National Institute for Combating Cybercrime and Terrorism
INCC · in co-authorship with the National Center for Cybersecurity, Intelligence and Counterterrorism (CNC)

OPINION ARTICLE · INSTITUTIONAL ANALYSIS

The day your company became part of a law it never read

The designation of the PCC and Comando Vermelho as terrorist organizations by the United States is not only a matter for those who fight crime. It changed the business environment and reaches entire sectors of the Brazilian economy, including companies certain that none of this concerns them. In this text, we explain in plain language what changed, who is affected and why.

Authors: INCC & CNC **Date:** June 2026 **Nature:** Informational and educational

TLP:WHITE · FREE DISTRIBUTION

PRESS · ASSOCIATIONS · PRIVATE SECTOR

← Back to Content

DOWNLOAD PDF

INTRODUCTION

An external fact that does not ask permission to enter

> In May 2026, the regulatory environment surrounding Brazilian companies changed. Most of them have not yet noticed.

In late May 2026, the United States government classified two Brazilian criminal factions, the Primeiro Comando da Capital (PCC) and the Comando Vermelho (CV), as terrorist organizations. It sounds like public security news, a police matter. The risk for companies, however, lies precisely there: this classification is not just about crime, it is about **money and contracts**. And anything involving money and contracts ends up reaching whoever moves funds and signs contracts, which today is almost every company.

The intent of this article is not to frighten anyone. It is to explain, clearly and without jargon, what this decision means in practice: which sectors it touches, how the international system discovers who is involved and, above all, why many companies that today say "this is not about me" also run a risk. In fact, that may be the most dangerous sentence a company can repeat right now, and throughout the text the reason becomes clear.

We write from the viewpoint of those who work with the subject every day: combating cybercrime and terrorism and intelligence applied to protecting organizations. Our goal is to offer companies, class associations, sector groups and public managers an honest information base, so each can *draw their own conclusions* about their level of exposure.

SECTION 1

What actually changed, in simple terms

The United States uses two legal labels for groups it considers terrorist, and the PCC and CV received both: **FTO** (Foreign Terrorist Organization) and **SDGT** (Specially Designated Global Terrorist). More important than memorizing these acronyms is understanding the consequence they trigger.

THE CONCEPT THAT CHANGES EVERYTHING: "MATERIAL SUPPORT"

With the designation, providing **"material support"** to these groups became a federal crime in the United States. And the concept of "material support" is deliberately **broad**. It is not just about giving money or weapons. It includes services, transportation, lodging, communication and even ordinary business that, without anyone noticing, ends up benefiting the group, including when this happens through third parties. Nor is it necessary to intend to help a terrorist act; it is enough for the benefit to reach the organization. And this rule may apply to conduct carried out **outside the United States**.

In practice, the comfortable border separating "organized crime" from "the company that just does business" collapsed. When a payment, a contract, a freight or a supplier touches, even distantly, an entity linked to these factions, that act may come to be treated under an anti-terrorism law, and no longer only under ordinary criminal law.

SECTION 2

Primary and secondary sanctions: the difference that decides who is hit

There is a point most analyses do not explain well. There are **two types** of sanction, and it is the difference between them that determines whether a Brazilian company "with nothing to do with the U.S." is exposed or not.

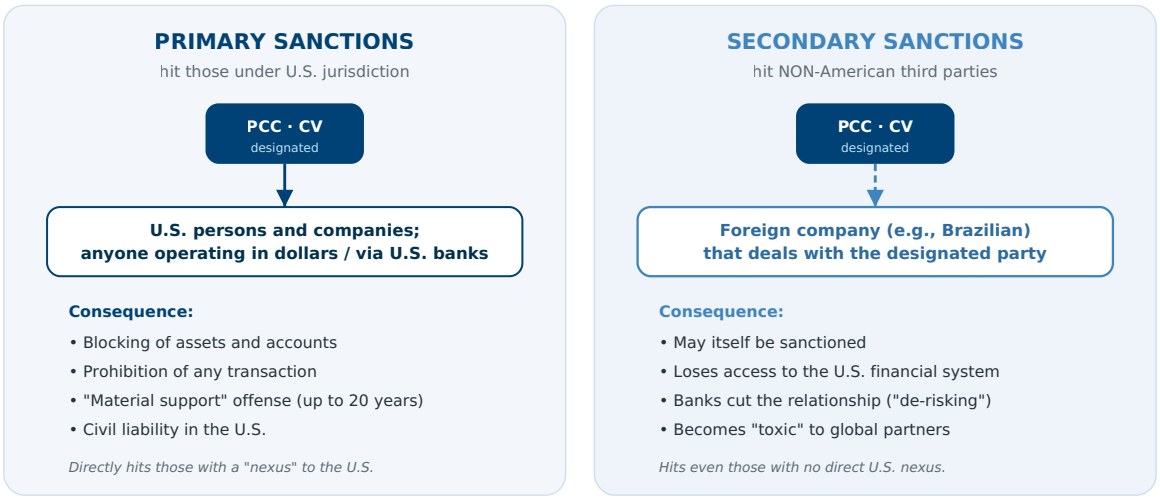

Fig. 1. Primary and secondary sanctions. Primary ones hit those under U.S. jurisdiction. Secondary ones reach non-American third parties that do business with the designated party, and it is this second route that makes the topic relevant for Brazilian companies "with no connection to the U.S."

Primary sanctions

They apply to those within the **legal reach of the United States**: American persons and companies and anyone who uses the country's financial system, which in practice includes almost everyone operating in dollars. For them, doing business with a designated party means asset freezes, a ban on operating and criminal risk for material support.

Secondary sanctions

This is where the game changes for Brazil. Secondary sanctions target **third parties who are not American**, such as a Brazilian company, when that company deals with a designated entity. The message is direct: if you do business with someone on the list, you may end up on the list too. You do not need a headquarters, a partner or an account in the United States to feel the effect. It is enough to depend, at some point, on the global financial system, and virtually every company depends on it.

AN ANALOGY TO REMEMBER

Think of the dollar as a road that, at some stretch, always passes through a tollbooth in the United States. You may be driving entirely within Brazil, but if your route crosses that tollbooth (and the route of international trade almost always crosses it), whoever controls the tollbooth can block your passage. Secondary sanctions work like that tollbooth. They do not require you to be American, only that you pass through there at some point.

SECTION 3

Why "checking a list" is not enough: the 50% Rule

Many companies imagine that protecting themselves is simple: just check whether the client's or supplier's name appears on some official sanctions list. It is not quite so. There is a rule, known as the **50% Rule**, that expands the reach of the sanction silently.

THE 50% RULE, EXPLAINED

If one or more sanctioned persons or entities hold, combined, **50% or more** of a company, that company also comes to be treated as sanctioned, **even if its name does not appear on any public list**. And that "subsidiary company" is not disclosed by anyone; discovering it is the responsibility of whoever is going to do business with it. That is why looking only at the official list misses precisely the risk hidden in the ownership structure and the ultimate owners of the business.

That is why real protection is not the one-off gesture of "checking a list." It is the ability to **see who is behind** each client, supplier and partner, and to do so continuously, since ownership structures change all the time.

SECTION 4

Who is affected: the three groups of sectors

Not all sectors are reached in the same way. To make this clear, it helps to split the economy into three groups: those hit **directly**, those hit **indirectly** and those that suffer **both effects at once**. The classification below is only analytical and educational. It serves for each organization to locate itself, not to point fingers.

DIRECTLY AFFECTED

have a jurisdictional nexus to the U.S.

- Banks and financial institutions
- Payment providers and fintechs
- Fuel and ethanol distribution
- Foreign trade, ports and international logistics
- Companies with shares/receipts traded in the U.S. (ADR)
- Capital markets and funds with international fundraising

DIRECTLY AND INDIRECTLY

combine both effects

- Export agribusiness (dollars/ports + traders' chain)
- Construction and real estate
- Insurance and reinsurance
- Telecommunications and data centers
- Technology and cloud with American suppliers
- Large groups with foreign branches or investors

INDIRECTLY AFFECTED

suffer the market/chain effect

- Retail, wholesale and marketplaces
- Healthcare and product distribution
- Small and medium companies in general
- Local services (factoring, regional transport)
- Local real estate agencies and builders
- Providers and suppliers of companies in the groups above

Each sector's position may vary according to the company's profile, such as use of dollars, exports, ownership structure and supplier chain. The table is a starting point, not a verdict.

Examples by sector: illustrative scenarios

The cases below are **hypothetical and illustrative**, created only to show how the mechanism works. None of them describes a real company.

Fuel distribution (direct)

A distributor buys product and pays suppliers in operations that, at some point, pass through dollar settlement. *How the risk appears:* if an intermediary in the chain has a hidden ownership link to a designated entity, the dollar operation may be blocked and the company enters the radar of primary and secondary sanctions.

Payments / fintech (direct)

A fintech processes thousands of transactions a day. *How the risk appears:* without screening the ultimate beneficiary and the 50% Rule, it may unknowingly intermediate funds linked to a blocked entity, which exposes it both to the American system and to the Brazilian regulator.

Export agribusiness (direct and indirect)

An exporter sells abroad (receives in dollars, uses ports) and buys from a scattered network of suppliers. *How the risk appears:* the sale exposes it directly (dollar/port nexus); the purchasing chain exposes it indirectly (a contaminated supplier transfers risk to it).

Construction and real estate (direct and indirect)

The sector is historically used for laundering funds. *How the risk appears:* directly, if it receives capital originating from a link to a designated party; indirectly, when banks and insurers reprice the entire sector out of caution.

Retail and marketplaces (indirect)

A marketplace connects thousands of sellers. *How the risk appears:* even without its own nexus, it may host a seller linked to a blocked entity, and the acquirer or the bank, upon noticing, restricts the operation of the whole platform.

Small and medium company (indirect)

A gas station, a regional carrier, a local real estate agency. *How the risk appears:* it is rarely a direct target, but it is cut off by the bank, the card machine or the insurer when the sector or the region comes under the market's risk lens.

SECTION 5

How the system discovers who is involved

A common question is: "but how would anyone find out?" The answer is a bit uncomfortable, because the discovery channels are many, automatic and interconnected. There need not be a targeted investigation for a company's name to surface.

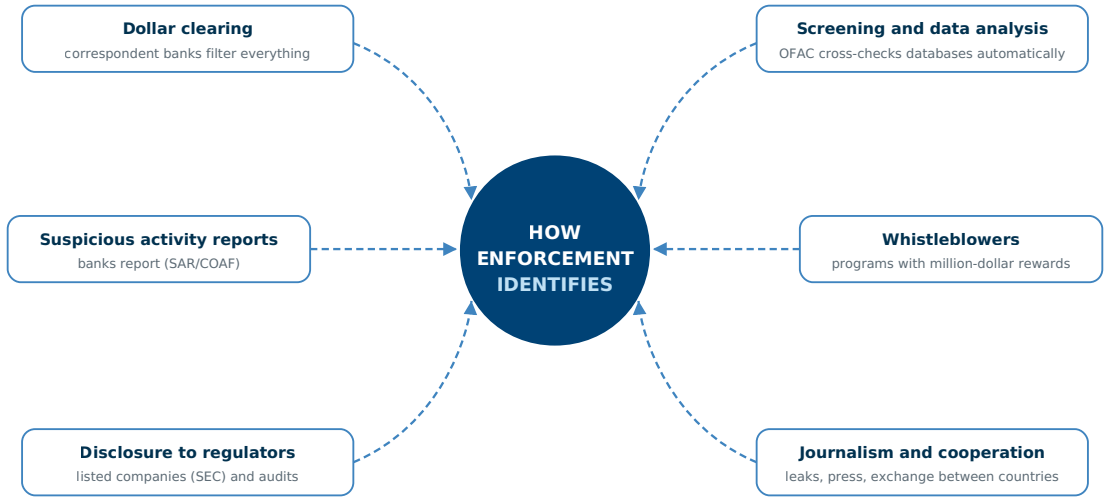

Fig. 2. The channels through which involvement is discovered. They work in parallel and cross each other. Most of the time there is not "one" investigation, but several sources pointing to the same name at the same time.

The most common path begins at the bank. Since almost every international operation passes, at some point, through a correspondent bank in the United States, that is where automatic filters compare each transaction against the sanctions lists and risk patterns. Added to that filter are the suspicious activity reports that financial institutions themselves are required to file, the data analysis done by authorities, the information that listed companies must disclose to regulators, investigative journalism and cooperation between countries. There is also a little-known detail: there are **programs that pay million-dollar rewards to whistleblowers**. With that, the incentive for an employee, a competitor or a former partner to report an irregularity becomes high and very concrete.

THE PRECEDENT THAT SHOWS THIS IS NOT THEORY

In 2022, the construction materials company **Lafarge** pleaded guilty, in the United States, to providing material support to terrorist groups and agreed to pay about **US$ 778 million**. It was the first major corporate case of this kind. The detail that matters most to Brazil is that the conduct happened **outside the United States**, by a company that was not American. Arguments such as "it was outside the country" and "it was not our intention" did not work as a defense.

SECTION 6

Why "this is not about me" is the riskiest sentence

For most companies, the first impact will not arrive as a criminal case. It will arrive silently, through the **reaction of their own partners**: the bank that closes the account "as a precaution," the card machine that raises the fee or withholds the receivable, the insurer that excludes coverage, the supplier who, already contaminated, passes the risk along. None of that waits for a sentence. The market usually moves before the courts.

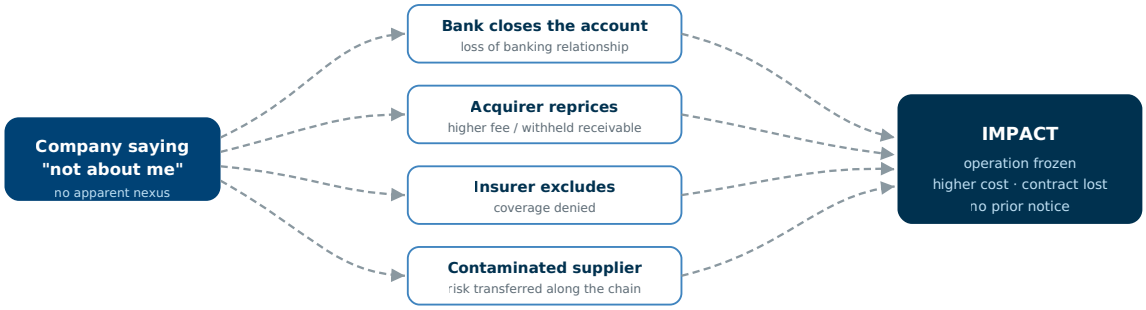

Fig. 3. The indirect contamination chain. The company need not have done anything wrong. One exposed partner is enough for the risk to reach it, and the impact usually comes from the market, not the courtroom.

That is why the sentence "this is not about me" is so risky: it confuses two different things, **not being at fault** and **not being exposed**. A company can be entirely reputable and still be hit because it did not *see* in time a risk that was already in its chain. Having no involvement protects the company from fault, but it does not protect it from the consequences.

SECTION 7

The questions every organization should be able to answer

It is not for this article to tell anyone what to do. It is only to propose a few honest questions. If your organization answers all of them calmly and with **documented evidence**, it is probably on a good path. If it stumbles on any, that is exactly where your exposure lives.

A FIVE-QUESTION TEST

- Can you say, today, whether any client, supplier or partner (including at the second and third level) has an ownership stake that crosses with a blocked entity?
- If your bank asked tomorrow what your company does to avoid dealing with a designated party, would you have a documented answer or just good intentions?
- How long would your organization take to *discover* that a supplier was added to a sanctions list: days, months, or only when a payment was refused?
- If an insurer, an acquirer or an investor reassessed your risk tomorrow, what would they find about your chain, and who, inside the company, would be able to explain it?
- Is there, in your organization, someone or some structure whose job is, continuously, to look outward and anticipate this kind of risk?

None of these questions is about technology or about buying a product. They all concern a single capability: **continuous visibility**, knowing before the market what exists in your own chain.

WHERE VISIBILITY IS BORN

No internal decree eliminates this risk. What truly helps is the ability to **systematically monitor** clients, suppliers, partners and the chain, and to react before the market reacts first. That capability has a name: **intelligence**. It can be internal, with a dedicated unit inside the company, or outsourced, through a specialized structure. Both forms are legitimate. The problem is the exposed organization having neither, because, without visibility, it ends up discovering the risk the worst way: when it has already become a consequence.

CONCLUSION

The difference is in seeing in time

The designation of the PCC and CV as terrorist organizations is, above all, a **fact of the environment**. It does not ask permission to enter the reality of companies, does not separate those who read the law from those who did not, and does not wait for each organization to realize it is exposed before taking effect. That effect has already begun.

There is no reason to panic, but every reason for clarity. The organizations that will get through this scenario with less turbulence are not necessarily those that fear the most nor those that spend the most. They are the ones that **see better**: they know who is in their chain, notice a shift in risk before the bank and the insurer, and can prove, with documents and not with rhetoric, that they act with diligence.

In this context, doing nothing is also a choice: that of discovering the risk later and in the worst way. Every institution, association and company reading this text already has enough information to ask a simple and slightly uncomfortable question: *am I seeing what I need to see?* The answer, and what to do with it, belongs to each one. The question, from now on, belongs to all.

INCC RESOURCE

A starting point for your organization

To help with this first step, INCC developed a self-assessment tool on the topic. It does not replace legal analysis nor deliver a definitive diagnosis, but it works as a starting point for your organization to better understand where it may be exposed and which questions to take to the compliance team and legal department.

SELF-ASSESSMENT TOOL

Take a test and see where to start

If you wish to take a test, go to the INCC website. In the **Compliance** section of the menu, you will find the application.

Access the tool on the INCC website

Sources and verification notes

We commit to separating what is fact confirmed in a primary source from what is interpretation. We always recommend consulting the official sources.

Primary

> **U.S. Department of State**: designation statement for Comando Vermelho and Primeiro Comando da Capital (May 2026).
> state.gov

> **Federal Register**: designation acts as FTO (INA §219) and SDGT (Executive Order 13224), published on 06/05/2026.
> federalregister.gov

> **OFAC / U.S. Treasury**: guidance on the 50% Rule (FAQ 399 and 401).
> ofac.treasury.gov

> **U.S. Department of Justice**: Lafarge case (guilty plea for material support, 2022).
> justice.gov

> **Legal basis**: 18 U.S.C. §2339B (material support); INA §219 (8 U.S.C. 1189); Executive Order 13224.

Caution notes

> Dates and legal framings for 2026 were checked against primary sources. Historical enforcement milestones from prior years are based on specialized legal analyses (secondary sources) and must be confirmed case by case.

> This article is informational and educational and **does not constitute legal advice**. Assessing the specific exposure of any organization requires dedicated professional analysis.

IMPORTANT NOTICE

This article is strictly informational and educational, made available to help your organization understand the topics addressed. Under no circumstances does its content replace the analysis, guidance or legal opinion provided by a duly licensed attorney specialized in the matter.

The information, analyses and conclusions presented here are general in nature, do not consider the particularities of each organization and should not be interpreted as a definitive diagnosis, legal opinion, compliance certification or guarantee of meeting legal, regulatory or contractual requirements. Any and all conclusions must be submitted to the validation of your institution's legal department, compliance area or specialized advisors.

If obtaining or distributing this material involves providing personal data, such as name and email address, the processing of that data is carried out in accordance with the institution's Privacy Policy and Cookie Policy.

We recommend that this material be saved or printed in PDF format for future reference and to track any adjustment actions identified by your organization.

DOWNLOAD PDF

National Institute for Combating Cybercrime and Terrorism (INCC)
in co-authorship with the **National Center for Cybersecurity, Intelligence and Counterterrorism (CNC)**
June 2026 · TLP:WHITE · free distribution, citation encouraged with attribution.