MITIGATING THE SANCTIONS RISK IN AML COMPLIANCE

NICK TURNER
FINTELEKT – 9TH ANNUAL SUMMIT (INDIA) 2019
7 NOVEMBER 2019
# Overview of Recent Trends

<table>
<thead>
<tr>
<th>Turkey / Syria / Iran</th>
<th>China / Iran</th>
<th>China / Hong Kong</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Executive Order 13894 of 14 October 2019 adopted in response to Turkish military offensive in Syria.</td>
<td>• Secondary sanctions against Chinese oil importer under Executive Order 13846 announced in July 2019.</td>
<td>• US Senate is considering the Hong Kong Human Rights and Democracy Act of 2019 after approval in House of Representatives, including human rights sanctions.</td>
</tr>
<tr>
<td>• Three ministers and two Turkish government ministries named as SDNs.</td>
<td>• On 25 September 2019, OFAC sanctioned two subsidiaries of COSCO and their executives for Iran-petroleum transactions.</td>
<td>• Use of the US Commerce Department’s “Entity List” has expanded to cover US-China trade concerns and human rights.</td>
</tr>
<tr>
<td>• The same week, OFAC announced the indictment of state-owned Halkbank for Iran violations.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*The SDNs were unsanctioned after nine days after the adoption of a ceasefire.*
OVERVIEW OF RECENT TRENDS (CONTINUED)

<table>
<thead>
<tr>
<th>Iran / Hizballah</th>
<th>Venezuela / Cuba</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Executive Order 13886 amends terrorism sanctions, authorizes correspondent account sanctions against foreign financial institutions.</td>
<td>• Executive Order 13884 blocking property of the Government of Venezuela—<em>not</em> an embargo.</td>
<td>• Publication of the “Framework for OFAC Compliance Commitments” guidance and emphasis on building effective sanctions compliance programs</td>
</tr>
<tr>
<td>• OFAC has named numerous persons as SDNs for activities supporting Hizballah and Iranian financing of terrorist groups in the Middle East.</td>
<td>• “Material assistance” sanctions for Venezuela-Cuba trading and Venezuelan SOEs.</td>
<td>• Increasing use of administrative subpoenas and continued investigations of North Korea front companies</td>
</tr>
<tr>
<td>• In August 2019, OFAC designated Lebanon’s Jammal Trust Bank as an SDN, putting the bank out of business.</td>
<td>• October 2019, additional tightening of Cuba embargo and revocation of Commerce Department licenses.</td>
<td></td>
</tr>
</tbody>
</table>
OVERVIEW OF SANCTIONS RISKS
WHO MUST FOLLOW OFAC SANCTIONS?

<table>
<thead>
<tr>
<th>US Persons</th>
<th>Non-US Persons</th>
</tr>
</thead>
</table>

**“US persons” must always comply with OFAC regulations**

**US Persons include:**
- US citizens/permanent residents – regardless of their physical location
- All persons who are physically located in the United States – regardless of their citizenship
- Corporations, partnerships, and other entities domiciled in the US, including branches and offices of non-US banks
- Overseas branches of US banks
- In the case Cuba and Iran sanctions, US persons also include the US-owned or controlled companies overseas.

**Non-US persons** must also follow OFAC rules under some circumstances

OFAC (and other US authorities) can assert jurisdiction over transactions involving a “US Element” which can include:
- US Persons
- The US financial system
- US-origin goods and technology
## WHAT IS THE US FINANCIAL SYSTEM?

<table>
<thead>
<tr>
<th>Element</th>
<th>Source</th>
</tr>
</thead>
</table>
| **US financial institutions**  
• US financial institutions | **Definition:** US financial institution (e.g., 31 CFR 560.327):  
“The term US financial institution means any US entity (including its foreign branches that is engaged in the business of accepting deposits, making, granting, transferring, holding, or brokering loans or credits, or purchasing or selling foreign exchange, securities, commodity futures or options, or procuring purchasers and sellers thereof, as principal or agent . . . The term includes those branches, offices, and agencies of foreign financial institutions that are located in the United states, but not such institutions' foreign branches, offices, or agencies.” |
| **Foreign branches of US financial institutions**  
• Foreign branches of US financial institutions |  |
| **US-based branches of non-US banks**  
• US-based branches of non-US banks |  |
| **US-based correspondent accounts**  
• US-based correspondent accounts |  |
| **Foreign subsidiaries of US financial institutions (Cuba and Iran)**  
• Foreign subsidiaries of US financial institutions (Cuba and Iran) | **Cuba:** 31 CFR 515.329 – **Definition:** Person subject to the jurisdiction of the United States; person subject to US jurisdiction  
“(d) Any corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by persons specified in paragraphs (a) or (c) of this section” (i.e., US persons).  
**Iran:** 31 CFR 560.215 – **Prohibitions on foreign entities owned or controlled by US persons**  
“(a) Except as otherwise authorized pursuant to this part, an entity that is owned or controlled by a United states person and established or maintained outside the United States is prohibited from knowingly engaging in any transaction, directly or indirectly, with the Government of Iran or any person subject to the jurisdiction of the Government of Iran that would be prohibited pursuant to this part if engaged in by a United States person or in the United States.” |
A Chinese manufacturer agrees to supply equipment to a buyer in Iran. The Iranian buyer arranges to have payment made in USD to the Chinese supplier via a third party distributor in Singapore. The Singapore company makes payment through its Singaporean bank. The payment clears through a US-based correspondent account before being credited to a bank account in Hong Kong.
There are currently five territories that are subject to comprehensive OFAC sanctions (embargoes):

- Crimea
- Cuba
- Iran
- North Korea
- Syria

US persons and companies – and sometimes their non-US subsidiaries – cannot do business with these countries in most cases, unless licensed by OFAC.
OFAC LIST-BASED SANCTIONS

Most OFAC programs are “List-Based Programs.” This means that only the individuals and companies on the list are subject to OFAC sanctions.

US persons and companies are restricted from doing business with individuals and entities on these lists, unless permitted by OFAC. US persons – including banks – must block (freeze) property and funds belonging to persons on the List of Specially Designated Nationals and Blocked Persons (SDN List).

- Balkans region
- Belarus
- Burundi
- Central African Republic
- Cuba
- **Cyber-related**
- Democratic Republic of Congo
- **Foreign US Election Interference**

- **Global Terrorists**
  - Iraq
  - Iran
  - Lebanon
  - Libya
- **Global Magnitsky**
- **Narcotics Traffickers**
- **Non-Proliferation**

- North Korea
- Somalia
- South Sudan
- Syria
- **Transnational Criminal Organizations**
- Ukraine/Russia
- Venezuela
- Yemen
- Zimbabwe

(Underlined lists are not country specific.)
OFAC sanctions apply to sanctioned persons (e.g. SDNs and SSI entities) as well as any entity that is owned 50% or more by one or more sanctioned persons.

Other Examples:
- Blocked Person X owns 50 percent of Entity A, and Entity A owns 50 percent of Entity B. Entity B is considered to be blocked.
- Blocked Person X owns 50 percent of Entity A and 50 percent of Entity B. Entities A and B each own 25 percent of Entity C. Entity C is considered to be blocked.
- Blocked Person X owns 50 percent of Entity A and 10 percent of Entity B. Entity A also owns 40 percent of Entity B. Entity B is considered to be blocked.
- Blocked Person X owns 50 percent of Entity A and 25 percent of Entity B. Entities A and B each own 25 percent of Entity C. Entity C is not considered to be blocked.
- Blocked Person X owns 25 percent of Entity A and 25 percent of Entity B. Entities A and B each own 50 percent of Entity C. Entity C is not considered to be blocked.
WHAT ARE SECONDARY SANCTIONS?

Secondary sanctions are used by the US Government to discourage non-US companies and individuals from engaging in activities that are contrary to US foreign policy or national security objectives.

- Apply to specified activities and “significant transactions”
- Include restrictions on correspondent accounts for Foreign Financial Institutions
- Principally used in relation to Iran, North Korea, Russia, Syria
- “Secondary Sanctions” do not require the involvement of a US Element.

For example, a foreign financial institution that engages in significant transactions with sanctioned Iranian banks could be placed on the Correspondent Account or Payable-Through Account Sanctions List (CAPTA List) (e.g. Bank of Kunlun).
EXTRATERRITORIALITY
NON-US BANKS AND US LAW ENFORCEMENT JURISDICTION

US law enforcement agencies are actively pursuing a number of investigations in Asia related to North Korean front companies. On 6 August 2019, the US Court of Appeals for the District of Columbia unsealed an opinion upholding a lower court’s decision to hold three Chinese banks in contempt for refusing to respond to subpoenas seeking information about North Korean front company operating in Hong Kong.

- The US courts held that the Chinese banks were required to respond to US law enforcement subpoenas even though the US Department of Justice (DOJ) did not utilize the US-China Mutual Legal Assistance mechanism.
- The courts found that two of the banks had submitted to US law enforcement jurisdiction when opening branches in the United States.
- The third bank was subject to US jurisdiction for the purposes of Section 319(b) of the USA PATRIOT Act, which authorizes the DOJ and Treasury Department to subpoena overseas records from any bank with a US-based correspondent account.
- US law enforcement agencies can seek records from banks with branches or correspondent accounts in the United States even if those records are held outside the United States if those records are related to activity in the US accounts.
LEVERAGING AML/CFT FOR SANCTIONS COMPLIANCE
Sanctions authorities, especially the US Office of Foreign Assets Control (OFAC), expect both financial institutions and companies to adopt risk-based programs based on international AML standards to detect and interdict sanctioned activity. The adoption of such a program can help mitigate enforcement penalties in the case of violations.

OFAC regulations do not require a formal [Sanctions Compliance Program (“SCP”)]; however, OFAC encourages organizations subject to U.S. jurisdiction (including but not limited to those entities that conduct business in, with, or through the United States or involving U.S.-origin goods, services, or technology), and particularly those that engage in international trade or transactions or possess any clients or counter-parties located outside of the United States, to adopt a formal SCP.

Financial institutions and companies are strongly encouraged to employ risk mitigation measures consistent with Financial Action Task Force standards designed to combat money laundering, and terrorist and proliferation financing. This includes the adoption of appropriate due diligence policies and procedures by financial institutions and non-financial gatekeepers and promoting beneficial ownership transparency for legal entities . . .
# SANCTIONS AND AML: SIDE BY SIDE

<table>
<thead>
<tr>
<th>Element</th>
<th>AML</th>
<th>Sanctions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rules</strong></td>
<td>• Financial Action Task Force (FATF)</td>
<td>• United Nations</td>
</tr>
<tr>
<td></td>
<td>• National AML regulators</td>
<td>• National governments</td>
</tr>
<tr>
<td></td>
<td>• Tendency toward consistency</td>
<td>• US-focused</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Tendency away from consistency</td>
</tr>
<tr>
<td><strong>Extraterritoriality</strong></td>
<td>• Regulators are jurisdiction-focused</td>
<td>• Regulators may assert universal jurisdiction</td>
</tr>
<tr>
<td></td>
<td>• Global standards, local compliance</td>
<td>• Global standards, global compliance</td>
</tr>
<tr>
<td><strong>Expectations</strong></td>
<td>• Risk rating of customers</td>
<td>• Prohibitions against dealing in property or services</td>
</tr>
<tr>
<td></td>
<td>• Identification of suspicious activity</td>
<td>• Regulatory reporting obligations</td>
</tr>
<tr>
<td></td>
<td>• Regulatory reporting obligation</td>
<td></td>
</tr>
<tr>
<td><strong>Methods</strong></td>
<td>• Risk assessments</td>
<td>• Risk assessments</td>
</tr>
<tr>
<td></td>
<td>• Policies/Procedures/Training</td>
<td>• Policies/Procedures/Training</td>
</tr>
<tr>
<td></td>
<td>• KYC/CDD/EDD</td>
<td>• KYC/CDD/EDD</td>
</tr>
<tr>
<td></td>
<td>• Transaction monitoring (post)</td>
<td>• Transaction screening (pre)</td>
</tr>
<tr>
<td></td>
<td>• Case investigations</td>
<td>• Blocking/rejecting</td>
</tr>
<tr>
<td></td>
<td>• STR filings</td>
<td>• Case Investigations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• STR or VSD fillings</td>
</tr>
<tr>
<td><strong>Standards</strong></td>
<td>• Risk-based approach</td>
<td>• Strict civil liability</td>
</tr>
<tr>
<td></td>
<td>• Criminal charges possible</td>
<td>• Criminal charges possible</td>
</tr>
<tr>
<td><strong>Systems</strong></td>
<td>• Name screening tools</td>
<td>• Name screening tools</td>
</tr>
<tr>
<td></td>
<td>• CDD system</td>
<td>• CDD system</td>
</tr>
<tr>
<td></td>
<td>• Transaction monitoring software</td>
<td>• Transaction screening software</td>
</tr>
<tr>
<td></td>
<td>• Workflow tools/Case management system</td>
<td>• Workflow tools/case management tool</td>
</tr>
<tr>
<td></td>
<td>• Management reporting</td>
<td>• Management reporting</td>
</tr>
<tr>
<td><strong>Personnel</strong></td>
<td>• Operational experience helpful</td>
<td>• Operational experience helpful</td>
</tr>
<tr>
<td></td>
<td>• Investigative/law agency experience helpful</td>
<td>• Legal/regulatory experience helpful</td>
</tr>
</tbody>
</table>
On 2 May 2019, OFAC the “Framework for OFAC Compliance Commitments” outlining the features of a sanctions compliance program that will be considered as part of the OFAC Enforcement Guidelines for both US and non-US companies. The five key elements include:

- Senior Management Commitment
- Sanctions Risk Assessment
- Internal Controls
- Testing and Auditing
- Training

The Framework is available at:

# OFAC COMPLIANCE FRAMEWORK

## HOW STRONG IS YOUR PROGRAM?

<table>
<thead>
<tr>
<th>Senior Management Commitment</th>
<th>Sanctions Risk Assessment</th>
<th>Internal Controls</th>
<th>Testing and Auditing</th>
<th>Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Senior management has reviewed and approved the Sanctions Compliance Program</td>
<td>1. The company conducts an OFAC risk assessment that adequately addresses potential risks and is updated as appropriate</td>
<td>1. Policies and procedures are written, easy to follow and designed to prevent misconduct</td>
<td>1. The testing and auditing function is accountable to senior management and has sufficient independence, authority, and resources</td>
<td>1. Training provides adequate information and is tailored to high-risk areas</td>
</tr>
<tr>
<td>2. Compliance units have sufficient authority and autonomy with direct reporting to senior management</td>
<td>2. The risk assessment is conducted according to a methodology and takes into account root causes of violations or weaknesses</td>
<td>2. Controls are based on the risk assessment and utilize appropriate technology</td>
<td>2. Testing and auditing procedures are appropriate for the company and take into account the risk assessment and internal controls</td>
<td>2. The scope of training is appropriate for the company’s services, customers, geographies, and other factors</td>
</tr>
<tr>
<td>3. Compliance units are given adequate resources, including people and technology</td>
<td>3. Controls are audited and tested</td>
<td>3. Controls are audited and tested</td>
<td>3. When weaknesses are discovered, the company takes immediate action to remediate them</td>
<td>3. The frequency of training is appropriate for the company’s risk profile</td>
</tr>
<tr>
<td>4. Senior management promotes a “culture of compliance”</td>
<td>4. Recordkeeping policies are appropriate</td>
<td>4. Recordkeeping policies are appropriate</td>
<td>4. Training is updated when weaknesses in internal controls are discovered</td>
<td>4. Training is updated when weaknesses in internal controls are discovered</td>
</tr>
<tr>
<td>5. Senior management demonstrates recognition of seriousness of potential violations</td>
<td>5. Controls are improved upon identification of weaknesses</td>
<td>5. Controls are improved upon identification of weaknesses</td>
<td>5. Training materials are easily accessible to all relevant staff</td>
<td>5. Training materials are easily accessible to all relevant staff</td>
</tr>
<tr>
<td></td>
<td>6. The program is communicated</td>
<td>6. The program is communicated</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. Personnel are appointed to implement the controls</td>
<td>7. Personnel are appointed to implement the controls</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Senior Management Commitment

1. Senior management has reviewed and approved the Sanctions Compliance Program
2. Compliance units have sufficient authority and autonomy with direct reporting to senior management
3. Compliance units are given adequate resources, including people and technology
4. **Senior management promotes a “culture of compliance”**
5. Senior management demonstrates recognition of seriousness of potential violations

Sanctions Risk Assessment

1. **The company conducts an OFAC risk assessment that adequately addresses potential risks and is updated as appropriate**
2. The risk assessment is conducted according to a methodology and takes into account root causes of violations or weaknesses
## OFAC COMPLIANCE FRAMEWORK (CONTINUED)

### HOW STRONG IS YOUR PROGRAM?

<table>
<thead>
<tr>
<th>Internal Controls</th>
<th>Testing and Auditing</th>
<th>Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Policies and procedures are written, easy to follow and designed to prevent misconduct</strong></td>
<td>1. The testing and auditing function is accountable to senior management and has sufficient independence, authority, and resources</td>
<td>1. Training provides adequate information and is tailored to high-risk areas</td>
</tr>
<tr>
<td>2. Controls are based on the risk assessment and utilize appropriate technology</td>
<td>2. Testing and auditing procedures are appropriate for the company and take into account the risk assessment and internal controls</td>
<td>2. The scope of training is appropriate for the company’s services, customers, geographies, and other factors</td>
</tr>
<tr>
<td>3. Controls are audited and tested</td>
<td>3. <strong>When weaknesses are discovered, the company takes immediate action to remediate them</strong></td>
<td>3. <strong>The frequency of training is appropriate for the company’s risk profile</strong></td>
</tr>
<tr>
<td>4. Recordkeeping policies are appropriate</td>
<td></td>
<td>4. Training is updated when weaknesses in internal controls are discovered</td>
</tr>
<tr>
<td>5. <strong>Controls are improved upon identification of weaknesses</strong></td>
<td></td>
<td>5. <strong>Training materials are easily accessible to all relevant staff</strong></td>
</tr>
<tr>
<td>6. The program is communicated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Personnel are appointed to implement the controls</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**19**

**OFAC COMPLIANCE FRAMEWORK (CONTINUED)**

**HOW STRONG IS YOUR PROGRAM?**

<table>
<thead>
<tr>
<th>Internal Controls</th>
<th>Testing and Auditing</th>
<th>Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Policies and procedures are written, easy to follow and designed to prevent misconduct</strong></td>
<td>1. The testing and auditing function is accountable to senior management and has sufficient independence, authority, and resources</td>
<td>1. Training provides adequate information and is tailored to high-risk areas</td>
</tr>
<tr>
<td>2. Controls are based on the risk assessment and utilize appropriate technology</td>
<td>2. Testing and auditing procedures are appropriate for the company and take into account the risk assessment and internal controls</td>
<td>2. The scope of training is appropriate for the company’s services, customers, geographies, and other factors</td>
</tr>
<tr>
<td>3. Controls are audited and tested</td>
<td>3. <strong>When weaknesses are discovered, the company takes immediate action to remediate them</strong></td>
<td>3. <strong>The frequency of training is appropriate for the company’s risk profile</strong></td>
</tr>
<tr>
<td>4. Recordkeeping policies are appropriate</td>
<td></td>
<td>4. Training is updated when weaknesses in internal controls are discovered</td>
</tr>
<tr>
<td>5. <strong>Controls are improved upon identification of weaknesses</strong></td>
<td></td>
<td>5. <strong>Training materials are easily accessible to all relevant staff</strong></td>
</tr>
<tr>
<td>6. The program is communicated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Personnel are appointed to implement the controls</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**OFAC COMPLIANCE FRAMEWORK (CONTINUED)**

**HOW STRONG IS YOUR PROGRAM?**

<table>
<thead>
<tr>
<th>Internal Controls</th>
<th>Testing and Auditing</th>
<th>Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Policies and procedures are written, easy to follow and designed to prevent misconduct</strong></td>
<td>1. The testing and auditing function is accountable to senior management and has sufficient independence, authority, and resources</td>
<td>1. Training provides adequate information and is tailored to high-risk areas</td>
</tr>
<tr>
<td>2. Controls are based on the risk assessment and utilize appropriate technology</td>
<td>2. Testing and auditing procedures are appropriate for the company and take into account the risk assessment and internal controls</td>
<td>2. The scope of training is appropriate for the company’s services, customers, geographies, and other factors</td>
</tr>
<tr>
<td>3. Controls are audited and tested</td>
<td>3. <strong>When weaknesses are discovered, the company takes immediate action to remediate them</strong></td>
<td>3. <strong>The frequency of training is appropriate for the company’s risk profile</strong></td>
</tr>
<tr>
<td>4. Recordkeeping policies are appropriate</td>
<td></td>
<td>4. Training is updated when weaknesses in internal controls are discovered</td>
</tr>
<tr>
<td>5. <strong>Controls are improved upon identification of weaknesses</strong></td>
<td></td>
<td>5. <strong>Training materials are easily accessible to all relevant staff</strong></td>
</tr>
<tr>
<td>6. The program is communicated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Personnel are appointed to implement the controls</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A “RISK-BASED APPROACH”

OFAC encourages a “risk-based” approach to sanctions compliance takes into account the unique risks associated with (1) customers, (2) products and services, (3) geographies, and (4) supply chains and counterparties.

For example, a company that buys petroleum products from importers who have exposure to Iran and pays for those goods in USD has more risk than a company that buys toys from a domestic factory and pays for them in RMB.

A company should focus its compliance resources on areas of elevated risk.
SANCTIONS DUE DILIGENCE

AML due diligence is focused on identifying specific pieces of information (nature of business, source of funds, etc.) for risk rating. Sanctions due diligence, on the other hand, is open ended and is aimed at assessing the likelihood that the counterparty has or will engage in activities with sanctioned persons or places and whether that activity presents a risk of violations through lack of compliance.

Examples of due diligence findings that could signify potential sanctions risks include:

- Headquarters, offices, or affiliates in sanctioned territories
- Sales or investment to sanctioned territories or to sanctioned persons
- Beneficial owners, directors, or officers who are sanctioned persons or who are located in sanctioned territories
- Significant customers with sanctions exposure
- Significant activities in higher sanction risk counties, such as landlocked countries
- Use of the US financial system, US currency or US-origin goods
- Customer in high risk industries, such as oil/gasoline, financial service, logistic, telecommunication
- Utilize products/services that are higher risk for sanctions, such as trade finance, virtual currencies, etc.
- Audit, compliance testing, or regulatory findings concerning sanctions compliance
- Adverse media about sanctions or sanctions evasion.
The UN Panel of Experts has highlighted deficiencies in banks’ customer due diligence processes as one of the weaknesses preventing the effective implementation of UN Security Council sanctions targeting North Korea.

166. An analysis of documents submitted by financial institutions of the Democratic People's Republic of Korea and their representatives to open bank accounts showed **insufficient due diligence performed by financial institutions during the onboarding process**. For example, the due diligence conducted by a major European bank for an application for a euro denominated account by a representative of the Korea Daesong Bank showed **no independent review or verification of the answers given on the anti-money laundering questionnaire**. A due diligence checklist indicated that despite negative public information about applicants (including an entry in the Thomson Reuters World Check database), the fact that the bank's regulator was the Central Bank of the Democratic People's Republic of Korea and that no audited documentation was available, the bank's compliance department recommended that the application be accepted.

**UN Panel of Experts on North Korea final report pursuant to UNSC Resolution 2345 (2017)**
5 March 2018 (published to the public 16 March 2018)
Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.
Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

OUR INTERNATIONAL NETWORK
32 OFFICES IN 21 COUNTRIES

Abu Dhabi
Amsterdam
Barcelona
Beijing
Brussels
Bucharest
Casablanca
Dubai
Düsseldorf
Frankfurt
Hong Kong
Istanbul
London
Luxembourg
Madrid
Milan
Moscow
Munich
Newcastle
New York
Paris
Perth
Prague
Rome
São Paulo
Seoul
Shanghai
Singapore
Sydney
Tokyo
Warsaw
Washington, D.C.

*Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.
Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.