C&G INSIGHTS



When the Rules Change:

What GCs Need to Know About Corporate Criminal Risk in Today's Most Challenging Markets

CO-AUTHORED BY CHRISTIAN EVERDELL AND ALLON LIFSHITZ
PARTNERS AT COHEN & GRESSER

www.cohengresser.com

COHEN & GRESSER

When the Rules Change:

What GCs Need to Know About Corporate Criminal Risk in Today's Most Challenging Markets

Introduction: The Compliance Map Has Been Redrawn

Much of today's corporate compliance framework was built for a world that no longer exists.

The legal risk profile for companies operating in high-risk markets has shifted significantly over the past two years. This shift stems from two key developments that most corporate legal teams are still working to fully understand and address.

The first is the designation of Mexican cartels as foreign terrorist organizations by the U.S. government. For companies with operations in Latin America, across industries as varied as manufacturing, agriculture, energy, financial services, and logistics, this is not a regulatory footnote. It is a full transformation of potential legal exposure. Payments that once raised questions under the Foreign Corrupt Practices Act now potentially implicate federal terrorism statutes. The difference in legal consequences is enormous.

The second challenge is the unpredictable movement of global sanctions. While certain forbidden jurisdictions see temporary or highly specific carve-outs, such as limited OFAC licensing in Venezuela, others like Iran face ever-expanding enforcement and secondary sanctions risks. Venezuela likely represents the most informative example: the current administration has eased sanctions in certain business sectors to allow investment while simultaneously making the pursuit of narcotrafficking organizations a top enforcement priority. Those two positions are not as contradictory as they sound. That said, navigating the space between them requires precision and clarity that most existing compliance programs do not provide.

The question companies face today is not simply how to stay on the right side of the rules when everyone around them is operating in uncharted gray areas. It is how to stay on the right side of the rules in markets where the rules are actively changing, where the line between encouraged and prohibited is unclear, and where the government's enforcement priorities may operate in two directions at once.

We have each spent significant portions of our careers on the inside of investigations into businesses operating in high-risk areas, including in federal prosecution roles that gave us a direct view of how the government builds its cases, what it looks for, and where companies make their most consequential mistakes. The following pages translate that experience into practical guidance for GCs who are operating in, or considering entry into, markets where these risks are most concentrated.

Part I:

The Cartel Terrorism Designation: What Actually Changed

The designation of Mexican cartels as foreign terrorist organizations should not be treated as just a compliance update. Instead, it may require significant changes to business operations in order to avoid massive legal risk.

Under the FCPA framework that governed risk for the past several decades, a payment to a cartel-affiliated government official raised questions about bribery and corruption. Under the terrorism framework that now applies, the same payment potentially constitutes material support for a designated foreign terrorist organization. This would represent a far different federal crime that carries consequences of an entirely different magnitude, including the possibility of criminal prosecution of the company and its executives under statutes that were designed for state sponsors of terror and their facilitators. This can result in significant prison terms and financial penalties, including a far-reaching forfeiture statute that applies in terrorism cases.

The Lafarge case established the template. Lafarge S.A., one of the world's largest cement manufacturers, pled guilty in 2022 to providing material support to ISIS and another terrorist group in order to keep operating a plant in Syria. The DOJ has made clear, across the Biden and Trump administrations, that it is looking for corporate cases in the Lafarge mold, and the cartel terrorism designations have expanded the pool of potential corporate defendants dramatically.

For companies with operations in Mexico and Latin America, the practical implications are significant. Payments to local officials, transportation providers, security contractors, or any entity that may have cartel affiliation, even indirect affiliation, now require a level of due diligence that standard third-party screening does not provide. The cartels operate in a variety of regions, and are sophisticated in how they embed themselves within legitimate-appearing business structures. Companies doing business in affected regions may have no awareness that a counterparty is cartel-connected.

Part II: OFAC and Thawing Jurisdictions: A New Kind of Compliance Problem

The sanctions environment has always required careful navigation. What is new is the particular complexity created by jurisdictions that are simultaneously reopening and remaining dangerous.

Venezuela is the clearest example. On one hand, policy signals from Washington suggest a willingness to permit specific categories of commercial engagement through targeted general licenses. On the other, regulatory and criminal enforcement signals make clear that companies whose payments flow, even inadvertently, toward narcotrafficking networks or Venezuelan-backed criminal syndicates face catastrophic risk under U.S. sanctions, money laundering, and anti-corruption laws. Also, where those funds touch designated terror groups operating inside the country, 'material support' exposure becomes a very real threat. Those two factors are not mutually exclusive, but the space between them is narrow and at times ambiguous. While Venezuela's opening presents real opportunities, businesses must still proceed with extreme caution and conduct thorough due diligence. Most importantly, the consequences of misjudging how best to navigate this landscape are severe.

The compliance challenge in these environments is not primarily about a company's initial intent. Companies operating in high-risk markets enter them intending to comply. The challenge is whether their compliance infrastructure is sophisticated enough to protect them when the ground shifts, including but not limited to:

- when a counterparty is designated,
- when a beneficial owner is identified, and
- when a political transition changes the legal status of an existing relationship.

Standard screening against published watchlists is a necessary starting point, but not a sufficient ending point.

For companies with exposure to newly reopening markets, we recommend building compliance frameworks around three questions that standard programs often do not ask:

- Who ultimately benefits from this transaction?
- What happens to our existing relationships if the regulatory status of this jurisdiction changes again?
- Do we have a documented, executable exit mechanism if we need to leave quickly?

To summarize, while easing OFAC sanctions create compelling opportunities for risk-tolerant companies, the regulatory trap remains wide open. Without exhaustive due diligence, businesses risk walking into the same enforcement minefield seen in Mexico, where seemingly routine commercial activity inadvertently touches designated criminal networks.

Part III: When the Government Comes Calling: The First 24 Hours

The decisions made in the first 24 hours after a government inquiry begins or becomes public are among the most consequential a company will face.

The first question is the company's status: Is it a witness, subject, or target? A bank receiving a subpoena for a customer's records is in a fundamentally different posture than a bank that is itself under investigation. The framing of the initial response, the selection of outside counsel, and the internal communication strategy should all be calibrated to that determination. Of equal importance is making the response quick and accurate, and involving experienced counsel.

The selection of outside counsel is critical. Knowing the relevant DOJ component, and its approach to prosecutions, matters. The approach a prosecutor from the National Security Division takes to a corporate resolution is not the same as the approach a prosecutor from the White Collar Section takes. In addition, those components work in partnership with U.S. Attorney's Offices, some of which have long histories of charging cases involving terrorism, bribery, and related crimes. Counsel who has experience with the components handling an investigation brings institutional knowledge that shapes every aspect of the defense strategy.

And if conduct is detected by a company before a government investigation commences, self-reporting requires serious deliberation. The DOJ currently offers significant cooperation credit to companies that report detected violations before the government discovers them independently. That credit is real and worth considering. But the decision to self-report should be made with a clear understanding of what is being reported, to whom, and what the likely response will be. These decisions should not be made as a reflexive first move, but should be considered in overall context. In some circumstances, premature or poorly framed self-reporting creates more exposure than it resolves.

GC Checklist:
Seven Things to Do Before Your Risk Becomes a Crisis

These are the questions every GC should be able to answer before their company has a problem in a high-risk market, and not after.

01 Have you mapped your actual third-party exposure in cartel-affected regions? Standard due diligence is not sufficient for markets where cartel affiliation is deliberately concealed within legitimate business structures. Engage specialized investigation firms for counterparties in high-risk jurisdictions before the relationship begins.

02 Do you know the difference between FCPA risk and terrorism statute risk? The cartel terrorism designations have changed the legal framework. Payments that raised FCPA questions now potentially implicate federal terrorism statutes. Make sure your compliance team understands what changed and when. The consequences of violating the terrorism statutes can be existential.

03 Do you have a documented exit mechanism for every high-risk relationship? If a counterparty is designated mid-transaction, can you exit the relationship cleanly and quickly? If the answer is not immediately clear, the compliance framework needs work.

04 Is your OFAC screening program calibrated for different types of sanctions exposure? Direct sanctions exposure is the starting point. Exposure arising from relationships with entities that do business with sanctioned parties requires a more sophisticated analysis, particularly for companies operating in the Gulf region.

05 Have you identified which DOJ office would handle an investigation of your company? Knowing the relevant component, its current priorities, and its recent enforcement history is not a luxury. It is critical preparation. Outside counsel who know the answers bring strategic value that generalist counsel cannot replicate.

06 Do you have a self-reporting protocol, and has it been reviewed in the past twelve months? The cooperation credit framework has changed. If your self-reporting protocol was designed for a different administration's enforcement environment, it may be calibrated incorrectly.

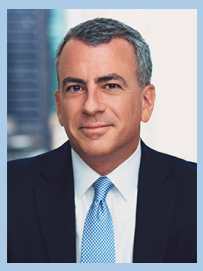
07 Is your duress analysis current? For companies operating in jurisdictions where coercive payments are a reality, the duress defense is narrow. Document the circumstances, involve counsel immediately when those circumstances arise, and understand that the defense can evaporate when the immediate threat resolves.

Why This Matters, and How Cohen & Gresser Can Help

Corporate national security risk is one of the most complex and consequential areas of legal practice for multinationals today. Because of this, it is an area where the cost of getting it wrong is measured not in fines but in criminal liability for the company and its executives.

Cohen & Gresser brings a combination of prosecutorial experience and sophisticated defense practice to exactly these issues. Our team has been on the inside of landmark cartel investigations, corporate terrorism prosecutions, and OFAC enforcement actions. We apply that experience directly to the work of helping clients build compliance frameworks that can withstand scrutiny, respond effectively when a government inquiry arrives, and navigate the increasingly complex geography of high-risk market engagement.

Whether you are evaluating your company's existing exposure, preparing to enter a newly reopening market, or responding to a government inquiry that arrived this morning, we would welcome the conversation.



Christian Everdell is a Partner in Cohen & Gresser's New York office, where he leads the firm's Privacy & Data Security practice and focuses on white collar criminal defense, OFAC sanctions, and regulatory enforcement. He served as an Assistant U.S. Attorney in the Southern District of New York, where he was a member of the Complex Frauds and Cybercrime Unit and the Terrorism and International Narcotics Unit.



Allon Lifshitz is a Partner in Cohen & Gresser's New York office, where his practice focuses on white collar criminal defense, government investigations, corporate national security matters, and complex civil litigation. He served as a federal prosecutor in the Eastern District of New York, where he prosecuted corporate national security cases and held several supervisory positions, including Deputy Chief of the Criminal Division.