TRENDS IN WHITE-COLLAR ENFORCEMENT: OVERVIEW AND OUTLOOK

October 27, 2022

Adam Hollingsworth
Partner
ahollingsworth@jonesday.com
216.586.7235

Justin Herdman
Partner
jherdman@jonesday.com
216.586.7113

CLE ACADEMY WEEK HOUSEKEEPING ITEMS

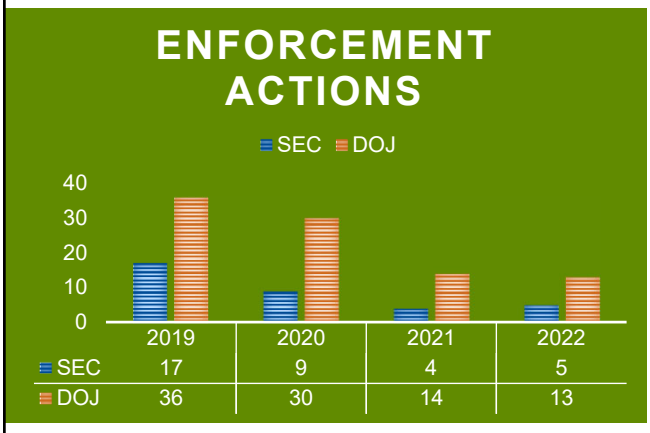
CLE Credit	Q & A	Evaluation Survey
During the presentation 2 CLE codes will appear. Please record those codes on your Affirmation Form. After your final CLE Academy Week session, forms should be emailed to jdcle@jonesday.com.	Please utilize the Q&A box to ask the presenters questions. If your question does not get addressed during the session, we will follow up with via email.	A new browser tab will open after the session ends. Please take a moment and let us know how we did!

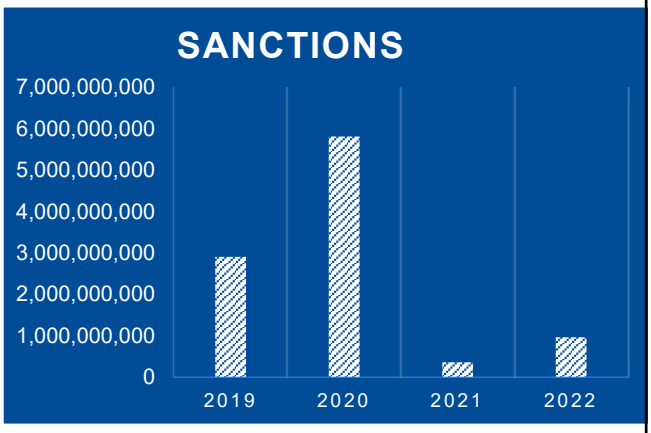
FCPA REVIEW

FOREIGN CORRUPT PRACTICES ACT ("FCPA") BASICS

- Contains both anti-bribery prohibitions and accounting requirements
- Applies to:
  - (1) persons with formal ties to the U.S.; and
  - (2) those who take action in furtherance of a violation while in the U.S.
- Five Basic Elements
- Covered entities can be subject to criminal charges resulting in imprisonment, fine, and penalties
- Bribe need not actually be paid; FCPA prohibits the offer, authorization, or promise to make such corrupt payment

FCPA STATISTICS AND TRENDS





SECOND CIRCUIT CLARIFIES FCPA JURISDICTION - *HOSKINS*

***United States v. Hoskins* – Second Circuit – August 2022**

- Hoskins charged with conspiracy to violate FCPA and substantive FCPA anti-bribery violations
- UK national, non-US resident
- Charged stemmed from Hoskins' alleged selection and authorization of bribery payments to Indonesian government officials while he was working from France
- District court found Hoskins directly violated the FCPA anti-bribery provisions as an agent of a domestic concern. Second Circuit affirmed on appeal
- Hoskins found guilty at trial, but district court granted Hoskin's motion for acquittal
- Second Circuit upheld district court acquittal

SECOND CIRCUIT CLARIFIES FCPA JURISDICTION - *HOSKINS*

***United States v. Hoskins* – Second Circuit – August 2022**

"While there is some evidence that Hoskins supported [Alstom Power] in his working relationship with the corporation, it is not sufficient to establish that [Alstom Power] ***exercised control over the scope and duration of its relationship with Hoskins***. ***Without this control over the relationship, there can be no finding of a principal-agent relationship within the meaning of the FCPA***."

NOTABLE FCPA ENFORCEMENT ACTIONS – GLENCORE

- Glencore made paid $100M to intermediary companies who secured improper advantages to obtain business with state-owned and-state controlled entities
  - Countries involved: Nigeria, Cameroon, Ivory Coast, Equatorial Guinea, Brazil, Venezuela, and the Democratic Republic of the Congo
- Glencore concealed the bribe payments by:
  - Entering into sham consulting agreements,
  - Paying inflated invoices, and
  - Using intermediary companies to make corrupt payments to foreign officials

NOTABLE FCPA ENFORCEMENT ACTIONS – GLENCORE

GLENCORE

DOJ – SDNY

- Conspiracy to violate FCPA
- $428.5M total criminal fine
- $272.2M criminal forfeiture
- 3-year independent compliance monitor
- No full cooperation credit
- Several factors influenced charging decision

NOTABLE FCPA ENFORCEMENT ACTIONS – GOL LINHAS AÉREAS INTELIGENTES

- GOL conspired to pay $3.8M in bribes to foreign officials in Brazil to secure legislation involving payroll and fuel tax reductions that financially benefitted GOL and other Brazilian airlines
  - GOL BoD member caused GOL to enter sham contracts with, and make payments to, entities connected to Brazilian officials
  - GOL maintained books and records falsely listing the corrupt payments as legitimate expenses

NOTABLE FCPA ENFORCEMENT ACTIONS – GOL LINHAS AÉREAS INTELIGENTES

- **SEC**:
  - Anti-bribery, books and records, internal accounting
  - $70M, but because of demonstrated financial condition and inability to pay, $24.5M
- **DOJ:**
  - Conspiracy to violate anti-bribery and books and records
  - $87M, but because of demonstrated financial condition and inability to pay, $17M
- Both SEC & DOJ noted GOL's cooperation and remedial acts, resulting in 25% reduction off guidelines fine range

TAKEAWAYS

1. FCPA enforcement activity has remained relatively stable since 2021, despite the Biden Administration's prior statements regarding aggressive enforcement.
2. DOJ must do more to prove foreign nationals acted as agents of domestic concerns for FCPA jurisdiction.
3. Recent enforcement actions like Glencore and Gol illustrate the Administration's emphasis on cross-border enforcement.

DEPUTY AG MONACO PROVIDES FURTHER REVISIONS TO CRIMINAL ENFORCEMENT POLICIES

- On September 15, 2022, Deputy Attorney General Lisa Monaco announced significant changes and updates to the Department of Justice's corporate criminal enforcement policies.
- The policy changes reflect DOJ's increasing focus on what it defines as "metrics" for evaluating the effectiveness of corporate compliance programs in making charging and resolution decisions as to companies.
- Companies should consider reviewing and, if appropriate, updating their compliance policies and procedures with the new DOJ policies in mind.

DEPUTY AG MONACO PROVIDES FURTHER REVISIONS TO CRIMINAL ENFORCEMENT POLICIES

- The DAG's Memorandum reinforces DOJ's commitment to aggressive enforcement of white-collar crime.
- Individual accountability remains a top DOJ priority.
- While the Memorandum contains provisions to further incentivize voluntary self-disclosures of suspected misconduct by companies, other policy changes make clear that a company's cooperation and compliance program will be closely scrutinized as part of any resolution process.

DEPUTY AG MONACO PROVIDES FURTHER REVISIONS TO CRIMINAL ENFORCEMENT POLICIES

- A company facing a DOJ criminal investigation should:
  - (i) expect DOJ to consider the adequacy of the corporate compliance program, including whether the company has adequate compensation clawback and mobile device policies;
  - (ii) understand that DOJ will consider the company's record of past misconduct (if any), and that certain types of prior misconduct will be treated differently than others; and
  - (iii) understand that to be eligible for full cooperation credit, the company must timely disclose all relevant, non-privileged facts about the misconduct of individuals.

DEPUTY AG MONACO PROVIDES FURTHER REVISIONS TO CRIMINAL ENFORCEMENT POLICIES

- As DOJ works to implement the new policies set forth in the Memorandum, companies should review their compliance programs to ensure that they adequately assess, monitor for, and remediate misconduct.
- Companies should specifically assess how their compensation systems encourage compliance and whether they are adequate to deter wrongdoing.

DEPUTY AG MONACO PROVIDES FURTHER REVISIONS TO CRIMINAL ENFORCEMENT POLICIES

- A company's decision whether to self-disclose potential corporate wrongdoing to DOJ is complex and requires thoughtful consideration on a case-by-case basis.
- While the Memorandum provides some additional clarity regarding DOJ's expectations for companies seeking maximum cooperation credit, a company's self-disclosure decision will necessarily depend on the specific facts and circumstances at issue.
- Such decisions should be driven by an informed assessment of all relevant considerations, including, but not limited to, DOJ policy.

DOJ ADDS RESIDENT DATA EXPERT

- Matt Galvin joined DOJ's Fraud Section in September
- Will be resident compliance and big data expert
- Brings expertise in program meant to identify troubling transaction patterns through data analytics and risk scoring

SEC SEEKS RESOURCES FOR GROWING WHISTLEBLOWER REPORTS

- SEC Chairman Gensler testified about SEC's need for additional resources to handle surge in whistleblower complaints
- SEC received 12,210 reports of alleged wrongdoing in SEC's FY 2021
- That figure doubled from the 6,911 submitted to SEC in FY 2020
- Gensler requested an 8% increase to SEC's budget for 2023
- Gensler hoped to hire 125 new employees – 44 aimed at investigating misconduct and accelerating litigation and 34 to support ongoing litigation
- Gensler estimated SEC would open approx. 1,500 investigations by end of FY 2022 with 30 more by end of 2023

NOTABLE CASES / PROSECUTIONS

theranos

NOTABLE CASES / PROSECUTIONS

"[C]ompanies are on the front lines in confronting today's geopolitical realities. In today's world, corporate crime regularly intersects with national security in areas like terrorist financing, sanctions evasion, and cybercrime." Lisa O. Monaco, Deputy Attorney General

- In October 2022, Lafarge S.A. and its Syrian subsidiary pled guilty to providing material support to foreign terrorist organizations.
- Lafarge admitted to paying ISIS and the Al Nusrah Front foreign terrorist organizations in exchange for permission to operate a cement plant in Syria from 2013 to 2014
- Lafarge generated approximately $70.3 million in revenue as a result of the scheme.
- This is the first corporate material support for terrorism prosecution.
- Lafarge was sentenced to probation and to pay penalties, including criminal fines and forfeiture, totaling $777.78 million.

KEY POINTS

TAKEAWAYS

DOJ:

1. Expect an increase in white-collar enforcement
2. Data becoming important in corporate compliance programs
3. Companies should consider reviewing and updating their compliance policies and procedures with the new DOJ policies in mind

SEC:

1. Expect to see an increase in enforcement with growing number of whistleblower complaints

SANCTIONS IMPLICATIONS FROM RUSSIAN WAR IN UKRAINE

- Sanctions have targeted institutions, state-owned enterprises, and political elites.
- Restrictions on debt and equity instruments.
- Broad range of financial and investment restrictions.
- Several countries have also imposed broad import and export controls restricting access to commodities, industrial products, software, technology, and luxury goods.
- Various sanctions regimes share common features but there remains significant variation in scope across regimes.
- Landscape will evolve over time; no one-size-fits-all approach.

BIDEN ADMINISTRATION AND DOJ CYBERSECURITY PRIORITIES

Executive Order 14028 – Improving the Nation's Cybersecurity	• Protecting against malicious cyber campaigns is a matter of national concern and a top priority for the Administration • The prevention, detection, assessment and remediation of cyber incidents is a top priority
DOJ Civil Cyber-Fraud Initiative	• DOJ will use the False Claims Act to identify, pursue and deter cyber vulnerabilities and incidents that arise with government contracts and grants • DOJ will hold accountable entities or individuals that put U.S. information or systems at risk

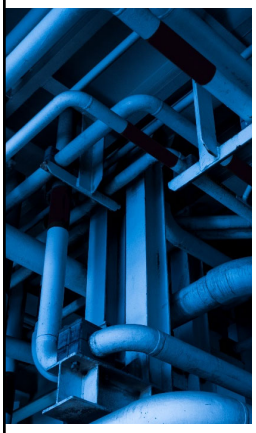
CYBERSECURITY FAILURES AND THE FALSE CLAIMS ACT

Knowing failures to comply with cybersecurity standards.	Knowing misrepresentation of security controls and practices.	Knowing failure to timely report suspected breaches.

BIDEN ADMINISTRATION CONSIDERS RANSOMWARE ATTACKS NATIONAL SECURITY PRIORITY

- The White House has elevated ransomware attacks to a national and international security issue
- Recently convened the largest multinational gathering to address the issue
- The White House has issued several rounds of guidance and best practices
- In September 2021, the Office of Foreign Assets Control (OFAC) issued an advisory highlighting potential sanctions risks for parties that make or facilitate payments to malicious cyber actors
- OFAC also designated a virtual currency exchange, SUEX OTC, S.R.O. ("SUEX"), for complicit financial services for the first time

CYBER REPORTING FOR CRITICAL INFRASTRUCTURE



- In March 2022, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act of 2022.
- Creates new requirements for operators of critical infrastructure to report certain cyber incidents and related ransom payments such as:
  - Report substantial cyber incidents to CISA within 72 hours.
  - Provide reports and updates to CISA until the incident has concluded.
  - Report ransom payment to CISA within 24 hours.
  - Preserve data related to cyber incidents or ransom payments in accordance with CISA procedures.

RANSOMWARE BEST PRACTICES FOR THE PRIVATE SECTOR

- Executive Order Best Practices: Multifactor authentication; endpoint detection and response; encryption; and skilled and empowered security teams
- Backup data, system images, and configurations
- Update and patch
- Test incident response plan
- Check the work of the security team
- Segment networks

UBER'S FORMER CSO CONVICTED IN DATA-BREACH COVERUP

- Uber's former head of security was found guilty of criminal obstruction for attempting to cover up a 2016 data breach.
- The 2016 breach saw tens of millions of customer and driver records stolen.
- After learning of the breach, Joseph Sullivan began a scheme to hide it from the FTC, which had been investigating a 2014 breach.
- Sullivan was fired in 2017 and in 2020 charged with one count of obstruction and one count of misprision of a felony.
- The trial is believed to be the first time a company executive has faced criminal prosecution over a hack.

ADDITIONAL CYBERSECURITY RESOURCES

- **Jones Day Insights**: *DOJ Announces Civil Cyber-Fraud Initiative*, October 2021, (https://www.jonesday.com/en/insights/2021/10/doj-announces-civil-cyberfraud-initiative)
- **Podcast**, **Jones Day Talks**: *A False Sense of Security: Cyber Disclosure Obligations for Public Contractors,* September 2021 (available on Apple Podcasts; Android; Google Play; and Stitcher)
- **Jones Day Insights**: *Cybersecurity Executive Order Establishes Framework to Strengthen Cybersecurity Elements of federal Government Contracts*, May 2021, (https://www.jonesday.com/en/insights/2021/05/cybersecurity-executive-order-establishes-framework-to-strengthen-cybersecurity-elements-of-federal-government-contracts)

FTC PROPOSED RULEMAKING REGARDING COMMERCIAL SURVEILLANCE AND DATA SECURITY

- The FTC announced in August 2022 that it is seeking public comment regarding its Advanced Notice of Proposed Rulemaking on commercial surveillance and data security.
- The FTC's goal is to determine whether to issue regulation to address commercial surveillance and lax data security.
- The FTC defines commercial surveillance as "the business of collecting, analyzing, and profiting from information about people."
- The FTC feels surveillance heightens the risks and stakes of data breaches, deception, manipulation, and other abuses.

KEY POINTS

TAKEAWAYS

1. Increased scrutiny of Federal Government contractors' and grantees' cybersecurity practices
2. Expect more rigorous incident reporting demands from Federal Government agencies
3. Self-reporting cybersecurity incidents—particularly ransomware incidents—may be considered a mitigating factor in enforcement actions

QUESTIONS?


JONES DAY
One Firm Worldwide®