IIB ANNUAL U.S. REGULATORY/COMPLIANCE ORIENTATION PROGRAM
ANTI-MONEY LAUNDERING/OFAC COMPLIANCE

**DAVID D. DIBARI (CLIFFORD CHANCE US LLP); TERESA PESCE (KPMG LLP);
DAN STIPANO (BUCKLEY SANDLER LLP); ALEXI VON KESZYCKI (DELOITTE ADVISORY)**

THURSDAY, DECEMBER 14, 2017

INTRODUCTION TO ANTI-MONEY LAUNDERING AND OFAC SANCTIONS COMPLIANCE

DAVID D. DIBARI, CLIFFORD CHANCE US LLP

WHAT IS MONEY LAUNDERING?

"Money laundering generally refers to financial transactions in which criminals, including terrorist organizations, attempt to disguise the proceeds, sources or nature of their illicit activities. Money laundering facilitates a broad range of serious underlying criminal offenses and ultimately threatens the integrity of the financial system." – U.S. Department of the Treasury

The process generally involves three stages:

1. **Placement** – Placing illicit funds into the financial system by converting those funds into some other financial instrument or medium;
2. **Layering** – Separating illicit funds from their source by involving those funds in a series of legitimate transactions; and
3. **Integration** – Involving funds in a series of transactions intended to make it appear that the funds have been derived from a legitimate source.

US ANTI-MONEY LAUNDERING STATUTES

The Money Laundering Control Act (MLCA) of 1986

- The MLCA is a complex criminal statute targeted toward financial transactions that involve the proceeds of certain specified unlawful activities, or that are intended to promote or conceal such activities.

- This also includes economic sanctions violations, FCPA violations, bank fraud, among many other “SUAs.”
- The transaction itself doesn’t need to include illegal proceeds if it is designed to conceal such activity.

KEY US ANTI-MONEY-LAUNDERING STATUTES

Bank Secrecy Act

- The “BSA” was enacted in 1970 to prevent banks and other financial institutions from being used as intermediaries for, or to hide the transfer or deposit of money derived from, criminal activity. The BSA is intended to safeguard the U.S. financial system and the financial institutions that make up that system from the abuses of financial crime, including money laundering, terrorist financing, and other illicit financial transactions.

- The BSA has been amended substantially over time, most significantly right after 9/11 with the passage of the USA PATRIOT Act.

USA PATRIOT Act

- Enacted in 2001 to further inhibit the use of the US financial system for illicit purposes through, among many other things, the imposition of new and heightened due diligence, monitoring, reporting, and recordkeeping requirements for US financial institutions, including MSBs.

BSA REGULATORY AND ENFORCEMENT AGENCIES

Financial Crimes Enforcement Network ("FinCEN"), a bureau of the U.S. Treasury, is the designated administrator of the BSA. In this capacity and in accordance with the USA PATRIOT Act, FinCEN issues regulations and interpretive guidance, provides outreach to regulated industries, supports the examination functions performed by federal banking agencies, and pursues civil enforcement actions when warranted. FinCEN relies on the federal banking agencies to examine banks within their respective jurisdictions for compliance with the BSA.

The Federal Banking Agencies are responsible for the oversight of the various banking entities operating in the United States, including foreign branch offices of U.S. banks. The federal banking agencies are required to include a review of the BSA compliance program at each examination of an insured depository institution.

The Federal Banking Agencies require each bank under their supervision to establish and maintain a BSA compliance program, which must be approved by the Board. The Federal Banking Agencies may use their authority to enforce compliance with appropriate banking rules and regulations, including compliance with the BSA.

A bank regulated by a Federal Banking Agency is deemed to have satisfied the AML program requirements of the USA PATRIOT Act if the bank develops and maintains a BSA compliance program that complies with the regulatory requirements and related guidance of its federal functional regulator governing such programs.

The Federal Financial Institutions Examination Council ("FFIEC") was established in March 1979 to prescribe uniform principles, standards, and report forms and to promote uniformity in the supervision of financial institutions. FFIEC Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual is an excellent primer and resource regarding regulatory expectations.

State Banking Agencies, for state-licensed banks, as a matter of supervision, safety and soundness, also have a role in monitoring BSA compliance. The DFS, in particular has been quite active in examining and enforcing BSA compliance for New York licensed banks.

Criminal Authorities at both the Federal and state level can and do bring cases against both institutions and individuals.

BACKGROUND: HISTORY OF US SANCTIONS

- Date back to the earliest days of US history
- Used as a wartime tactic to weaken the enemy
- Now a standard tool of US foreign policy

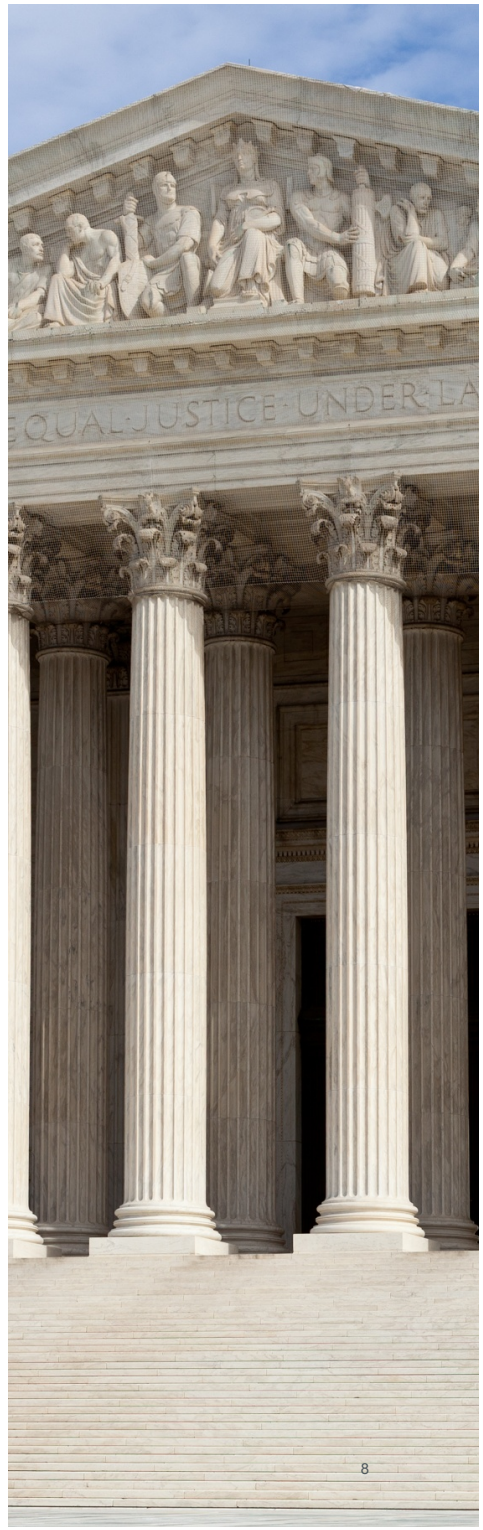
(slide created by OFAC)

OFFICE OF FOREIGN ASSETS CONTROL (OFAC)

OFAC is an office of the US Department of the Treasury that implements and administers economic sanctions under applicable US laws.

OFAC's sanctions programs are based on U.S. foreign policy and national security goals against targeted individuals and entities such as foreign countries, regimes, terrorists, international narcotics traffickers, and those engaged in certain activities such as the proliferation of weapons of mass destruction or transnational organized crime. OFAC acts under Presidential wartime and national emergency powers, as well as various authorities granted by specific legislation, to impose controls on transactions and to freeze assets under U.S. jurisdiction. OFAC has been delegated responsibility by the Secretary of the Treasury for developing, promulgating, and administering U.S. sanctions programs. Some sanctions are multilateral, and some are unilateral.

- International Emergency Economic Powers Act ("IEEPA")
- Trading with the Enemy Act of 1917 ("TWEA")
- Joint Comprehensive Plan of Action ("JCPOA")
- Countering America's Adversaries Through Sanctions Act ("CAATSA")



OFAC SANCTIONS PROGRAMS

OFAC sanctions programs may be imposed against whole countries or targeted individuals and entities.

- Comprehensive Country-wide Sanctions Programs: Crimea, Cuba, Iran, North Korea and Syria.
- Country-based Specially Designated Nationals (SDNs): Balkans Region, Belarus, Burundi, Central Africa Republic, DR Congo, Iraq, Libya, Lebanon, Libya, Somalia, South Sudan, Ukraine/Russia, Venezuela, Yemen, Zimbabwe.
- Activity-based Specially SDNs: terrorism, weapons proliferation, narcotics trafficking and other nefarious activities, and Foreign Sanctions Evaders (FSEs).
- Sectoral Sanctions: entities operating in certain sectors of Russia's economy designated on the Sectoral Sanctions Identifications (SSI) list.
- Venezuela Financial Sanctions: the Government of Venezuela and Petroleos de Venezuela.
- The sanctions require US persons either to block or to reject transactions, depending on the applicable program. In either case, there follows reporting and record keeping obligations.

OFAC has the authority, through a licensing process, to permit certain transactions that would otherwise be prohibited under its regulations.

Export Denied Persons (listed by US Commerce and State Departments).

KEY ENFORCEMENT AGENCIES

OFAC does not conduct examinations, but does bring very significant enforcement actions against banks, both US-based and banks located outside the United States if they have utilized correspondent accounts inside the United States. On November 9, 2009, OFAC issued a final rule entitled "Economic Sanctions Enforcement Guidelines" in order to provide guidance to persons subject to its regulations. The document explains the procedures that OFAC follows in determining the appropriate enforcement response to apparent violations of its regulations. Some enforcement responses may result in the issuance of a civil penalty that, depending on the sanctions program affected, may be as much as $289,238 per violation or twice the amount of a transaction, whichever is greater. The Guidelines outline the various factors that OFAC takes into account when making enforcement determinations, including the adequacy of a compliance program in place within an institution to ensure compliance with OFAC regulations. OFAC encourages banks to take a risk-based approach to designing and implementing an OFAC compliance program. OFAC has issued targeted guidance to various industries, including to banks that is available on their website.

Federal Banking Agencies examine a bank's OFAC Compliance Program, including its OFAC risk assessment, and evaluate OFAC compliance programs to ensure that all banks subject to their supervision comply with the sanctions. Banks should establish and maintain an effective, written OFAC Compliance Program that is commensurate with their OFAC risk profile (based on products, services, customers, and geographic locations). Similar to the AML Compliance Program, the OFAC Compliance Program should identify higher-risk areas, provide for appropriate internal controls for screening and reporting, establish independent testing for compliance, designate a bank employee or employees as responsible for OFAC compliance, and create training programs for appropriate personnel in all relevant areas of the bank.
FFIEC Examination Manual has an OFAC module and is an excellent primer and resource regarding regulatory expectations.

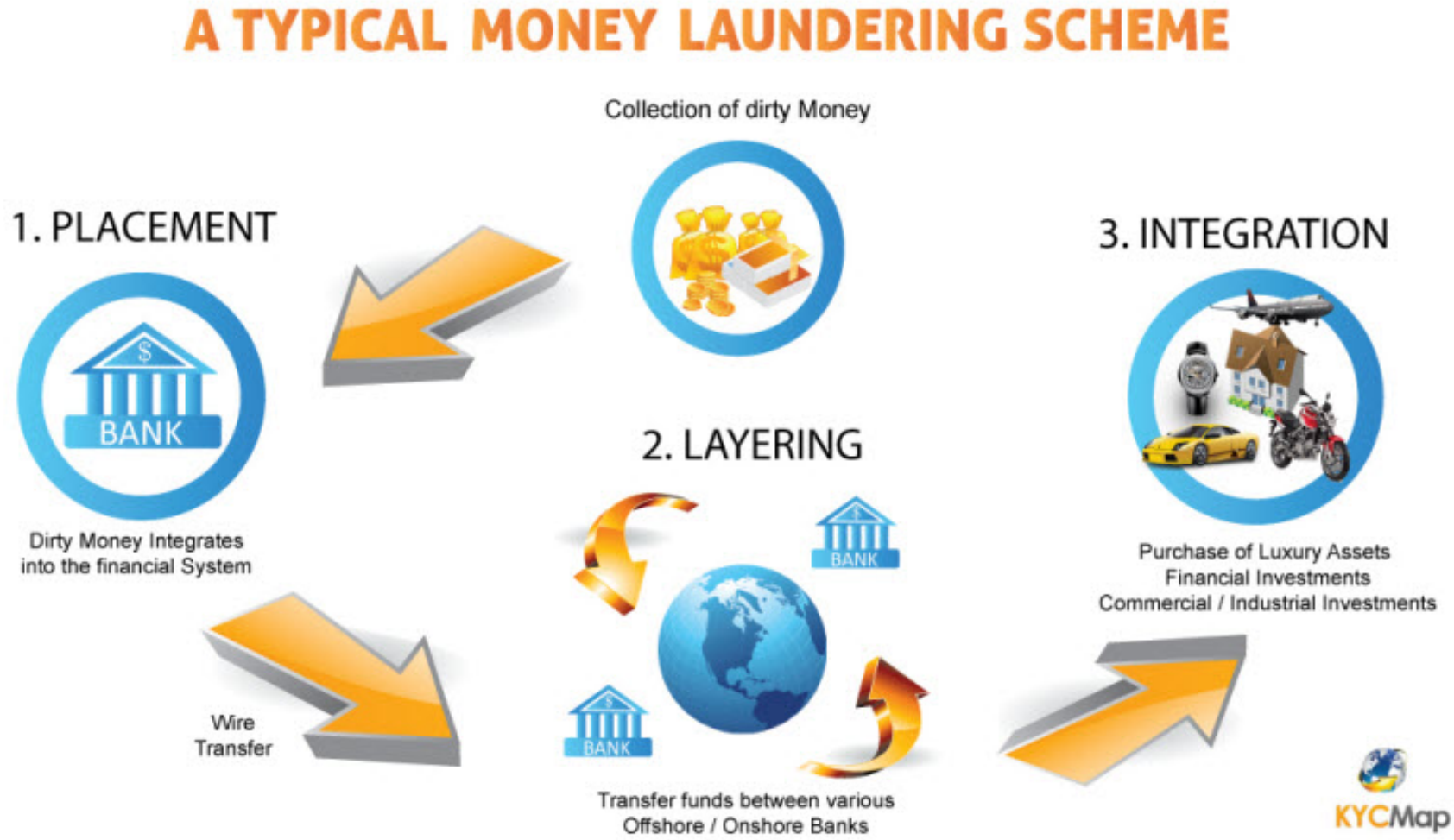
DFS has been involved in numerous investigations/enforcement actions involving OFAC compliance of New York licensed banks. As a result of these investigations and its regular examinations for safety and soundness, DFS has stated that it has "identified shortcomings in the transaction monitoring and filtering programs of these institutions attributable to a lack of robust governance, oversight, and accountability at senior levels." In response, DFS now have gone further than any Federal Banking Agency issuing a new rule, Part 504. This new regulation sets forth in some detail DFS' expectations as to the required attributes of a Transaction Monitoring and Filtering Program and require that the Board of Directors or Senior Officer(s) to submit an annual certification regarding the institution's compliance with the Part 504 requirements.

Criminal Authorities at both the Federal and state level can and do bring cases against both institutions and individuals.

BSA requirements

Teresa Pesce,
KPMG LLP

What is Money Laundering?



Dirty funds derived from Specified Unlawful Activity result in “Clean” funds

What is Terrorist Financing?

Terrorist Financing is the **financial support of terrorism**, which is any act "intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act"

Article 2, International Convention for the Suppression of the Financing of Terrorism
United Nations, 1999

Terrorist Financing (TF) can be from unlawful or legitimate sources:

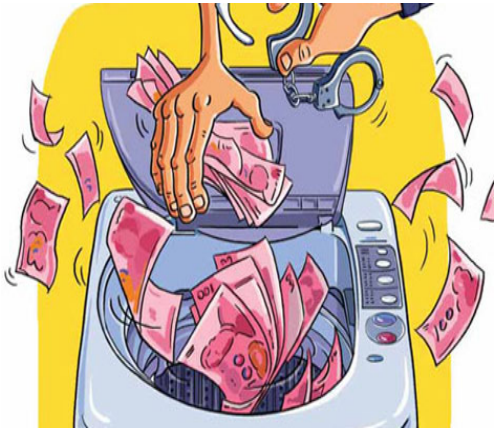
Unlawful Sources	Legitimate Sources
• Extortion • Kidnaping • Narcotics trafficking • Smuggling • Fraud • Theft • Identity theft • Use of conflict diamonds • Improper use of charitable or relief funds • Robbery	• Charitable donations • Foreign government sponsors • Business ownership • Personal Employment

Money Laundering v. Terrorist Financing

Money Laundering & Terrorist Financing share many similarities…

Similarities:

- Similar methods used to conceal source or purpose of funds:
  - Currency smuggling
  - Structured deposits or withdrawals
  - Purchases of various types of monetary instruments
  - Credit, debit, or prepaid cards
  - Funds transfers
  - Informal banking (e.g., hawalas) or informal trade value systems
  - Use of Shell Companies



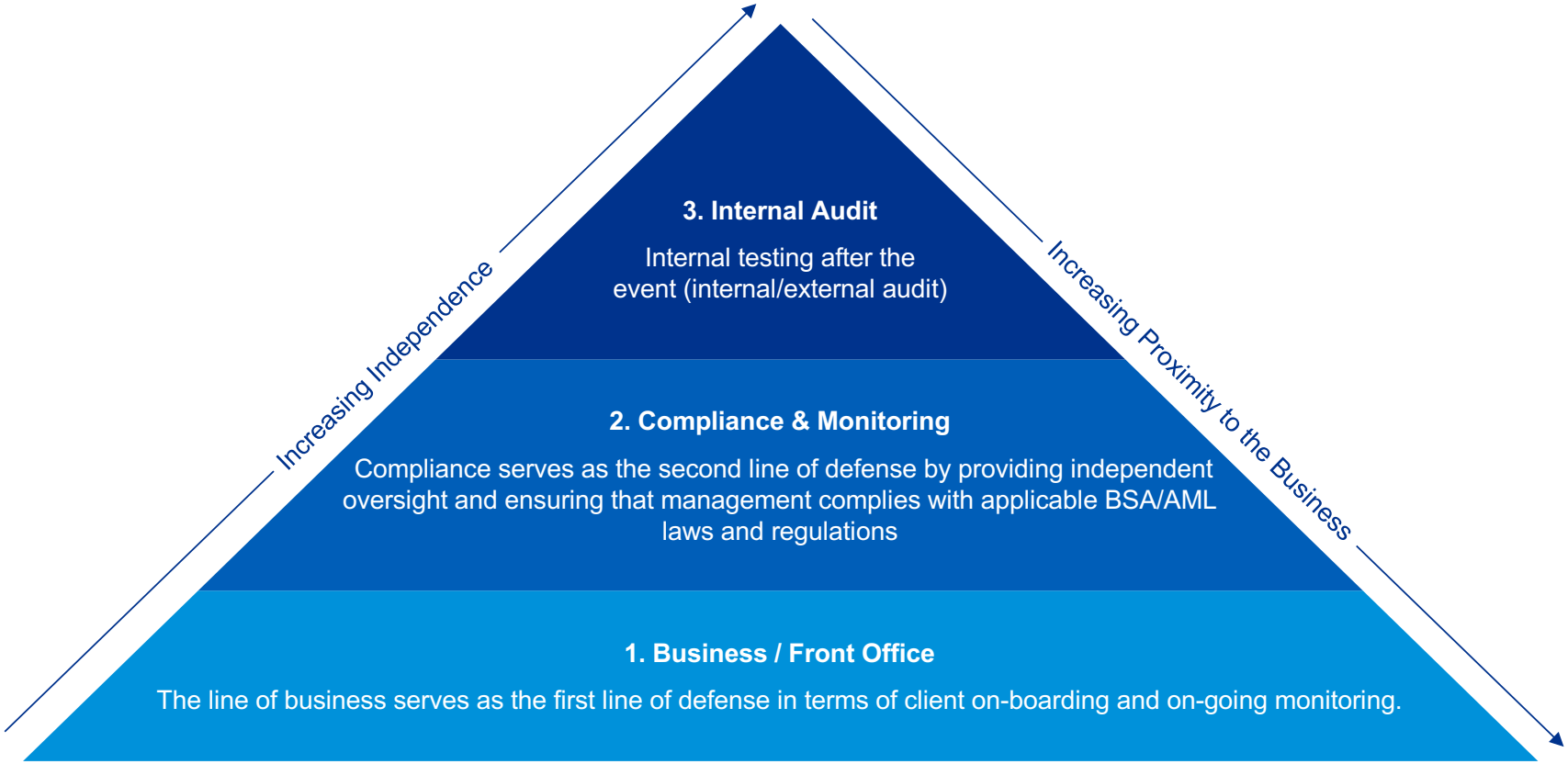
But, have distinct differences:

Differences:

- Motivation
- Legitimate funds can source terrorist financiers whereas money laundering is sourced by illicit funds
- Emphasis on concealing source of funds (money laundering) v. emphasis on concealing purpose of funds (terrorist financing)

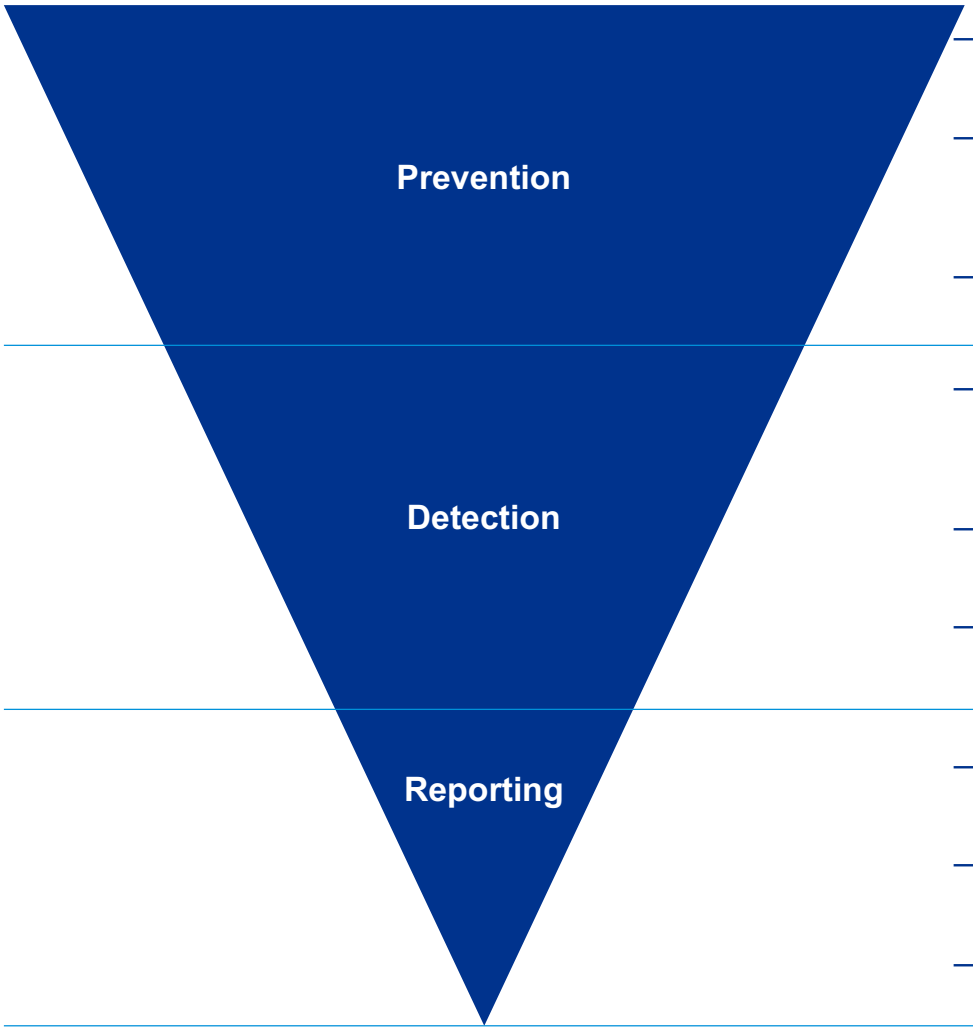
Role of Financial Institutions

- Financial institutions have a significant role to play in preventing money laundering and counter-terrorist financing, and should have controls in place to help guard against them.
- As depicted in the pyramid below, financial institutions generally employ a **'three lines of defense'** model for guarding against money laundering and counter-terrorist financing.



BSA program

Prevention, detection, and reporting



Prevention

- Implementation of Customer Identification Program (CIP)
- Execution of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) requirements
- Cooperation with federal agencies, such as FinCEN and OFAC

Detection

- Front office employees knowing their customers & understanding expected transactional activity
- Employees staying alert to possible suspicious activity
- Monitoring and reporting unusual transactions to the Compliance Officer

Reporting

- BSA Compliance Officer conducting due diligence investigations
- Reporting of potentially suspicious activity to FinCEN
- Updating customer's profile, if warranted

KPMG

Five Pillars of an Effective AML Program

USA PATRIOT Act Section 352

Anti-money laundering programs

— The “Five Pillars” of an effective AML Program

1. **Internal controls**
2. **Designated AML compliance officer***
3. **Ongoing employee training**
4. **Independent testing**
5. **Customer due diligence**

* The AML Compliance Officer should have Board-designated authority to carry out his/her role and responsibilities.

Pillar 1

Internal controls

Comprehensive plan and set of internal controls, including:

- Documented policies and procedures
- AML compliance program continuity
- Risk-based customer due diligence
- Dual controls and segregation of duties, to the extent possible
- Sufficient controls and monitoring systems for timely detection and reporting of suspicious activity
- Incorporation of AML compliance as a strict condition of employment
- Adherence to all reporting and record retention requirements
- Management reports

Pillar 2

Designated BSA compliance officer

1. Independence
2. Experience
3. Sufficient authority
4. Sufficient resources
5. Understanding of the bank's business
6. Compliance self-assessments
7. Communication
   - Board of Directors
   - Senior Management

Pillar 3

Ongoing employee training

Who?

— All client-facing employees

— Other lines of business supervisors/reviewers

— Relevant operations

— Risk personnel

— Senior management and board of directors

What?

— Tailored training for each line of business or area of responsibility

— Adequate and comprehensive, covering the institution's policies, procedures, and particular AML risks

— Training schedule and attendance tracking

When?

— At least annually

Pillar 4

Independent testing

- ***Independent*** (i.e., conducted by internal audit department, outside auditor, consultant or other qualified independent party who is not involved in the daily oversight or operation of the organization's AML compliance program)
- ***Ongoing***, periodic review of AML compliance program (at least annually)
- Employ ***well-considered risk-based approaches*** in auditing, resulting in sufficient attention to higher-risk areas and processes, and with frequency
- ***Sufficient coverage, with appropriate methodology*** that defines scope and depth of testing, with particular emphasis on high-risk operations (products, services, customers, and geographic locations)
- ***Deploy sufficient levels of qualified audit resources*** dedicated to auditing AML programs, their process, and controls.
- Ensure ***timely follow-up*** with management on urgent findings and escalation of these to management and audit committees if lack of management response/implementation of corrective actions
- Use internal staff or consultants who possess the ***requisite credentials, experience, and subject matter training and expertise***
- Provide adequate ***supporting documentation*** for work papers
- Ensure ***direct access and reporting to the Board of Directors/Audit Committee***

Pillar 5

Customer due diligence

- Compliance with the CDD Rule becomes mandatory on May 11, 2018.
- Requires financial institutions to identify the account's beneficial owners for new accounts opened on or after May 11, 2018
- What is a Beneficial Owner?
  - Each individual, who, directly or indirectly, owns 25% or more of the equity interests of a legal entity customer; and
  - A **single individual** with significant responsibility to control, manage, or direct a legal entity customer, including an executive officer or senior manager (e.g., a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer); or any other individual who regularly performs similar functions (i.e., the control prong).
- Under this definition of beneficial ownership, a legal entity will have a total of between one and five beneficial owners
  - (i.e., one person under the control prong and zero to four persons under the ownership prong).

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia

Deloitte.

Office of Foreign Assets Control (OFAC) and Economic Sanctions

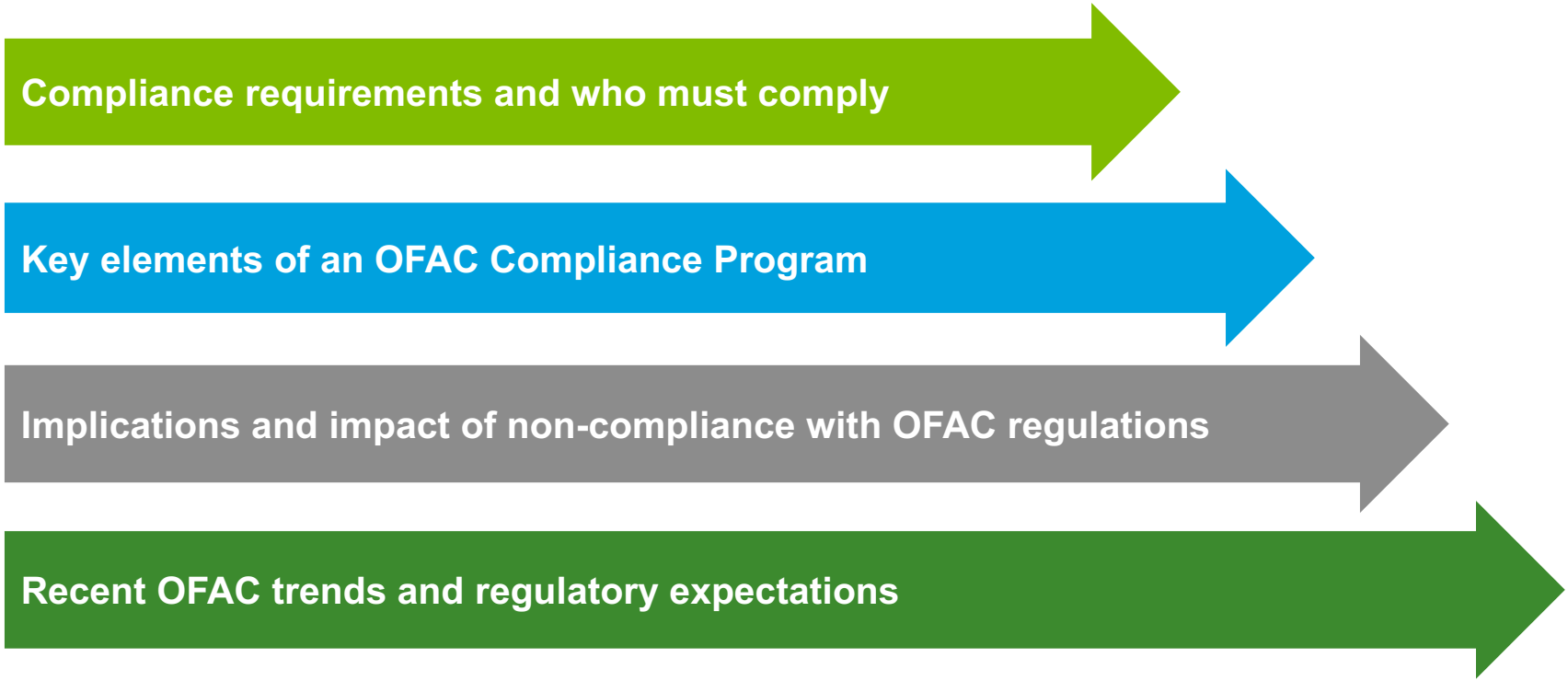
Understanding the Requirements and Importance of Compliance

December 14, 2017

Alexi Von Keszycki, Managing Director
Deloitte Advisory, 571-421-4240

Office of Foreign Assets Control

Overview:



Origin of OFAC

What role does it play?

- The Office of Foreign Assets Control (“OFAC”) is an office of the U.S. Department of the Treasury and responsible for the administration and enforcement of U.S. economic and trade sanctions.

- OFAC itself was formally created in December 1950, when President Truman declared a national emergency and blocked all Chinese and North Korean assets subject to U.S. jurisdiction.

- The sanctions further US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States.

- OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under U.S. jurisdiction.

Unique features about OFAC

OFAC requires all US persons to comply with sanctions laws and regulations

Every transaction (regardless of the amount) that a US financial institution engages in is subject to OFAC regulations

OFAC is a strict liability regulatory regime – penalties can accrue with no knowledge of the violations

An OFAC compliance program should be tailored to each institution's OFAC risk profile

Who is required to comply with OFAC regulations

The following individuals and entities are required to comply with OFAC regulations:

- All U.S. persons regardless of where they are located
- All persons and entities located within the U.S., including U.S. branches of foreign banks
- All U.S. incorporated entities and their foreign branches
- All foreign subsidiaries owned or controlled by U.S. companies
  - Note that this only applies for certain sanctions programs, e.g., North Korea and Cuba

Secondary sanctions supplement other sanctions programs by targeting non-U.S. persons (primarily foreign financial institutions and foreign sanctions evaders) who do business with individuals, countries, regimes, and organizations in Iran.

Sanctions programs

OFAC administers 27 different sanctions programs. The sanctions can be either comprehensive or targeted, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals. The below list illustrates the diversity of the sanctions programs:

- Balkans-Related Sanctions
- Belarus Sanctions
- Burundi Sanctions
- Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA)
- Central African Republic Sanctions
- Counter Narcotics Trafficking Sanctions
- Counter Terrorism Sanctions
- Cuba Sanctions
- Cyber-related Sanctions
- Democratic Republic of the Congo-Related Sanctions
- Iran Sanctions
- Iraq-Related Sanctions
- Lebanon-Related Sanctions
- Libya Sanctions
- Magnitsky Sanctions
- Non-Proliferation Sanctions
- North Korea Sanctions
- Rough Diamond Trade Controls
- Somalia Sanctions
- Sudan and Darfur Sanctions
- South Sudan-related Sanctions
- Syria Sanctions
- Transnational Criminal Organizations
- Ukraine-/Russia-Related Sanctions
- Venezuela-Related Sanctions
- Yemen-Related Sanctions
- Zimbabwe Sanctions

OFAC and other sanctions lists

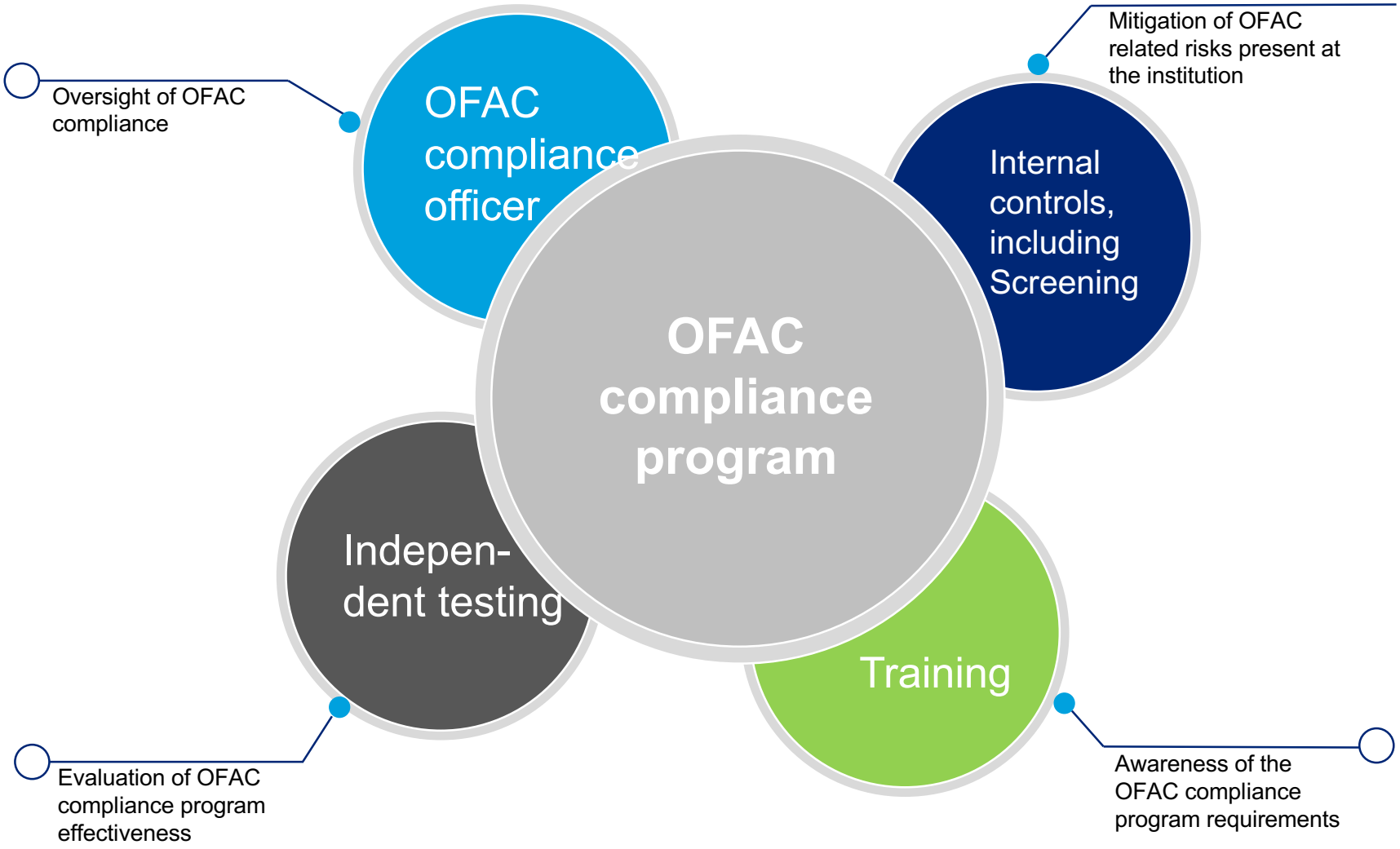
A major component of OFAC sanctions are lists Specially Designated Nationals and Blocked Persons (SDN) list.

OFAC maintains other, so called non-SDN lists, which are also available on its website.

- Specially Designated Nationals and Blocked Persons (e.g. SDN list)
- Sectoral Sanctions Identifications List
- Foreign Sanctions Evaders List
- Non-SDN Palestinian Legislative Council List
- Non SDN Iranian Sanctions List
- The List of Foreign Financial Institutions Subject to Part 561 (the “Part 561 List”)

Overview of an OFAC compliance program

Key components and goals



Components of an OFAC compliance program

Screening

The effectiveness of sanctions screening is critical in meeting regulatory requirements and preventing an institution from processing prohibited transactions or doing business with an SDN.

- OFAC screening can be performed using manual or automated methods, but should utilize up-to-date OFAC and other sanctions lists either compiled internally or managed by a third party vendor.

- The screening process is performed at customer onboarding and periodically through the life of the customer. Transaction screening involves filtering certain data fields, primarily funds transfer transactions, for potential matches to the SDN and other list or prohibited countries.

- Institutions “tune” (i.e. establish thresholds tolerances) for maximizing effectiveness for screening OFAC identified names.

Customer Due Diligence

Secondary and sectoral sanctions require understanding clients, client relationships, and transactions.

OFAC imposed penalties

Cost of non-compliance

OFAC regulations possess strict liability. The intent to violate OFAC requirements has no impact of whether a violation has occurred.

Violations can jeopardize U.S. foreign policy and national security goals; therefore, fines can be substantial.

Per OFAC regulations, penalties can include:

- Criminal penalties for willful violations range up to $20 million and 30 years in prison; or,
- Civil penalties for violations range up to $1 million for each violation or twice the value of certain transactions, depending on the type of violation.

OFAC imposed penalties (cont.)

Broader consequences

Broader implications of penalties and consequences for OFAC violations can be significant and can include:

- Fines from multiple regulatory agencies;
- Remediation costs;
- Legal costs; and,
- Revocation of U.S. banking license.

Furthermore, the reputational damage associated with OFAC penalties can be sever, causing clients to withdraw their business and other financial institutions to refuse to do business with penalized parties.

Mitigation of OFAC civil penalties include: adequacy of OFAC compliance program, egregiousness of the violations, compliance history, and cooperation.

OFAC enforcement policy and implementation

Type of responses to apparent violations

A. No action

B. Request for additional information

C. Cautionary letter

D. Finding of violation

E. Civil monetary penalty

F. Criminal referral

G. Other administrative action

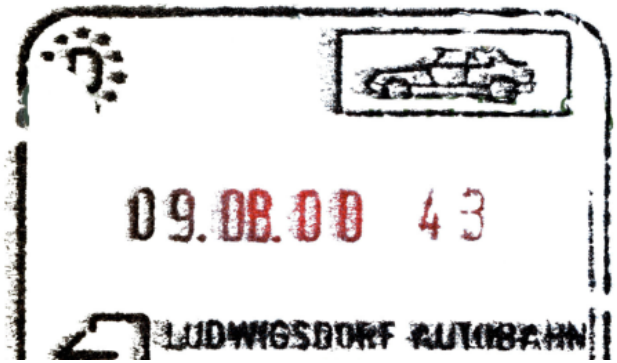
OFAC enforcement actions

Recent penalties and forfeitures

Financial Institution (Year of Action)	OFAC and / or Criminal Penalties and Forfeitures
American Honda Finance Corporation (2017)	$87,255
Toronto-Dominion Bank (2017)	$516,105
Barclays Bank PLC (2016)	$2,485,890
Banco do Brasil (2015)	$139,500
PayPal, Inc. (2015)	$7,658,300
Commerzbank AG (2015)	$258,660,796
Bupa Florida Group (2014)	$128,704
Zulutrade, Inc. (2014)	$200,000
Citigroup (2014)	$217,841
AIG (2014)	$279,038
BNP (2014)	$963,619,900
Total	**$1,233,993,329**

Recent OFAC trends

- U.S. sanctions against Russia
  - Sectoral sanctions
  - Change of the 50% ownership rule
- U.S. Sanctions and secondary sanctions – Iran and North Korea
- Malicious cyber-enabled activities
- U.S. sanctions against Cuba



Regulatory expectations

- Due to the importance of U.S. foreign policy and national security goals supervisors and law enforcement expect institutions to comply with sanctions requirements regardless of their complexity.

- Institutions of all sizes and risk profiles should devote applicable expertise, resources, and technological solutions to ensuring effective sanctions compliance.

- When apparent sanctions violations occur prompt reporting and corrective action is expected.

Resources: General OFAC information and guidance

In addition to providing guidance on specific sanctions programs, OFAC provides information on a number of sanctions-related issues that span multiple programs or that may affect specific industries

- Frequently asked questions (FAQs)
- Apply for an OFAC license online
- Guidance and Information for industry groups
- Interpretative rulings on OFAC policy
- Civil penalties and enforcement information
- OFAC reporting forms
- Legal library (includes regulations, statutes and executive orders)
- OFAC training and events
- Other non-treasury sanctions-related resources

BUCKLEY SANDLER

Enforcement actions

Daniel P. Stipano
Partner, Buckley Sandler LLP

Enforcing agencies

- Supervisory Agencies
- FinCEN
- Functional Regulators
- Department of Justice
- State and Local prosecuting agencies

Remedies - Institutions

- Supervisory Actions
- Informal Enforcement Actions
- Formal Enforcement Actions
- Civil Money Penalties
- Criminal Sanctions
- Monitorship

Remedies - Individuals

- Reprimands
- Civil Money Penalties
- Cease and Desist Orders
- Removal and Prohibition
- Civil Injunction

Enforcement Process – Federal Banking Agencies

- FBAs are required to examine for compliance with the program requirement at every examination.
- FBAs are also required to report problems with a bank's program to the Board of Directors.
- If the bank has a defective program or fails to correct the problems that were reported to the Board, the FBAs are required to use their C&D authority to correct the problem.
- FBAs can also use supervisory tools and informal remedies.

Trends and Recent Cases

- Megabank (DFS - $180 million)
- Agricultural Bank of China ($215 million)
- Banamex (FDIC - $140 million)
- Deutsche Bank (DFS and FCA) $609 million
- Merchants Bank (OCC - $1 million)
- Habib Bank (DFS - $225 million)
- Lone Star Bank (FinCEN - $2 million)

Individual Liability

- Haider
- Gibraltar
- Usher and Ramchandani (Citibank, JP Morgan)
- Banamex
- Fang and Fletcher (JP Morgan)

Common Bases for Action

- Customer Due Diligence/Enhanced Due Diligence
- Risk assessment/risk rating
- Monitoring
- Foreign correspondent banking/private banking
- Suspicious activity reporting process
- Audit

Avoiding Problems

- Importance of strong AML program
- Strong risk governance and risk management
- Pro-active approach to addressing problems
- Transparency
- Good supervisory relationships

CLIFFORD

CHANCE

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

WWW.CLIFFORDCHANCE.COM