Morgan Lewis

GLOBAL PUBLIC COMPANY ACADEMY: SEC ENFORCEMENT TRENDS AND PRACTICAL CONSIDERATIONS

Kelly Gibson, Erin Martin, Carolyn Welshhans, Mims Zabriskie

May 21, 2025

© 2025 Morgan, Lewis & Bockius LLP

Presenters



Kelly L. Gibson

Partner | Philadelphia / New York



Erin E. Martin

Partner | Washington DC / New York



Carolyn M. Welshhans

Partner | Washington DC



Mims Zabriskie

Partner | Philadelphia

Program Overview

- Enforcement Priorities (What is In and Out, and Remedies)
- Financial Disclosures
- Reg FD
- Insider Trading
- Corporate Perquisites
- Cybersecurity
- Getting Ahead of the SEC

Enforcement Priorities

Morgan Lewis | Global Public Company Academy

SEC Enforcement Priorities



Enforcement Priorities That are 'Out'

- Crypto
- Stand alone off channel communications/books and records
- Creative theories (e.g., Panuwat)



Substantive Areas of Enforcement That are 'In'

- Insider trading (back to basics)
- Fraud and cases that sound in fraud
- AI (new)



Effect on Remedies

- Focus on disgorgement/returning money to investors/clients
- Expect penalties to return to supportable amounts
- Cooperation, remediation, and ICCs
- Individual Accountability

Financial Disclosures

Morgan Lewis | Global Public Company Academy

Financial Disclosures:

Earnings estimates, analyst expectations, and more

Accounting Rules

- Inflating sales
- Channel stuffing
- Prematurely recognizing revenue
- Misclassifying revenue/expenses
- Improperly adjusting reserve accounts

Other Disclosures (non-GAAP)

- Can choose to tout other metrics
- But if a company does so, cannot be materially misleading
- Also have to disclose material risks or changes about those metrics
- Examples: types of sales, types of customers, etc.

SEC Cases

- Fraud charges
- Individual liability
- Large penalties and disgorgement
- Incentive compensation repaid
- Officer and director bars
- Bars for accountants/CPAs

Insider Trading

Morgan Lewis | Global Public Company Academy

Insider Trading



Reglatory scrutiny

SEC and FINRA conduct surveillance using trading data to detect potentially suspicious trading around market-moving announcements



Timely profits + market moves

Profits/losses avoided can be small (less than $100,000) but still trigger investigations when well-timed



Business transactions

Trading ahead of announcements regarding M&A, licensing agreements, earnings results, etc.



Product information

Trading ahead of announcements regarding FDA and CMS decisions, clinical trial results, etc.



Larger events

Regulatory notice may be spurred by larger events (e.g., the pandemic or market volatility) or after the SEC is already looking at a company (e.g., for disclosures)



Types of traders

Employees at all levels of a company (executives, IT managers, consultants, etc.), family members, friends, etc.



Morgan Lewis | Global Public Company Academy

Reg FD:
Selective disclosures, even with no insider trading

Prohibited conduct

- Public companies cannot selectively disclose material, nonpublic information
- Includes disclosures to institutional investors and securities analysts
- To cure, the company must publicly disclose the information not more than 24 hours later

Ex: MNPI and the FDA

- After two meetings with the FDA, company disclosed status of drug approval with plain vanilla language
- But executive provided sell-side analysts with further details (e.g., meeting was "very positive and productive")
- Did not provide public with the further details for another month

SEC action

- NYSE noticed the stock price and volume moves after the analysts published positive notes
- The SEC investigated, charged the company with violating Reg FD, and the company paid a $200,000 penalty.

Corporate Perquisites

Morgan Lewis | Global Public Company Academy

SEC rules related to perquisites disclosure

- Item 402 of Regulation S-K requires companies to disclose in the Summary Compensation Table of the proxy statement the total value of a named executive officer's perquisites (or "perks") if those perquisites exceed $10,000.
  - If the value of a single perquisite exceeds the greater of $25,000 or 10% of the total value of all perquisites reported, then the type and amount of such perquisite must also be identified in a footnote.
- A benefit is not a perquisite if it is "generally available on a nondiscriminatory basis to all employees" or if it is "integrally and directly related to the performance of the executive's duties."
- The SEC does not require a company to have any intention or knowledge of wrongdoing in order to impose fines or penalties.

SEC rules related to perquisites disclosure

- In recent years, the SEC has challenged companies' failures to disclose executive perquisites in proxies, often related to airline travel and other personal benefits.
  - In certain cases, the company's failure to disclose was due to the executive's failure to inform the company that it took certain flights or obtained certain benefits for personal non-business reasons. In those cases, the executive may also be under investigation in his personal capacity.
- The investigations have often led to settlements, and in many cases, penalties.
- The settlements have been disclosed in publicly available orders, which generally set forth the company's remedial efforts, and whether the company cooperated with the SEC's investigation.
- The SEC has not imposed penalties in certain cases where companies cooperated with investigations and self-reported the failures.

Cybersecurity

Morgan Lewis | Global Public Company Academy

What Disclosure is Required in SEC Filings?

- Current Reports on Form 8-K:
  - Disclosure of material cybersecurity incidents that address:
    - the material aspects of the nature, scope and timing of the incident; and
    - the material impact or reasonably likely material impact on the company, including its financial condition and results of operations.
  - Due date:
    - Within four business days of determining that such incident is *material.*

What Disclosure is Required in SEC Filings?

- Annual Reports on Form 10-K:
  - Disclosure regarding cybersecurity matters that address:
    - processes employed by companies to assess, identify and manage cybersecurity risks;
    - whether any cybersecurity risks have materially affected or are reasonably likely to materially affect a company's business strategy, results of operations or financial condition;
    - management's role in assessing and managing material risks from cybersecurity threats; and
    - boards of directors' oversight of cybersecurity risk.

Materiality Assessment

- Information is material if there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if a disclosure would significantly alter the total mix of information made available to investors.

- Materiality is viewed from both a quantitative and qualitative perspective.

- SEC provided non-exhaustive list of factors that it expects a public company to consider in assessing materiality:
  - Reputational damage;
  - Data theft;
  - Asset, intellectual property, or business value loss;
  - Harm to customer or vendor relationships;
  - Competitive harm; and
  - The possibility of litigation or regulatory investigation or actions.

Additional SEC Guidance

- Post-adoption, the SEC provided additional guidance to clarify expectations:
  - Item 1.05 of Form 8-K should only be used for *material* cybersecurity incidents.
    - Historical practice included disclosure under Item 7.01 or Item 8.01 of Form 8-K to disclose cybersecurity incidents, including those that may not be material;
    - Early Item 1.05 of Form 8-K filings disclosed cybersecurity incidents where the materiality determination had not yet been made.
- Staff comment letters on Form 10-K disclosures focused on material noncompliance and information related to the role of third parties.

How to Prepare



Focus on public companies

Sensitive customer information

Nonpublic company information



SEC scrutiny

SEC pays attention to news reports, company filings, whistleblower reports, market reactions, referrals from criminal authorities, etc.



How did the hack work?

SEC will want to understand how the hack worked and focus on whether the company is on top of it, whether there is an ongoing issue, etc.



What were investors told?

SEC will review disclosures to investors and compare to what the company said internally about the incident and its cyber risks more generally



Did anyone monetize?

SEC will analyze trading data to determine whether the hackers traded on stolen information or whether any insiders traded ahead of news of the hack

Getting Ahead of the SEC

Morgan Lewis | Global Public Company Academy

Getting ahead of the SEC:
Proactive steps

SEC Filings:
Periodically review SEC filings and consider whether risk disclosures, financial disclosures, etc. need updated from an SEC ENF perspective

Other Public Statements:
Periodically review statements on website and other public forums and consider whether they remain accurate and timely

Knowledge:
Does the company understand what data it has, where the data is kept, and what employees have knowledge in case something does happen that would spark SEC interest?

Policies and Procedures:
Are the policies and procedures updated with an eye toward SEC rules and areas of interest?

Training:
Is the company's training for its employees tailored appropriately for its risks?

If something important happens:
Does it merit a disclosure to investors and/or SEC? Consider carefully what investors are being told in light of SEC precedent


Questions?
Morgan Lewis
Global Public Company Academy

Kelly L. Gibson



Kelly Gibson
Philadelphia | New York
+1.215.963.5121 | +1.212.309.6287
kelly.gibson@morganlewis.com

Kelly Gibson is the co-leader of the firm's securities enforcement practice and the firm's ESG and sustainability advisory practice. She previously held numerous national and regional leadership roles at the US Securities and Exchange Commission (SEC), including serving as the acting deputy director of the Division of Enforcement, as leader of the Enforcement Division's nationwide Climate and ESG Task Force, and as director of the SEC's Philadelphia Regional Office. Kelly advises and defends public companies, financial services clients, and their executives in SEC, self-regulatory organization (SRO), and state enforcement matters, and in internal investigations.

Erin E. Martin



Erin E. Martin
Partner
Washington, D.C.
+1.202.739.5729
erin.martin@morganlewis.com

Erin Martin counsels public companies and their boards with respect to securities regulation, capital markets transactions, and corporate governance matters, drawing on her long tenure at the US Securities and Exchange Commission (SEC) in the Division of Corporation Finance. Erin regularly advises on complex SEC disclosure and compliance issues, including environmental, social, and governance (ESG) considerations and crypto asset matters. Erin is the leader of the corporate and business transactions practice in the Washington, DC office.

Carolyn M. Welshhans



Carolyn M. Welshhans
Partner
Washington, D.C.
carolyn.welshhans@morganlewis.com

Carolyn held a number of senior leadership roles at the US Securities and Exchange Commission (SEC) before joining Morgan Lewis, including associate director of the SEC's Division of Enforcement, acting chief of the division's Crypto Assets and Cyber unit, and acting data officer for the division. She also served as an assistant director in the enforcement division's Cyber and Market Abuse units. Carolyn advises and defends public companies, startups, financial institutions, and their executives in investigations by the SEC and other financial regulators and in internal investigations.

While at the SEC, Carolyn supervised numerous significant enforcement actions that covered the entire breadth of the SEC enforcement program, including public company disclosure, accounting, and internal controls violations, cybersecurity, investment advisers, broker-dealers, market structure, unregistered offerings, insider trading, and manipulative trading. Carolyn draws on her government experience to work closely with the firm's investment management, corporate and business transactions, labor and employment, white collar defense, and cybersecurity, incident response, and privacy practices to advise clients on enforcement, regulatory, and litigation matters.

Mims Maynard Zabriskie



Mims Maynard Zabriskie
Partner
Philadelphia
mims.zabriskie@morganlewis.com

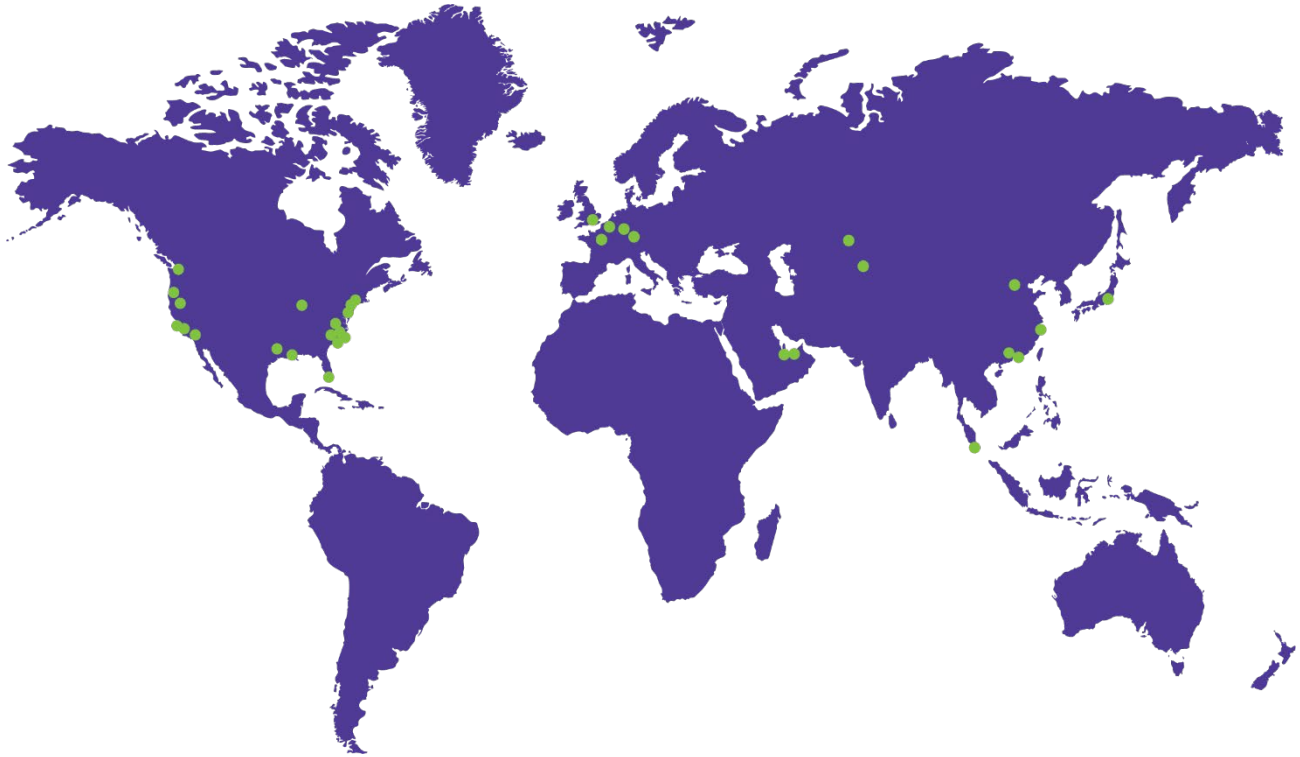
Mims Maynard Zabriskie advises on complex executive compensation and employee benefit plan matters, including the design, negotiation, and implementation of executive compensation, equity compensation, and tax–qualified retirement plans and shareholder approval of equity plans. She counsels large publicly and privately owned businesses, including Fortune 500 enterprises, as well as technology companies, colleges and universities, and other non-profit entities, on a range of legal issues related to executive compensation governance, and employee benefit plans.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Astana
Beijing
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong
Houston
London
Los Angeles
Miami
Munich
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Seattle
Shanghai
Shenzhen
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington



Morgan Lewis

Our Beijing, Shanghai, and Shenzhen offices operate as representative offices of Morgan, Lewis & Bockius LLP.
In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong.

THANK YOU

© 2025 Morgan Lewis

Morgan, Lewis & Bockius LLP, a Pennsylvania limited liability partnership
Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.
Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.
Our Beijing, Shanghai, and Shenzhen and offices operate as representative offices of Morgan, Lewis & Bockius LLP.
In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong.

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship.
Prior results do not guarantee similar outcomes. Attorney Advertising.