Navigating Fast-Changing Political Waters

Evolving Compliance Strategies for a Rapidly Changing Environment

Jay Greenberg
Ernst & Young LLP

Andrew Olsen
Stewart Title

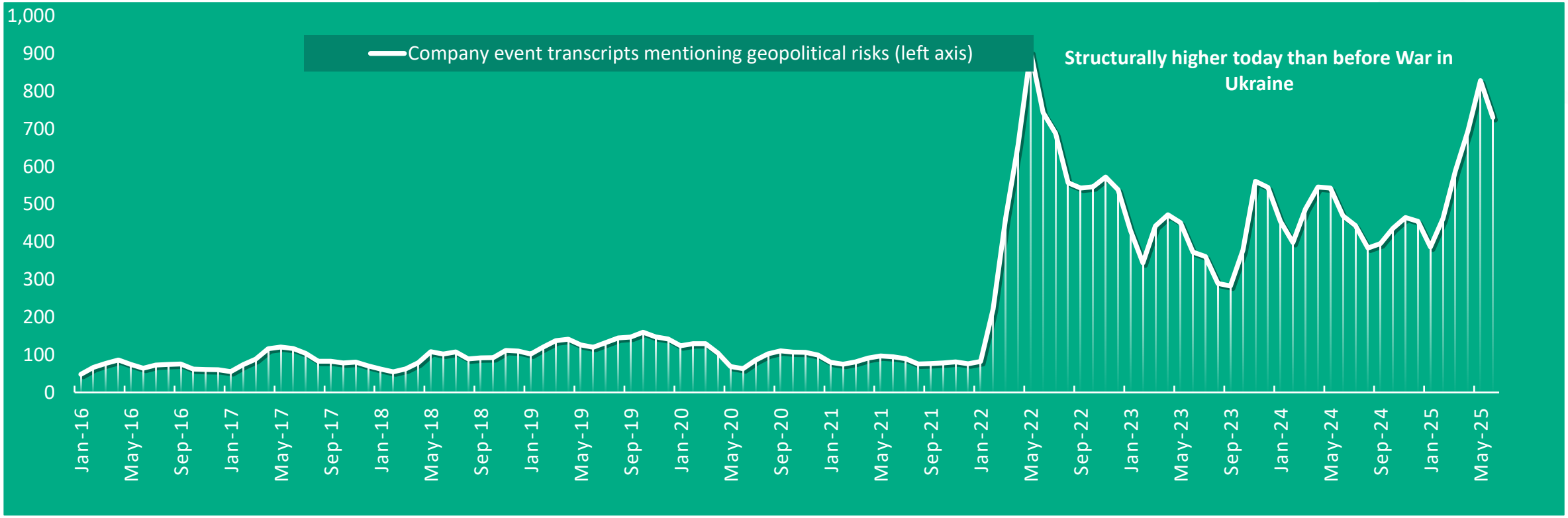
SAI360

Disclaimer

- Views expressed in this presentation are those of the speakers and do not necessarily represent the views of Ernst & Young LLP or other members of the global EY organization.
- This presentation has been prepared for general informational or training purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.
- Neither EY nor any member firm thereof shall bear any responsibility whatsoever for the content, accuracy or security of any third-party websites that are linked (by way of hyperlink or otherwise) in this presentation.
- EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.
-

This is still (relatively) new …

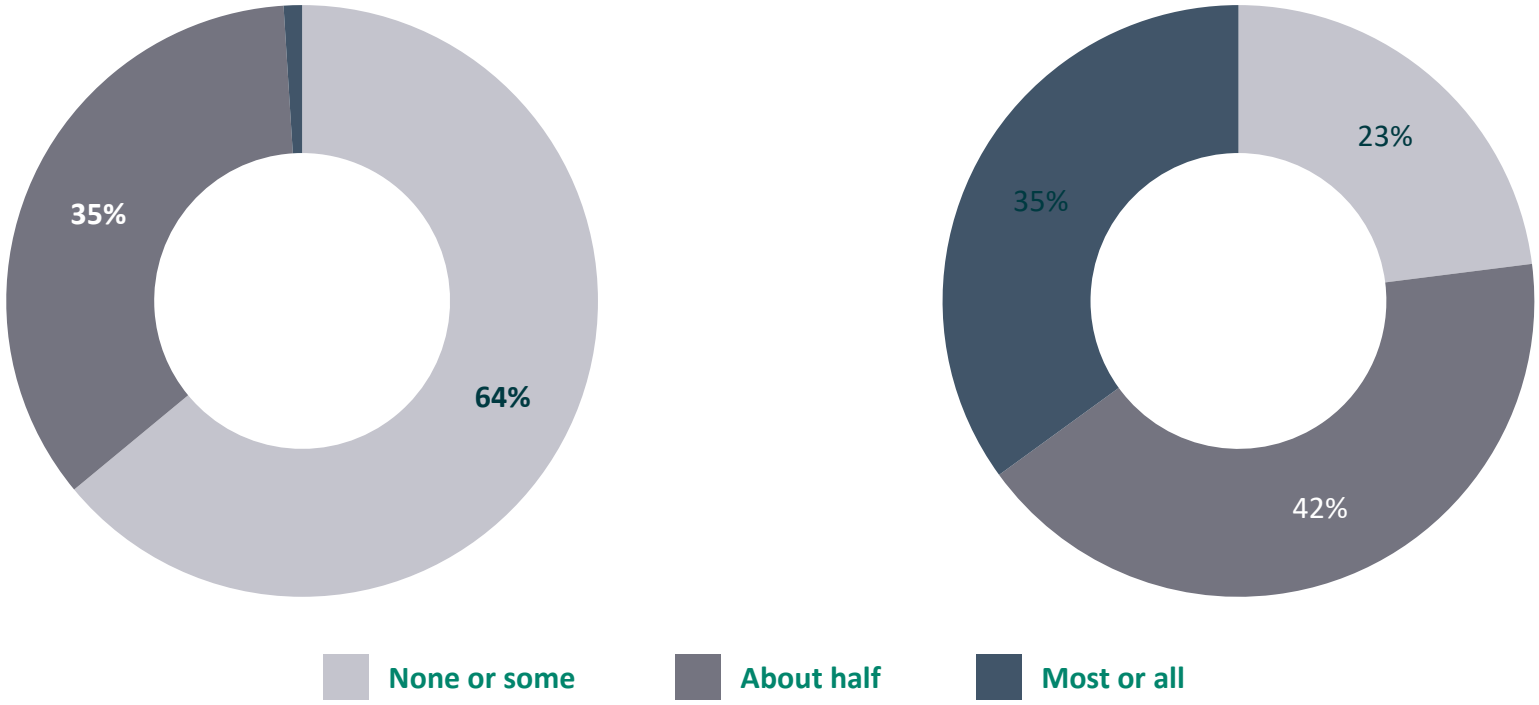
Company mentions of political risk skyrocketed in 2022 and have stayed higher due to the risk landscape



Source: Alphasense; EY Insights analysis
Note: The terms tallied in company event transcripts were “geopolitical risk(s),” “geopolitical,” “geopolitics” and “political risk(s).” This data is presented as a rolling three-month average.

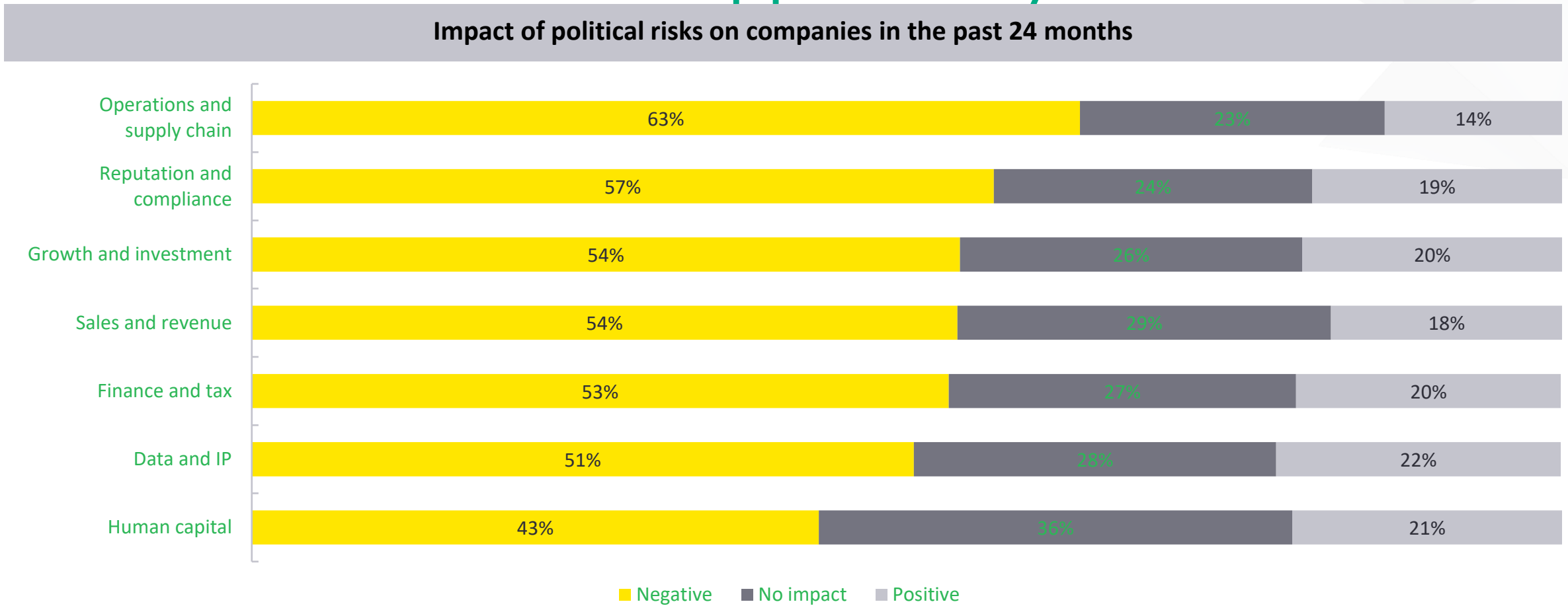
Businesses self-assess experiencing greater difficulty in predicting emerging risks

Of the political risk events that impacted your company over the past year, what proportion of them were unexpected?



Source: EY-Parthenon Geostrategy in Practice Survey 2021, 2025

Model the impact across your organization and balance risk and opportunity



Source: EY-Parthenon Geostrategy in Practice Survey 2025

8 Critical Compliance Topics

1

Anti-Money Laundering

AML obligations and risks

2

Digital Currency

Crypto compliance exposure

3

Relaxed Standards

Federal regulatory rollback risks

4

Cartel Exposure

Buying and selling risk

5

Sanctions

Current and shifting regimes

6

Fraud & Prosecutions

HHS and enforcement trends

7

Self-Reporting & Amnesty

Voluntary disclosure programs

8

Supply Chain Risk

3rd and 4th party exposure

Anti-Money Laundering (AML)

What It Is

Legal framework requiring detection and reporting of suspicious financial activity

Governed by BSA, FinCEN rules, and FATF international standards

Applies to banks, fintechs, insurers, and increasingly non-financial firms

Why It Matters

Fines exceed $1B+ for major violations; personal liability for officers

Cross-border transactions create multi-jurisdictional exposure

Non-bank entities increasingly targeted by FinCEN enforcement

Challenges

High volume of transactions overwhelms manual review processes

Shell company structures obscure beneficial ownership

Evolving typologies: crypto and trade-based money laundering

Regulatory uncertainty

Opportunities

AI and ML tools dramatically improve transaction monitoring accuracy

Public-private information sharing programs (FinCEN 314b)

Strong AML posture builds customer and regulator trust

Actions

Conduct AML risk assessment across all business lines

Update beneficial ownership verification procedures

Train frontline staff on red-flag recognition

Review automated monitoring thresholds quarterly

Consider outsourcing reporting requirements

Digital Currency Compliance

What It Is

Compliance obligations for crypto, stablecoins, and CBDC transactions

Governed by FinCEN, OFAC, SEC and CFTC with overlapping jurisdictions

Includes KYC/AML duties for virtual asset service providers (VASPs)

Why It Matters

Crypto used in sanctions evasion; OFAC has issued crypto-specific guidance

Companies receiving crypto payments face same AML obligations as banks

Regulatory clarity is increasing and enforcement is accelerating

Challenges

Pseudonymous transactions make tracing difficult

DeFi protocols lack centralized compliance controls

Cross-border transfers bypass traditional banking rails

Opportunities

Blockchain analytics tools enable transaction tracing

Early compliance positioning builds competitive fintech advantage

Proactive engagement with regulators signals good faith

Actions

Classify digital assets used or received by your business

Integrate crypto wallet screening into OFAC/sanctions checks

Update KYC (Know Your Customer) procedures for counterparties using crypto

Monitor FinCEN and OFAC crypto guidance monthly

Relaxed Compliance Standards

What It Is

Lowered de-prioritization of enforcement in ESG, FCPA, and certain AML rules

Rollback of compliance guidance

Reduced enforcement activity at DOJ, SEC, FinCEN

Why It Matters

State-level enforcement (NY, CA) continues or intensifies independently

Foreign regulators (EU, UK) are increasing scrutiny of US firms

Future administration may reverse rollbacks; past conduct is still prosecutable

Challenges

Compliance fatigue: if they are not enforcing it, why invest?

Difficulty maintaining program rigor without visible regulatory pressure

Inconsistent messaging across federal agencies creates uncertainty

Opportunities

Window to update programs quietly without regulatory scrutiny

Organizations that maintain standards gain competitive trust advantage

Use period to conduct internal audits and remediate gaps

Actions

Do not reduce compliance program investment based on perceived leniency

Document your compliance rationale for each jurisdiction

Monitor state AG offices for independent enforcement actions

Prepare for regulatory reversal and maintain audit trails

Cartel Exposure

What It Is

Executive Order designated Mexican cartels as Foreign Terrorist Organizations (FTOs)

US companies face IEEPA/material support liability for cartel transactions

Applies to supply chains, logistics, and distribution in cartel-controlled regions

Why It Matters

Criminal liability even if cartel involvement was unintentional

Payment of protection fees to cartels equals material support of terrorism

Manufacturing, agriculture and retail sectors most exposed in Mexico operations

Challenges

Cartel affiliates often disguised as legitimate local vendors or logistics firms

Ground-level employees may pay fees without management knowledge

Limited third-party intelligence on cartel-controlled territories

Opportunities

Proactive due diligence creates strong legal defense

Whistleblower and self-disclosure programs offer path to reduced liability

Reshoring or nearshoring supply chains reduces cartel-zone exposure

Actions

Map all Mexico/Latin America operations against cartel territory data

Add FTO-designation screening to vendor onboarding

Establish anonymous local reporting channel for payment coercion

Consult DOJ/OFAC for voluntary disclosure if past payments identified

Sanctions: Current and Shifting Landscape

What It Is

OFAC administers 30+ active sanctions programs (Russia, Iran, China, DPRK, Cuba)

SDN List, Sectoral Sanctions, and secondary sanctions apply to US persons globally

Strict liability standard: intent is not a defense

Why It Matters

Russia/Ukraine sanctions remain active despite political shifts

China technology export controls expanding under BIS/OFAC coordination

Secondary sanctions risk: non-US subsidiaries doing business with sanctioned parties

Challenges

SDN list changes can occur overnight; screening must be near-real-time

50% ownership rule: indirect exposure through partially sanctioned entities

US-EU divergence creating compliance conflicts for multinationals

Opportunities

OFAC Voluntary Self-Disclosure program offers significant penalty reduction

General licenses provide compliant pathways in some restricted markets

Robust screening systems are now cloud-accessible and affordable

Actions

Implement automated SDN/OFAC screening with daily list updates

Apply the 50% ownership rule to all counterparty structures

Brief board on current geopolitical sanctions exposure quarterly

Review licenses for any transactions touching restricted jurisdictions

Fraud, HHS and Prosecution Trends

What It Is

Federal enforcement of healthcare fraud via HHS Office of Inspector General

False Claims Act (FCA): qui tam ("he who brings an action for the king as well as for himself") provisions allow private citizen suits

DOJ Civil Fraud and Criminal Division pursue wire, mail and procurement fraud

Why It Matters

Finance, insurance and billing companies increasingly named in fraud investigations

FCA recoveries in the billions

Individual executives face criminal liability, not just fines

Challenges

Whistleblower protections incentivize internal reporting directly to DOJ

Complex billing relationships obscure fraud in supply chains

Retroactive prosecution risk from legacy billing practices

Opportunities

Early internal detection enables self-disclosure before whistleblower filing

Robust compliance programs cited as mitigating factor in DOJ prosecutions

Proactive engagement with OIG advisory opinions reduces ambiguity

Actions

Audit billing and claims processes for FCA exposure

Implement a confidential internal reporting hotline, strengthen Code of Conduct, demonstrate culture of compliance

Train finance and operations staff on fraud red flags

Review all government-adjacent contracts for compliance obligations

Self-Reporting and Amnesty Programs

What It Is

Voluntary self-disclosure (VSD) programs exist at DOJ, OFAC, BIS, and FinCEN

Antitrust leniency: first company to self-report cartel activity gets immunity

DOJ Corporate Enforcement Policy rewards proactive disclosure with reduced charges

Why It Matters

OFAC VSD can reduce civil penalties by 50% or more

DOJ may decline prosecution entirely for timely and full disclosure

Discovery by regulators before self-report eliminates most benefits

Challenges

Disclosure triggers full investigation; scope may expand beyond original issue

Timing is critical: late disclosure loses preferential treatment

Multi-agency exposure: disclosing to one agency may trigger others

Opportunities

First-in advantage: antitrust leniency rewards speed with full immunity

Demonstrates good-faith compliance culture to regulators

Allows controlled narrative vs. reactive enforcement defense

Actions

Establish a VSD decision protocol with legal counsel pre-approved

Include self-reporting triggers in your compliance incident response plan

Know the current VSD windows for OFAC, DOJ, and BIS

Document all investigation steps from point of discovery

Supply Chain Compliance

What It Is

Third-party risk: compliance obligations of your direct vendors

Fourth-party risk: your vendors' vendors, often invisible to compliance teams

UFLPA, FCPA, and sanctions apply across the entire supply chain

Why It Matters

Companies are becoming increasingly more responsible for ensuring that suppliers are compliant

FCPA enforcement holds companies liable for bribes paid by agents and distributors

Reputational damage from supply chain violations spreads rapidly

Challenges

Sub-tier suppliers are often unknown to the buying company

Contractual audit rights rarely exercised below tier 2

Geographic concentration in high-risk jurisdictions is common

Tariffs, sanctions, and economic conditions squeezing downstream suppliers may cause them to stray from compliance

Opportunities

Greater awareness and understanding of regulatory requirements make it easier to place contractual terms on downstream suppliers

Supply chain mapping tools now provide n-tier visibility

Diversifying supplier base reduces concentration and compliance risk

Strong supply chain compliance improves ESG ratings and investor confidence

Actions

Map your n-tier vendors and review consistently

Screen all new vendors against OFAC, BIS, and FTO lists

Implement contractual controls over downstream vendors to the extent possible

Ongoing monitoring of suppliers is key

Key Takeaways

1 **AML**

AML obligations now extend beyond banks: any business processing financial flows needs a program

2 **Digital Currency**

Crypto transactions carry full AML and sanctions exposure: treat them like wire transfers

3 **Relaxed Standards**

Reduced federal enforcement today does not erase liability tomorrow or from states: maintain your program

4 **Cartel Exposure**

FTO designation means paying cartel-linked protection fees is now a terrorism financing charge

5 **Sanctions**

Strict liability means a single unintentional SDN match can cost millions: automate screening now

6 **Fraud & HHS**

Qui tam whistleblowers are the top source of FCA cases: build internal detection first

7 **Self-Reporting**

Being first to self-disclose can convert criminal exposure into a civil settlement

8 **Supply Chain**

You are responsible for what your vendors' vendors do: map beyond tier 2