USA AML fines 2008 – 2016: Common and Recurring Themes: The 20-point checklist

The list below is a summary of my analysis of key USA fines and assessments for AML between 2008-2016 (53 reviewed in total) and common recurring themes identified. Some of the key Sanctions fines have been reviewed as well. This list is by no means exhaustive and should not be considered as a source of regulatory requirements. Please scroll down to the end of the post for the list of fines reviewed.

If you enjoy reading this post and find it useful; then there are chances someone else will as well. Please share it with your views to your contacts and spread the knowledge.

If you have read my post on UK AML fines; you will notice that in general the common recurring themes for USA and UK fines are very similar. In this post, I have listed new themes / additional information on themes common with UK fines where available in the USA fines.

USA AML Fines for Depository Institutions, Credit Unions, Broker-dealers, MSBs, Gambling and Precious Metals Business ("Firm"):  

1. Business Strategy, Culture of Compliance and Senior Management Oversight (The most common theme):  

- Wilful Blindness.  
- Obvious contempt for US banking regulations.  
- Misled regulators:  
  - Extensive efforts over the years to evade regulatory oversight (local and USA regulators).  
  - Falsifying business records.  
- Allowed Financial Crime Compliance problems to fester:  
  - Significant AML program deficiencies remained pervasive and systemic.  
  - Management was aware of failure but did not take action.  
  - Remedial measures for the firm’s due diligence policies and procedures were either not implemented or implemented inadequately, even after the adverse findings and formal action by the regulator.  
  - Failed to correct previously identified systemic weaknesses.  
  - Failure to comply with previous regulatory actions and/or agreements (e.g., consent order).  
- Changed country of incorporation numerous times, partly due to the inability to adhere to regulatory requirements.  
- Openly advertised the firm to its potential customer base as willing to facilitate the evasion of AML regulations.  
- Widely recognized by its high risk customers for ease of use.  
- Failed to report misconduct to the regulator in a timely manner.  
- Ignored red flags or high risk indicators.  
- Ignored impact on personal lives - In spite of multiple SAR’s over a considerable period of time, the firm did not do enough to protect the pain and financial suffering of it’s innocent customers.  
- Individual Accountability emphasized in regulatory actions especially where  
  - Individual ignored impact on personal lives.
- Knowingly facilitating transactions on behalf of third-party money launderers acting on behalf of transnational criminal organizations.
- Compliance Officer often ignored the AML program.

2. AML Governance:
   - Resources:
     - Unqualified and/or inadequate staff in compliance.
     - The AML and Compliance officers held other full-time positions within the firm, did not have experience with or training in AML requirements, and spent minimal time dealing with AML matters.
     - The AML officer did not attend meetings with regulators to discuss examination findings, nor was the AML officer provided copies of examination reports detailing AML deficiencies.
     - Management failed to hire knowledgeable and experienced personnel to fill critical roles despite repeat criticisms by the regulator.
   - MI and Reporting: Branches did not relay concern to the head office about complex structures and transactions.

3. References used during examination:
   Fines by local regulators indicating:
   - Failure to comply with the local law.
   - Weak AML controls and customer due diligence.
   - Failure to comply with European regulation no. 1781/2006 on information on the payer accompanying the transfers of funds.

4. Policies and Procedures:
   - Disregarded the most basic AML requirements.
   - Failure to maintain a compliance program reasonably.
   - Failure to have and/or implement procedures for Information Sharing.
   - Deficient due diligence policies and procedures for assessing customer risk.
   - Failure to have group-wide policies and procedures to ensure that
on a risk basis, customer transactions at foreign branch locations can be assessed, aggregated, and monitored.

- foreign branch suspicious activity involving customers of other bank branches are effectively communicated to other affected branch locations and applicable AML operations staff.

- Due diligence procedures lacked the scope and specificity necessary to adequately evaluate risk, thereby disabling its ability to identify potential suspicious activity. Moreover, even those inadequate due diligence procedures were never implemented by the firm.

- **U.S dollar demand drafts:** Policies for U.S dollar demand drafts did not address criteria for opening demand draft relationships with foreign financial institutions, acceptable and unacceptable types of transactions, and criteria for closing demand draft relationships as warranted.

- **Incorrect Policy Requirements:** Relied on an inaccurate and misleading AML policy to train its staff. The AML policy failed to provide instructions, or provided wrong instructions, concerning the AML obligations and filing of AML reports. For example, it encouraged employees to provide notice to customer if they were about to conduct a cash transaction that would put them over the $10,000 threshold for the filing of a Currency Transaction Report, thereby possibly encouraging structured transactions. The policy also lacked instructions on when an employee should file a Suspicious Activity Report (SAR).

5. Risk Assessment Methodology and Enterprise Wide Risk Assessment:

- Failure to have an overall adequate risk assessment.
- Failure to have an enterprise wide risk assessment.
- Failure to assess its risk exposure within the context of products, services, customers, transaction types or geographical reach of the institution.
- Ineffective Risk rating process. Lack of understanding of basic AML requirements resulted in the failure to identify, evaluate and risk rate dozens of higher risk accounts to mitigate potential AML risks.
• Failure to periodically review risk rating process to ensure that all high-risk customers were identified.

6. Due Diligence:
• Customer Information:
  ▪ Customer profiles were missing altogether, or provided too little information to ascertain a customer’s potential risk.
  ▪ Firm could not capture customer identification information such as name or account number.
  ▪ Transactions and reports contained only the business name and included no identifying information on the underlying individuals.

• Review of high-risk accounts was inadequate and often not performed within a reasonable period of time.
• **Trigger Events and Unusual Activity:** There were no procedures in place to validate customer risk profiles, explain significant changes in transaction behavior, or place parameters on variances from expected transaction behavior. Instead of assessing activity that varied from expected activity for identifying suspicious transactions, the firm changed the customer's profile to reflect the actual activity, thereby negating any ability to detect suspicious activity.
• **Reliance:** Blindly relied on a third-party vendor to conduct due diligence for all customers.

7. Transaction Monitoring:
• Inadequate automated transaction monitoring systems to support the volume, scope, and nature of international money transfer transactions conducted.

• Failure to adequately audit its high risk areas and the transactions conducted in those areas.

• Monitoring procedures included occasional review of transactions only greater than $10,000 threshold.
The monitoring system was routinely tuned so that the number of alerts generated by the system with respect to international correspondent banks remained constant at a small number. As a result, the firm instituted arbitrary limits on the flagging and review of transactions for suspicious activity based solely on the inadequate number of staff available to review these alerts.

**Wire transfer monitoring**
- Was manual involving review of hard copies of wire transfer messages.
- Involved review of only single transactions, no consideration was given to review of multiple transactions, involving the same parties over periods of time.

**Pouch activity monitoring**
- Did not address identification of repeat customers, repeat payer’s, or other potentially suspicious trends and patterns.
- Did not aggregate multiple items payable to the same payee or beneficiary subjecting only single transactions exceeding $5000 to monitoring.

**Cash Transactions:**
- Systems did not always aggregate cash activity between accounts belonging to one customer.
- Firm routinely conducted cash transactions utilizing a particular transaction code (originally intended for employee transactions) which would not identify the transact or or affiliated account. With the use of this transaction code, the firm could not capture customer identification information such as name or account number. Therefore, the firm had no way to determine which customer or individual was conducting cash transactions (e.g., purchasing monetary instruments with cash or cashing checks) and no way to track cash transaction activity. Transactions processed using this code would not appear on the firm’s Large Cash Transaction Report (“LCTR”) which was the only report used to file currency transaction reports.
In addition, the firm’s employees were aware that transactions processed using this code would not appear on the LCTR, thus enabling customers and
non-customers to structure cash transactions without any risk of detection. Despite this knowledge, Bank employees continued to use the code for considerable number of years and thereby prevented those transactions from being reported.

8. Suspicious Activity Reporting:

• Violations of the Requirement to Report Suspicious Transactions.
• Failure not only to file a few reports but not at all with no AML program in place.
• Did not adequately identify, research, report, and monitor suspicious activities occurring through the Branch’s funds transfers, pouch activity, demand draft services, and correspondent relationships, and did not adequately audit and independently test such activities.
• Extended period of time over which the violations occurred and/or insufficient reports impaired the usefulness of the suspicious activity reports to law enforcement investigators.
• Failure to monitor accounts for suspicious activity, relative to the types of products and services, volume of business and nature of customers at the bank.
• Failure to file suspicious activity reports on transactions involving illicit proceeds from a corruption scheme especially spanning over number of years.
• Despite evidence of nested accounts, failed to detect and review "nested" accounts for suspicious transactions.
• Request for Information (RFI): AML Operations / AML Investigations frequently had difficulties getting responses to requests for information generated in connection with automated transaction monitoring “alerts.” Because RFIs went unanswered for considerable period of time without SARs being filed, alerts were often closed without any response to the pending request. As a result of these deficiencies, the firm cleared numerous AML “alerts” based on its own perfunctory Internet searches and searches of public source databases but without ever receiving responses to its requests for information.
9. Specific Customer Relationships, Products and Services:

- **Types of Customer, Products and Services highlighted in the fines:**
  Transactions with high-risk jurisdictions, Wire transfers, dollar drafts, demand draft services, correspondent relationships, leasing, pouch activity, Trusts, privately-owned automated teller machines, non-customer services such as cashing "on-us" checks, monetary instruments, merchant credit card processing, Bulk Travelers Cheques, Bearer Share Account, Bulk Cash Movements, Casa de Cambio, “wholesaling” or “bulk check cashing”, Remote Deposit Capture (“RDC”), International cash letter (“ICL”), Suspicious Penny Stock trading, Pump-and-Dump Schemes, Shell Companies, Other complex financial products to siphon off funds.

- **Correspondent Banking:**
  - Maintained correspondent accounts with institutions that posed heightened risks of money laundering and terrorist financing. Despite the risk the firm did not design and implement internal controls tailored to it's high risk business lines.
  - Failure to conduct sufficient due diligence and/or transaction monitoring on its foreign correspondent bank accounts.

- **Affiliate Relationships:**
  - Taking on High Risk Affiliates without adequate controls.
  - Inadequate Information Sharing Among Affiliates.

- **Relationships with MSBs:**
  - Unregistered MSB.
  - Selling Virtual Currencies without registration.
  - Failure by the bank to develop AML policies, procedures and controls related to maintaining accounts of MSBs. E.g., because of a standing practice not to open accounts for check cashing businesses. However, the Bank failed to realize that the definition of an MSB extends beyond check cashers. Even
after identification of two money transmitter accounts by regulators, the firm did not assess risk in this area or review its customer base.

10. Audit (External and Internal):
   - Deficient independent testing.
   - Did not follow regulatory recommendation that a third party evaluate the bank’s BSA program. Misled regulators by indicating this recommendation was given strong consideration at the highest levels of the firm but decided against taking action on it, when in fact, this recommendation was not considered at all.

11. Training:
   - Nonexistent training.
   - Did not have formalized ongoing AML training for all employees. In fact, the training was limited to showing a videotape and circulating memos to certain employees. The training was not job specific or documented.

12. Law Enforcement Inquiries:
    Bank failed to understand the significance of subpoenas received from law enforcement. The receipt of a grand jury subpoena should cause a financial institution to conduct a risk assessment and account review of the subject customer.

13. Record Keeping and Reporting:
   - Violations of the Currency Transaction Reporting Requirements.
   - Failure to maintain accurate books and records.

14. Sanctions:
   - Sanctions violations.
   - Firm used non-transparent payment messages, known as cover payments, to conceal the involvement of sanctioned entities.
• Payment stripping: Removed information identifying sanctioned entities from payment messages, in transactions processed through financial institutions in the United States.

15. Terrorist Financing:
Disregarded Terrorist Links.

16. USA PATRIOT Act:
Failed to comply with Section 314(a) of the USA PATRIOT Act, a program requiring financial institutions to search their records to locate accounts and transactions of persons that may be involved in terrorism or money laundering.

17. Specific Failures by specific types of businesses:
MSBs:
• Failure to register as an MSB.
• Repeatedly wired funds to a high-risk jurisdiction with reckless disregard for AML requirements.
• Failure to file even a single SAR.
• Employees also allowed customers to conduct transactions without verifying and retaining required identification information and also allowed customers to conduct money transfers by using expired identification documents.
• “Wholesaling” or “Bulk check cashing.” Unless mitigated by proper AML controls, these practices present significant risks to the transparency of transactions and can seriously inhibit investigative efforts to follow money trails. Attempted to conceal these transactions by withholding business records such as checks and adding machine tapes. Arrangement continue for considerable number of years.

Gambling:
• “Card Club” gaming establishments with no AML controls.
• Helped high-end gamblers avoid detection of large cash transactions by agreeing not to file either Currency Transaction Reports (CTRs) or Suspicious Activity Reports (SARs).
• Accommodated patrons who desired to conduct financial transactions with large amounts of cash without the casino reporting the transactions.
• Allowed a blind spot to exist in its compliance program – private gaming salons – enabling some of the most lucrative, and riskiest, financial transactions to avoid the scrutiny of the compliance program.

18. Recommended Reading:
You may have read in detail the significant fines reported in the press. In addition, I would also like to recommend reading the case history for the actions below for their unique typologies, techniques and the impact they have had on society.

• 2010- Pamrapo Savings Bank, S.L.A., of Bayonne, N.J.
• 2014 - MoneyGram

19. Extract of Messages from FinCEN Director James H. Freis, Jr:
“Financial institutions choose their customer base and the geographic areas they wish to serve; those choices drive their regulatory compliance obligations,”

“A financial institution that recklessly disregards its obligations under the Bank Secrecy Act and continues to operate without an effective anti-money laundering program, despite repeated warnings and a business focus on areas of recognized high risk, should expect to be penalized. The severity of this joint enforcement action is reflective of just such conduct. This is not a case of interpretation of technical issues or about minor lapses in compliance”.

20. Conclusion:
The outcome of these assessments as we all know in general is one or all of the following - Consent orders, fines, criminal charges, prison sentence, closure of business, removal of license to operate as an individual or business and damage to reputation. The U.S. Regulators are also expanding their reach abroad and to different types of sectors.
The importance of having and implementing an effective AML program is not just about meeting the regulatory obligations. It also very much impacts the personal lives of many innocent people and may cause reputational impact to your organization or industry. The fines and assessments detail many cases where controls were not implemented and impacted personal lives. E.g.,

“With his willful violations, he created an environment where fraud and money laundering thrived and dirty money rampaged through the very system he was charged with protecting. His inaction led to personal savings lost and dreams ruined for thousands of victims.”

“In a case, judges misused their positions as judges to profit from, among other things, sending thousands of juveniles to detention facilities in which they had a financial interest. A Conahan was on FNCB’s board of directors and controlled accounts at the Bank through which he processed the proceeds of his illegal activity.”

In our roles as part of three lines of defense, we may be aware of such control weaknesses (e.g., not enough information about the customer, unusual activity not identified or reported and/ignored), may believe it to be someone else’s problem or may be too busy and so may not take action when appropriate. That inaction might cause reputational damage to our company or impact someone’s life in the future.

Think about it.

References:
https://www.fincen.gov/news_room/ea/
http://www.occ.gov/topics/compliance-bsa/bsa/other-gov-agencies-aml-ctf.html
http://www.justice.gov/

Fines Reviewed:
• 2008 – 2016: All FinCEN fines and GTO's

• Significant fines by other authorities (e.g., US Department of Justice, OCC, NYDFS)
  - 2009 - Lloyds TSB Bank Plc, Credit Suisse
  - 2010 - Wachovia Bank NA.
  - 2012 - Standard Chartered, HSBC, ING Bank N.V.
  - 2013- RBS, Bank of Tokyo Mitsubishi Settlement
  - 2014 - Standard Chartered Bank
  - 2015 - BNP Paribas, Commerzbank AG
  - 2016 - Individual (Sawan Shah aka Sunny) for MSB

For further updates to this post and for my other posts, please follow me on [https://uk.linkedin.com/in/anuratan](https://uk.linkedin.com/in/anuratan)

Written by Anu Ratan, Senior Global AML Policy and Advisory Manager, Independent AML Practitioner

© Anu Ratan posted on LinkedIn in January, 2016. Unauthorized use and/or duplication of this analysis without express and written permission from this site’s author and/or owner is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to Anu Ratan and this site with appropriate and specific direction to the original content.