicious Activity Reports and Other Reports and Statements” Sets forth the rules for savings associations or service corporations for filing a SAR with the appropriate federal law enforcement agencies and the U.S. Treasury.