COUNTRY COMPARATIVE GUIDES 2023

The Legal 500 Country Comparative Guides

United States

WHITE COLLAR CRIME

Contributor

Diaz Reus International Law Firm

Javier Coronado

Partner | jcoronado@diazreus.com

Michael Diaz, Jr.

Global Managing Partner | mdiaz@diazreus.com

This country-specific Q&A provides an overview of white collar crime laws and regulations applicable in United States.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

UNITED STATES
WHITE COLLAR CRIME

1. What are the key financial crime offences applicable to companies and their directors and officers? (E.g. Fraud, money laundering, false accounting, tax evasion, market abuse, corruption, sanctions.) Please explain the governing laws or regulations.

The following are some of the key financial crimes prosecuted at the U.S. federal level:

a. Crimes related to money laundering and terrorist financing activities, which include domestic money laundering 18 U.S.C. § 1956(a)(1), international money laundering 18 U.S.C. § 1956(a)(2), transacting in proceeds of specified unlawful activity 18 U.S.C. § 1957(a), money services businesses ("MSBs") violations 18 U.S.C. §1960(b), willful violations of the Bank Secrecy Act ("BSA") 31 U.S.C. §§ 5321-5322, bulk cash smuggling 31 U.S.C. § 5332, providing material support to terrorists 18 U.S.C. § 2339A, and providing material support or resources to designated foreign terrorist organizations 18 U.S.C. § 2339B.
b. Corporate fraud, including violations of the mail and wire fraud statutes 18 U.S.C. §§ 1341, 1343, securities fraud 15 U.S.C. § 78ff(a) and 15 U.S.C. § 77(x), bank fraud 18 U.S.C. § 1344, tax fraud 26 U.S.C. §§ 7201, 7206, embezzlement 18 U.S.C. § 656, and false statements in matters within the jurisdiction of the executive, legislative, or judicial branch of the U.S. Government 18 U.S.C. § 1001.
c. Violations of U.S. Anti-corruption statutes, including the Foreign Corrupt Practices Act of 1977 ("FCPA") 15 U.S.C. § 78dd-1, et seq., which punishes the bribery of foreign officials, and statutes prohibiting the bribery of U.S. officials, such as 18 U.S.C. § 201 (bribery of public officials and witnesses), and 18 U.S.C. § 666 (theft or bribery concerning programs receiving Federal funds).
d. Insider trading, which is typically prosecuted under Section 10(b) of the Exchange Act and Rule 10b-5, which broadly prohibit the use of a "deceptive device", the making of a false statement, or engaging in an act that operates as a fraud or deceit in connection with the purchase or sale of a security.
e. Sanctions evasion under the laws pertaining the economic sanctions administered by the Office of Foreign Assets Control ("OFAC"), such as the International Emergency Economic Powers Act 50 U.S.C. §§ 1701–1707. Typically, the U.S. Government will criminally prosecute willful violations of OFAC Sanctions, or violations of the reporting and recordkeeping requirements for Sanctions 31 C.F.R. §§ 501.601–06.
f. Crimes punishing cryptocurrency-related crimes, which include fraud and related activity in connection with computers 18 U.S.C. § 1030, wire fraud 18 U.S.C. §1343, money laundering 18 U.S.C. §1956, and fraud and related activity in connection with identification documents, authentication features, and information 18 U.S.C. §1028.

2. Can corporates be held criminally liable? If yes, how is this determined/attributed?

Yes, corporations may be held criminally liable. A State or Federal statute will typically provide the legal basis for authorities to investigate and prosecute the corporation, as well as the way in which a corporation's criminal liability should be determined. Additionally, under the common law doctrine of *respondeat superior*, a corporation may be held criminally liable based on the actions of its directors, officers, employees, or other agents if those actions were within the scope of the agent's duties and benefited or sought to benefit the corporation. The corporation need not to profit from an agent's criminal actions for it to be held liable.

According to DOJ's *Principles of Federal Prosecution of*

Business Organizations, there are eleven factors that federal prosecutors should consider in deciding whether to criminally charge a corporation: (1) the nature and seriousness of the offense, including the risk of harm to the public and priorities, if any, governing the prosecution of corporations for particular categories of crime; (2) the pervasiveness of wrongdoing within corporation, including the complicity in, or the condoning of, the wrongdoing by corporate management; (3) the corporation's history of similar misconduct, including prior criminal, civil, and regulatory enforcement actions against it, both domestically and internationally; (4) the corporation's willingness to cooperate, including as potential wrongdoing by its current and former employees, directors, officers and agents, as well as other individuals and entities that engaged in the misconduct under investigation; (5) the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging or resolution decision; (6) the corporation's timely and voluntary disclosure of wrongdoing; (7) the corporation's remedial actions, including any efforts to implement an adequate and effective corporate compliance program or to improve an existing one, to replace responsible management, to discipline or terminate wrongdoers, or to pay restitution; (8) collateral consequences, including whether there is disproportionate harm to shareholders, pension holders, employees, and others not proven personally culpable, as well as impact on the public arising from the prosecution; (9) the adequacy of remedies such as civil or regulatory enforcement actions, including remedies resulting from the corporation's cooperation with relevant government agencies; (10) the adequacy of the prosecution of individuals responsible for the corporation's malfeasance; and (11) the interest of any victims, including what steps the corporation has taken to identify potential victims, or other persons or entities who were significantly, even if indirectly, harmed by the criminal conduct, and what steps the corporation has taken to mitigate such harm.

3. What are the commonly prosecuted offences personally applicable to company directors and officers?

Absent clear legislative intent to exclude corporate agents from personal responsibility for acts they commit; they cannot use the corporate entity as a shield against liability for their crimes. Accordingly, directors and officers may be held criminally liable under the offences listed in response to question number 1. Additionally, these individuals may be prosecuted for conspiring to commit, and/or aiding and abetting, these crimes.

4. Who are the lead prosecuting authorities which investigate and prosecute financial crime and what are their responsibilities?

At the federal level, the following Government agencies often participate in the investigation and prosecution of financial crimes in the U.S.:

i. Department of Justice ("DOJ"), which includes the US Attorney's Office ("USAO") in each federal district and the Federal Bureau of Investigation (FBI), has the power to investigate and prosecutes federal crimes, or bring civil enforcement actions. Additionally, DOJ has created recently new units for Russians and asset recovery.
ii. Department Homeland Security ("DHS"), through divisions such as Homeland Security Investigations ("HSI"), U.S. Immigration and Custom Enforcement ("ICE"), and U.S. Customs and Border Protection ("CBP"), investigates crimes related to cross-border criminal activities that threaten the U.S. security and economy, as well as criminal enterprises that engage in a broad range of illicit activity including narcotics smuggling, human trafficking, gang violence, trade-based money laundering and other financial crimes, intellectual property theft, and customs fraud.
iii. Securities and Exchange Commission ("SEC"), through its Enforcement Division, investigates possible violations of federal securities laws and the regulations promulgated thereunder. The SEC prosecutes violations through civil enforcement actions and administrative proceedings and makes referrals to the DOJ for criminal prosecution.
iv. The U.S. Secret Service has the responsibility to investigate crimes against the U.S. financial system committed by international criminals and in the cyber space.
v. U.S. Drug Enforcement Administration ("DEA") may also investigate financial crimes related to drug trafficking activities.
vi. The Commodity Futures Trading Commission ("CFTC") investigates possible violations of the Commodity Exchange Act and its regulations. It prosecutes violations through civil enforcement actions and administrative proceedings and makes referrals to the DOJ for criminal prosecution.
vii. The Internal Revenue Service ("IRS") has broad powers to investigate potential violations of the federal tax laws and may refer conduct to the DOJ's Tax Division or to a USAO for criminal prosecution.

viii. The Federal Trade Commission ("FTC") conducts investigations of potential violations of the Federal Trade Commission Act. The FTC may bring civil actions in court to enforce its regulations or make referrals to DOJ for criminal prosecution.
ix. The U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"), which receives, analyzes, and disseminates financial transactions data for law enforcement purposes in the U.S., especially in aid of criminal investigations and prosecutions to combat violations of the U.S. Bank Secrecy Act, money laundering, terrorism financing, fraud, tax evasion, and narcotics trafficking.

5. Which courts hear cases of financial crime? Are trials held by jury?

State or federal courts hear cases of financial crime that fall under the court's jurisdiction, which is determined based on the statute that was allegedly violated by the criminal suspect, the specific circumstances of the crime, the place in which the crime took place, and on the involvement of a federal agency in the criminal investigation and/or prosecution. Typically, cases of financial crime are heard by a U.S district court as such crimes often involve violations of federal law, cross state lines, or involve the channels or instrumentalities of commerce, such as the U.S. financial system. The U.S. does not have courts specialized in hearing financial crime cases.

In cases of financial crime, defendants are generally entitled to trial by jury pursuant to Article III, Section 2 of the U.S. Constitution, and the Sixth Amendment. A criminal defendant may waive the right to a jury trial and seek a bench trial before a judge. Moreover, the U.S. Supreme Court has held that defendants have a constitutional right to a jury trial only in "serious" criminal cases. Petty offenses—those that carry the possibility of six months or less in jail—are not guaranteed a jury trial. The U.S. Supreme Court's ruling, though, sets a minimum standard. States are free to provide greater jury-trial rights to criminal defendants, not less.

6. How do the authorities initiate an investigation? (E.g. Are raids common, are there compulsory document production or evidence taking powers?)

An investigation is usually initiated when a government agency receives credible information reporting an activity that violates federal or state laws or regulations, including criminal activity or regulatory infractions. Such information may come from a human source (like the victim, a witness, or an informant), a written report (like a suspicious activity report), a request made by a foreign Government, or even from publicly available sources. An often used method to obtain information, is for the U.S. Government to revoke the U.S. visa of the subjects of a criminal investigation so that person is incentivized to come forward and inquire and/or cooperate with law enforcement authorities.

The Government may compel the production of information, documents, and testimony relevant to the case through subpoenas, which in the context of criminal investigations are typically issued by grand juries. Federal grand juries are selected by the court in each federal judicial district and are organized under the supervision and direction of the chief judge of a federal district court. At the state level, the selection, organization, and supervision of a grand jury may vary. A search warrant authorizes a law enforcement agency to search designated premises and seize specific items or documents.

7. What powers do the authorities have to conduct interviews?

Government investigators may interview a person who is or may be in possession of information relevant to the matter under investigation. Generally, investigators will seek a person to voluntarily appear for interview at an agreed location or designated Government facility. U.S. agents typically may not stop or summon a person for interview unless they have a warrant or court order to do so, or have developed specific articulable facts that the person being questioned is, or is attempting to be, engaged in an offense against the U.S. However, such protections may not apply at the U.S. border or its functional equivalent, which is one of the reasons why investigation agencies may seek the assistance of U.S. Customs and Border Protection, a division of the U.S. Department of Homeland Security, to stop a person at a transportation hub for interview.

At the federal level, when the Government requires the testimony of a person in connection with an ongoing criminal investigation, it may seek a Grand Jury subpoena compelling that person's declaration. This subpoena may also be used to order the person to produce records material to the criminal investigation. States provide for similar legal avenues for law enforcement to compel the appearance of a person for interview. The difference between the two sovereigns is

that, with a state subpoena compelling a person's appearance for interview, statutory use immunity may attach automatically. In the federal system, use immunity is not automatic and must be always negotiated with the Government before someone appears for interview.

8. What rights do interviewees have regarding the interview process? (E.g. Is there a right to be represented by a lawyer at an interview? Is there an absolute or qualified right to silence? Is there a right to pre-interview disclosure? Are interviews recorded or transcribed?)

Interviewees do not generally have a right to be represented by a lawyer at an interview. The Sixth Amendment right to right to assistance of counsel applies to the custodial interrogation of a criminal suspect, or during the critical stages of a criminal proceeding after the suspect has been charged by the authorities. In practice, however, law enforcement agencies may allow an interviewee to attend an interview accompanied by counsel, even if the interviewee has no criminal exposure.

If the interview is conducted in circumstances such that a reasonable person might conclude that the person is not free to leave (i.e., the interview is "custodial"), Miranda rights will attach, and the Government will be required to advise that person about (1) the right to remain silent, (2) that anything the person says may be used in court, (3) the right to an attorney resent during questioning, and that, if the person is indigent, an attorney will be provided at no cost to represent him/her. Upon receiving the Miranda warnings, subsequent voluntary statements made by the criminal suspect to a Government agent will be admissible in court.

There is no right to pre-interview disclosure of evidence and the interviews may not be recorded or transcribed (although, in practice, they are). Further, interviewees have no right to receive a copy of such recording/transcript.

Depending on the skill, experience, and relationship with law enforcement authorities, some or much of this information can be obtained by defense counsel before the interview.

9. Do some or all the laws or regulations governing financial crime have extraterritorial effect so as to catch conduct of nationals or companies operating overseas?

Federal legislation is presumed not to apply extra-territorially, and due process requires U.S. authorities to only prosecute crimes that have a U.S. nexus. However, federal statutes grant jurisdiction for U.S. law enforcement to investigate and prosecute international crime based on the text of the statute and legislative intent. For example, the Money Laundering Control Act of 1986 may be used to target foreign individuals and financial institutions involved in money laundering activities if the financial transaction takes place in whole or in part in the U.S. or, if the foreign financial institutional maintains a bank account at a U.S. financial institution. Foreign persons that conspire to violate, or cause a violation of, U.S. criminal laws, may also face criminal prosecution in the U.S. This is currently a much-debated issue in corruption cases prosecuted under the U.S. FCPA statute.

10. Do the authorities commonly cooperate with foreign authorities? If so, under what arrangements?

U.S. authorities and foreign authorities frequently and commonly cooperate for the investigation and prosecution of financial crime. For instance, U.S. authorities regularly obtain information overseas through the more than 40 mutual legal assistance treaties ("MLAT") that have been ratified by the U.S. The MLATs also provide means for seizing assets located in other jurisdictions. Additionally, the U.S. is a party to the Inter-American Convention Against Corruption, which provides for evidence sharing between 34 American countries.

Further, FinCEN works closely with the Financial Intelligence Units (FIU's) of other countries to share, analyze, and disseminate with U.S. law enforcement information coming from suspicious activity reports prepared by financial institutions around the world.

11. What are the rules regarding legal professional privilege? Does it protect communications from being produced/seized by financial crime authorities?

Attorney client-privilege and the work-product doctrine limit the U.S. Government's ability to obtain information and documents from attorneys during a criminal

investigation. The evidentiary attorney-client privilege precludes the discovery of a client's communication to a lawyer whom the client reasonably believes represents the client when the circumstances indicate a desire by the client for confidentiality.

The attorney-client does not attach to statements made to an attorney not regarding legal advice or services sought by the client, to discovery of the facts underlying the communication, or to communications made to an attorney who is acting in a capacity other than as a lawyer. Moreover, under the crime/fraud exception to the attorney-client privilege, clients may not prevent discovery of communications made to enable or aid the commission of what the client knew or should have known was a crime or fraud.

The attorney-client privilege is treated slightly differently when the defendant is a corporation. Some states limit the privilege to communications received by an attorney from a member of the "control group" of the corporation. However, in federal cases where federal law controls, the privilege extends to communications by non-control group employees about matters within the employee's corporate duties made for the purpose of obtaining legal advice for the corporation.

Under the work-product doctrine, documents prepared by or for a party or by or for a party's attorney in anticipation of litigation, are also protected. However, these documents are subject to discovery if the party seeking disclosure (i) demonstrates a substantial need for the information, and (ii) cannot obtain the information by any other means without undue hardship. The mental impressions, conclusions, and trial tactics of a lawyer are protected from discovery, regardless of another party's need for the information or inability to otherwise obtain it.

12. What rights do companies and individuals have in relation to privacy or data protection in the context of a financial crime investigation?

The U.S. government has extensive investigatory powers to obtain private and financial information material to an ongoing criminal investigation.

The Fourth Amendment to the U.S Constitution confers privacy rights to U.S individuals and companies that may limit the Government's ability, both at the state and federal level, to obtain private records in connection with a financial crime investigation. Specifically, the Fourth Amendment establishes the people's right to be secure in their persons, houses, papers, and effects, as well as protection against unreasonable searches and seizures. In the context of bank records, however, the Supreme Court has held that individuals and companies do not have an expectation of privacy protected under the Fourth Amendment. See *United States v. Miller*, 425 U.S. 435 (1976).

In response to the Court's decision in Miller, the Congress passed the Right to Financial Privacy Act of 1978 ("RFPA"), which confers some federal statutory protections for personal financial records. Notably, this Act generally requires banks to provide individuals with notice when bank records are being subpoenaed, and an opportunity to be heard with respect to that request. RFPA also establishes standing to seek judicial relief against violations of the appropriate procedures laid out in the RFPA.

However, the RFPA has been amended several times to permit greater access without customer notice to information requested for criminal law enforcement purposes and for certain intelligence activities. Additionally, the RFPA does not govern requests for financial records made by or state or local governments, and the RFPA only protects the records of individuals and partnerships with 5 or fewer partners. Moreover, the Federal Government may use investigatory tools different from a subpoena or a search warrant to obtain records material to a financial crime investigation, including interviews with human sources that might be in possession of the information sought by the Government, or mutual legal assistance requests with other countries. The Government may also be in possession of the relevant information in connection the filing of a Suspicious Activity Report (SAR) by a financial institution.

As a result, U.S. investigatory agencies will generally be able to access the documents, electronic information, and other data of companies and individuals in connection with a criminal investigation.

13. Is there a doctrine of successor criminal liability? For instance in mergers and acquisitions?

State and federal law generally enforce the doctrine of successor criminal liability in the context of financial crime. Accordingly, a successor corporation may be held derivatively liable for the criminal acts of the predecessor corporation. Whether the successor will be liable is often dependent on whether the transaction involved a merger, a consolidation, or an asset acquisition.

In both a merger and a consolidation, the predecessor corporation is dissolved and only one corporation survives. In this instance, the surviving corporation will generally be held liable for the predecessor's criminal acts. For this reason, companies will often structure the transaction as an asset acquisition. However, even in this instance, U.S. law establishes exceptions that may result in the buyer assuming the seller's criminal liability, such as when the buyer expressly or impliedly assumes the liability, buyer is an alter ego of the seller, the asset acquisition is deemed a de facto merger/consolidation, or when the transfer was fraudulent or intended to avoid liabilities.

U.S. Government agencies encourage companies to conduct due diligence prior to the transaction and improve compliance programs and internal controls after the transaction. These compliance efforts are a factor that authorities generally consider favorably when deciding whether to prosecute an apparent violation of U.S. laws and regulations, or for calculating the appropriate penalty.

14. What factors must prosecuting authorities consider when deciding whether to charge?

First and foremost, State Department policies, priorities and directives targeting specific individuals, countries, companies, industries, and groups. Additionally, DOJ's *Principles of Federal Prosecution* advise federal prosecutors to weigh the following considerations in deciding whether to charge individuals: federal law enforcement priorities; the nature and seriousness of the offense; the deterrent effect of prosecution; the person's culpability in connection with the offense; the person's history of criminal activity; the person's willingness to cooperate in the investigation or prosecution of others; person's personal circumstances, interests of any victims, and the probable sentence or other consequences if the person is convicted. State prosecutors consider similar factors when deciding whether to bring criminal charges against an individual.

15. What is the evidential standard required to secure conviction?

The evidential standard required by U.S. law to obtain a criminal conviction is "beyond a reasonable doubt." Accordingly, prosecutors are required to persuade the jury (or the judge in a bench trial) that there is no other reasonable explanation that can result from the evidence presented for the case at trial. The trier of facts must be fully satisfied and entirely convinced to a moral certainty that the evidence presented proves the guilt of the defendant. This standard of proof is much higher than the standard generally required in civil cases, which is named "preponderance of the evidence," and requires a certainty greater than 50 percent.

16. Is there a statute of limitations for criminal matters? If so, are there any exceptions?

The statute of limitations for most federal crimes is five years. See 18 U.S.C 3282. However, some crimes have longer statutes of limitations such as bank fraud (ten years), tax crimes (six-years), major fraud against the U.S. government (seven years), or crimes involving banks and other financial institutions (10 years). Also, the statute of limitations may be "tolled" (legally suspended) (i) during periods of fugitivity, (ii) on application of the United States, during the pendency of an official request to a foreign court or authority to obtain evidence located in a foreign country; or (iii) in the absence of a legal provision if the Government and the defendant enter into a voluntary tolling agreement.

17. Are there any mechanisms commonly used to resolve financial crime issues falling short of a prosecution? (E.g. Deferred prosecution agreements, non-prosecution agreements, civil recovery orders, etc.) If yes, what factors are relevant and what approvals are required by the court?

The U.S. has mechanisms to resolve financial crime issues falling short of a prosecution. In fact, U.S. prosecutors often resolve financial crime cases through non-prosecution agreements ("NPAs"), and deferred prosecution agreements ("DPAs"). Under an NPA, the DOJ does not prosecute the target of the investigation if the target agrees to cooperate with the Government and to implement remedial and/or compliance measures. The NPA is not filed with the court, and instead is kept between the parties.

Under a DPA, the Government files a charging document with the Court, and it simultaneously requests that the prosecution be postponed for the purpose of allowing the target of the criminal investigation to demonstrate good conduct. DPAs generally require the defendant to pay a monetary penalty, waive the statute of limitations, cooperate with the Government, admit the facts underlying the criminal charges, and implement compliance and/or remediation commitments. If the

defendant complies with the DPA, the Government moves to dismiss the criminal charges or civil enforcement action.

In deciding to enter into a DPA or a NPA with the target of the criminal investigation, federal prosecutors will take into consideration the factors set forth by the Principles of Federal Prosecution (see answer to question 14 above). The Government does not require the court's approval for entering into a DPA or a NPA with the target.

18. Is there a mechanism for plea bargaining?

Yes. Plea agreements require the defendant to accept all or some of the criminal charges, in exchange of one of the following actions of the Government: "(A) not bring, or will move to dismiss, other charges; (B) recommend, or agree not to oppose the defendant's request, that a sentence or sentencing range is appropriate or that a provision of the Sentencing Guidelines, or policy statement, or sentencing factor does or does not apply (such a recommendation or request does not bind the court); or (C) agree that a specific sentence or sentencing range is the appropriate disposition of the case, or that a provision of the Sentencing Guidelines, or policy statement, or sentencing factor does or does not apply (such a recommendation or request binds the court once the court accepts the plea agreement)." Fed. R. Crim. Pro. 11(c).

19. Is there any requirement or benefit to a corporate for voluntary disclosure to a prosecuting authority? Is there any guidance?

The U.S. Bank Secrecy Act ("BSA") requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering. Specifically, the BSA requires financial institutions to report FinCEN suspicious activity that might signify money laundering, tax evasion, Sanctions evasion, or other criminal activities. Additionally, U.S. Government agencies often reward voluntary self-disclosure with declinations to pursue enforcement actions, and/or reduction in the civil or criminal penalty that would otherwise be sought by the agency.

For example, the DOJ has implemented the Corporate Enforcement Policy "CEP" to provide incentives and benefits to companies that voluntarily self-disclose misconduct, fully cooperate, and undertake remedial actions, including a presumption of a declination to criminally prosecute the company, absent aggravating circumstances. Similarly, OFAC encourages anyone who may have potentially violated OFAC-administered regulations to disclose the apparent violation to OFAC, and voluntary self-disclosure to OFAC will result in a reduction in the base amount of any proposed civil penalty.

20. What rules or guidelines determine sentencing? Are there any leniency or discount policies? If so, how are these applied?

At the federal level, courts determine criminal sentences based on the Federal Sentencing Guidelines, which are non-binding rules established by the U.S. Sentencing Commission in an attempt to uniform sentencing policy and calibrate sentences depending upon factors related both to the subjective guilt of the defendant and to the actual harm caused by the crime. While the Guidelines are not mandatory, federal judges must consider them when deciding a criminal defendant's sentence. Accordingly, when a judge determines within his or her discretion to depart from the Guidelines, the judge must explain what factors warranted the increased or decreased sentence.

Relevant to criminal white-collar cases, the Sentencing Guidelines take into consideration the defendant's acceptance of responsibility, which may be shown by the fact that the defendant made a restitution before sentencing and/or assisted authorities in the investigation or prosecution of the crime by providing complete information about the defendant's involvement in it or by giving timely notice of his or her intent to plead guilty. Additionally, a court may consider a downward departure from the minimum penalty set forth by the Sentencing Guidelines based on the defendant's substantial assistance in the investigation or prosecution of another person who has committed an offense. For example, in *U.S. v. Edoardo Orsoni*, Case No. 19-CR-20725-MGC, Edoardo Orsoni, the former general counsel at U.S. based Citgo Petroleum and Venezuela's state-owned oil company Petróleos de Venezuela SA (PDVSA) pleaded guilty to conspiracy to defraud the U.S., was sentenced by the U.S. District Court for the Southern District of Florida to only three years' probation based on Orsoni's substantial cooperation with DOJ's expanding investigation into corruption connected to Citgo, PDVSA, and Venezuela.

Similarly, in *USA v. Cedeno, Case 9:17-cr-80242-RLR*, the Southern District of Florida amended the judgement against Alejandro Andrade, the former national treasurer of Venezuela, so his criminal sentence was reduced from

ten to four years of prison based on his substantial cooperation with the U.S. Government in the prosecution of other individuals accused of significant acts of corruption. In November of 2018, Andrade had pleaded guilty to one count of conspiracy to commit money laundering and, as part of his guilty plea, Andrade admitted that he received over $1 billion in exchange for using his position to select Venezuelan contractors.

21. In relation to corporate liability, how are compliance procedures evaluated by the financial crime authorities and how can businesses best protect themselves?

U.S. financial crime authorities generally evaluate if the organization has used a "risk-based approach" to design, implement, and periodically update compliance programs. Accordingly, the compliance program of each organization should be different and tailored to the company's products, clients, and to the risks associated to the jurisdictions in which the company has operations. Nevertheless, U.S. authorities typically expect organization to develop the following essential components of compliance:

- Management Commitment: ensuring senior management commitment to the company's compliance with U.S law.
- Risk Assessment: conducting frequent risk assessments to identify and mitigate specific risks.
- Internal Controls: developing and deploying policies and procedures to identify, interdict, escalate, report, and maintain records pertaining to activity prohibited by U.S law.
- Testing and Audit: identifying and correcting weaknesses and deficiencies.
- Training: ensuring all relevant personnel are provided tailored training on the pertinent U.S law.

U.S. authorities generally have three inquiries: is the company's compliance program well designed? is it being applied in good faith? and does it work in practice?

To protect themselves from financial crimes, aside from designing, implementing, and updating Sanctions/AML/FCPA compliance programs, a company should carefully review any transaction involving high-risk persons or jurisdictions to confirm whether the U.S. Government's authorization is required. If necessary, companies should request the Government's interpretative guidance when available before moving forward with the transaction.

22. What penalties do the courts typically impose on individuals and corporates in relation to the key offences listed at Q1?

Individuals that are convicted of these offenses without entering into a plea agreement with the Government, are typically sentenced to long terms of imprisonment, substantial fines, and/ or disgorgement of ill-gotten gains. A convicted corporation may be subject to stiff fines, and the Court may also appoint a monitor to oversee the corporation's affairs through a term of probation, and/or prohibit its operations within the U.S. for a period of time.

23. What rights of appeal are there?

The U.S. Constitution does not guarantee criminal defendants a right to appeal. See *McKane v. Durston*, 153 U.S. 684 (1894). Accordingly, the questions of who can file an appeal and which issues are appealable are determined by federal and state rules of appellate procedure. In the federal system, after a defendant is found guilty, the defendant may appeal to the Circuit Court based on specific errors that might have occurred at trial. The defendant may appeal a guilty verdict, but the Government cannot appeal if a defendant is found not guilty. Either side in the criminal case may appeal with respect to the sentence that is imposed after a guilty verdict. Once an appeal is decided by a circuit court judge, a defendant can try to appeal that decision to the United States Supreme Court, but the Court is not required to hear an appeal in every case and takes only a small number of cases each year.

24. How active are the authorities in tackling financial crime?

The U.S. has long been a leader in the global effort to fight financial crime, as recognized in the periodic evaluations conducted by Financial Action Task Force (FATF), the most prestigious inter-governmental policymaking body in the area of anti-money laundering (AML). The U.S. has a robust AML, Anti-corruption, and Economic Sanctions regime that is enforced by a strong government architecture and has received the highest possible ratings for investigating and prosecuting financial crime.

Each year, the U.S. Department of Justice criminally prosecutes over 1,200 money laundering cases, including various complex and often international prosecutions against persons and businesses—including major financial institutions—that enable money laundering related to serious offenses such as narcotics

trafficking, fraud, and corruption. Further, the U.S. works with partner countries and international organizations to. The U.S. has also supported, through technical assistance and other means, the development and implementation of robust national-level AML and Anti-corruption regimes in multiple jurisdictions around the world.

The current U.S. administration is taking steps towards an increase in the number of investigations and prosecutions of financial crime. For instance, throughout 2023, the Department of Justice's National Security Division ("NSD"), the Department of Commerce's Burau of Industry and Security ("BIS"), and the Department of the Treasury's Office of Foreign Assets Control ("OFAC") have implemented aggressive measures to fight Sanctions evasion schemes. NSD appointed a Chief Counsel for Corporate Enforcement and added twenty-five new prosecutors to address sanctions evasion, export control violations, and similar economic crimes. BIS's Office of Export Enforcement implemented a new "dual-track system" to prioritize resolutions and investigations in matters involving export control evasion. OFAC has designated over 300 individuals and companies, with touchpoints in more than 20 jurisdictions, in an effort to deter circumvention of Sanctions.

Additionally, pursuant to the 2023 budget for the Department of Treasury, FinCEN received $190 Million in discretionary appropriations to boost efforts to combat terrorist financing and money laundering. The Office of Terrorism and Financial Intelligence received $216 Million – an increase of $21 million above the fiscal year 2022 – for investments related to the enforcement of OFAC sanctions programs.

Furthermore, the U.S. and its allies established a multilateral Russian Elites, Proxies, and Oligarchs ("REPO") Task Force to collaborate on the enforcement of economic sanctions related to Russia through coordination of law enforcement agencies, joint investigations to track sanctioned assets, and information sharing regarding Russian activity. As of March 9, 2023, when the latest Joint Statement from the REPO Task Force was published by the U.S. Department of Treasury, the members of the REPO Task Force had been successful in the blocking or freezing of more than $58 billion worth of sanctioned Russians' assets.

25. In the last 5 years, have you seen any trends or focus on particular types of offences, sectors and/or industries?

In recent years the U.S. prioritizes law enforcement actions targeting the following criminal activity, in no particular order:

Corruption. Consistent with President Biden's 2021 National Security Memorandum, the fight against corruption is a priority for the U.S. Government, and law enforcement agencies frequently investigate and prosecute instances in which corrupt actors and their financial facilitators have sought to exploit vulnerabilities in the U.S. financial system to launder and obscure bribes and/or the proceeds of corruption.

Cybercrime. The U.S. Government is particularly concerned about cyber-enabled, financial crime, ransomware attacks, and the misuse of cryptocurrency and other virtual assets for laundering of illicit proceeds. In fact, since 2021, the U.S. Government has increased its efforts to investigate and prosecute criminal activity in the virtual currency space. For example, in October of 2021, the DOJ created a National Cryptocurrency Enforcement Team (NCET) that coordinates enforcement efforts of various criminal violations involving digital assets including wire fraud, mail fraud, securities fraud, and money laundering.

Terrorist Financing. Since the terrorist attacks of September 11, 2001, the U.S. Government pursues efforts to combat foreign actors such as ISIS, Al Qaeda, Hezbollah and Iran's Islamic Revolutionary Guard Corps, as well as domestic violent extremist threats. Further, because terrorist groups require financing to recruit and support their operations, to prevent such financing is a priority for U.S. law enforcement.

Fraud. Bank, consumer, healthcare, securities, investment, and tax fraud are believed by the Government to generate the largest share of illicit proceeds in the U.S. Critically, fraud related to the COVID-19 pandemic is of particular concern to the DOJ and other U.S. agencies.

Transnational Criminal Organization Activity ("TCOs"). U.S. law enforcement targets international organized crime networks, as well as their involvement in a wide array of illicit activities, including cybercrime, drug trafficking, human trafficking, weapons trafficking and intellectual property theft. While Mexican and Russian TCOs are deemed priority threats by U.S. agencies, Africa and Asia-based TCOs are becoming more significant each year.

Drug Trafficking Organization Activity. U.S. agencies are increasingly interested on professional money laundering networks in Asia that facilitate the exchange of Chinese and U.S. currency or serve as brokers in trade-based money laundering schemes. Notably, the U.S. seeks to fight schemes to launder drug money by

facilitating the exchange of cash proceeds from Mexican DTOs to Chinese citizens residing in the United States, including the use of front companies or couriers to deposit cash derived from the sale of narcotics into the U.S. banking system.

Human Trafficking and Human Smuggling. The Government is reportedly interested in the variety of mechanisms used by human trafficking and human smuggling networks to move illicit proceeds, including cash smuggling and establishing shell or front companies to hide the true nature of their business.

Proliferation Financing. U.S. agencies are determined to investigate the proliferation and support networks that seek to exploit the U.S. financial system to move funds that will be used either to acquire weapons of mass destruction, or in furtherance of state-sponsored weapons programs, including the evasion of United Nations or U.S. sanctions.

26. Have there been any landmark or notable cases, investigations or developments in the past year?

Cryptocurrency, known for its investment potential and as a means of payment, sets itself apart by being encrypted and utilizing blockchain technology. The FTX cryptocurrency exchange platform rose rapidly on 2019, but it crashed in November 2022. FTX's downfall stemmed from the leaking of its balance sheet, which revealed a lack of diversification and excessive interdependence between affiliated companies. This led to FTX's collapse, causing significant depreciation in the value of its cryptocurrency (FTT) and prompting mass withdrawals by customers. The company's founder, Bankman-Fried, faced multiple fraud charges, including money laundering, wire fraud, campaign finance violations, and securities fraud, resulting in his arrest on December 12, 2022. FTX also faced a class-action lawsuit from investors and celebrity endorsers, accusing the platform of false representation, deceptive conduct, and the misuse of funds in a Ponzi scheme.

The result of Bankman-Fried's arrest prompted discussions about regulating the cryptocurrency industry by the SEC and Congress. Unlike traditional U.S. banks with government-backed deposit insurance, the lack of such backup for cryptocurrency exchanges poses major challenges in case of bankruptcy.

On the other hand, over the past year, the U.S Government implemented additional efforts to aggressively investigate and prosecute international corruption. DOJ criminally charged individuals and corporations for FCPA violations in connection with the bribery of foreign officials in or from countries such as Ecuador, Malaysia, France, and Brazil. Moreover, OFAC sanctioned several individuals and entities under the Global Magnitsky Sanctions ("GLOMAG"), including, among others, nationals from Lebanon, Belarus, Mexico, Venezuela, United Arab Emirates, China, Syria, and North Korea.

Pursuant to GLOMAG, OFAC may sanction foreign persons and entities believed to be involved in serious human rights abuses or corruption in any foreign country, as well as those who assist or provide material support, including goods and services, to the designated persons or the targeted activities. Sanctioned individuals and entities are added to OFAC's List of Specially Designated Nationals and Blocked Persons (the "SDN List"), and all their property and interests in property, within or transiting U.S. jurisdiction or in the possession or control of U.S. persons, are categorically blocked.

The U.S. has also developed new initiatives to deter money laundering, corruption and other criminal activity in Central America, including the 2022 and 2023 editions of the Section 353 List of Corrupt and Undemocratic Actors for Guatemala, Honduras, and El Salvador (also known as the "Engel List"). The Engel List is an annual report that the State Department submits to the Congress identifying individuals that the agency believes have engaged in acts of significant corruption, and exposes the individuals to visa cancellations and/or OFAC Sanctions. Also, in March 2023, the DOJ and the SEC released a Spanish Edition of a Resource Guide of the U.S. FCPA. This Guide is meant to serve as a resource for law enforcement partners, companies, practitioners, and the public with the aim to fight against corruption in Spanish speaking countries.

Most recently, NSD, BIS, and OFAC published a Tri-Seal Compliance Note (the "Compliance Note") on the Voluntary Self-Disclosure of Potential Violations ("VSD") of Sanctions, export controls, and national security laws. In this Compliance Note, NSD encourages companies to promptly disclose potential criminal violations of U.S. sanctions and export control laws. More specifically, the Compliance Note confirms that companies may avoid criminal liability by voluntarily self-disclosing potential violations, sharing all relevant non-privileged facts, providing NSD timely access to material documents and information, and by effectively remediating any compliance deficiencies and implementing a robust compliance and ethics program. This enforcement policy extends to other corporate crimes related to national security, including laws against terrorist financing, and potential violations of the regulations administered by

the Committee on Foreign Investment in the U.S.

Similarly, in the Compliance Note, BIS strongly encourages companies to voluntarily disclose potential violations of the Export Administration Regulations and confirms that timely and full cooperation with BIS will result in lower civil penalties pursuant to BIS's settlement guidelines, if the disclosing entity faces enforcement actions. OFAC also encourages voluntary disclosures of apparent sanctions violations. As highlighted in the Compliance Note, OFAC considers VSDs as a mitigating factor in determining enforcement actions for a particular case.

Additionally, the Compliance Note highlights the substantial monetary rewards that whistleblowers may receive from FinCEN for providing information regarding Sanctions and export control violations. Indeed, the Compliance Note confirms that, consistent with the whistleblower framework introduced by the Anti-Money Laundering Act of 2020 and the Anti-Money Laundering Whistleblower Improvement Act, successful enforcement actions related to certain U.S. export control violations could be eligible for financial awards under the Whistleblower Provisions.

27. Are there any planned developments to the legal, regulatory and/or enforcement framework?

Regarding cryptocurrency industry, there is an ongoing debate regarding which federal agency should assume the role of the primary regulator for cryptocurrencies: the Commodity Futures Trading Commission ("CFTC") or the SEC. Both agencies have been actively pursuing enforcement actions against cryptocurrencies under their perceived jurisdiction.

This conflict emerges from the uncertainty about which digital assets fall under the regulatory authority of the CFTC as commodities and which fall under the SEC's domain as securities. The competing claims of jurisdiction from both the CFTC and the SEC underscore the need for greater clarity in distinguishing between these categories. Moreover, an underlying issue persists regarding whether the current regulatory framework of the SEC and CFTC is adequate for effectively overseeing crypto markets or if legislative action is required.

As the landscape of crypto regulation continues to evolve, new regulatory framework is likely to emerge, incorporating the regulatory authority of both the SEC and CFTC. For example, a bipartisan bill was introduced on July 12, 2023, in the U.S. Senate with the goal of ensuring consumer protection and responsible financial innovation in the realm of cryptocurrency. The bill proposes to include crypto assets within the regulatory scope and designates oversight authority primarily to the CFTC. The bill's key feature is the granting of exclusive jurisdiction to the CFTC for regulating transactions involving most forms of cryptocurrency. Despite this, the SEC would maintain partial jurisdiction over digital assets as outlined in the bill. It remains pending the approval of the bill.

In other matters, on September 30, 2022, FinCEN issued a final rule regarding Beneficial Ownership Information Reporting Requirements. The final rule requires certain companies, including domestic and foreign corporations and LLCs, domestic entities created by filings with a secretary of state (or similar), and foreign entities registered to do business in any U.S. jurisdiction, to file with FinCEN reports that identify two categories of individuals: (i) the beneficial owners of the entity; and (ii) the company applicants of the entity. The rule provides that a beneficial owner is an individual who, directly or indirectly, either owns or controls at least 25% of the reporting entity or exercises substantial control over the reporting entity.

The above final rule implements Section 6403 of the Corporate Transparency Act ("CTA") and is intended to help prevent and combat money laundering, terrorist financing, corruption, tax fraud, and other illicit activity while minimizing the burden on entities doing business in the United States. The rule will take effect on January 1, 2024. On March 24, 2023, FinCEN also released additional guidance materials on its final rule establishing BOI requirements. The guidance materials include a BOI Key questions, reporting dates, frequently asked questions, and other resources to aid the public, and in particular the small business community, in understanding the new reporting requirements.

Further, on December 15, 2022, FinCEN proposed a regulation regarding Beneficial Ownership Information Access and Safeguards, that will be reported to FinCEN pursuant to Section 6403 of the CTA enacted into law as part of the AML Act. The proposed regulations would implement the strict protocols on security and confidentiality required by the CTA to protect sensitive personally identifiable information ("PII") reported to FinCEN. The Notice of Proposed Rulemaking ("NPRM") explains the circumstances in which specified recipients would have access to BOI and outlines data protection protocols and oversight mechanisms applicable to each recipient category. The disclosure of BOI to authorized recipients in accordance with appropriate protocols and oversight will help law enforcement and national security agencies prevent and combat money laundering, terrorist financing, tax fraud, and other illicit activity, as

well as protect national security. FinCEN is also proposing regulations to specify when and how reporting companies can use FinCEN identifiers to report the BOI of entities.

Additionally, related to FinCEN's implementation of the AML and CTA Acts, on January 17, 2023, FinCEN issued two notices seeking comments from all interested parties on (1) the mechanism that FinCEN proposes to use in collecting BOI from covered companies (the "BOI Report Notice"), and (2) the application FinCEN proposes to use when requiring individuals to obtain a FinCEN identifier (the "FinCEN Identifier Notice").

Another development worth nothing is that, on December 29, 2022, President Biden signed the Anti-Money Laundering Whistleblower Improvement Act (the "2022 AML Act"), which amends and strengthens the existing 2021 Anti-Money Laundering Act and enhances the incentives and protections for whistleblowers reporting violations related to money laundering. The 2022 AML Act includes provisions related to the following topics:

- **Coverage Expansion**. The Act broadens the scope of reporting requirements to include violations of financial management rules and OFAC Sanctions.
- **Whistleblower Protection**. The Act provides strong protections to whistleblowers, allowing both U.S. and international employees to be eligible for awards if they provide original information leading to successful enforcement actions and significant monetary sanctions.
- **Minimum Whistleblower Award**. The Act establishes a minimum whistleblower award of 10% of the collected monetary sanctions, ensuring that whistleblowers are incentivized to come forward. This minimum award structure creates a stronger incentive for employees to report suspected violations.
- **Revolving Fund**. The Act establishes a dedicated revolving fund to pay whistleblower awards, funded by the monetary sanctions collected from covered actions and the investment income of the fund. This change removes the dependence of awards on congressional appropriations and provides more stability and certainty in award payments.

For employers operating in the financial sector and subject to these laws, the Act means an increased likelihood of receiving reports from employees regarding potential violations. To protect themselves, employers should maintain robust compliance practices, respond effectively to reports that require investigation, and ensure that whistleblowers are safeguarded from retaliation for their reports.

28. Are there any gaps or areas for improvement in the financial crime legal framework?

Nowadays, there is a huge gap on regulating cryptocurrency in comparison with other countries. For example, in Brazil Cryptocurrency regulation was voted late last year in the Brazilian congress. Further, the Brazil Cryptocurrency regulation came into force on June 20, 2023. Likewise, the European Council adopted a package of rules known as Markets in Crypto Assets. The rules were endorsed by the European Parliament lawmakers in April 2023, and it is expected for them to start taking effect in phases starting in July 2024.

In other matters, as part of the U.S. efforts to fight financial crime, OFAC has the power to impose the so-called financial death penalty on domestic and foreign individuals and entities by adding their names to the List of Specially Designated Nationals and Blocked Persons (SDN List). While grounds for such listing vary across the statutory authorities that OFAC administers and enforces, the consequence for persons added to OFAC's SDN List is always the same: anyone who falls within U.S. jurisdiction is barred from transacting with them, and all of their U.S. property is immediately blocked. Over the years, scholars, practitioners, and non-governmental associations have raised concerns about OFAC's powers, including the lack of substantial checks on the designation of persons in the SDN List. These concerns about OFAC's list-based sanctions have increased due to the creation of new grounds whereby persons can be added to the SDN List.

One concern about OFAC's list-based sanctions, namely the lack of a deadline for OFAC to resolve the petitions that sanctioned individuals or entities may submit seeking removal from the SDN List (also known as "delisting petitions"). Indeed, Congress did not establish a specific deadline for OFAC to resolve such petitions. OFAC is required to meet the general requirement under the Administrative Procedure Act to complete administrative matters within "a reasonable time." As a result, OFAC can reportedly take years to review and arrive to a determination.

To address this area for improvement, Congress could create a statutory deadline for OFAC to respond delisting petitions. For instance, Congress can model this delisting deadline based on the deadline that the U.S. Secretary of State ("SecState") has under the Immigration and

Nationality Act (INA) to decide the “revocation” petitions of organizations designated as Foreign Terrorist Organizations. Indeed, INA establishes a 180-day deadline for SecState to decide these petitions.

The establishment of a specific time frame for completion of the process would not only benefit persons seeking relief from OFAC but may positively impact the effectiveness of Sanctions. Designated parties will see their cases moving along rather than pending for years, and may be more motivated to cooperate with OFAC in its intelligence gathering efforts, including in providing OFAC information about other Sanction targets, potential targets, transactions conducted in violation of Sanctions, criminal activity, or other information relevant to the U.S. national security.

Contributors

Javier Coronado
Partner
jcoronado@diazreus.com

Michael Diaz, Jr.
Global Managing Partner
mdiaz@diazreus.com