LexisNexis®
RISK SOLUTIONS

TECHNICAL REFERENCE GUIDE

Data Segments

for the LexisNexis® WorldCompliance™ Data Plus Service

BIS217-EN_US — 20 April 2021

The recipient of this material (hereinafter "the Material") acknowledges that it contains confidential and proprietary data the disclosure to, or use of which by, third parties will be damaging to LexisNexis Risk Solutions and its affiliated companies (hereinafter "LexisNexis"). Therefore, recipient agrees to hold the Material in strictest confidence, not to make use of it other than for the purpose for which it is being provided, to release it only to employees requiring such information, and not to release or disclose it to any other party. Upon request, recipient will return the Material together with all copies and modifications, if any, to LexisNexis.

LexisNexis shall not be liable for technical or editorial errors or omissions contained herein. The information in this publication is subject to change without notice and is provided "as-is" without a warranty of any kind. Nothing herein should be construed as constituting a warranty, as any applicable warranty is exclusively contained in your signed agreement with LexisNexis.

All names, addresses, birth dates or other identifying information in the text, or on the sample reports and screens shown in this document, are of fictitious persons and entities and have been created for illustrative purposes only. Any similarity to the name of any real person, school, business, other entity, address, date of birth, or other identifying information is purely coincidental.

Due to the nature and origin of public record information, the public records and commercially available data sources used in reports may contain errors.

The LexisNexis WorldCompliance Data and LexisNexis WorldCompliance Data Plus services are not provided by "consumer reporting agencies," as that term is defined in the Fair Credit Reporting Act (15 U.S.C. 1681, et seq.) (FCRA), and do not constitute "consumer reports," as that term is defined in the FCRA. Accordingly, the WorldCompliance Data and WorldCompliance Data Plus services may not be used in whole or in part as a factor in determining eligibility for credit, insurance, employment or for any other eligibility purpose that would qualify it as a consumer report under the FCRA.

Contents

WorldCompliance Data Plus

The LexisNexis® WorldCompliance™ Data Plus service lets you incorporate LexisNexis® WorldCompliance™ data into your processing to help your organization perform due diligence and comply with global mandates and government regulations. WorldCompliance data can help your organization identify individuals, companies, and other entities as part of a risk-based approach to AML (anti-money laundering) and CTF (counter-terrorist financing) screening.

Available Segments

The WorldCompliance data is organized into multiple segments for easier integration into your processes.

The file contains the following segments of risk data:

- `Adverse Media`
  See "Adverse Media Segment" on page 5.
- `Enforcement`
  See "Enforcement Segment" on page 26.
- `PEP`
  See "PEP Segment" on page 49.
- `Sanctions`
  See "Sanctions Segment" on page 58.
- `SOE`
  See "SOE Segment" on page 59.
- Additional Segments
  See "Additional Segments" on page 62.

The file may also include `Registrations` data. See "Registrations Segment" on page 63.

To receive the `Registrations` *data, you must formally request the data.*

Adverse Media Segment

Adverse media information originates from monitoring credible open source media for events that meet the qualifying standards and definitions.

WorldCompliance researchers apply an `Adverse Media` segment to the entity to indicate that a published news source described a crime that was committed. Media coverage is gathered from various credible news sources that include web sites, international newspapers, magazines and periodicals, broadcasts, press releases, and news wires.

WorldCompliance researchers also apply at least one of the following subcategories:

Aircraft Hijacking

An aircraft hijacking incident involves an individual or a group (including accomplices) that unlawfully attempts, commits, or conspires to seize, takeover, or exercise control of an in-transit, government or commercial common-carrier aircraft with wrongful intent or by force, violence, threat of force or violence, or any form of intimidation. Aircraft hijacking incidents can include acts in connection with or in furtherance of terrorism, terrorism financing, money laundering, organized crime, political asylum, hostage taking, or political or administrative concession by authorities.

Excluded Incidents

- Private aircraft theft
- Truck hijacking
- Carjacking
- Maritime piracy

Antitrust violations

An antitrust violation incident involves an entity that attempts, conspires, or commits violations to acts or laws that are intended to promote fair competition that protects commerce and trade from abusive business practices. These incidents include national regulatory agencies or law enforcement agencies with jurisdictional claims over both domestic and foreign conduct and domestic and foreign parties. Abusive business practices can include the following examples:

- Unfair competition (such as mergers, acquisitions, or takeovers of one firm by another if the effect will substantially lessen competition)
- Restraint of trade
- Monopolies
- Price-fixing
- Price discrimination
- Market-dividing
- Interlocking directorates (an individual who makes business decisions for competing companies)
- Bid-rigging

Excluded Incidents

- Private antitrust actions
- Natural persons who are associated with the subject entity, unless they are specifically accused or charged with wrongdoing
- Private anti-trust actions
- Antitrust disputes brought to the World Trade Organization

Arms Trafficking

An arms trafficking incident involves an individual or a group that attempts, commits, or conspires to divert contraband weapons, munitions, or explosives from lawful commerce into the illegal market by way of direct purchase, trade, dealing, or smuggling in contravention of international laws and regulations, the prescribed laws of the subject legal jurisdiction, or in violation of any extraterritorial laws to which the entity is subject. These efforts can include acts in furtherance of political destabilization, terrorism, civil war, regional conflicts, extra-judicial paramilitary activity, organized crime, or in connection with other related AML predicate offenses that demonstrate an elevated risk of abuse of the financial system.

Excluded Incidents

- Illegal or unauthorized weapons possession
- Incidents that lack evidence of an organized pattern of abuse, conspiracy, or financial motive (for example, a single instance of an illicit gun sale through a straw purchaser)

Bank Fraud

A bank fraud incident involves an individual or a group that knowingly attempts, commits, or conspires to execute an organized and systemic plan, scheme, or con to defraud a financial institution or to obtain any of the moneys, funds, credits, assets, securities, or other property that is owned by, or under the custody or control of, a financial institution by means of false or fraudulent pretenses, representations, or promises.

Excluded Incidents

- NSF (non-sufficient funds)
- Bank fraud that does not demonstrate an organized and systemic attempt to defraud a financial institution

Bribery

A bribery incident involves an individual or a group that attempts, commits, or conspires to offer, give, receive, or solicit currency or something of value to a national or foreign government official, a private individual, or a person in charge of a public, legal, or fiduciary duty to influence or directly alter the person's or group's actions for the following purposes:

- Disobey or avoid complying with international or national laws and regulations or local or extraterritorial laws to which the entity may be subject.
- Encourage an entity to perform a service to which the payer is entitled even without the payment, also known as facilitation payments or grease payments.

Included Incidents

- Participation in, or association with, the conspiracy to commit, attempt to commit, aid and abet, facilitate, or counsel the commission of the event
- United Kingdom: facilitation payments

Excluded Incidents

- The private demonstration of good will
- Campaign donations from corporations or individuals to political candidates (the relationship does not occur directly enough) consistent with the approved activity within the subject jurisdictions
- The customary giving and receiving of gifts of limited monetary value as prescribed by law
- Circumstances where a payment, gift, offer, or promise of anything of value to a foreign official may qualify as an affirmative defense
- A payment, gift, offer, or promise of anything of value that is lawful under the written laws and regulations of the foreign official's, political party's, party official's, or candidate's country
- A payment, gift, offer, or promise of anything of value that is a reasonable and legal expenditure
- Events that are consistent with approved activity within the subject jurisdictions

  These events can include the customary giving and receiving of gifts of limited monetary value as prescribed by law.
- A payment, gift, offer, or promise of anything of value that is directly related to the promotion, demonstration, or explanation of products or services or that are directly related to the execution or performance of a contract with a foreign government or agency (for example, travel and lodging expenses)
- Conduct that is considered a routine "governmental action" exception by the FCPA (Foreign Corrupt Practices Act)

  Routine governmental actions include the following actions that are ordinarily and commonly performed by a foreign official:
  - Obtain permits, licenses, or other official documents to qualify a person to do business in a foreign country.
  - Process governmental papers such as visas or work orders.
  - Provide police protection.
  - Provide mail pick-up and delivery.
  - Schedule inspections that are associated with contract performance or inspections that are related to the transit of goods across the country.
  - Provide telephone service.
  - Provide power and water supply.
  - Load and unload cargo.
  - Protect perishable products or commodities from deterioration.

Burglary

A burglary incident involves an individual or a group that attempts, commits, or conspires to unlawfully enter a structure with the intent to commit a crime to further terrorism, terrorism financing, illicit flows in the financial system, money laundering, organized crime, corruption, hostage taking, or other related AML predicate offenses.

Excluded Incidents

Burglaries that are not part of an organized or systemic plan or scheme that are unlikely to involve the illicit flow or transfer of funds through the financial system

Conspiracy

A conspiracy incident involves an agreement, plan, or scheme that involves an overt act between two or more people that is formed for the purpose of committing, by their joint efforts, an illegal or criminal act in connection with, or in furtherance of, criminal acts that are connected to terrorism, terrorism financing, money laundering, organized crime, political or administrative concession by authorities, or other related AML predicate offenses.

Excluded Incidents

Conspiracies that are not in furtherance of a predicate offense or that are unlikely to involve the illicit flow or transfer of funds through the financial system

Corruption

A corruption incident involves a public official, a private citizen, or a fiduciary that attempts, conspires, or commits an illegal or wrongful act to facilitate an abuse of the powers and influence that are afforded to their office or station to procure a financial benefit or other type of benefit for themselves or for another person, so that both parties, or a single individual, can disobey or avoid complying with international or national laws and regulations or local or extraterritorial laws to which the entity may be subject.

There are many forms of corruption that may involve public-private or public-public relationships. The following types of corruption are a few examples:

- Grand corruption is the act by a group or an individual at the highest levels of government that alter, misrepresent, or distort policies or the central functioning of the state or that require significant erosion of the legal, political, and economic systems to enable leaders to benefit at the expense of the public good.
- Petty corruption is the abuse of power that involves the exchange of very small amounts of money or the granting minor favors for preferential treatment.

Excluded Incidents

Events that are consistent with the approved activity within the subject jurisdictions

These events can include the customary giving and receiving of gifts of limited monetary value as prescribed by law.

Counterfeiting

A counterfeiting incident involves an individual or a group that attempts, commits, or conspires to copy, imitate, or alter an item to increase the value or to reproduce an item without authorization with the intent to present or use the copy as the genuine or original item. An item can include the following examples:

- Obligations and securities
- Currency
- Documents that are issued by government agencies or international organizations
- Bonds
- Bids
- Contracts
- Proposals
- Public records
- Affidavits
- Federal court documents
- Seals of government agencies or international organizations

Excluded Incidents

Counterfeiting not in connection with or in furtherance of terrorism, terrorist financing, money laundering, organized crime, political or administrative concession by authorities, or other related AML predicate offenses or that are unlikely to involve the illicit flow or transfer of funds through the financial system

Crimes Agnst Humanity (Crimes Against Humanity)

A crime against humanity incident involves an individual or a group that knowingly attempts, commits, or conspires to conduct or participate in a widespread or systematic attack against a civilian population as directed by an organization, group, government, state military, or paramilitary. The following acts are examples of crimes against humanity when acknowledged by an authoritative institution such as a government, the UN (United Nations), or the EU (European Union):

- Apartheid involves acts that are committed in the context of an institutionalized regime or systematic oppression and domination by one racial group over any another racial group or groups and that are committed with the intention of maintaining that regime.
- The deportation or forcible transfer of a population is the forced displacement of persons by expulsion or other coercive acts from the area in which they are lawfully present without grounds that are permitted under national law.
- An enforced disappearance is the arrest, detention, or abduction of persons by, or with the authorization or support of, a state or political organization and a refusal to acknowledge the deprivation of freedom or provide information on the fate or whereabouts of those persons with the intention of removing them from the protection of the law for a prolonged period of time.
- Enslavement is the exercise of any or all powers in the right of ownership to a person (for example, human trafficking).
- Extermination is the intentional infliction of conditions of life that is calculated to bring about the destruction of a population in whole or in part. Inflictions can include the deprivation of access to food and medicine or the deprivation of reproductive capacities.
- Genocide involves acts that are designed and committed with the intent to bring about the destruction of a group in whole or in part.
- Murder is the killing of another human being.
- Persecution involves acts against an identifiable group on political, racial, national, ethnic, cultural, or religious or gender grounds.
- Sexual violence can include rape, sexual slavery, or any other form of sexual violence of comparable gravity.
- Torture is the intentional infliction of severe mental or physical pain or suffering.

Cybercrime

A cybercrime incident involves an individual or a group that unlawfully attempts, commits, or conspires to use the internet, electronic communications networks, or information systems in an organized and systemic manner as a tool to conduct fraudulent transactions, theft of data for financial gain, prohibit transactions, or transmit the proceeds of fraud to financial institutions or to others that are connected with the scheme in furtherance of terrorism, terrorism financing, money laundering, organized crime, corruption, hostage taking, or other related AML predicate offenses.

Excluded Incidents

- Cybercrimes that are not likely to involve the illicit flow or transfer of funds through the financial system or a heightened risk of abuse of the financial system
- Cybercrimes that involve software piracy for personal use

Drug Trafficking

A drug trafficking incident involves an individual or a group that attempts, commits, or conspires to engage in organized and systemic illicit trade that involves the cultivation, manufacture, distribution, sale, importation, exportation, or dispensation of substances which are subject to drug prohibition or controlled distribution laws. These incidents can include acts in conjunction with or in furtherance of political destabilization, terrorism, civil war, regional conflicts, extra-judicial paramilitary activity, organized crime, or in connection with other related AML predicate offenses that demonstrate an elevated risk of abuse of the financial system.

Excluded Incidents

- Mere possession of a substance subject to drug prohibition
- Funds that are transferred or activities in connection with medical marijuana or recreational marijuana in jurisdictions which have authorized or decriminalized commercial commerce
- Incidents that lack evidence of an organized pattern of abuse, conspiracy, or material financial motive

  (for example, a single instance of a small quantity of drugs that fails to demonstrate evidence of an organized scheme of “distribution for profit”)
- Incidents that are unlikely to involve the illicit flow or transfer of funds through the financial system

Embezzlement

An embezzlement incident involves an individual or a group that attempts, commits, or conspires to misappropriate personal or government financial assets from entities that have been lawfully entrusted with the care of the assets or by the entrusted entities themselves (for example, employee, clerk, agent, trustee, public officer, or other person that acts in a fiduciary character) to covertly and fraudulently convert these assets for their own use or benefit or transfers the assets to a third party for their own use and benefit.

Environmental Crimes

An environmental crime incident involves an individual or a group that attempts, commits, or conspires to systemically and willfully engage in illegal acts that directly harm the environment and aim at benefiting individuals or groups or organizations from the exploitation of, damage to, or trade or theft of natural resources. These acts are in contravention of international environmental laws and regulations, the prescribed environmental laws of the subject legal jurisdiction, or in violation

of any extraterritorial laws to which the entity is subject with the willful intent to secure material financial advantage through profit or cost avoidance from the activity. These incidents can include the following acts:

- Dumping industrial wastes into water bodies
- Illicit trading in hazardous waste
- Trafficking endangered species or government-protected environmental goods
- Smuggling of Ozone-depleting substances
- Illegal logging and trade of stolen timber in violation of the wildlife laws

Excluded Incidents

- Instances of neglect or instances that do not demonstrate a financial incentive
- Lacey Act violations

Espionage

An espionage incident involves an individual or a group that attempts, commits, or conspires to secretly gather political, military, or economic information about a foreign or domestic government or commercial enterprise for the purpose of placing one's own government or corporation at some strategic or financial advantage. This information includes trade secrets from a private enterprise.

Explosives

An explosives incident involves an individual or a group that attempts, commits, or conspires to perpetrate an organized or systemic criminal act that involves explosives or other destructive devices in connection with or in furtherance of terrorism, terrorism financing, money laundering, organized crime, political asylum, hostage taking, political or administrative concession by authorities, or other acts for financial gain. These acts can include possessing, importing, manufacturing, transferring, transporting, or dealing in explosive materials without a license. A destructive device can include any explosive, incendiary, or poison gas, bomb, grenade, rocket, mine, or missile.

Extort-Rack-Threats (Extortion, Racketeering, or Threats)

An extortion incident involves an individual or a group that attempts, commits, or conspires to obtain money, property, or services from a person or institution in an organized and systemic manner through a pattern of illegal activity that employs the wrongful use of physical or threatened force, violence, fear, property damage, damage to the person's reputation, extreme financial hardship, or under cover of unfavorable government action. Extortion involves obtaining consent through these illegal coercive actions that remove the victim's free will.

Financial Crimes

A financial crime incident involves an individual or a group that attempts, commits, or conspires to unlawfully convert money or property with the intent to gain personal benefit. These incidents include financial crimes that are not covered by another financial subcategory. The following financial crimes are a few examples:

- White-collar crimes (for example, bankruptcy fraud, illicit payments)
- Systemic and organized financial crime
- Illegally obtaining banking information
- Trade secret fraud
- Structuring financial translations (also known as smurfing)
- Loan sharking or usury
- Skimming
- Financial crimes that are likely to involve the illicit flow or transfer of funds through the financial system
- Financial crimes in conjunction with or in furtherance of money laundering, political destabilization, terrorism, terrorist financing, civil war, regional conflicts, extra-judicial paramilitary activity, organized crime, or in connection with other related AML predicate offenses that demonstrate an elevated risk of abuse of the financial system

Forgery

A forgery incident involves an individual or a group that attempts, commits, or conspires to alter or replicate an original document or write a false signature with the intent to defraud for the illegal benefit of the person or persons who committed the forgery. Forgery must demonstrate an organized and systemic scheme in connection with or in furtherance of terrorism, terrorism financing, money laundering, organized crime, political asylum, political or administrative concession by authorities, or other related AML predicate offenses with willful purpose of financial gain. These incidents can include the forgery of checks, stamps, or artwork.

Fraud

A fraud incident involves an individual or a group that operates in an organized and systemic manner to intentionally or knowingly attempt, conspire, or commit to misrepresenting a material, existing fact or deceiving an entity that relies on the misrepresentation in order to deprive the entity of its money, property, or legal right. These incidents include fraud that is not covered by another subcategory.

Excluded Incidents

Fraud for personal gain without financial involvement or that is unlikely to involve the illicit flow or transfer of funds through the financial system

Fugitive

A fugitive incident involves a person who flees a jurisdiction or prison to avoid arrest, prosecution for a crime, imprisonment, or to avoid giving testimony in any criminal proceeding.

Excluded Incidents

Fugitives whose alleged activity does not meet the prescribed definition of other risk categories in the database

Gambling Operations

A gambling operation incident involves an individual or a group that attempts, commits, or conspires to conduct, finance, manage, supervise, direct, or own all or part of an illegal, organized, gambling business. This business may be done in furtherance of organized crime, terrorism financing, or other related AML predicate offense. These gambling operations demonstrate an organized and systemic approach that are likely to involve the illicit flow or transfer of funds through the financial system or a heightened risk of abuse of the financial system. Gambling operations is also known as illegal gaming.

Excluded Incidents

- Gambling operations that are not organized and systemic
- Gambling operations that are unlikely to involve the illicit flow or transfer of funds through the financial system or a heightened risk of abuse of the financial system

Healthcare Fraud

A healthcare fraud incident involves an individual or a group that operates in an organized and systemic matter that attempts, commits, or conspires to execute a scheme or a hoax to defraud any healthcare benefit program or insurer or to obtain by means of false or fraudulent pretenses, representations, or promises any of the money or property owned by, or under the custody or control of, any healthcare benefit program or insurer. The following practitioner schemes are a few examples:

- Obtaining subsidized or fully covered prescription pills that are unneeded and then selling them on the black market for a profit
- Billing by practitioners for care that they never rendered
- Filing duplicate claims for the same service rendered
- Altering the dates, description of services, or identities of members or providers
- Billing for a non-covered service as a covered service
- Modifying medical records
- Intentional incorrect reporting of diagnoses or procedures to maximize payment
- Accepting or giving illicit payments for member referrals
- Waiving member co-pays
- Prescribing additional or unnecessary treatment
- Providing false information when applying for programs or services
- Forging or selling prescription drugs

Excluded Incidents

- Healthcare fraud that does not demonstrate an organized and systemic approach
- Healthcare fraud that involves innocent misrepresentations

Human Rights Abuse

A human rights abuse incident involves an individual or a group that attempts, commits, or conspires to violate basic human rights and freedoms that fundamentally and inherently belong to an individual. Human rights are established by international agreement, convention, custom, or national law acts when acknowledged by an authoritative institution. These institutions include government agencies, the UN, the EU, non-governmental organizations that work in these areas, and credible open-source media. These events can include acts in furtherance of political destabilization, terrorism, civil war, regional conflicts, organized crime, or in connection with other related AML predicate offenses that demonstrate an elevated risk of abuse of the financial system. The following human rights are a few examples:

- The right to life
- The freedom from torture
- The right to a fair trial
- The right to freedom of assembly and association (for example, membership or formation of political parties or trade unions)
- The freedom of religion, expression, security, and asylum
- The freedom from slavery or servitude
- The freedom from arbitrary arrest, detention, or exile

Human Trafficking

A human trafficking incident involves an individual or a group that attempts, commits, or conspires in the recruitment, transportation, transfer, harboring, or receipt of persons by means of the following acts for the purpose of exploitation or commercial gain:

- Threat or use of force or other forms of coercion
- Abduction
- Deception
- Fraud
- Abuse of power or of a position of vulnerability
- Giving or receiving of payments or benefits to achieve the consent of a person who has control over another person

Exploitation can include prostitution of others, other forms of sexual exploitations, forced labor services, servitude, slavery or practices similar to slavery, or the removal of organs.

Insider Trading

An insider trading incident involves an individual or a group that attempts, commits, or conspires to buy or sell a security while in possession of, or having access to, material, private, confidential, or non-public information about the security in breach of a fiduciary duty or other relationship of trust and confidence.

Insurance Fraud

An insurance fraud incident involves an individual or a group that attempts, commits, or conspires to perform a duplicitous act in a systemic and organized scheme with the intent to obtain an improper payment from an insurer. These incidents include the following fraud schemes:

- Hard fraud occurs with the deliberate destruction of property for the purpose of collecting on the insurance policy.
- Soft fraud occurs when a policyholder exaggerates an otherwise legitimate claim or when an individual applies for an insurance policy and lies about certain conditions or circumstances to lower the policy's premium.

ISIS Foreign Support

ISIS Foreign Support incidents include an individual or a business with a recognized affiliation with ISIS (Islamic State in Iraq and Syria) or ISIS groups that provides material support to ISIS through means that violate state anti-terrorism laws. The following actions are a few examples of material support:

- Donating, soliciting, or providing financial resources to ISIS operations
- Facilitating material support in the form of military equipment, recruitment, illicit trade, and smuggling
- Conducting attacks as a member of the organization
- Conducting attacks in the name of the organization even without material support (also known as LWA or a lone wolf attack)

  LWAs are defined as attacks or actions by individuals who are not officially connected to, or acting on behalf of, a state-recognized terrorist organization. LWAs are not supported monetarily or otherwise by ISIS. These individuals are inspired by these organizations and decided on their own to act in the name of ISIS.

Foreign supporters are also defined as ISIS members who take the following actions:

- Carrying out or support attacks on their own countries in support of the Islamic State
- Providing means of support, such as, voice overs on ISIS-produced videos, video technical support, managing content on ISIS-owned websites, or procurement of resources and services for the benefit of ISIS groups

Kidnapping

A kidnapping incident involves an individual or a group that attempts, commits, or conspires to unlawfully seize and carry away a person against their will, by force or fraud, with the intent to hold for ransom or reward, use as a hostage, accomplish or aid in the commission of a felony or flight from a felony, inflict physical harm, violate or abuse sexually, terrorize, or interfere with the performance of any governmental or political function. Kidnapping is also known as abduction.

Excluded Incidents

- Parental kidnapping
- Kidnapping that does not demonstrate a financial motive or an organized and systemic approach
- Kidnapping that is not in furtherance of terrorism, terrorism financing, money laundering, organized crime, hostage taking (ransom), political or administrative concession by authorities, or other related AML predicate offenses

Labor Violations

A labor violation incident involves an individual or a group that attempts, commits, or conspires to violate labor laws that define the rights of employees and protect them from employer retaliation for exercising those legal rights or reporting violations to the proper authorities.

These violations can include the following acts:

- Interfering or restraining employees in the exercise of their rights
- Dominating or interfering with the formation or administration of any labor organization
- Discriminating in regards to the hiring or tenure of employment
- Encouraging or discouraging membership in a labor organization
- Refusing to collectively bargain with the representatives of employees
- Violating child labor laws
- Violating labor laws in a way that demonstrates a willful intent to secure material financial advantage
- Violating labor laws in a way that likely involves the illicit flow or transfer of funds through the financial system or a heightened risk of abuse of the financial system

Excluded Incidents

- Labor violations that are unlikely to involve the illicit flow or transfer of funds through the financial system
- Civil claims of labor violations

Money Laundering

A money laundering incident involves an individual or a group that attempts, commits, or conspires to engage in any act or scheme that aims to conceal or disguise the identity, source, and destination (also known as placement, layering, and integration) of illegally obtained proceeds so that they appear to have originated from legitimate or legal sources.

Mortgage Fraud

A mortgage fraud incident involves an individual or a group that operates in an organized and systemic manner that intentionally and knowingly provides any material misstatement, misrepresentation, or omission of information that an underwriter or lender must use to fund, purchase, or insure a loan. The following types of fraud are a few examples:

- Fraud for profit involves an organized, systemic, and elaborate scheme that usually involves collusion among many persons such as a mortgage broker or loan processor and that is committed through single or multiple loans or transactions to gain illicit proceeds from property sales. Fraud for profit is also known as industry insider fraud.
- Fraud for criminal enterprise involves the purchase of real estate with illegally obtained funds (for example, drug activity) to clean or "launder" the money so that the money appears to be obtained by legal means.
- Fraud for property involves deliberate misrepresentations of income, assets, or debt to obtain a mortgage or more favorable terms for the purpose of purchasing a property for primary residence. Fraud for property is also known as fraud for housing.

Murder

A murder incident involves an individual or a group that attempts, commits, or conspires to unlawfully kill a natural person with intent, malice aforethought, and with no legal authority or excuse in furtherance of terrorism, terrorism financing, money laundering, organized crime, political asylum, hostage taking, political or administrative concession by authorities, or other related AML predicate offenses.

Excluded Incidents

- Crimes of passion
- Murder that is not in connection with or in furtherance of money laundering, terrorism, terrorist financing, money laundering, organized crime, hostage taking, political or administrative concession by authorities, or other related AML predicate offenses
- Murder that does not demonstrate an organized and systemic approach

Organized Crime

An organized crime incident involves a group of three or more persons that act in concert within a formalized structure and that attempt, commit, or conspire to engage in long-term criminal activities in a systematic manner to obtain, directly or indirectly, a financial or other material benefit through illegal activities in one or more illegal economic sectors in one or more jurisdictions.

Included Incidents

- Organized crime that demonstrates a planned, systematic nature of criminal activity that range from national to international in scale
- Organized crime that is likely to involve the illicit flow or transfer of funds through the financial system or demonstrate a heightened risk of abuse of the financial system
- Organized crime in connection with or in furtherance of terrorism, terrorist financing, money laundering, hostage taking, political or administrative concession by authorities, or other related AML predicate offenses

Excluded Incidents

- Organized crime that is unlikely to involve the illicit flow or transfer of funds through the financial system
- Organized crime that is politically motivated terrorism, rather than profit driven
- Organized crime that does not demonstrate a heightened risk of abuse of the financial system

Peonage

A peonage incident involves an individual or a group that attempts, commits, or conspires to enforce servitude upon an individual against their will by restraining their liberty (freedom from restraint is the ability to decide for one's self, or free will) and compelling them to labor in payment of a debt or obligation (real or pretended). Peonage is also known as debt servitude or debt slavery.

Pharma Trafficking (Pharmaceutical Products Trafficking)

An incident of pharmaceutical products trafficking involves an individual or a group that attempts, commits, or conspires to engage in the manufacture, trade, transport, and distribution of fake, stolen, or illicit medicines and medical devices in an organized and systemic manner in contravention of international laws and regulations, the prescribed laws of the subject legal jurisdiction, or in violation of any extraterritorial laws to which the entity is subject.

Excluded Incidents

- A single instance of selling pharmaceutical products
- Small-scale prescription drug sales

Piracy

A piracy incident involves an individual or a group that attempts, commits, or conspires to engage in any criminal act of violence, detention, or depredation. These acts are perpetrated by the crew or the passengers of a private ship or aircraft that is directed on the high seas, against another ship, aircraft, or against persons or property committed for private benefit. These acts include incidents that are outside a state’s sovereign maritime borders, and are applicable under universal jurisdiction where states or international organizations can claim criminal jurisdiction of an accused person or group regardless of where the alleged crime was committed.

Included Incidents

- Maritime piracy in international waters
- Piracy incidents that involve vessels at sea or on a river

Pollution

A pollution incident involves an individual or a group that attempts, commits, or conspires in an organized and systemic manner to wrongfully contaminate the atmosphere, soil, or water with harmful or potentially harmful substances to secure a material financial advantage through profit or cost avoidance that are likely to have an adverse effect on the natural environment or life. Pollution incidents also include incidents with the willful intent to secure material financial advantage through profit or cost avoidance from the activity or are determined by the courts to be criminally negligent acts.

Pornography

A pornography incident involves an individual or a group that attempts, commits, or conspires to engage in the organized and systemic and unlawful production, sale, or distribution of scenes (represented through books, magazines, photographs, films, or other media) of sexual behavior that is designed to arouse sexual interest in contravention of international laws and regulations or in violation of any extraterritorial laws to which the entity is subject, specifically as they relate to incidents in connection with or in furtherance of child endangerment, human trafficking, bribery, or other related AML predicate offense.

Price Manipulation

A price manipulation incident involves an individual or a group that attempts, commits, or conspires to deliberately attempt to interfere with the free and fair operation of the legitimate economy and financial system to create a misleading price or market for currencies, commodities, or securities with the intent of securing a financial or other material benefit for themselves or others in one or one or more jurisdictions.

RICO (Racketeer Influenced and Corrupt Organizations)

A RICO incident involves an individual or a group that attempts, commits, or conspires to violate the RICO Act by engaging in a pattern of wrongdoing (for example, racketeering or AML predicate offenses) as a member of a criminal enterprise or organization. Although this law is specific to the United States, LexisNexis® Risk Solutions recognizes international equivalent violations in contravention of international laws and regulations or in violation of any extraterritorial laws to which the entity is subject.

Securities Fraud

A securities fraud incident involves an individual or a group that attempts, commits, or conspires to defraud, deceive, or induce investors in an organized and systemic manner to make a purchase or a sale decision based on misrepresenting information, providing false information, withholding key information, intentionally offering bad advice, or offering or acting on inside information. The following types of securities fraud are a few examples:

- Manipulating stock prices
- Insider trading of securities
- Falsifying required regulatory reporting to authorities
- Falsifying accounting reports
- Third-party misrepresentation

Smuggling

A smuggling incident involves an individual or a group that acts in an organized and systemic manner and that attempts, commits, or conspires to knowingly, willfully, and intentionally bring items into, or remove items from, a country or to facilitate the transportation, concealment, or sale of such items after importation to avoid taxation, obtain goods that are prohibited by a certain region, or for material, financial gain.

Excluded Incidents

- Smuggling incidents such as an individual who smuggles a prohibited object as a souvenir when returning from a trip
- Smuggling incidents that lack a clear pattern of abuse or material financial motive

Stolen Property

A stolen property incident involves an individual or a group that attempts, commits, or conspires to receive, hold or possess, transport, distribute, or sell goods, in an organized and systemic manner, with the knowledge that they have been acquired by theft, larceny, robbery, or other unlawful means.

Included Incidents

Stolen property incidents that involve the systemic and organized possession, receipt, transport distribution, or sale of stolen property

These incidents are limited to incidents of stolen property with clear evidence of financial gain with an alleged risk of the illicit flow or transfer of funds through the financial system.

Excluded Incidents

- Minor thefts by an individual
- Incidents where an entity did not know or could not have reasonably known that the goods were stolen

Tax Evasion

A tax evasion incident involves an individual or a group that attempts, commits, or conspires to engage in a systemic and organized scheme to facilitate the intentional and fraudulent underpayment or non-payment of taxes by deliberately withholding information or misrepresenting or concealing the nature of financial affairs to the tax authorities to reduce or completely eliminate tax liability.

Included Incidents

- Tax evasion that demonstrates an illegal scheme to avoid paying taxes
- Tax evasion that demonstrates a pattern of avoiding tax payments
- Tax evasion that demonstrates a risk of the illicit flow or transfer of funds through the financial system or a heightened risk of abuse of the financial system

Excluded Incidents

Tax evasion that does not demonstrate an organized or systemic approach, such as a single instance of failure to file a federal tax return

Terrorism

Terrorism, or more accurately political violence, is a complicated social and political phenomenon and there is no single accepted definition. For example, in some countries, the law characterizes terrorist acts that are carried out within the state as domestic extremism. Similarly, the motivations for an individual's or group's violent acts may involve ideological, separatist, ethnic, religious, or state-sponsored aims. LexisNexis Risk Solutions recognizes the complexity of identifying terrorist activities and the individuals or groups that perpetrate these acts. LexisNexis Risk Solutions uses the following core criteria to identify terrorist acts:

- The use of physical or coercive violence
- The use of these acts is to install fear
- The use of these means to effect government or international organization policies or actions that further certain political or social causes
- The acts are perpetrated by individuals or organized groups

LexisNexis Risk Solutions uses the following core criteria to identify the groups that are involved in terrorist acts:

- The group is recognized by a government or international organization.
- The group attempts, commits, or conspires to engage in the unlawful use of physical violence or the threat of violence (coercion) or intimidation.
- The group's actions involve acts that are dangerous to human life against civilian persons, government officials, or the destruction of property.
- The group acts within a single country or across sovereign borders and territories.
- The group acts to influence or affect the policies or actions of government or international organization or populations.
- The group acts in the furtherance of certain political or social objectives.

LexisNexis Risk Solutions uses the following core criteria to identify the individuals who are involved in terrorist acts:

- The individual is a known member of a group that has been recognized by a government or international organization.
- The individual's group has publicly claimed the individual to be associated with the organization and acting on its behalf.
- The individual's group attempts and conspires to engage in the unlawful use of physical violence or the threat of violence (coercion) or intimidation.
- The individual's group's actions involve acts that are dangerous to human life against civilian persons, government officials, or the destruction of property.
- The individual's group acts within a single country or across sovereign borders and territories.
- The individual's group acts to influence or affect the policies or actions of governments or international organizations or population.
- The individual's group acts in the furtherance of certain political or social objectives.

Included Incidents

LexisNexis Risk Solutions recognizes the seriousness of LWAs (lone wolf attack), which are attacks or actions by individuals who are not officially connected to, or acting on behalf of, a state-recognized terrorist organization. These individuals are not supported materially, monetarily, or otherwise by a recognized terrorist organization, but they are inspired by the terrorist group's ideology or aims. These individuals decide on their own to act in the organization’s name.

Terrorism acts include acts that are perpetrated within the United States that are legally classified as domestic extremism, which include an individual who acts alone or with accomplices according to the above criteria and who may not hold an affiliation with a foreign terrorist group.

Excluded Incidents

- Incidents that do not include a political or social motivation and that do not intend to affect the policies or actions of government or international organizations
- Incidents that are motivated by domestic violence or personal grudges or vendettas

War Crimes

A war crime incident involves an individual or a group that has been indicted, wanted, accused, or charged by a national government or international organization or judiciary body and that attempts, commits, or conspires to violate the laws, treaties, customs, or practices that govern military or armed conflict between international and non-international states or parties. War crimes may be committed by government armed forces, irregular armed forces (guerrillas and insurgents), military and political leaders, members of the judiciary, or industrialists. The following war crimes are a few examples:

- Atrocities or offenses against person or property
- Murder, ill treatment, or deportation to slave labor of a civilian population in an occupied territory
- Murder or ill treatments of prisoners of war or persons on the seas
- Killing of hostages
- Biological experiments
- Plunder
- Wanton destruction of cities, towns, or villages
- Devastation that is not justified by military necessity

Wire Fraud

A wire fraud incident involves an individual or a group that attempts, commits, or conspires to engage in a systemic and organized scheme that uses communications (for example, postal mail, telephone calls, fax machines, television, wire, or radio) to obtain money or property by means of false or fraudulent pretenses, representations, promises, or transmissions for the purpose of financial gain.

Included Incidents

Mail fraud

WMD (Weapons of Mass Destruction)

A weapons of mass destruction incident involves an individual or a group that attempts, commits, or conspires to unlawfully manufacture, possess, sell, deliver, display, use, threaten to use, or make readily accessible to others CBRN (chemical, biological, radiological, or nuclear) weapons or high explosives that are capable of a high order of destruction or of being used in such a manner as to destroy large numbers of people, cause death or serious physical harm to a large number of humans, or cause mass destruction to human-made structures (for example, buildings), natural structures (for example, mountains), or the biosphere. WMDs are also known as ABC (atomic, biological, or chemical) weapons.

Enforcement Segment

Enforcement information originates from monitoring material that is published by official government agencies, industry regulators, and disciplinary boards for events that meet the qualifying standards and definitions.

WorldCompliance researchers apply an `Enforcement` segment to the data to indicate that an official government agency has taken action against the entity.

WorldCompliance researchers also apply at least one of the following subcategories:

Administrative

An administrative incident involves a communication by a regulatory authority against an individual or entity as a result of misconduct, legal violations, or fiduciary duty breaches. These violations resulted in an investigation, warning, or notice that does not include a fine or carry a temporary prohibition or permanent prohibition to conduct business or fulfill the duties of office. These violations include warnings for late filings or disclosures of financial information to regulatory bodies.

Aircraft Hijacking

An aircraft hijacking incident involves an individual or a group (including accomplices) that unlawfully attempts, commits, or conspires to seize, takeover, or exercise control of an in-transit, government or commercial common-carrier aircraft with wrongful intent or by force, violence, threat of force or violence, or any form of intimidation. Aircraft hijacking incidents can include acts in connection with or in furtherance of terrorism, terrorism financing, money laundering, organized crime, political asylum, hostage taking, or political or administrative concession by authorities.

Excluded Incidents

- Private aircraft theft
- Truck hijacking
- Carjacking
- Maritime piracy

Antitrust violations

An antitrust violation incident involves an entity that attempts, conspires, or commits violations to acts or laws that are intended to promote fair competition that protects commerce and trade from abusive business practices. These incidents include national regulatory agencies or law enforcement agencies with jurisdictional claims over both domestic and foreign conduct and domestic and foreign parties. Abusive business practices can include the following examples:

- Unfair competition (such as mergers, acquisitions, or takeovers of one firm by another if the effect will substantially lessen competition)
- Restraint of trade
- Monopolies
- Price-fixing
- Price discrimination
- Market-dividing
- Interlocking directorates (an individual who makes business decisions for competing companies)
- Bid-rigging

Excluded Incidents

- Private antitrust actions
- Natural persons who are associated with the subject entity, unless they are specifically accused or charged with wrongdoing
- Private anti-trust actions
- Antitrust disputes brought to the World Trade Organization

Arms Trafficking

An arms trafficking incident involves an individual or a group that attempts, commits, or conspires to divert contraband weapons, munitions, or explosives from lawful commerce into the illegal market by way of direct purchase, trade, dealing, or smuggling in contravention of international laws and regulations, the prescribed laws of the subject legal jurisdiction, or in violation of any extraterritorial laws to which the entity is subject. These efforts can include acts in furtherance of political destabilization, terrorism, civil war, regional conflicts, extra-judicial paramilitary activity, organized crime, or in connection with other related AML predicate offenses that demonstrate an elevated risk of abuse of the financial system.

Excluded Incidents

- Illegal or unauthorized weapons possession
- Incidents that lack evidence of an organized pattern of abuse, conspiracy, or financial motive (for example, a single instance of an illicit gun sale through a straw purchaser)

Asset Freeze

An asset freeze incident involves a government or court action that restricts, suppresses, or confiscates an entity's financial assets, funds, economic resources, or non-financial assets to ensure that these funds are not made available, directly or indirectly, for the entity’s benefit, by persons that act on their behalf, or at their direction within or outside of the issuing authority's jurisdiction. Asset freezes are frequently included in “smart sanctions” or “targeted sanctions” strategies.

Bank Fraud

A bank fraud incident involves an individual or a group that knowingly attempts, commits, or conspires to execute an organized and systemic plan, scheme, or con to defraud a financial institution or to obtain any of the moneys, funds, credits, assets, securities, or other property that is owned by, or under the custody or control of, a financial institution by means of false or fraudulent pretenses, representations, or promises.

Excluded Incidents

- NSF (non-sufficient funds)
- Bank fraud that does not demonstrate an organized and systemic attempt to defraud a financial institution

Bribery

A bribery incident involves an individual or a group that attempts, commits, or conspires to offer, give, receive, or solicit currency or something of value to a national or foreign government official, a private individual, or a person in charge of a public, legal, or fiduciary duty to influence or directly alter the person's or group's actions for the following purposes:

- Disobey or avoid complying with international or national laws and regulations or local or extraterritorial laws to which the entity may be subject.
- Encourage an entity to perform a service to which the payer is entitled even without the payment, also known as facilitation payments or grease payments.

Included Incidents

- Participation in, or association with, the conspiracy to commit, attempt to commit, aid and abet, facilitate, or counsel the commission of the event
- United Kingdom: facilitation payments

Excluded Incidents

- The private demonstration of good will
- Campaign donations from corporations or individuals to political candidates (the relationship does not occur directly enough) consistent with the approved activity within the subject jurisdictions
- The customary giving and receiving of gifts of limited monetary value as prescribed by law
- Circumstances where a payment, gift, offer, or promise of anything of value to a foreign official may qualify as an affirmative defense
- A payment, gift, offer, or promise of anything of value that is lawful under the written laws and regulations of the foreign official's, political party's, party official's, or candidate's country
- A payment, gift, offer, or promise of anything of value that is a reasonable and legal expenditure
- Events that are consistent with approved activity within the subject jurisdictions

  These events can include the customary giving and receiving of gifts of limited monetary value as prescribed by law.
- A payment, gift, offer, or promise of anything of value that is directly related to the promotion, demonstration, or explanation of products or services or that are directly related to the execution or performance of a contract with a foreign government or agency (for example, travel and lodging expenses)
- Conduct that is considered a routine "governmental action" exception by the FCPA

  Routine governmental actions include the following actions that are ordinarily and commonly performed by a foreign official:
  - Obtain permits, licenses, or other official documents to qualify a person to do business in a foreign country.
  - Process governmental papers such as visas or work orders.
  - Provide police protection.
  - Provide mail pick-up and delivery.
  - Schedule inspections that are associated with contract performance or inspections that are related to the transit of goods across the country.
  - Provide telephone service.
  - Provide power and water supply.
  - Load and unload cargo.
  - Protect perishable products or commodities from deterioration.

Burglary

A burglary incident involves an individual or a group that attempts, commits, or conspires to unlawfully enter a structure with the intent to commit a crime to further terrorism, terrorism financing, illicit flows in the financial system, money laundering, organized crime, corruption, hostage taking, or other related AML predicate offenses.

Excluded Incidents

Burglaries that are not part of an organized or systemic plan or scheme that are unlikely to involve the illicit flow or transfer of funds through the financial system

Conspiracy

A conspiracy incident involves an agreement, plan, or scheme that involves an overt act between two or more people that is formed for the purpose of committing, by their joint efforts, an illegal or criminal act in connection with, or in furtherance of, criminal acts that are connected to terrorism, terrorism financing, money laundering, organized crime, political or administrative concession by authorities, or other related AML predicate offenses.

Excluded Incidents

Conspiracies that are not in furtherance of a predicate offense or that are unlikely to involve the illicit flow or transfer of funds through the financial system

Corruption

A corruption incident involves a public official, a private citizen, or a fiduciary that attempts, conspires, or commits an illegal or wrongful act to facilitate an abuse of the powers and influence that are afforded to their office or station to procure a financial benefit or other type of benefit for themselves or for another person, so that both parties, or a single individual, can disobey or avoid complying with international or national laws and regulations or local or extraterritorial laws to which the entity may be subject.

There are many forms of corruption that may involve public-private or public-public relationships. The following types of corruption are a few examples:

- Grand corruption is the act by a group or an individual at the highest levels of government that alter, misrepresent, or distort policies or the central functioning of the state or that require significant erosion of the legal, political, and economic systems to enable leaders to benefit at the expense of the public good.
- Petty corruption is the abuse of power that involves the exchange of very small amounts of money or the granting minor favors for preferential treatment.

Excluded Incidents

Events that are consistent with the approved activity within the subject jurisdictions

These events can include the customary giving and receiving of gifts of limited monetary value as prescribed by law.

Counterfeiting

A counterfeiting incident involves an individual or a group that attempts, commits, or conspires to copy, imitate, or alter an item to increase the value or to reproduce an item without authorization with the intent to present or use the copy as the genuine or original item. An item can include the following examples:

- Obligations and securities
- Currency
- Documents that are issued by government agencies or international organizations
- Bonds
- Bids
- Contracts
- Proposals
- Public records
- Affidavits
- Federal court documents
- Seals of government agencies or international organizations

Excluded Incidents

Counterfeiting not in connection with or in furtherance of terrorism, terrorist financing, money laundering, organized crime, political or administrative concession by authorities, or other related AML predicate offenses or that are unlikely to involve the illicit flow or transfer of funds through the financial system

Crimes Agnst Humanity (Crimes Against Humanity)

A crime against humanity incident involves an individual or a group that knowingly attempts, commits, or conspires to conduct or participate in a widespread or systematic attack against a civilian population as directed by an organization, group, government, state military, or paramilitary. The following acts are examples of crimes against humanity when acknowledged by an authoritative institution such as a government, the UN, or the EU:

- Apartheid involves acts that are committed in the context of an institutionalized regime or systematic oppression and domination by one racial group over any another racial group or groups and that are committed with the intention of maintaining that regime.
- The deportation or forcible transfer of a population is the forced displacement of persons by expulsion or other coercive acts from the area in which they are lawfully present without grounds that are permitted under national law.
- An enforced disappearance is the arrest, detention, or abduction of persons by, or with the authorization or support of, a state or political organization and a refusal to acknowledge the deprivation of freedom or provide information on the fate or whereabouts of those persons with the intention of removing them from the protection of the law for a prolonged period of time.
- Enslavement is the exercise of any or all powers in the right of ownership to a person (for example, human trafficking).
- Extermination is the intentional infliction of conditions of life that is calculated to bring about the destruction of a population in whole or in part. Inflictions can include the deprivation of access to food and medicine or the deprivation of reproductive capacities.
- Genocide involves acts that are designed and committed with the intent to bring about the destruction of a group in whole or in part.
- Murder is the killing of another human being.
- Persecution involves acts against an identifiable group on political, racial, national, ethnic, cultural, or religious or gender grounds.
- Sexual violence can include rape, sexual slavery, or any other form of sexual violence of comparable gravity.
- Torture is the intentional infliction of severe mental or physical pain or suffering.

Cybercrime

A cybercrime incident involves an individual or a group that unlawfully attempts, commits, or conspires to use the internet, electronic communications networks, or information systems in an organized and systemic manner as a tool to conduct fraudulent transactions, theft of data for financial gain, prohibit transactions, or transmit the proceeds of fraud to financial institutions or to others that are connected with the scheme in furtherance of terrorism, terrorism financing, money laundering, organized crime, corruption, hostage taking, or other related AML predicate offenses.

Excluded Incidents

- Cybercrimes that are not likely to involve the illicit flow or transfer of funds through the financial system or a heightened risk of abuse of the financial system
- Cybercrimes that involve software piracy for personal use

Debarred

A debarred incident involves an entity that has been officially prohibited, excluded, or banned by a regulatory agency or professional trade organization from the following activities:

- Practicing a profession
- Associating with persons of a particular profession
- Conducting business with a governmental or transnational organization
- Enjoying certain privileges, memberships, or practices
- Participating in specified business transactions, dealings, or contracts

Disciplined

A disciplined incident involves incidents where a regulatory authority has imposed a fine, suspension, cease and desist order, or other forms of temporary or permanent corrective action that was a result of violating a code or law or engaging in improper practices or unlawful business activities.

Disqualified

A disqualified incident involves an entity that has been declared permanently or temporarily ineligible, unfit, or unqualified in their current position or has been deprived of their legal, official, or other rights or privileges, or categorized as “disqualified” specifically by a regulatory authority, which may be the result of misconduct, legal violations, or fiduciary duty breaches in a specified jurisdiction.

Drug Trafficking

A drug trafficking incident involves an individual or a group that attempts, commits, or conspires to engage in organized and systemic illicit trade that involves the cultivation, manufacture, distribution, sale, importation, exportation, or dispensation of substances which are subject to drug prohibition or controlled distribution laws. These incidents can include acts in conjunction with or in furtherance of political destabilization, terrorism, civil war, regional conflicts, extra-judicial paramilitary activity, organized crime, or in connection with other related AML predicate offenses that demonstrate an elevated risk of abuse of the financial system.

Excluded Incidents

- Mere possession of a substance subject to drug prohibition
- Funds that are transferred or activities in connection with medical marijuana or recreational marijuana in jurisdictions which have authorized or decriminalized commercial commerce
- Incidents that lack evidence of an organized pattern of abuse, conspiracy, or material financial motive

  (for example, a single instance of a small quantity of drugs that fails to demonstrate evidence of an organized scheme of "distribution for profit")
- Incidents that are unlikely to involve the illicit flow or transfer of funds through the financial system

Embezzlement

An embezzlement incident involves an individual or a group that attempts, commits, or conspires to misappropriate personal or government financial assets from entities that have been lawfully entrusted with the care of the assets or by the entrusted entities themselves (for example, employee, clerk, agent, trustee, public officer, or other person that acts in a fiduciary character) to covertly and fraudulently convert these assets for their own use or benefit or transfers the assets to a third party for their own use and benefit.

End Use Control

An end use control incident involves an entity that is associated with dual-use (items that have both commercial and military or proliferation applications) and military hardware or technology exports whose sale and trade pose an elevated risk of violating non-proliferation regulations and sanctions. End users are entities that are abroad that receive and ultimately use exported and re-exported items and that may not be the forwarding agent or intermediary, but may be the purchaser or ultimate buyer or financier.

The following lists are examples of the military end-use export control lists that may list these entities:

- U.K. Export Control Organization's End-Use Controls list
- Japan's Ministry of Economy, Trade and Industry End-User list
- U.S. Export Administration Regulations list

Environmental Crimes

An environmental crime incident involves an individual or a group that attempts, commits, or conspires to systemically and willfully engage in illegal acts that directly harm the environment and aim at benefiting individuals or groups or organizations from the exploitation of, damage to, or trade or theft of natural resources. These acts are in contravention of international environmental laws and regulations, the prescribed environmental laws of the subject legal jurisdiction, or in violation

of any extraterritorial laws to which the entity is subject with the willful intent to secure material financial advantage through profit or cost avoidance from the activity. These incidents can include the following acts:

- Dumping industrial wastes into water bodies
- Illicit trading in hazardous waste
- Trafficking endangered species or government-protected environmental goods
- Smuggling of Ozone-depleting substances
- Illegal logging and trade of stolen timber in violation of the wildlife laws

Excluded Incidents

- Instances of neglect or instances that do not demonstrate a financial incentive
- Lacey Act violations

Espionage

An espionage incident involves an individual or a group that attempts, commits, or conspires to secretly gather political, military, or economic information about a foreign or domestic government or commercial enterprise for the purpose of placing one's own government or corporation at some strategic or financial advantage. This information includes trade secrets from a private enterprise.

Excluded Party

An excluded party incident involves an individual or a business that is subject to administrative and statutory exclusions across the United States government and is excluded from receiving federal contracts, certain federal subcontracts, or certain federal financial and non-financial assistance and benefits. These entities may already have been debarred or suspended from practice by a government agency or professional association, under investigation for legal violations, or under criminal indictment (for example, entities that are listed on the Excluded Party List Systems).

Explosives

An explosives incident involves an individual or a group that attempts, commits, or conspires to perpetrate an organized or systemic criminal act that involves explosives or other destructive devices in connection with or in furtherance of terrorism, terrorism financing, money laundering, organized crime, political asylum, hostage taking, political or administrative concession by authorities, or other acts for financial gain. These acts can include possessing, importing, manufacturing, transferring, transporting, or dealing in explosive materials without a license. A destructive device can include any explosive, incendiary, or poison gas, bomb, grenade, rocket, mine, or missile.

Extort-Rack-Threats (Extortion, Racketeering, or Threats)

An extortion incident involves an individual or a group that attempts, commits, or conspires to obtain money, property, or services from a person or institution in an organized and systemic manner through a pattern of illegal activity that employs the wrongful use of physical or threatened force,

violence, fear, property damage, damage to the person's reputation, extreme financial hardship, or under cover of unfavorable government action. Extortion involves obtaining consent through these illegal coercive actions that remove the victim's free will.

Financial Crimes

A financial crime incident involves an individual or a group that attempts, commits, or conspires to unlawfully convert money or property with the intent to gain personal benefit. These incidents include financial crimes that are not covered by another financial subcategory. The following financial crimes are a few examples:

- White-collar crimes (for example, bankruptcy fraud, illicit payments)
- Systemic and organized financial crime
- Illegally obtaining banking information
- Trade secret fraud
- Structuring financial translations (also known as smurfing)
- Loan sharking or usury
- Skimming
- Financial crimes that are likely to involve the illicit flow or transfer of funds through the financial system
- Financial crimes in conjunction with or in furtherance of money laundering, political destabilization, terrorism, terrorist financing, civil war, regional conflicts, extra-judicial paramilitary activity, organized crime, or in connection with other related AML predicate offenses that demonstrate an elevated risk of abuse of the financial system

Forgery

A forgery incident involves an individual or a group that attempts, commits, or conspires to alter or replicate an original document or write a false signature with the intent to defraud for the illegal benefit of the person or persons who committed the forgery. Forgery must demonstrate an organized and systemic scheme in connection with or in furtherance of terrorism, terrorism financing, money laundering, organized crime, political asylum, political or administrative concession by authorities, or other related AML predicate offenses with willful purpose of financial gain. These incidents can include the forgery of checks, stamps, or artwork.

Fraud

A fraud incident involves an individual or a group that operates in an organized and systemic manner to intentionally or knowingly attempt, conspire, or commit to misrepresenting a material, existing fact or deceiving an entity that relies on the misrepresentation in order to deprive the entity of its money, property, or legal right. These incidents include fraud that is not covered by another subcategory.

Excluded Incidents

Fraud for personal gain without financial involvement or that is unlikely to involve the illicit flow or transfer of funds through the financial system

Fugitive

A fugitive incident involves a person who flees a jurisdiction or prison to avoid arrest, prosecution for a crime, imprisonment, or to avoid giving testimony in any criminal proceeding.

Excluded Incidents

Fugitives whose alleged activity does not meet the prescribed definition of other risk categories in the database

Gambling Operations

A gambling operation incident involves an individual or a group that attempts, commits, or conspires to conduct, finance, manage, supervise, direct, or own all or part of an illegal, organized, gambling business. This business may be done in furtherance of organized crime, terrorism financing, or other related AML predicate offense. These gambling operations demonstrate an organized and systemic approach that are likely to involve the illicit flow or transfer of funds through the financial system or a heightened risk of abuse of the financial system. Gambling operations is also known as illegal gaming.

Excluded Incidents

- Gambling operations that are not organized and systemic
- Gambling operations that are unlikely to involve the illicit flow or transfer of funds through the financial system or a heightened risk of abuse of the financial system

Healthcare Fraud

A healthcare fraud incident involves an individual or a group that operates in an organized and systemic matter that attempts, commits, or conspires to execute a scheme or a hoax to defraud any healthcare benefit program or insurer or to obtain by means of false or fraudulent pretenses,

representations, or promises any of the money or property owned by, or under the custody or control of, any healthcare benefit program or insurer. The following practitioner schemes are a few examples:

- Obtaining subsidized or fully covered prescription pills that are unneeded and then selling them on the black market for a profit
- Billing by practitioners for care that they never rendered
- Filing duplicate claims for the same service rendered
- Altering the dates, description of services, or identities of members or providers
- Billing for a non-covered service as a covered service
- Modifying medical records
- Intentional incorrect reporting of diagnoses or procedures to maximize payment
- Accepting or giving illicit payments for member referrals
- Waiving member co-pays
- Prescribing additional or unnecessary treatment
- Providing false information when applying for programs or services
- Forging or selling prescription drugs

Excluded Incidents

- Healthcare fraud that does not demonstrate an organized and systemic approach
- Healthcare fraud that involves innocent misrepresentations

Human Rights Abuse

A human rights abuse incident involves an individual or a group that attempts, commits, or conspires to violate basic human rights and freedoms that fundamentally and inherently belong to an individual. Human rights are established by international agreement, convention, custom, or national law acts when acknowledged by an authoritative institution. These institutions include government agencies, the UN, the EU, non-governmental organizations that work in these areas, and credible open-source media. These events can include acts in furtherance of political destabilization,

terrorism, civil war, regional conflicts, organized crime, or in connection with other related AML predicate offenses that demonstrate an elevated risk of abuse of the financial system. The following human rights are a few examples:

- The right to life
- The freedom from torture
- The right to a fair trial
- The right to freedom of assembly and association (for example, membership or formation of political parties or trade unions)
- The freedom of religion, expression, security, and asylum
- The freedom from slavery or servitude
- The freedom from arbitrary arrest, detention, or exile

Human Trafficking

A human trafficking incident involves an individual or a group that attempts, commits, or conspires in the recruitment, transportation, transfer, harboring, or receipt of persons by means of the following acts for the purpose of exploitation or commercial gain:

- Threat or use of force or other forms of coercion
- Abduction
- Deception
- Fraud
- Abuse of power or of a position of vulnerability
- Giving or receiving of payments or benefits to achieve the consent of a person who has control over another person

Exploitation can include prostitution of others, other forms of sexual exploitations, forced labor services, servitude, slavery or practices similar to slavery, or the removal of organs.

Insider Trading

An insider trading incident involves an individual or a group that attempts, commits, or conspires to buy or sell a security while in possession of, or having access to, material, private, confidential, or non-public information about the security in breach of a fiduciary duty or other relationship of trust and confidence.

Insurance Fraud

An insurance fraud incident involves an individual or a group that attempts, commits, or conspires to perform a duplicitous act in a systemic and organized scheme with the intent to obtain an improper payment from an insurer. These incidents include the following fraud schemes:

- Hard fraud occurs with the deliberate destruction of property for the purpose of collecting on the insurance policy.
- Soft fraud occurs when a policyholder exaggerates an otherwise legitimate claim or when an individual applies for an insurance policy and lies about certain conditions or circumstances to lower the policy's premium.

Interstate Commerce

An interstate commerce incident involves an individual or a group that attempts, commits, or conspires to unlawfully purchase, sell, or exchange of commodities, money or goods through transport by land or water in contravention of interstate laws and regulations, the prescribed laws of the subject legal jurisdiction, or in violation of any extraterritorial laws to which the entity is subject. Interstate commerce includes the movement of goods and services across U.S. state borders.

ISIS Foreign Support

ISIS Foreign Support incidents include an individual or a business with a recognized affiliation with ISIS (Islamic State in Iraq and Syria) or ISIS groups that provides material support to ISIS through means that violate state anti-terrorism laws. The following actions are a few examples of material support:

- Donating, soliciting, or providing financial resources to ISIS operations
- Facilitating material support in the form of military equipment, recruitment, illicit trade, and smuggling
- Conducting attacks as a member of the organization
- Conducting attacks in the name of the organization even without material support (also known as LWA or a lone wolf attack)

  LWAs are defined as attacks or actions by individuals who are not officially connected to, or acting on behalf of, a state-recognized terrorist organization. LWAs are not supported monetarily or otherwise by ISIS. These individuals are inspired by these organizations and decided on their own to act in the name of ISIS.

Foreign supporters are also defined as ISIS members who take the following actions:

- Carrying out or support attacks on their own countries in support of the Islamic State
- Providing means of support, such as, voice overs on ISIS-produced videos, video technical support, managing content on ISIS-owned websites, or procurement of resources and services for the benefit of ISIS groups

Kidnapping

A kidnapping incident involves an individual or a group that attempts, commits, or conspires to unlawfully seize and carry away a person against their will, by force or fraud, with the intent to hold for ransom or reward, use as a hostage, accomplish or aid in the commission of a felony or flight from a felony, inflict physical harm, violate or abuse sexually, terrorize, or interfere with the performance of any governmental or political function. Kidnapping is also known as abduction.

Excluded Incidents

- Parental kidnapping
- Kidnapping that does not demonstrate a financial motive or an organized and systemic approach
- Kidnapping that is not in furtherance of terrorism, terrorism financing, money laundering, organized crime, hostage taking (ransom), political or administrative concession by authorities, or other related AML predicate offenses

Labor Violations

A labor violation incident involves an individual or a group that attempts, commits, or conspires to violate labor laws that define the rights of employees and protect them from employer retaliation for exercising those legal rights or reporting violations to the proper authorities.

These violations can include the following acts:

- Interfering or restraining employees in the exercise of their rights
- Dominating or interfering with the formation or administration of any labor organization
- Discriminating in regards to the hiring or tenure of employment
- Encouraging or discouraging membership in a labor organization
- Refusing to collectively bargain with the representatives of employees
- Violating child labor laws
- Violating labor laws in a way that demonstrates a willful intent to secure material financial advantage
- Violating labor laws in a way that likely involves the illicit flow or transfer of funds through the financial system or a heightened risk of abuse of the financial system

Excluded Incidents

- Labor violations that are unlikely to involve the illicit flow or transfer of funds through the financial system
- Civil claims of labor violations

Money Laundering

A money laundering incident involves an individual or a group that attempts, commits, or conspires to engage in any act or scheme that aims to conceal or disguise the identity, source, and destination (also known as placement, layering, and integration) of illegally obtained proceeds so that they appear to have originated from legitimate or legal sources.

Mortgage Fraud

A mortgage fraud incident involves an individual or a group that operates in an organized and systemic manner that intentionally and knowingly provides any material misstatement, misrepresentation, or omission of information that an underwriter or lender must use to fund, purchase, or insure a loan. The following types of fraud are a few examples:

- Fraud for profit involves an organized, systemic, and elaborate scheme that usually involves collusion among many persons such as a mortgage broker or loan processor and that is committed through single or multiple loans or transactions to gain illicit proceeds from property sales. Fraud for profit is also known as industry insider fraud.
- Fraud for criminal enterprise involves the purchase of real estate with illegally obtained funds (for example, drug activity) to clean or "launder" the money so that the money appears to be obtained by legal means.
- Fraud for property involves deliberate misrepresentations of income, assets, or debt to obtain a mortgage or more favorable terms for the purpose of purchasing a property for primary residence. Fraud for property is also known as fraud for housing.

Most Wanted

A most wanted incident involves a highly sought-after entity on a Most Wanted List that is sought by law enforcement in connection with an investigation of a crime that has been committed in connection with or in furtherance of political destabilization, terrorism, terrorism financing, money laundering, political asylum, hostage taking, and political or administrative concession by authorities, civil war, regional conflicts, extra-judicial paramilitary activity, organized crime, or in connection with other related AML predicate offenses that demonstrate an elevated risk of abuse of the financial system.

Excluded Incidents

Entities that are sought after for crimes not in connection with or in furtherance of political destabilization, terrorism, terrorism financing, money laundering, political asylum, hostage taking, and political or administrative concession by authorities, civil war, regional conflicts, extrajudicial paramilitary activity, organized crime, or in connection with other related AML predicate offenses that demonstrate an elevated risk of abuse of the financial system

These incidents do not include any entities on monitored Most Wanted Lists.

Murder

A murder incident involves an individual or a group that attempts, commits, or conspires to unlawfully kill a natural person with intent, malice aforethought, and with no legal authority or excuse in furtherance of terrorism, terrorism financing, money laundering, organized crime, political asylum, hostage taking, political or administrative concession by authorities, or other related AML predicate offenses.

Excluded Incidents

- Crimes of passion
- Murder that is not in connection with or in furtherance of money laundering, terrorism, terrorist financing, money laundering, organized crime, hostage taking, political or administrative concession by authorities, or other related AML predicate offenses
- Murder that does not demonstrate an organized and systemic approach

N/A (Not Applicable)

The N/A subcategory is applied when an enforcement action should be included, but the action cannot be categorized into another subcategory.

Organized Crime

An organized crime incident involves a group of three or more persons that act in concert within a formalized structure and that attempt, commit, or conspire to engage in long-term criminal activities in a systematic manner to obtain, directly or indirectly, a financial or other material benefit through illegal activities in one or more illegal economic sectors in one or more jurisdictions.

Included Incidents

- Organized crime that demonstrates a planned, systematic nature of criminal activity that range from national to international in scale
- Organized crime that is likely to involve the illicit flow or transfer of funds through the financial system or demonstrate a heightened risk of abuse of the financial system
- Organized crime in connection with or in furtherance of terrorism, terrorist financing, money laundering, hostage taking, political or administrative concession by authorities, or other related AML predicate offenses

Excluded Incidents

- Organized crime that is unlikely to involve the illicit flow or transfer of funds through the financial system
- Organized crime that is politically motivated terrorism, rather than profit driven
- Organized crime that does not demonstrate a heightened risk of abuse of the financial system

Peonage

A peonage incident involves an individual or a group that attempts, commits, or conspires to enforce servitude upon an individual against their will by restraining their liberty (freedom from restraint is the ability to decide for one's self, or free will) and compelling them to labor in payment of a debt or obligation (real or pretended). Peonage is also known as debt servitude or debt slavery.

Pharma Trafficking (Pharmaceutical Products Trafficking)

An incident of pharmaceutical products trafficking involves an individual or a group that attempts, commits, or conspires to engage in the manufacture, trade, transport, and distribution of fake, stolen, or illicit medicines and medical devices in an organized and systemic manner in contravention of international laws and regulations, the prescribed laws of the subject legal jurisdiction, or in violation of any extraterritorial laws to which the entity is subject.

Excluded Incidents

- A single instance of selling pharmaceutical products
- Small-scale prescription drug sales

Piracy

A piracy incident involves an individual or a group that attempts, commits, or conspires to engage in any criminal act of violence, detention, or depredation. These acts are perpetrated by the crew or the passengers of a private ship or aircraft that is directed on the high seas, against another ship, aircraft, or against persons or property committed for private benefit. These acts include incidents that are outside a state's sovereign maritime borders, and are applicable under universal jurisdiction where states or international organizations can claim criminal jurisdiction of an accused person or group regardless of where the alleged crime was committed.

Included Incidents

- Maritime piracy in international waters
- Piracy incidents that involve vessels at sea or on a river

Pollution

A pollution incident involves an individual or a group that attempts, commits, or conspires in an organized and systemic manner to wrongfully contaminate the atmosphere, soil, or water with harmful or potentially harmful substances to secure a material financial advantage through profit or cost avoidance that are likely to have an adverse effect on the natural environment or life. Pollution incidents also include incidents with the willful intent to secure material financial advantage through profit or cost avoidance from the activity or are determined by the courts to be criminally negligent acts.

Pornography

A pornography incident involves an individual or a group that attempts, commits, or conspires to engage in the organized and systemic and unlawful production, sale, or distribution of scenes (represented through books, magazines, photographs, films, or other media) of sexual behavior that is designed to arouse sexual interest in contravention of international laws and regulations or in violation of any extraterritorial laws to which the entity is subject, specifically as they relate to incidents in connection with or in furtherance of child endangerment, human trafficking, bribery, or other related AML predicate offense.

Price Manipulation

A price manipulation incident involves an individual or a group that attempts, commits, or conspires to deliberately attempt to interfere with the free and fair operation of the legitimate economy and financial system to create a misleading price or market for currencies, commodities, or securities with the intent of securing a financial or other material benefit for themselves or others in one or one or more jurisdictions.

RICO (Racketeer Influenced and Corrupt Organizations)

A RICO incident involves an individual or a group that attempts, commits, or conspires to violate the RICO Act by engaging in a pattern of wrongdoing (for example, racketeering or AML predicate offenses) as a member of a criminal enterprise or organization. Although this law is specific to the United States, LexisNexis Risk Solutions recognizes international equivalent violations in contravention of international laws and regulations or in violation of any extraterritorial laws to which the entity is subject.

Securities Fraud

A securities fraud incident involves an individual or a group that attempts, commits, or conspires to defraud, deceive, or induce investors in an organized and systemic manner to make a purchase or a sale decision based on misrepresenting information, providing false information, withholding key information, intentionally offering bad advice, or offering or acting on inside information. The following types of securities fraud are a few examples:

- Manipulating stock prices
- Insider trading of securities
- Falsifying required regulatory reporting to authorities
- Falsifying accounting reports
- Third-party misrepresentation

Smuggling

A smuggling incident involves an individual or a group that acts in an organized and systemic manner and that attempts, commits, or conspires to knowingly, willfully, and intentionally bring items into, or remove items from, a country or to facilitate the transportation, concealment, or sale of such items after importation to avoid taxation, obtain goods that are prohibited by a certain region, or for material, financial gain.

Excluded Incidents

- Smuggling incidents such as an individual who smuggles a prohibited object as a souvenir when returning from a trip
- Smuggling incidents that lack a clear pattern of abuse or material financial motive

Stolen Property

A stolen property incident involves an individual or a group that attempts, commits, or conspires to receive, hold or possess, transport, distribute, or sell goods, in an organized and systemic manner, with the knowledge that they have been acquired by theft, larceny, robbery, or other unlawful means.

Included Incidents

Stolen property incidents that involve the systemic and organized possession, receipt, transport distribution, or sale of stolen property

These incidents are limited to incidents of stolen property with clear evidence of financial gain with an alleged risk of the illicit flow or transfer of funds through the financial system.

Excluded Incidents

- Minor thefts by an individual
- Incidents where an entity did not know or could not have reasonably known that the goods were stolen

Tax Evasion

A tax evasion incident involves an individual or a group that attempts, commits, or conspires to engage in a systemic and organized scheme to facilitate the intentional and fraudulent underpayment or non-payment of taxes by deliberately withholding information or misrepresenting or concealing the nature of financial affairs to the tax authorities to reduce or completely eliminate tax liability.

Included Incidents

- Tax evasion that demonstrates an illegal scheme to avoid paying taxes
- Tax evasion that demonstrates a pattern of avoiding tax payments
- Tax evasion that demonstrates a risk of the illicit flow or transfer of funds through the financial system or a heightened risk of abuse of the financial system

Excluded Incidents

Tax evasion that does not demonstrate an organized or systemic approach, such as a single instance of failure to file a federal tax return

Terrorism

Terrorism, or more accurately political violence, is a complicated social and political phenomenon and there is no single accepted definition. For example, in some countries, the law characterizes terrorist acts that are carried out within the state as domestic extremism. Similarly, the motivations for an individual's or group's violent acts may involve ideological, separatist, ethnic, religious, or

state-sponsored aims. LexisNexis Risk Solutions recognizes the complexity of identifying terrorist activities and the individuals or groups that perpetrate these acts. LexisNexis Risk Solutions uses the following core criteria to identify terrorist acts:

- The use of physical or coercive violence
- The use of these acts is to install fear
- The use of these means to effect government or international organization policies or actions that further certain political or social causes
- The acts are perpetrated by individuals or organized groups

LexisNexis Risk Solutions uses the following core criteria to identify the groups that are involved in terrorist acts:

- The group is recognized by a government or international organization.
- The group attempts, commits, or conspires to engage in the unlawful use of physical violence or the threat of violence (coercion) or intimidation.
- The group's actions involve acts that are dangerous to human life against civilian persons, government officials, or the destruction of property.
- The group acts within a single country or across sovereign borders and territories.
- The group acts to influence or affect the policies or actions of government or international organization or populations.
- The group acts in the furtherance of certain political or social objectives.

LexisNexis Risk Solutions uses the following core criteria to identify the individuals who are involved in terrorist acts:

- The individual is a known member of a group that has been recognized by a government or international organization.
- The individual's group has publicly claimed the individual to be associated with the organization and acting on its behalf.
- The individual's group attempts and conspires to engage in the unlawful use of physical violence or the threat of violence (coercion) or intimidation.
- The individual's group's actions involve acts that are dangerous to human life against civilian persons, government officials, or the destruction of property.
- The individual's group acts within a single country or across sovereign borders and territories.
- The individual's group acts to influence or affect the policies or actions of governments or international organizations or population.
- The individual's group acts in the furtherance of certain political or social objectives.

Included Incidents

LexisNexis Risk Solutions recognizes the seriousness of LWAs (lone wolf attack), which are attacks or actions by individuals who are not officially connected to, or acting on behalf of, a state-recognized terrorist organization. These individuals are not supported materially, monetarily, or otherwise by a recognized terrorist organization, but they are inspired by the terrorist group's ideology or aims. These individuals decide on their own to act in the organization's name.

Terrorism acts include acts that are perpetrated within the United States that are legally classified as domestic extremism, which include an individual who acts alone or with accomplices according to the above criteria and who may not hold an affiliation with a foreign terrorist group.

Excluded Incidents

- Incidents that do not include a political or social motivation and that do not intend to affect the policies or actions of government or international organizations
- Incidents that are motivated by domestic violence or personal grudges or vendettas

Unauthorized

An unauthorized incident involves entities that are not officially permitted, approved, or licensed to practice, sell, advise, provide services, or engage in other regulated activity in a specified jurisdiction as reported by a regulatory authority.

War Crimes

A war crime incident involves an individual or a group that has been indicted, wanted, accused, or charged by a national government or international organization or judiciary body and that attempts, commits, or conspires to violate the laws, treaties, customs, or practices that govern military or armed conflict between international and non-international states or parties. War crimes may be committed by government armed forces, irregular armed forces (guerrillas and insurgents), military and political leaders, members of the judiciary, or industrialists. The following war crimes are a few examples:

- Atrocities or offenses against person or property
- Murder, ill treatment, or deportation to slave labor of a civilian population in an occupied territory
- Murder or ill treatments of prisoners of war or persons on the seas
- Killing of hostages
- Biological experiments
- Plunder
- Wanton destruction of cities, towns, or villages
- Devastation that is not justified by military necessity

Wire Fraud

A wire fraud incident involves an individual or a group that attempts, commits, or conspires to engage in a systemic and organized scheme that uses communications (for example, postal mail, telephone calls, fax machines, television, wire, or radio) to obtain money or property by means of false or fraudulent pretenses, representations, promises, or transmissions for the purpose of financial gain.

Included Incidents

Mail fraud

WMD (Weapons of Mass Destruction)

A weapons of mass destruction incident involves an individual or a group that attempts, commits, or conspires to unlawfully manufacture, possess, sell, deliver, display, use, threaten to use, or make readily accessible to others CBRN (chemical, biological, radiological, or nuclear) weapons or high explosives that are capable of a high order of destruction or of being used in such a manner as to destroy large numbers of people, cause death or serious physical harm to a large number of humans, or cause mass destruction to human-made structures (for example, buildings), natural structures (for example, mountains), or the biosphere. WMDs are also known as ABC (atomic, biological, or chemical) weapons.

PEP Segment

The PEP segment contains information about individuals who act in a senior prominent public function, their family members, and associates.

The international community recognizes that PEPs (politically exposed persons) occupy positions that can be abused for the purpose of committing money-laundering offenses and related AML predicate offenses. These offenses include corruption and bribery or activities that are related to terrorist financing. The WorldCompliance PEP (politically exposed person) entity inclusion principles follow the systemic principles that are set by the FATF (Financial Action Task Force) and the Wolfsberg Group. The FATF is an intergovernmental body that sets standards for combating money laundering and terrorism finance. The Wolfsberg Group is an association of global banks that develops frameworks to implement FATF recommendations.

The FATF and the Wolfsberg Group broadly outline PEPs as individuals who are or have been entrusted with prominent domestic or foreign public positions. These positions include heads of state or government, senior politicians, senior government, judicial or military officials, senior executives of state owned enterprises, and senior political party officials. The WorldCompliance data includes individuals who are currently entrusted or who were previously entrusted with prominent public functions within their national governments or who are or were tasked with representing their governments in foreign relations. A national PEP holds an office within a sovereign government and entity, while an international PEP serves within an IO (international organization) or a regional organization. PEPs also include individuals who serve in national and international NGOs (non-governmental organizations) which are at a high risk for financial gain. In WorldCompliance, these individuals are categorized as primary PEPs.

The FATF recognizes that understanding a PEP's family members and close personal and business relationships are crucial to maintaining transparency in the international financial system as these individuals can serve as avenues for illicit activities or terrorist support on behalf of a PEP or in collusion with a PEP. Personal relationships may include connections among individuals that are widely known, publicly known, or that are reported by open-source news media. The nature of these relationships depends on social, cultural, and economic contexts. The family relationships of a PEP include lineage that is established through biological ancestry, adoption, legal guardianship, marriage, or civil forms of partnership.

In WorldCompliance, the family members of PEPs; the individuals who are related to PEPs by hereditary, marriage, or civil partnerships; and individuals who are socially or politically connected to primary PEPs are categorized as secondary PEPs. Secondary PEPs also include MSOEs (members of state-owned enterprises), MSWFs (members of sovereign wealth funds), and businesses that are controlled by PEPs. These entities are secondary PEPs because of their relationship to either a primary PEP, an SOE (state-owned enterprise) or an SWF (sovereign wealth fund).

PEP Categorization

An entity can have multiple primary and secondary records in the PEP segment. For example, an individual may hold more than one primary PEP role and also qualify as a secondary PEP by way of a family member or associate relationship to other primary PEPs.

These PEP profiles can be further grouped into subcategories. The subcategories for primary PEPs define the position in which a PEP serves or served. For a list of possible subcategories, see Primary PEP Subcategories. The subcategories for secondary PEPs qualify the relationship to the primary PEP. For a list of possible subcategories, see Secondary PEP Subcategories.

PEP Country Association

PEPs have a PEP country association. For primary PEPs, this country is the country that employs the primary PEP. In other words, this country is the jurisdiction where the PEP holds the qualifying PEP position. For secondary PEPs, this country is the PEP country association of the primary PEP that the secondary PEP is related to.

PEP Framework

WorldCompliance researchers identify PEPs using administrative levels, which are also referred to as administrative divisions. Administrative levels are a standard method of how countries and territories organize themselves politically across the globe. LexisNexis Risk Solutions map the administrative levels within each sovereign state and territory to create a PEP framework to identify individuals with prominent positions.

The framework lets WorldCompliance researchers identify relevant governing institutions within each administrative division. These divisions include executive, judicial, military, legislative, and other offices. Within those institutions, senior roles, or primary PEPs, are identified and profiled.

Every primary PEP role is tied to a specific administrative unit, which is the name of the jurisdiction where the governing institution has authority. Each administrative unit is tied to a specific administrative type that varies by country and territory. These administrative types include areas such as a state, province, municipality, prefecture, region, department, and city. In turn, the administrative unit and the administrative type maps to a WorldCompliance administrative level.

This framework ensures that WorldCompliance coverage includes those who hold prominent positions within a country or territory, and therefore have the most access to resources and influence. The examples in the following table illustrate how the framework can be used to apply a risk-based approach to PEP screening.

PEP Framework Examples

Administrative Level	Administrative Unit	Administrative Type	Governing Institution	Governing Role
Subnational	Scotland	Region	Scottish Assembly	Member of Scottish Assembly
Subnational	Alagoas (Brazil)	State	Public Ministry of Alagoas	Attorney General of Justice
National	Germany	Country	Parliament of Germany, Bundestag	Member from Hildesheim
Civic	Sahriatpur (Dhaka, Bangladesh)	Division	Office of the Deputy Commissioner of Shariatpur District	Deputy Commissioner
National	Canada	Country	Shadow Cabinet of Canada	Shadow Minister for Public Services and Procurement
Metro	Cape Town (South Africa)	Municipality	Government of Cape Town	Mayor

The framework includes the following administrative levels:

International

International-level PEPs represent nation states in foreign relations with other countries such as embassy officials. This level also includes international organizations, such as various UN organizations, the International Monetary Fund, and the World Bank.

National

National-level PEPs represent and perform duties within government institutions that operate at the level of a nation state. National PEPs include heads of state, government officials, cabinet ministers, judges, and military leaders.

Subnational

Subnational PEPs represent and perform duties that are directed to a community or geographical area that is equivalent to a state in the United States. Some countries use different terms to define this level (for example, province or region). Subnational PEPs include governors, legislators, and judges.

Civic

Civic-level PEPs hold senior positions at levels of government whose equivalence is lower than a U.S. state. Entities that are profiled to the civic level usually include areas that have special governance arrangements like Taiwan, Bosnia, and Herzegovina. Entities that are profiled at the civic level are rare.

Metro

Metro-level PEPs hold the position of mayor, treasurer, or equivalent position within selected metropolitan governments. Most countries have metro-level PEPs, which are determined by several factors:

- Territory capitals (all included)
- Population rank, varies by country size
- Transit hub: ports, interstate highways, airport
- Disputed status (ownership sovereignty)
- Economic importance: financial centers, national government grants and investments, budget
- High risk cities with any of the following factors:
  - Major border towns
  - Experience high immigrations or emigration
  - FATF gray list or geographic targeting orders
  - Trafficking hubs
  - Staging grounds for war
  - Adjacent to high risk index states

Country-specific PEPs

Some sovereign states have gone beyond the systemic principles that are set by FATF and the Wolfsberg Group when defining PEPs in their national laws or regulations. These PEPs usually serve in government within a lower-level administrative unit (such as a city or municipality) that would not meet the general standards outlined by FATF. WorldCompliance researchers flag these PEPs as being country-specific. WorldCompliance coverage of these PEPs is determined on a country-by-country basis.

Former PEPs

WorldCompliance PEP entity inclusion principles follow the systemic principles set by the FATF and the Wolfsberg Group. While there is no globally accepted time period for a PEP status after leaving their public function, the entity may still pose a risk due to the corruption risk and political situation in their PEP country and the level of informal influence by virtue of their previous office or function.

To help you mitigate this risk and to manage former PEPs according to your own risk-based approach, WorldCompliance researchers maintain separate PEP records for each role an individual has or had. Each role is marked with an `Active` indicator, and each role that is not active has a completed expiration date. Sometimes role expiration dates are not provided in sources, even when the PEP is no longer in the role. WorldCompliance researchers indicate whether the expiration date was located in an official government source or derived from the date of a news article.

WorldCompliance researchers retain PEP profiles up to 20 years from the deceased date of the PEP unless the entity has associated negative information (enforcement, sanctions, or adverse media). If the PEP has associated negative news, the PEP profile is retained indefinitely unless the charges against the PEP have been dropped or the PEP has been acquitted.

For primary PEPs who were once chiefs of state, the **Position** field contains the former chief of state role even if the individual has held other PEP roles since. This data organization is to highlight the prominence of this position.

Primary PEP Subcategories

WorldCompliance data includes various types of primary PEPs.

WorldCompliance researchers may apply any of the following subcategories to each primary PEP record:

Chief of State

A chief of state is an individual, individuals, or body of persons that acts as the formal public representative of a sovereign country. This role and its functions vary according to the country's political system. Chiefs of state include heads of government who are responsible for the daily executive and legislative decision-making for the country; and heads of state who serve as the highest-ranking representative of the sovereign state.

Diplomat

An individual who represents the interests of a government in its sovereign relations with other sovereign states, entities, and international organizations or regional organizations through an embassy or permanent mission. Diplomatic roles include senior positions that have been determined by a review of United States, French, United Kingdom, and Spanish diplomatic ranks, because these countries have historically influenced global standards for diplomatic roles.

The following senior roles are included in this subcategory:

- Consuls

  A consul is an individual who is appointed by their government to protect and promote that government's citizens and interests abroad in a host country's consulate. This individual is a salaried foreign service professional and enjoys the same rights and privileges as embassy officials (for example, diplomatic immunity).
- Embassy or Consulate Personnel

  Embassies contain the offices of the foreign ambassador, diplomatic representatives, and their staff. The embassy, led by the ambassador, is a foreign government's official representation in another country. The embassy is usually in the capital of a foreign country. Foreign ambassadors, certain diplomatic representatives, their families, and associates are considered PEPs.
- Honorary Consul

  An honorary consul is an individual who is a prominent and respected member of a country (for example, an artist or businessperson) who serves a consulate in a foreign country. Sometimes honorary consuls are not the same nationality as the consulate in which they serve. Unlike career consuls, honorary consuls may not enjoy diplomatic immunity, may not have diplomatic passports, and may not be paid for their consular service. However, as honorary consuls are established through government treaty, the nature of their roles and responsibilities may change. Honorary consuls often represent small countries in cities where there are no embassies or established consulates.

Govt Branch Member (Government Branch Member)

A government branch member is an individual who is elected or appointed to a senior position or a civil service position within a national government's executive branch. Civil servants are individuals who are employed in national executive government institutions and who are appointed or hired by decision of an authorized public institution in accordance with the civil service law and a structured hiring process. Civil servants differ from elected officials in that these individuals occupy permanent positions and their employment does not change with a political change of government.

Intelligence

Intelligence roles include individuals who serve in a national government agency and who are responsible for the collection, analysis, integration, and interpretation of information through HUMINT (human intelligence), PHOTINT (photograph intelligence), SIGINT (signals intelligence), OSINT (open sourced intelligence), GEOINT (geographic intelligence), CI (counter intelligence), and other methods. This information informs executive-level decision makers concerning a country's national security and foreign policy objectives or the competitive interests of the state.

Intl Org Leadership (International Organization Leadership)

This role includes an individual that holds a senior position within an IO, who represents the interests of the organization itself and not specific sovereign countries who hold membership. This role includes high-level leadership to the World Bank, UN, and ROs such as the EU. IOs and ROs are

bodies whose membership is formed and determined by treaty or agreement among three or more sovereign states that create a body with a permanent secretariat to perform ongoing tasks on behalf of the organization's goals.

Exclusions

Individuals who represent a country with another sovereign state or entity in their bilateral (country-to-country, entity-to-entity, or country-to-entity) relations are profiled in the `Diplomat` subcategory

Judiciary

Judiciary roles include an individual who is elected or appointed to a senior role (for example, a judgeship, senior advisory, prosecutor, or defense roles) within a judicial body whose position involves interpreting legal codes and laws, deciding the outcome of cases, or determining punishments for legal infringements.

Law Enforce Auth (Law Enforcement Authority)

LEAs (law enforcement authorities) are individuals who are senior members of a national government agency or national police force tasked with upholding legal authority within a sovereign state. The principal functions of these national agencies are prevention, detection, and investigation of crime and the apprehension of alleged offenders who have committed offenses within these countries. LEAs may have relationships with a cooperative body (for example, Europol or Interpol) that facilitate cooperation among national law enforcement bodies to pursue offenders who are sought for investigations or crimes spanning several countries, or who have fled to other countries to evade national authorities.

Legislature

Legislative roles include individuals who are elected or appointed to a senior position within a national government's legislative branch and who are typically responsible for law-making in a sovereign nation. Senior roles include officials who occupy offices at the national level or the state level and their governing institutions for each sovereign state and entity.

Military

A military role includes an individual who currently serves or has previously served in a sovereign state's armed forces where they have made combat, operational, or policy decisions. This role includes individuals in leadership positions within a national internal security force, and military advisory functions to senior executive and legislative decision makers.

NGO Leadership (Non-Governmental Organization Leadership)

This role includes an individual who holds a senior position within a national or transnational non-profit, private citizen group (including individuals that hold offices within international organizations or regional organizations) and who is significantly engaged in enterprises that can be abused for financial gain. Transnational leaders attempt to influence national leaders to make decisions based on the NGO (non-governmental organization) goals through direct contact or through participation

in IOs and ROs. NGOs bring citizen concerns to governments, provide expertise and information to policy makers, advocate and monitor government policies and international agreements, and sometimes provide aid and services that governments cannot furnish.

Senior Party Member

A senior party member is an individual who occupies a senior leadership position within a national-level or regional-level political party, who holds decision-making powers that involve finance, policy platforms, candidate support, and elected and nominated office holders. Individuals organize into political parties to affect political processes within governments and to place people into government positions who share their ideas and opinions on issues that can influence policy outcomes and direct resources to their constituents.

Traditional Leadership

Traditional leaders are individual members of a traditional or tribal body within a country who have inherited or have been appointed to a leadership position in accordance with the customs and traditions of the area. Their functions may involve the regulation and control of social behaviors within a group, or the semi-autonomous governing authority of a geographical area. Typically, their authority is derived by order of a national government, but in some cases they may constitute a tribal or family-based authority that refuses to recognize a state's sovereignty even as it occupies land within a state's political borders (for example, groups within the FATA (Federally Administered Tribal Areas) of Pakistan).

Union Leadership

A union leadership role includes an individual who occupies a senior leadership position in a trade or labor union or association, who officially and publicly represents the interests of the union or association's membership to government officials to influence country laws and regulations. This individual also engages in collective bargaining on behalf of its membership with government or corporate entities and with international organizations and regional organizations.

Secondary PEP Subcategories

WorldCompliance data includes various types of secondary PEPs.

WorldCompliance researchers may apply any of the following subcategories to each secondary PEP record:

Associate

An associate is an entity with a close demonstrated business, personal, or social relationship with a primary PEP that may serve as a conduit for illicit financial activities. These associate relationship types include realtors, accountants, independent political advisers who are employed by PEPs from outside formal government institutions (for example, Think Tanks), and close friends of PEPs as reported in respected media outlets.

Attorney

An attorney is an accredited legal professional who may act on behalf of a primary PEP or at a primary PEP's direction. The FATF considers attorneys to be DNFPBs (designated non-financial business and profession). Attorneys can facilitate corruptive practices that include money laundering and its predicate offenses or the financing of terrorism on behalf of PEP clients. Attorneys may be involved in managing trusts; buying and selling real estate; managing money, securities or other assets and accounts; or organizing, operating, or buying and selling companies and businesses.

Family Member

A family member is an individual who is a family member of a primary PEP by adoption, marriage, civil, or hereditary lines. Coverage includes the following relationships: `Wife`, `Ex-Wife`, `Husband`, `Ex-Husband`, `Brother`, `Brother-in-Law`, `Sister`, `Sister-in-law`, `Aunt`, `Uncle`, `Mother`, `Mother-in-Law`, `Father`, `Father-in-Law`, `Son`, `Son-in-law`, `Daughter`, `Daughter-in-law`, `Grandfather`, `Grandmother`, `Grandchild`, `Domestic Partner`, `Niece`, `Nephew`, `Cousin`, `Spouse`, and `Relative`. Adopted members, half members, and step members are also included in these relationship types.

MSOE (Member of a State Owned Enterprise)

An MSOE is an individual or group that holds an executive decision-making role in the governing body of an SOE such as the board of directors and C-level management; or an individual or group that hold senior management positions, such as a company or a senior executive of a company that conducts the day-to-day operations of an SOE.

This role also includes individuals who already hold senior government positions and serve in other capacities and individuals who are private citizens who are hired or appointed by the state to serve in management or decision-making and advisory capacities.

Individuals may already be PEPs because they hold senior offices in government service, or they may be private citizens. Their service as senior executive member of an SOE governing body designates them as PEPs in accordance with the FATF recommendations.

MSWF (Member of a Sovereign Wealth Fund)

An MSWF is an individual or group that holds an executive decision-making role in the governing body of an SWF (sovereign wealth fund) such as the board of directors and C-level management; or an individual or group that hold senior management positions, such as a company or a senior executive of a company that conducts the day-to-day operations of an SWF.

This role includes individuals who already hold senior government positions and serve in other capacities, as well as those who are private citizens hired or appointed by the state to serve in management or decision-making and advisory capacities.

Individuals may already be PEPs because they hold senior offices in government service, or they may be private citizens. Their service as senior executive member of an SWF governing body designates them as PEPs in accordance with FATF Recommendations.

PEP Controlled Bus (PEP Controlled Business)

A PEP-controlled business is a privately held legal entity that is controlled by a primary PEP, either directly or through an attorney, through family members or close associates, where the primary PEP holds at least 20 percent of ownership and receives a personal financial benefit.

Exclusions

PEP-controlled businesses do not include companies where PEPs are on the board of directors of a private company, unless that company is a state-owned enterprise. PEP positions that serve managerial roles within an SOE are profiled under the `SOE` segment. An SOE is a public holding that is formed for the benefit of the state, not the PEP.

Sanctions Segment

A sanction is a legal and public decree by a regional organization, an international organization, or sovereign government that imposes restrictive measures on a foreign state or entity to advance certain foreign policy or national security objectives.

WorldCompliance researchers monitor targeted sanctions lists that are published by national, regional, and international organizations. To provide flexible options for sanctions screening, LexisNexis Risk Solutions provides the following forms of sanctions profiles:

Single Sanctions

LexisNexis Risk Solutions provides profiles that are associated with a single sanctions source. These profiles are created when a government agency that is tasked with administering sanctions adds an entity to a targeted sanctions list that is included in WorldCompliance coverage. These profiles contain only data that was sourced from the single sanctions source. An example of a single sanctions source is `US-U.S. Office of Foreign Asset Control (OFAC) - SDN List`. A given entity can be listed on any number of single sanctions sources. Each single sanctions profile is linked to a consolidated profile.

Consolidated Sanctions

LexisNexis Risk Solutions also provides a consolidated profile for each sanctioned entity. This profile is associated with a WorldCompliance curated source, `Consolidated Sanctions List`. The profile is a collection of data that the single sanctions sources provide for the entity as well as data that is located in publicly available, non-sanctions sources and from various WorldCompliance value-added sources. Examples of publicly available data are native script names, DOB (date of birth) values, IDs, and addresses. Examples of data from WorldCompliance value-added sources are vessels data from IHS Markit™ and BIC (Business Identifier Code) numbers from SWIFT (Society for Worldwide Interbank Financial Telecommunication).

There is one consolidated profile for each sanctioned entity in the WorldCompliance database. WorldCompliance sanctions coverage is global, so selecting the `Consolidated Sanctions List` source effectively searches a consolidated view of every sanctioned entity in the WorldCompliance global coverage. As they effectively act as a repository for all information that is located for the entity, consolidated profiles also tend to contain more data than the associated single sanctions source profiles (for example, more aliases).

IHS Vessel Data

LexisNexis Risk Solutions contracts with IHS Markit to provide vessel data in `Consolidated Sanctions List` profiles. This data includes IMO (International Maritime Organization) numbers, former names, the names of various companies that are associated with the vessel (such as group beneficial owner and ship manager), and certain countries that are associated with these companies.

IHS Markit is the global custodian of the unique number identifier that is assigned to every vessel by the UN IMO. This IMO number is the global standard for vessel identification as the number is the only permanent characteristic of a vessel. For more information, see https://ihsmarkit.com.

SOE Segment

WorldCompliance researchers profile an SOE because its connection to government funding can make the SOE vulnerable to corruption. WorldCompliance researchers profile organizations that are at least one percent owned at the national or subnational level.

FATF recommends that financial institutions understand the ownership of an SOE. FATF also recommends that financial institutions perform enhanced due diligence on SOE leadership and management executives, who are considered to be PEPs.

An SOE is a legal entity (a corporation or a service) that is created or owned in whole or in part by a single government, or in cooperation with other governments, that undertakes activities for a specific commercial purpose on behalf of its investor states. An SOE is typically formed to make profits for the state; however, an SOE can provide services that may not make a profit but provide a necessary benefit to a country's citizenry (for example, transportation or mail services). These services and projects include healthcare, transport, utilities, university-level education institutions, construction, energy, and telecommunications. Governments determine the purpose of the SOE and appoint individuals who implement business strategies.

An SOE in WorldCompliance data can be an SWF (sovereign wealth fund). An SWF is a special purpose investment fund or arrangement that is created and owned by a single government or in cooperation with other governments. Governments create an SWF to hold, manage, and administer state assets to achieve certain macroeconomic objectives. Governments derive these assets from many sources. Examples include a country's balance of payments surplus, foreign currency operations, fiscal surpluses, and proceeds from the privatization of industries or commodity exports (for example, oil).

The government owner sets the purpose of the SWF, appoints the members of its governing bodies, and conducts oversight on their actions. Based on the goals that the government has set for the SWF, these governing bodies set the strategies and policies for the management of the SWF. The governing bodies depend on the type of SWF. Usually, the governing body is a board of directors, a committee, or a commission; however, the governing body can also be a ministry of finance or central bank when the SWF is a pool of assets.

An SOE or an SWF is labeled as active or inactive based on its current ownership status. If the SOE or the SWF has at least one percent cumulative government ownership, the SOE or the SWF is marked as active. If the SOE or SWF is wholly privatized and has less than one percent cumulative government ownership, the status is inactive.

WorldCompliance researchers also apply at least one of the following subcategories:

Majority

The entity is owned by only one country and that country owns 50 percent or more of the entity.

Minority

The entity is owned by only one country and that country owns less than 50 percent of the entity.

Multiple Majority

The entity is owned by two or more countries and those countries together own 50 percent or more of the entity.

Multiple Minority

The entity is owned by two or more countries and those countries together own less than 50 percent of the entity.

SWF

The entity is an SWF (sovereign wealth fund).

Each SOE has at least one ownership country association. This country indicates the sovereign state that has as stake in the SOE. When the percentage is available, an ownership percentage is provided per ownership country. When no percentage can be located, the ownership country is provided with no percentage. To cover the risk of unknown ownership percentages, `Majority` or `Multiple Majority` is included as the subcategory. The ownership percentage per country is calculated based on company to company relationships in the SOE ownership tree. The company to company ownership percentage is provided in the `Relationships` segment.

Governments create companies and SWFs to provide a host of services to their populations and often form partnership companies with other governments to fund very large projects in many sectors and jurisdictions. WorldCompliance refers to these sectors and jurisdictions as *domains*.

WorldCompliance researchers may apply any of the following domains:

- `Agriculture-Forestry`

  Companies that produce crops, fish, or other animals and companies that work in hunting or forestry
- `Arts-Recreation`

  Libraries, museums and archives, and companies that manage or oversee sports activities, amusement parks, or gambling operations
- `Construction`

  Companies that are created for state-funded building and civil engineering projects
- `Finance-Insurance`

  State-owned banks, credit companies, insurers, and pension service companies
- `Healthcare`

  Hospitals, clinics, and medical service businesses
- `Higher Education`

  Public colleges and universities
- `Info Comms Tech` (Information, Communications, and Technology)

  Companies that are involved in television or movies, broadcasting, telecommunication, and information services
- `Manufacturing`

  Companies that build, assemble, or otherwise convert raw materials into products
- `Public Services`

  Companies that provide services to the people who live within a jurisdiction that do not fit the other domains

  Examples include postal services, water treatment and supply, sewerage, waste management, or recycling.
- `Real Estate`

  Companies that buy, sell, or manage land and property
- `Resource Extraction`

  Companies that produce or refine oil, gas, electric, hydroelectric, nuclear, wind, solar, or coal energy; and companies that quarry or mine metals, gems, or stone

  This sector includes companies in the energy sector.
- `Retail-Trade`

  Sales, trade, and tourism companies
- `Security`

  Security companies with government contracts that provide protection services
- `Transportation`

  Railroads, airlines, airports, and other forms of public transportation
- `Utilities`

  Companies who deliver electricity, natural gas, steam, or air conditioning to customers

Additional Segments

WorldCompliance also includes additional data segments that do not align with the other data segments. WorldCompliance researchers profile these entities due to their relationship to an entity that has been named in a targeted sanctions source in WorldCompliance coverage.

WorldCompliance researchers may apply any of the following segments:

Associated Entity

Profiles that have an `Associated Entity` segment applied to them have a relationship with at least one sanctioned entity. Associated entities are referred to in sanctions sources, but are not explicitly named as sanctioned entities in those sources. The name of a family member or associate is sometimes provided in a sanctions source within the background information for a sanctioned entity. When the family member or associate is not sanctioned in their own right, WorldCompliance researchers apply the `Associated Entity` segment and the `N/A` subcategory to the entity and link that entity to the sanctioned entity. The sanction source that names the entity is included in the `Associated Entity` segment. These entities are not only individuals; they may also be organizations or other types of entities.

SWIFT BIC Entity

WorldCompliance researchers create a profile for each sanctioned branch and operational unit of sanctioned institutions based on BIC numbers using data that is sourced from SWIFT. SWIFT is the ISO (International Organization for Standardization) registration authority for BIC numbers, which the agency issues to financial and non-financial institutions. The BIC is used to address messages, route business transactions, and identify business parties. WorldCompliance researchers apply the `SWIFT BIC Entity` segment to these profiles.

Ownership Or Control

OFAC (Office of Foreign Assets Control), the EU, and HMT (Her Majesty's Treasury in the United Kingdom) stipulate that entities that are owned or controlled by subjects that are named in certain sanctions they administer should also be considered as sanctioned,without going so far as to name the owned or controlled entities on their targeted sanction lists. LexisNexis Risk Solutions helps clients screen for potential sanctions risk by including entities that are found in open source research to be owned or controlled by the relevant sanctioned entities.

WorldCompliance researchers apply the `Ownership Or Control` segment to these profiles, as well as a unique source that indicates the OFAC, EU, or HMT sanctions source of the sanctioned entity that prompted its inclusion. In addition, each profile is linked through a relationship to the immediate "parent" sanctioned entity. A description of the relationship that prompted the entity's inclusion, along with the ownership percentage (when available) and the date that the information was located is provided in the **Remark** field. The ownership percentages that are provided for an entity can total more than 100 percent based on available reported information.

Ownership information that is related to sanctioned subjects is known to change on a very frequent basis, sometimes without public reporting. Therefore, this data should be used as a pointer to potential sanctions risk that may require further due diligence. The information

is intended to serve as an indication of ownership or control that exists or existed between two entities as indicated in public sources as of the indicated date rather than an absolute indicator of ownership or control percentages.

Registrations Segment

`Registrations` data include entities that have registered with certain enforcement or regulatory agencies for specific purposes. An entity's inclusion in a registrations source may therefore indicate that the entity is conforming to regulations, particularly in the case of the `FATCA Reg Inst` (FATCA (Foreign Account Tax Compliance Act) Registered Institutions) segment.

To receive the `Registrations` data, you must formally request the data.

The `Registrations` data includes the following segments:

FATCA REG INST

The `FATCA REG INST` (FATCA Registered Institutions) subcategory includes profiles of financial institutions that are foreign to the United States that have registered with the IRS (Internal Revenue Service) to confirm their compliance with the U.S. FATCA law. For example, a foreign correspondent bank that needs to transfer payments through U.S. banks. If the FFI (foreign financial institution) is in this data set, the FFI is compliant with IRS law. If the FFI is not present in the data, the U.S. financial institution can transfer the payment, but the FATCA law requires the institution to withhold 30 percent of the payment. For more information, see the IRS website at http://www.irs.gov/Businesses/Corporations/IRS-FFI-List-FAQs.

IHS Reg Vessels

The `IHS Reg Vessels` (IHS Registered Vessels) subcategory includes the profiles of vessels that are registered with IHS Markit. Each vessel has a country flag that is associated with a high-risk country on the FATF “call for action” list or the FATF list[1] of “countries with strategic deficiencies.”

LexisNexis Risk Solutions contracts with IHS Markit to provide this data.

IHS Markit is the global custodian of the unique number identifier that is assigned to every vessel by the UN IMO. This IMO number is the global standard for vessel identification as the number is the only permanent characteristic of a vessel. For more information, see https://ihsmarkit.com.

1 “High-risk and non-cooperative jurisdictions,” FATF, accessed 15 November 2016, http://www.fatf-gafi.org/countries/#high-risk

“Improving Global AML/CFT Compliance: on-going process – 24 June 2016,” FATF, accessed 15 November 2016, http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/fatf-compliance-june-2016.html

Marijuana Reg Bus

The `Marijuana Reg Bus` (Marijuana Registered Business) subcategory includes profiles of aggregated MRB (marijuana registered business) lists that are issued by U.S. states. Coverage includes an MRB that is officially licensed for medical or recreational use. Examples include the following types of businesses:

- Cultivators
- Processors
- Distributors
- Retailers
- Wholesalers

UAE MSB

The `UAE MSB` subcategory includes profiles of entities that have registered as an MSB (money services business) with the Central Bank of the United Arab Emirates.

The United Arab Emirates Central Bank issued Resolution No. 123/7/1992 on 29 November 1992. One of the most important provisions of the resolution restricts “money changing” business licenses to only institutions that were established according to United Arab Emirates commercial law. The resolution also requires that the natural person be a United Arab Emirates national of not less than 21 years of age. In case of companies, the national shareholding should not be less than 60 percent of the total paid-up capital. The regulation set the minimum capital at one million dirhams or two million dirhams, depending on the scope of activities that the applicant wants to undertake.

Global financial institutions can benefit from screening this data to ensure the United Arab Emirates MSB is registered with the United Arab Emirates government. For more information, see the source details at https://www.centralbank.ae/sites/default/files/2018-10/List-of-Moneychangers30092014_2.pdf.

US MSB

The `US MSB` subcategory contains profiles of entities that have registered as an MSB, as required by the BSA (Bank Secrecy Act) regulations at 31 CFR (Code of Federal Regulations) 1022.380(a)-(f). FinCEN (Financial Crimes Enforcement Network) administers the BSA regulations. An MSB includes providers that service money orders, traveler’s checks, money transmission, check cashing, currency exchange, currency dealing, and prepaid access. For more information, see the source details at http://www.fincen.gov/financial_institutions/msb/msbstateselector.html.

An MSB is considered high risk because the business can be used for money laundering or other financial crimes. Registering with FinCEN confirms that the MSB has an AML program in place to manage risk. This data lets you screen your customers to determine if those customers are registered with FinCEN and therefore are complying with AML requirements and implementing a program with necessary controls and procedures.

When available in the FinCEN source, the following information is provided for entities with the `US MSB` subcategory:

Receive Date

The receive date is the date that the registration form was received.

Authorized Signature Date

The authorized signature date is the date that the registration form was signed.