Trends in Sanctions and AML Enforcement

June 2018
PRESENTED BY
Peter M Piatetsky | Woori Bank
Agenda

1. OFAC Enforcement Actions
   1. Ericsson
   2. Takeaways
2. AML Enforcement Actions
   1. Chardan
   2. Aegis
   3. Nonghyup
   4. Takeaways
3. Individual Responsibility
4. Needs Assessment
5. Examples and Mitigation Strategies
6. Tail Wagging the Dog – Branch and Head Office
7. Heightened Scrutiny of Asian Banks
   1. Why?
8. Korean Banks
9. North Korea
10. Q & A
Recent OFAC Enforcement Actions

- Only one action this year, but a doozy…

- June, 2018: Ericsson

In late 2011, the high temperatures in Sudan caused some of Ericsson’s equipment to malfunction. In response, two now former EAB employees – a radio systems expert and project manager (“EAB Employee #1”), and a senior engagement director within EAB’s business unit responsible for managing the implementation of the Sudanese project (“EAB Employee #2”) – contacted an EUS subject matter specialist and director of business development with EUS’s Hosted Satellite Group (“EUS Employee”) to request assistance. The EUS Employee initially responded in a January 2, 2012 email to EAB Employee #1 and his manager (“EAB Manager”) among other EAB employees: “Please do not address any emails relating to this country [Sudan] to me. It is a serious matter and Ericsson can get fined and I can get fired.”

Notwithstanding the email cited above, the EAB personnel continued to discuss how to repair the damaged equipment with the EUS Employee while no longer referencing Sudan by name. For
Recent OFAC Enforcement Actions

Ericsson

Example, on January 27, 2012, EAB Employee #1 sent an email referencing Sudan by name to the EAB Manager and EUS Employee, to which the EAB Manager responded in Swedish “do not use that word :).” Additionally, on February 22, 2012, the EUS Employee sent an email with “East Africa” in the subject line advising EAB Employee #1 and EAB Employee #2 on how to move forward with the Sudan project given the heat constraints.

On or about February 28, 2012, the EUS Employee met with EAB Employee #2 and the Chief Operating Officer (COO) of Ericsson’s principal subcontractor, BCom, in Barcelona, Spain at a sales conference to specifically discuss the overheating problem in Sudan. The group decided to solve the issue by purchasing an export controlled U.S.-origin satellite hub capable of withstanding the heat.

On March 22, 2012, at the direction of Employee #1, EAB purchased a satellite hub from a U.S.-based company for delivery to BCom’s office in Geneva, Switzerland. On or about March 28, 2012, EAB Employee #1 exchanged emails with Ericsson’s compliance department explaining what the satellite hub was for and why its purchase was necessary. Ericsson’s compliance department informed EAB Employee #1 that the supply of such a satellite hub to Sudan would violate Ericsson’s internal policy regarding sanctions compliance.
Despite the information from Ericsson’s compliance department, the EUS Employee, EAB Employee #1, and BCom’s COO agreed to provide the location of the customer purchasing the satellite hub as “Botswana” if future questions arose. Subsequently, on or about April 2, 2012, EAB Employee #1 structured Ericsson’s purchase of the satellite hub into a multistage transaction between EAB and BCom. The multistage transaction involved transshipping the hub through Switzerland and Lebanon, and ultimately to Sudan. Every stage of the transaction except the last was invoiced. BCom did not issue an invoice to EAB for the final stage of the transaction taking the satellite hub from Lebanon to Sudan. Ericsson has since terminated its relationship with BCom.
Recent OFAC Enforcement Actions

Ericsson

- Total fine - $145,893
  - Mitigated because of self disclosure
  - Penalty could have been $360,230 + a compliance monitor
TAKEAWAYS

- Self disclose
- Self disclose
- Self disclose
TAKEAWAYS

▸ Holland and Hart analysis shows that 73 percent of OFAC’s monetary penalties from 2013 to the present have been assessed against companies that did not file voluntary disclosures.

▸ Filing should not be late. Meaning – after a third party (usually another bank involved in the transaction) has already filed on the problematic transaction.

▸ Credit – Jeremy Paner – Of Counsel – Holland and Hart

▸ https://www.lexology.com/library/detail.aspx?g=18b2cd91-1758-45b7-8e80-74ebeb6ca3fa
Recent AML Enforcement Actions

- Continued trend of individual responsibility
- Focus on cases where institution should have, but did not, file SARs

- Chardan Capital Markets
  - May 2018
  - SEC
  - $1 million penalty for Chardan
  - $15,000 penalty for Chardan CCO, Jerard Basmagy

- Aegis Capital Corporation
  - March 2018
  - SEC
  - $750,000 penalty for Aegis
  - CEO - $40,000
  - CO - $20,000
Recent AML Enforcement Actions
Chardan

From at least October 2013 through June 2014 (the “relevant period”), Chardan, a registered broker-dealer, failed to file Suspicious Activity Reports (“SAR” or “SARs”) when it knew, suspected, or had reason to suspect that certain penny stock transactions it executed on behalf of its customers involved the use of its firm to facilitate fraudulent activity or had no business or apparent lawful purpose. During the relevant period, Chardan’s anti-money laundering (“AML”) policies and procedures stated that Chardan would file SARs “for transactions that may be indicative of money laundering activity,” including, among other things, “heavy trading in low-priced securities” and “trading that constitutes a substantial portion of all trading for the day in a particular security.” The policies listed a number of specific examples or “red flags” of suspicious activities related to heavy trading in low priced securities and large volume trading that should have triggered internal reviews and, in some instances, SAR filings. In particular, the policies required Chardan’s then Chief Compliance Officer (“CCO”) and AML Officer to investigate potential red flags, monitor trading for patterns of suspicious activity, and file SARs.

Despite having policies which set forth red flags of suspicious activities and the requirement to review those red flags, Chardan did not conduct the requisite review of significant penny stock liquidations that occurred through seven customer accounts during the relevant period.
Recent AML Enforcement Actions

Chardan

the firm. Given the suspicious nature of its customers’ transactions, related red flags, and the requirements of its written policies, Chardan should have filed SARs on numerous occasions and did not produce a written analysis or other records supporting the reasonableness of why SARs did not need to be filed.

Chardan’s AML Policies and Procedures

2. As part of its AML program, Chardan adopted written policies and procedures (“Chardan’s Policies”) concerning knowing its customers and monitoring large-volume trading. Chardan purchased template AML policies and procedures from a third-party compliance firm and modified the policies for the firm.

3. Chardan’s Policies required the firm to file SARs for transactions that “may be indicative of money laundering activity.” In that context, Chardan defined suspicious activities, among other things, as including “a wide range of questionable activities; examples include trading
6. Chardan failed to comply with its statutory responsibilities, or to implement its own policies, regarding the high volume sales of penny stocks and other red flags related to the transactions of the seven customers at issue. Chardan monitored its customers’ trading, but did not do so sufficiently to identify suspicious activity. Chardan’s actual practices did not comport with its documented procedures. Specifically, as noted above, the AML Officer was responsible for “reviewing reports and other available information to detect questionable patterns of activity.” However, despite the requirements of its policies, Chardan did not always conduct the required review. As a result, Chardan failed to file SARs as required by Section 17(a) of the Exchange Act and Rule 17a-8 thereunder and did not produce a written analysis of other records supporting the reasonableness of why SARs did not need to be filed.
Recent AML Enforcement Actions

Chardan

In some cases, the large volume penny stock sales transactions through the DVP/RVP accounts, along with other red flags, should have caused Chardan to gather additional information about how its customers acquired their shares and how long the customers had held the stock. Chardan’s then CCO and AML Officer had responsibility for implementing the relevant Chardan Policies, as well as actually filing SARs. Initially, when Chardan’s customers began selling large quantities of penny stocks, insufficient diligence or monitoring was done for these transactions in contravention of Chardan’s Policies. Over time, the process for evaluating transactions in low-priced securities evolved. first, Chardan adopted a policy requiring customers to provide a legal opinion with respect to the legality of the transactions; later, a policy was adopted requiring customers to provide additional documentation related to how they obtained shares. Chardan’s then CCO and AML Officer was responsible for implementing this process. Despite the evolution of Chardan’s Policies related to transactions in low-priced securities, Chardan failed to collect documents sufficient to show how each of its customers obtained their shares for dozens of transactions that should have raised red flags under Chardan’s Policies contemporaneously with customers’ trading. In addition, insufficient monitoring was done for patterns of suspicious activity as required under Chardan’s Policies.
Recent AML Enforcement Actions
Chardan

15. In addition to the transaction documents provided by customers, Chardan’s then CCO and AML Officer reviewed a daily trade blotter containing quantity and price of shares sold by customers. However, despite internal policies that required Chardan’s then CCO and AML Officer to look for patterns of suspicious activity and red flags related to transactions in low-priced securities, Chardan’s then CCO and AML Officer insufficiently looked into suspicious patterns or potential red flags regarding issuers, their principals, or their trading volume. Had he done so sufficiently, he would have identified suspicious activity related to customers’ sales of low-priced securities.

17. In certain instances, when FINRA staff and the Commission’s staff separately requested any files in the possession, custody, or control of Chardan related to certain transactions in low-priced securities as part of their respective regulatory inquiries and the Commission’s investigation in this case, Chardan’s then CCO and AML Officer requested that registered representatives contact customers and obtain those documents. Neither he nor any other Chardan employee had previously done so despite the requirements of Chardan’s Policies described in paragraph 12 above. Chardan’s then CCO and AML Officer then provided the documents to regulatory staff without noting that Chardan obtained those documents only after receiving the request. As a result, the regulatory staff believed that the documents were in Chardan’s files at the time of the transactions when, in fact, Chardan received the documents after the receipt of the regulatory inquiry.
TAKEAWAYS
Charadan

- The person who “owns” the compliance program will increasingly be held responsible, especially at a small institution.
- If you buy template documents, they still bind you.
- If you do not file a SAR on suspicious activity, document why not.
- Follow your own policy and procedures – i.e. if you’re supposed to collect documents, collect the documents.
Recent AML Enforcement Actions

Aegis

From at least late 2012 through early 2014, Aegis, a registered broker-dealer, failed to file Suspicious Activity Reports ("SARs") on hundreds of transactions when it knew, suspected, or had reason to suspect that the transactions involved the use of the broker-dealer to facilitate fraudulent activity or had no business or apparent lawful purpose. Many of the transactions involved red flags of potential market manipulation, including high trading volume in companies with little or no business activity during a time of simultaneous promotional activity. Aegis did not file SARs on these transactions even when it specifically identified AML red flags implicated by these transactions in its written supervisory procedures.

Although Aegis had written supervisory procedures concerning AML compliance, the firm’s internal trade review mechanisms to identify the AML red flags listed in its written supervisory procedures were ineffective. For example, the trading surveillance system used by Aegis was ineffective as it did not analyze low-priced securities transactions in Delivery Versus Payment/Receive Versus Payment accounts ("DVP/RVP").

3. During the relevant period, Aegis had specific written supervisory procedures concerning compliance with its AML responsibilities. Aegis’ written supervisory procedures expressly identified Aegis’ AML CO as the individual responsible for deciding whether Aegis needed to file a SAR. Moreover, Aegis’ written supervisory procedures stated that all Aegis employees were obligated to “promptly report to the [AML CO] any known or
11. Initially, Aegis used the basic version of the trade review system to monitor its transactions, but this system did not analyze DVP/RVP transactions. Subsequently, in July 2013, Aegis upgraded to the enhanced version of the trade review system.

12. Unlike the basic version, the enhanced version allowed users like Aegis to enable the system to analyze DVP/RVP accounts. Despite the receipt of specific alerts of suspicious trading in DVP/RVP accounts described below, however, Aegis did not enable until April 2015 the enhanced version of the trade review system to analyze DVP/RVP accounts.

14. Each year, Aegis required all employees to complete a computerized training module that included training on AML issues, including SAR filing. None of these modules, however, included any discussion of the red flags associated with low-priced securities transactions. Accordingly, Aegis’ employees – including those employees responsible for reviewing trades – never received any training from Aegis that included examples of the red flags associated with low-priced securities transactions that were outlined in the firm’s written supervisory procedures.
Recent AML Enforcement Actions

Aegis

i. Aegis’ Clearing Firm Identified AML Red Flags in Aegis’ Low-Priced Securities Business and Described Them to Aegis in AML Alerts


21. The New Clearing Firm communicated these AML red flags by, among other things, sending AML Alerts directly to senior Aegis personnel, including the then-AML COs. These AML Alerts identified specific suspicious low-priced securities transactions occurring at Aegis.

22. Despite receiving these AML Alerts, Aegis did not file any SARs concerning the identified transactions. Nor did Aegis create any written analyses or compile other records indicating that it considered filing SARs. Moreover, Aegis did not take any steps to determine why its own surveillance systems were failing to detect these suspicious transactions.
TAKEAWAYS
Aegis

- Generic training is not enough. Employees need training specific to risks at hand – especially those mentioned in policies and procedures.
- If your business partner warns you of suspicious activity, especially if it warrants an account closing – file the SAR.
- Properly configure your transaction monitoring system!
Recent AML Enforcement Actions

- NongHyup Bank
  - December 2017
  - DFS
  - $11 million penalty for the bank
  - Consent Order
  - Replacement of key personnel at bank
Recent AML Enforcement Actions
NongHyup

7. The Department conducted three examinations of the New York Branch since the Branch commenced operations in 2013, the results of which are concerning. Ideally, a bank’s examination ratings should improve over time as the institution receives the benefit of the guidance provided by the examiners and works to implement solutions to issues uncovered during the examinations. As described more fully below, the opposite occurred at NongHyup – each successive examination uncovered an increasing number of deficiencies in connection with the New York Branch, including its transaction monitoring processes and procedures.
10. One noted deficiency arose from the Branch’s failure to establish “transaction monitoring” rules necessary to ensure the identification of potentially suspicious activity. Attention to detail in the operation of these monitoring and filtering systems is essential. A transaction monitoring system must be designed to address the specific risks encountered by the institution in conducting its various business lines. Effective transaction monitoring necessitates a system that can be adjusted to changes in risk profiles, and which can be audited routinely. Skilled, adequately-trained staff is also necessary to operate and oversee these systems competently.

11. In addition to deficiencies in its transaction monitoring protocol, the New York Branch failed to review all of the suspicious activity alerts that were identified. Moreover, the review that was undertaken by compliance staff often went unresolved within the time frame mandated by the BSA. Branch compliance staff also failed to maintain records necessary to adequately document the rationales for final decisions made regarding the disposition of suspicious activity alerts.
Recent AML Enforcement Actions

NongHyup

13. The Department’s examination identified a number of other deficiencies. In the critical area of “Know Your Customer” due diligence, for example, which requires banks to collect and review a certain quantity of information concerning bank customers and update this information periodically, the New York Branch failed to conduct the necessary level of due diligence on the NongHyup Head Office account, specifically with regard to the documented purpose of the account and anticipated activity.

14. New York Branch procedures also failed to screen the NongHyup Head Office account against lists of prohibited persons and entities, such as the Specially Designated Nationals (“SDN”) list issued by the U.S. Treasury Department’s Office of Foreign Assets Control (“OFAC”). The SDN list identifies, among other things, known and suspected terrorist actors, financiers and organizations.

15. Nor was there any screening to determine whether members of NongHyup executive management might be a Politically Exposed Person (“PEP”), or had otherwise been cited negatively in publicly available information. A “politically-exposed person” is defined as
Recent AML Enforcement Actions
NongHyup

16. The 2014 Examination also identified a significant deficiency in the structure of the compliance function. The Deputy General Manager and Compliance Officer also served in the additional role of Audit Liaison, which includes facilitating the audit process as well as mediating differences between the New York Branch and the outside auditor retained by the Bank. This created a conflict of interest which could have materially impaired the audit process, as the employee had managerial responsibility over some business lines at the same time he was required to ensure that this area of business operations maintained compliance with laws and regulations and was properly audited.
Recent AML Enforcement Actions
NongHyup

21. The 2015 Examination also determined that the New York Branch’s compliance function lacked sufficient resources to execute its assigned tasks. It also found that existing staff was insufficiently trained. Despite the substantial volume of U.S. dollar clearing conducted by the Branch, it employed only one transaction monitoring analyst, who was promoted to full-time staff only a few months before the 2015 Examination was conducted. Examiners found that this full-time analyst lacked the required understanding of the criteria by which to review and address transaction monitoring alerts. Moreover, Branch staff responsible for compliance in the trade finance line of business also lacked significant or even relevant compliance experience in the applicable BSA/AML field.

22. When the Bank terminated the New York Branch’s Chief Compliance Officer in 2015 due to performance issues, the Bank replaced him with another Compliance Officer who similarly lacked subject-matter expertise necessary to adequately perform the role. The 2015
19. One critical deficiency identified related again to the New York Branch’s transaction monitoring program. A report by the Branch’s outside auditor, issued in April 2014, noted that the Compliance Officer who was in the position at the time, admitted he had manipulated transaction monitoring rule thresholds simply to reduce the total amount of alerts generated by the system. This alteration was not intended to fine tune the system, for example, by limiting false positive alerts or to adjust the system to reflect updated risks. It was carried out solely to reduce the workload of the compliance staff, which did not have sufficient resources.

20. The audit report containing this finding was circulated to management at both the New York Branch and the Head Office. No one in either location took any action regarding the manipulation of the rule thresholds.
TAKEAWAYS

NongHyup

1. Prioritize fixing exam findings immediately
2. Ensure senior management (Head Office for foreign branches) has a response and action plan to findings
3. For AML purposes – U.S. branches must treat their HO like a customer, not as part of the same organization
4. Configure your transaction monitoring systems and don’t allow a backlog
5. Audit and compliance functions must be separate
6. Ensure staffing meets needs – conduct an assessment
Trends – Individual Responsibility

▶ Especially relevant for smaller banks and U.S. branches of foreign banks
▶ Small compliance team
▶ Complicated and high risk business lines
  ▶ Foreign dollar clearing
  ▶ Correspondent banking
  ▶ Trade finance
  ▶ Loans to large foreign corporates with complicated operating and ownership structure
  ▶ Remittances
<table>
<thead>
<tr>
<th>Need</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 AML Risk Assessment</td>
<td>Annual</td>
</tr>
<tr>
<td>2 OFAC Risk Assessment</td>
<td>Annual</td>
</tr>
<tr>
<td>3 Country risk assessment</td>
<td>Annual</td>
</tr>
<tr>
<td>4 Transaction monitoring testing</td>
<td>Annual</td>
</tr>
<tr>
<td>5 Transaction monitoring validation</td>
<td>Annual</td>
</tr>
<tr>
<td>6 Policy and Procedure updates</td>
<td>At least semi-annually</td>
</tr>
<tr>
<td>7 Customer risk assessment</td>
<td>Likely annually</td>
</tr>
<tr>
<td>8 Correspondent bank risk assessment</td>
<td>Annual</td>
</tr>
<tr>
<td>9 Training</td>
<td>Monthly</td>
</tr>
<tr>
<td>10 Monthly reports for senior management</td>
<td>Monthly</td>
</tr>
<tr>
<td>11 Quality Control on alerts</td>
<td>Weekly</td>
</tr>
<tr>
<td>12 OFAC alerts</td>
<td>Daily</td>
</tr>
<tr>
<td>13 SAR alerts</td>
<td>Daily</td>
</tr>
<tr>
<td>14 Customer due diligence &amp; BO</td>
<td>With every new customer or triggering event</td>
</tr>
</tbody>
</table>
Sanctions screening algorithm example

• An existing customer, Fauna Investment LLC, asks a bank to remit a wire to its account with another bank. The outgoing wire, sent as a SWIFT 103, includes the following information for originator party and originator bank:
  • :50A: Fauna Invest. LLC
  • :54A: BOELKPPY
  • :54D: Bank of East LandPyongyang
• The US dollar payment is then routed to the intermediary bank.

“BOELKPPY” is the SWIFT code for a sanctioned bank. The screening system could have interdicted the message based on the code. However, the code was not added to the sanctions list by compliance.

“Bank of East Land” is a sanctioned bank. However, because the name of the bank is compressed with the name of a city, the screening system did not interdict the payment.

Credit: EY
A customer, Gonzalez & Sons Marine Shipping Supplies, is seeking a Letter of Credit from its financial institution to support the shipment of goods from a vendor in China. The Letter of Credit includes the additional parties:

- Shipping vessel: M/S Liberia
- Intermediary shipper address: 123 Aqua Street, Sunrise, Florida

“Cristina Goiricelaya Gonzales” is a designated entity and alerts would be generated on the customer, Gonzalez & Sons. The exact customer name could be added to a “good guy” list that would suppress alerts. The good guy list should itself be subject to routine review.

“M/S Aqua” is a sanctioned vessel and alerts would be generated on the address of the intermediary shipper. A rule could be designed to suppress alerts between addresses and vessels.
Intermediary point vulnerabilities example: movement of funds

Step 1
A customer located in Turkey seeks to send funds to Crimea, a jurisdiction subject to OFAC sanctions. Turkey does not have any sanctions on Crimea and banks are not obligated to follow US sanctions.

Step 2
The payment is sent to the New York branch of a European bank in a MT202 COV message, with no underlying documentation citing Crimea as the ultimate destination of the funds.

Step 3
The funds are next sent to a Russian bank with a branch near the border with Crimea, with the beneficiary listed as a Russian entity that does not appear on the list of OFAC sanctioned entities.

Step 4
The funds are collected by the ultimate beneficial owner in Russia, or forwarded on to a bank in Crimea.

Credit: EY
Step 1  
An entity located in North Korea seeks to export coal internationally, circumventing OFAC sanctions restrictions.

Step 2  
North Korean vessels transport coal shipments to an isolated port in Asia, which acts as the intermediary point for access to the global market.

Step 3  
Ships sailing under a “flag of convenience” retrieve the coal, and transport it on to other ports in Asia. The product is stated to have originated in the intermediary port.

Step 4  
Any bank that facilitated payments for this transaction have violated OFAC sanctions. Even if acting unwittingly, under the ‘strict liability’ provision any actor can be held accountable for their involvement in such activity.

Credit: EY
## Trade finance red flags

<table>
<thead>
<tr>
<th>#</th>
<th>Red Flags</th>
<th>#</th>
<th>Red Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Customers conducting business in higher-risk jurisdictions</td>
<td>10</td>
<td>The commodity is shipped to, through or from a jurisdiction designated (e.g. by the FATF or United Nations) as higher-risk for financial crime activities</td>
</tr>
<tr>
<td>2</td>
<td>Obvious misrepresentation of quantity or type of goods imported or exported</td>
<td>11</td>
<td>Export of goods without any corresponding purchase of raw materials or finished goods</td>
</tr>
<tr>
<td>3</td>
<td>Shipment locations or description of goods not consistent with letter of credit</td>
<td>12</td>
<td>Sudden increase in volume of exports by a new exporter</td>
</tr>
<tr>
<td>4</td>
<td>Customers involved in potentially higher-risk activities, including activities that may be subject to export/import restrictions (e.g., equipment for military or police organizations of foreign governments, weapons, or certain natural resources such as metals, ore, and crude oil etc.)</td>
<td>13</td>
<td>Advance inward remittance against exports without justifiable reasons</td>
</tr>
<tr>
<td>5</td>
<td>Mis-declaration of value (e.g. over-valuation) of goods</td>
<td>14</td>
<td>Export documents which are not duly authenticated by export regulating agency were accepted by the bank</td>
</tr>
<tr>
<td>6</td>
<td>Payment or payment requests of proceeds to a third-party unrelated to customer</td>
<td>15</td>
<td>Unusual deposits i.e., use of cash or negotiable instruments in round denominations to fund bank accounts and to pay for goods and services</td>
</tr>
<tr>
<td>7</td>
<td>Unnecessarily complex transaction structure possibly designed to obscure the true nature of the transaction</td>
<td>16</td>
<td>Inward remittances in multiple accounts and payments made from multiple accounts</td>
</tr>
<tr>
<td>8</td>
<td>Items shipped that are inconsistent with the nature of the customer’s business</td>
<td>17</td>
<td>Transfer pricing</td>
</tr>
<tr>
<td>9</td>
<td>Transaction involves the use of repeatedly amended or frequently extended L/Cs or changes to the beneficiary or location of payment without legitimate commercial reasons</td>
<td>18</td>
<td>Presence of Free Trade Zones/Special Economic Zones</td>
</tr>
<tr>
<td></td>
<td></td>
<td>19</td>
<td>Circuitous route of shipment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>20</td>
<td>Circuitous route of financial transaction</td>
</tr>
<tr>
<td></td>
<td></td>
<td>21</td>
<td>Significant discrepancies between description, quality and quantity of the goods on the documents and the actual goods shipped</td>
</tr>
<tr>
<td></td>
<td></td>
<td>22</td>
<td>Transaction does not make economic sense</td>
</tr>
</tbody>
</table>

Credit: EY
## Trade Finance data search tools and approaches

Compliance investigations into trade finance activity requires research into a combination of open source databases and internal documentation, especially as related to pricing, shipping patterns, and involvement of business lines. The information below demonstrates the tools that can be used by financial institutions to review potential red flags.

<table>
<thead>
<tr>
<th>Trade Finance Red Flags</th>
<th>Tools and information sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obvious misrepresentation of quantity or type of goods imported or exported</td>
<td>· Open source searches (i.e., Google) for size of shipped goods</td>
</tr>
<tr>
<td></td>
<td>· CIA World FactBook for information on origin country of goods</td>
</tr>
<tr>
<td></td>
<td>· WTO data on shipping trends, price, and origin country</td>
</tr>
<tr>
<td>Mis-declaration of value (e.g. over-valuation) of goods</td>
<td>· Open source searches for current and historical pricing data</td>
</tr>
<tr>
<td></td>
<td>· Subscription services on pricing data, including Platts, to understand if listed values of goods are near market values</td>
</tr>
<tr>
<td>Items shipped that are inconsistent with the nature of the customer’s business</td>
<td>· Open source search for company websites, including historical archive webpages (i.e., Archive Way Back Machine)</td>
</tr>
<tr>
<td></td>
<td>· Dun &amp; Bradstreet for listings of business activity</td>
</tr>
<tr>
<td></td>
<td>· NAICs codes</td>
</tr>
<tr>
<td></td>
<td>· Bloomberg</td>
</tr>
<tr>
<td>Circuitous route of shipment</td>
<td>· Lloyd’s List Intelligence services on shipping trends and details</td>
</tr>
<tr>
<td></td>
<td>· Publicly available marine traffic tracking tools (i.e., Marine Traffic or Vessel Tracker)</td>
</tr>
<tr>
<td>Presence of Free Trade Zones/Special Economic Zones</td>
<td>· Open source information on companies established within Free Trade Zones, commodity-focus</td>
</tr>
<tr>
<td></td>
<td>· Open source information on historical shipments</td>
</tr>
</tbody>
</table>

Credit: EY
Strategies for risk mitigation

Collection of Data
• Understand what intermediary points may pose a risk for your institution and evaluate the scope of exposure
• Ensure that when reviewing SWIFT messages, you are receiving all information associated with the transaction from head office or other affiliated institutions. E.g. information in a 202 message is included in a 202COV.

Tiered Screening
• Where sanctioned countries or jurisdictions are not mentioned in payment details, detection is difficult
• The combination of specific paired keywords can aid in generating alerts with a nexus to intermediary points that may be high risk. Previous block and rejection reports as well as voluntary self disclosures that involved an intermediary point can guide the selection of these keywords.

Use all Available Information
• Open source information can be found by analysts reviewing sanctions alerts and leveraged to gain greater insight into transactions with a possible sanctions nexus
• Dunn and Bradstreet, Lexis Nexis, and Bloomberg can all provide additional information on companies
• Marine tracking sites can help trace the source and destination of goods, including through intermediary ports

Regularly Test Screening Systems
• Ongoing testing and calibration of sanctions screening systems remains the best defense against sanctions violations
• Making an effort to ensure that screening systems accurately capture and screen against all available information that may include a sanctions nexus, significantly improves the likelihood of intercepting the transaction or identifying a customer with whom there is a sanctions concern

Credit: EY
Tail Wagging the Dog

► U.S. compliance requirements are the strictest globally

► U.S. branches and agencies of foreign banks have to be better at compliance than their own Head Office

► Must ensure key items:
  ► 1. HO must understand importance of U.S. compliance
  ► 2. HO must screen relevant lists, especially OFAC list
  ► 3. HO must send all relevant information
Heightened Scrutiny of Asian Banks – select cases

“The regulatory gaze and enforcement attention is facing east [and Asian banks] haven’t been leading the pack in terms of financial risk management” – Juan Zarate, former senior White House and Treasury official

- MUFG - 2015
- Habib Bank – 2017
- NongHyup – 2017
- Hua Nan – 2018
- ZTE – 2018
FINES FOR BANKS THAT BREACHED U.S. OFAC SANCTIONS

2010
- RBS (ABN Amro) $500 million
- Barclays $298 million
- Compass Bank $607,000
- Wells Fargo $67,500

2011
- JP Morgan $88.3 million
- Commerzbank AG $175,500
- Societe Generale $111,359

2012
- HSBC $1.9 billion
- Standard Chartered $667 million
- Bank of Tokyo-Mitsubishi $8.6 million
- National Bank of Abu Dhabi $855,000

2013
- RBS $100 million
- Intesa Sanpaolo $3 million
- Bank of Guam $27,000
- Deutsche Bank $18,900

2014
- BNP Paribas $8.9 billion
- Clearstream Banking $152 million
- Bank of America $16.6 million
- Bank of Tokyo-Mitsubishi UFJ $315 million

2015
- Commerzbank AG $1.45 billion
- Crédit Agricole $329 million
- Banco do Brasil, S.A. $139,500
- National Bank of Pakistan $28,800

2016
- Barclays Bank PLC $2.48 million
- United Arab Emirates

2017
- Toronto-Dominion Bank PLC $516,105
- Netherlands

KEY:
- Bank Location
- Sanctioned Countries/Entities: Burma, Cuba, Iran, Libya, Sudan, Zimbabwe
- Global Terrorism Sanctions
- Narcotics Trafficking
- Bank Fine $US

© 2018 Thomson Reuters. The information contained in this document is for general information purposes only and is not intended to be used as professional or legal advice. Thomson Reuters makes no representation or warranties in this document and accepts no liability for any loss or damage caused as a result of any use of this information.
New York DFS Consent Orders

- May 1, 2018  Consent Order to The Goldman Sachs Group, Inc.
- January 4, 2018  Consent Order to Western Union Financial Services, Inc.
- December 21, 2017  Consent Order to NongHyup Bank, and NongHyup Bank, New York Branch
- November 13, 2017  Consent Order to Credit Suisse AG and Credit Suisse AG, New York Branch
- August 24, 2017  Surrender Order to Habib Bank and Habib Bank, New York Branch
- April 21, 2017  Consent Order to Standard Chartered Bank
- January 30, 2017  Consent Order to Deutsche Bank AG and Deutsche Bank AG New York Branch
- December 15, 2016  Consent Order to Intesa Sanpaolo S.p.A.
- November 4, 2016  Consent Order to Agricultural Bank of China Limited
- August 19, 2016  Consent Order to Mega International Commercial Bank of Taiwan (PDF)
Most Active Regulators

Global AML / Sanctions Fines 2008 - 2018

Data from Fenergo and U.S. Treasury
Korean Banks

- 6 out of 7 major Korean banks operating in the U.S. are under a consent order or investigation
  - (source: regulatory press releases and news)

- Heightened scrutiny due to high risk business
  - Iran ties
  - Crypto currency

- Similar risk profiles
  - Regulators often have one person look at a group of banks by region.
North Korea Sanctions Update
THANK YOU QUESTIONS?

In addition to the ACAMS Chapter Webpage you can also find us on LinkedIn at http://www.linkedin.com/groups?gid=2202988&trk=myg_ugrp_ovr

Follow us on Twitter @ACAMSOCAL

Feel free to send any suggestions or comments to: socalacams@yahoo.com.