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

Less than 30 days after the PCC and CV were designated terrorist organizations by the U.S. Government, Brazil already receives the first sanctions, on companies and individuals. No one is off this radar. Is your company already taking action?

On July 1, 2026, the U.S. Treasury sanctioned two Brazilian individuals, three companies from São Paulo and one company from Portugal for ties to the PCC. It was the first action of its kind after the factions were designated terrorist organizations, and it came 26 days after the FTO designation took effect. This text explains what happened, why no company is beyond the reach of this regime and, based exclusively on official sources, what to do, whom to notify and with which documents, should your organization find any evidence.

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

TLP:WHITE · FREE DISTRIBUTION

PRESS · ASSOCIATIONS · PRIVATE SECTOR

← Back to Content

DOWNLOAD PDF

> When we published, in this same series, that the designation of the PCC and Comando Vermelho would change the Brazilian business environment, a common objection was that the practical effects would take years. They took 26 days.

On July 1, 2026, the U.S. Treasury's Office of Foreign Assets Control, OFAC, announced the inclusion of two Brazilians, three São Paulo companies and one Portuguese company on the SDN blocking list, for ties to the Primeiro Comando da Capital. According to the Treasury itself, it was OFAC's third action against the PCC's structure, but the first after the faction was designated a terrorist organization, and the first to use, against companies linked to the group, the anti-terrorism legal basis of Executive Order 13224. What was a thesis became a precedent. And precedent, in this regime, is the technical name for "it will happen again."

THE DATES THAT MATTER, WITHOUT ROUNDING

May 28, 2026: the State Department designates the PCC and CV as Specially Designated Global Terrorists (SDGT), with immediate effect, and announces the intention to designate them as Foreign Terrorist Organizations (FTO). **June 5, 2026:** the FTO designation is published in the Federal Register and takes effect. **July 1, 2026:** OFAC announces the first sanctions against persons and companies for ties to the PCC since the designation. From the FTO taking effect to the sanctions, **26 days** passed. From the initial May 28 announcement, 34 days. This article's title uses the first count, and we make a point of showing both: transparency with dates is part of the method.

THE FACT

WHAT EXACTLY HAPPENED ON JULY 1

According to the Treasury's official statement, the sanctioned network operated between Florida and São Paulo and allegedly laundered more than 30 million dollars in drug proceeds generated in the United States, using cryptocurrencies to bring the money back to Brazil for the benefit of the PCC. The action was the outcome of an investigation led by a homeland security task force, with the FBI's Miami field office and the money laundering section of the Department of Justice. In January 2026, six members of the Florida branch had already been arrested and indicted in U.S. Federal Court.

Designated, according to the Treasury, were: two Brazilian individuals identified as operators of the São Paulo core; three São Paulo companies in the financial services, payments and construction sectors; and a transport and warehousing company from the Lisbon region, in Portugal, belonging to the same group. The full names appear in the official statement and on the SDN list, both public and cited in the sources at the end. It is worth the note our series always makes: inclusion on the SDN list is an administrative act of the U.S. Executive, based on the allegations and evidence gathered by that government, and not a judicial conviction.

WHY THIS ACTION IS DIFFERENT FROM PREVIOUS ONES AGAINST THE PCC

OFAC had already acted against the PCC in 2021 (designation of the organization) and in 2024 (a financial operator), always based on the counter-narcotics executive order, E.O. 14059. The July 1, 2026 action is the first to add to that basis **Executive Order 13224, the anti-terrorism instrument**. In practice, companies and persons linked to the faction come to be treated under the same legal regime applied to financiers of terrorist groups: asset freezes, exposure of anyone transacting with them, risk of secondary sanctions for foreign financial institutions and the possibility of criminal liability for material support. It is the machinery we described in the two previous articles of this series, now in motion.

THE REACH

WHY "NO ONE IS OFF THIS RADAR" IS NOT A FIGURE OF SPEECH

The Treasury's statement devotes an entire section to the implications of the action, and it deserves careful reading by any Brazilian manager. Three points, all taken from the official text:

First, the 50% Rule is already active. Any company owned, directly or indirectly, individually or jointly, 50% or more by the now-blocked persons is also blocked, even if its name does not appear on any list. Discovering this is the responsibility of whoever does business with it, not of the U.S. government.

Second, civil liability does not require intent. OFAC may impose civil penalties for sanctions violations on a strict liability basis. An American company, or an operation that passes through the United States, can be punished even without knowing the counterparty was blocked. That is precisely why banks and business partners cut relationships at the first sign of risk, the de-risking effect that hits innocent third parties.

Third, the statement expressly warns that non-Americans are also within reach. The official text prohibits foreigners from causing or conspiring to cause violations by Americans, and warns that foreign financial institutions facilitating significant transactions for the designated parties may suffer secondary sanctions, losing access to correspondent accounts in the United States. For a Brazilian bank, this is not a regulatory detail, it is an existential risk. And the bank, to protect itself, transfers that demanding standard to every client in its portfolio.

HOW THIS SHOWS UP IN THE REAL LIFE OF AN ORDINARY COMPANY

None of the examples below requires a conscious link to a faction. They are commercial gestures of any given week:

- The **real estate agency** that rents a warehouse to a front company is, in the eyes of the sanctions regime, providing a service to the sanctioned network.
- The **carrier** that delivers electronics to a company controlled by a designated party transports on behalf of the network, even without knowing.
- The **accounting firm** that keeps closing the books of a blocked company provides it a service after the block.
- The **fintech or card-machine company** that processes the receipts of a merchant linked to the network intermediates funds of a blocked entity; it was for services of this kind that payment companies were listed on July 1.
- The **vehicle or phone store** whose products end up in the group's structure appears in its supply chain.
- The company that provides **receivables advance** to a contaminated client is, in practice, financing its operation.
- The **marketplace** that hosts a hidden seller linked to a sanctioned party may see the acquirer restrict the entire platform.
- And the most everyday example of all: the **company's bank** checks lists every day. When the filter lights up, the account closes first and the explanation, if it comes, comes later.

A RELATIONSHIP WITH A SANCTIONED PARTY ENDS IMMEDIATELY. KEEPING IT, OR NOT ACTING, IS THE SHORTEST PATH TO THE LIST

Banks, companies and institutions that discover a direct or indirect relationship with the sanctioned persons and companies must **immediately end new operations, payments and contracts with them**. The basis for this is in the official acts themselves: Executive Order 13224 allows designating anyone who provides material assistance, sponsorship or financial, material or technological support to a designated party, and it was precisely for acting "on behalf of or for the benefit of" a designated party that the second individual and the four companies were listed on July 1. Continuing to operate with a sanctioned party, or simply doing nothing after finding out, is the behavior that turns a third party into a target. Two technical points avoid a serious error: first, whoever has a U.S. nexus and holds a sanctioned party's assets **does not return or transfer those assets**; the obligation is to block and report to OFAC, and returning them would itself be a violation. Second, the termination must be documented and conducted with the legal team, for the labor and contractual reasons already noted in this text. Speed and formality, together.

The cascade effect that reaches even the small company

The sanction hits six names. The financial system, however, reacts to risk, not to the list: banks, card acquirers, insurers and fintechs recalibrate filters for the entire sector and ownership environment of the designated parties. *A company with no relationship to the case may be affected merely by sharing a sector, region or operating profile, and will discover this through the blocking of an operation, not through a notification.*

THE VACUUM

THE QUESTION ALMOST NO ONE CAN ANSWER: "SO, NOW WHAT DO I DO?"

Since the May designation, we have been talking with companies, class associations, firms and public managers. The observation that follows is institutional, the fruit of that experience, and the reader should treat it as the assessment of those who work on the topic, not as a statistic: **we have not found, up to the closing of this text, a Brazilian public or private institution with a clear, tested and documented procedure on what to do upon finding evidence of a link between a**

client, supplier or partner and a designated organization. There is goodwill, there are quality legal alerts, there is growing concern. What there is not is an operational routine: whom to notify, within what deadline, with which documents, preserving which evidence.

This is not a criticism of anyone in particular. The U.S. sanctions regime is a technical world of its own, which until a month ago seemed an exclusive subject for international banks. The designation changed the audience for this subject without asking permission. The problem is that, in this regime, improvisation is costly: reporting wrongly, late or to the wrong agency can turn a victim company into an investigated one.

THE PATH

THE ORGANIZATIONAL RESPONSE: A DEDICATED INTELLIGENCE UNIT

The defense that works in this environment is not a stand-alone legal opinion or a one-off check against a list. It is a permanent capability. The most efficient way to build it, in the assessment of INCC and CNC, is to set up an **intelligence unit specialized in organized crime and counterterrorism** serving the organization itself, even if small, including outsourced. And here comes the warning that runs against the instinct to cut costs: **intelligence for combating organized crime and counterterrorism is not a discipline you learn by doing**. The unit must be formed, or hired, with professionals of proven experience in these two areas, whoever the provider is. Putting in-house people to learn through their own mistakes is a risk that rarely justifies the savings: in this field, the first mistake can already be the ignored alert, the false positive that brings down a legitimate contract or the report made to the wrong agency. What defines the unit, therefore, is not size, it is function and experience:

- **Continuous screening of counterparties:** clients, suppliers, partners and ultimate beneficial owners checked against the official sanctions lists, recurrently and not only at onboarding, because lists and ownership structures change all the time.
- **Ultimate beneficial owner view and the 50% Rule:** the ability to see who is behind each company, adding up the stakes of any sanctioned parties, which is where the invisible risk lives.
- **Written response protocol:** the step-by-step of what to do when facing an alert, with responsible parties, deadlines and channels defined before the crisis,

including the guide for communicating with authorities we detail in the next section.

- **Evidence preservation:** organized keeping of contracts, payment instructions, invoices, bills of lading and check records, which are exactly the documents the official agencies request.
- **Interface with legal, compliance and authorities:** the unit does not replace the attorney or the compliance officer; it feeds both with structured information and maintains the channel with public agencies.

None of this requires a large structure, and the screening and initial diagnosis can be done with free public tools, including those INCC itself provides, described below. What is not advisable to skimp on is the experience of whoever does the analysis: the tool finds the name, but it is the analyst with real experience in organized crime and counterterrorism who recognizes the pattern, reads the context and knows what to do with the finding.

THE PROTOCOL

I FOUND EVIDENCE. NOW WHAT? THE OFFICIAL STEP-BY-STEP GUIDE

Everything that follows was taken from official sources of the U.S. and Brazilian governments, cited at the end. There is no inference of ours in the deadlines, channels and documents listed. The overall design is this:

1. **Preserve and document**
   Contracts, payments, invoices, shipments, check records. Nothing is discarded.

2. **Freeze the relationship and involve legal and compliance**
   No new transaction with the counterparty until professional assessment.

3. **Check the U.S. nexus**
   Assets or operations under U.S. jurisdiction create a duty to block and report to OFAC.

4. **Report to OFAC within 10 business days, if a reporting duty exists**
   Via the ORS system. Blocked property and rejected transactions are mandatory to report.

5. **Report in Brazil**
   A regulated sector reports to COAF via SISCOAF; evidence of a crime goes to the Federal Police

6. **Assess voluntary self-disclosure and keep monitoring**
   If the company itself may have violated a sanction, voluntary disclosure reduces the penalty.

Recommended response flow. Steps 3 to 6 follow official channels and deadlines of the U.S. and Brazilian governments, detailed below.

In the United States: the four official channels

1. OFAC: BLOCKED PROPERTY AND REJECTED TRANSACTIONS (MANDATORY FOR THOSE WITH A U.S. NEXUS)

Anyone under U.S. jurisdiction holding a designated party's property must block it and **report to OFAC within 10 business days**, under rule 31 C.F.R. §501.603. Rejected transactions follow the neighboring rule, §501.604, with the same deadline. The report is filed in the official online system, the **OFAC Reporting System (ORS)**, and access registration is requested by email at OFACReport@treasury.gov. There is also an annual report of property that remains blocked, due by September 30. The rule lists the documents and data required in the initial report, among them: identification and contact of the filer; description of the transaction and the parties involved, including banks; identification of the sanctioned target and its interest in the property; description and location of the property, with account numbers and references; date of the block; value in dollars; action taken; legal basis of the block; and **copies of payment instructions, checks, letters of credit, bills of lading, invoices and other transaction documents**.

2. OFAC: DOUBT ABOUT A POSSIBLE "MATCH" AND SELF-DISCLOSURE

For compliance questions, such as a possible name hit in screening, the official channel is OFAC's **Compliance Hotline**, at ofac.treasury.gov. If the internal analysis concludes that the company itself may have taken part, even without intent, in a prohibited transaction, there is the **Self Disclosure Portal**, the voluntary disclosure portal. Under OFAC's official enforcement guide, self-disclosure is a mitigating factor and reduces the base for calculating any civil penalty. The decision to use this channel should be made with specialized legal advice.

3. FINCEN: FINANCIAL INSTITUTIONS AND THE URGENT CHANNEL FOR TERRORISM

Financial institutions subject to U.S. regulation must file a **Suspicious Activity Report (SAR)** with FinCEN, the Treasury's financial intelligence unit. For suspicion linked to terrorism, FinCEN maintains an urgent hotline, the **Financial Institutions Hotline, 1-866-556-3974**, available 24 hours, which speeds the arrival of information to authorities and does not replace the SAR. FinCEN also maintains a **whistleblower reward program**: anyone providing information about a sanctions violation that leads to penalties above 1 million dollars may receive an award, as highlighted in the Treasury's own July 1 statement.

4. FBI: THE CHANNEL OPEN TO ANYONE, IN ANY COUNTRY

Any person, company or institution, inside or outside the United States, can report information about terrorist activity or a U.S. federal crime directly to the FBI, through the official form **tips.fbi.gov** or by phone at **1-800-CALL-FBI**. The report can be anonymous. It was, worth remembering, an FBI Miami investigation that gave rise to the July 1 sanctions.

In Brazil: the two channels the company needs to know

COAF: FOR THE SECTORS OBLIGATED UNDER THE MONEY LAUNDERING LAW

Companies in the sectors listed in Article 9 of Law No. 9,613/1998, among them financial institutions, payment providers, real estate agencies, high-value goods trade, factoring and accounting, have the legal duty to report operations suspected of money laundering or terrorism financing to **COAF**, exclusively through the electronic portal **SISCOAF**. A good-faith report does not create civil or administrative liability for the reporter, by express provision of Article 11 of the same law. The exact deadlines vary according to each sector's regulator, so the safe guidance is to report immediately after concluding the internal analysis and to confirm the applicable deadline in your regulator's rule.

FEDERAL POLICE: WHEN THERE IS EVIDENCE OF A CRIME

Evidence of a link to a designated faction often constitutes evidence of a crime in Brazil, such as criminal organization, money laundering or the offenses of the Anti-Terrorism Law (Law No. 13,260/2016). In these cases, the path is a **criminal report to the Federal Police**, accompanied by the documentation preserved in step 1. Companies that do not belong to the obligated sectors of Law 9,613 do not report to COAF, but they can and should contact the Federal Police when there is evidence of a crime.

A LEGAL CAVEAT NO ONE SHOULD SKIP

No Brazilian law obliges a private company to comply with U.S. sanctions. The Brazilian rule that requires immediate compliance with sanctions, Law No. 13,810/2019, deals with UN Security Council resolutions, not with U.S. lists. A Brazilian company's exposure to U.S. sanctions is **practical and financial**, through access to dollars, banks and partners, and **legal when there is a U.S. nexus**. That is why every decision to block, terminate a contract or report must go through the company's legal team: acting excessively, without basis, also creates risk, including labor and contractual risk.

INCC RESOURCE · FREE

Before hiring anything, measure the problem for free

INCC keeps on its website, at no cost and with no commercial strings, two tools for this situation: the **check of sanctioned persons and companies**, which INCC operates connected directly to the official U.S. government database, being, according to the Institute itself, the first Brazilian institution to establish this direct connection; and a **self-assessment** that shows, in a few steps, your organization's maturity level and points of exposure. This article, like the whole series, is informational: the tools exist so that each company understands its own situation and decides its next steps autonomously.

Go to www.incc.org.br

THE TIME

WHY THE URGENCY, THIS TIME, IS NOT ALARMISM

Three reasons, all factual. First: the pace. Between the FTO designation taking effect and the first sanctions, 26 days passed, and the Treasury has been announcing actions against Latin American criminal networks in sequence, week after week. Second: the method. The July 1 statement describes ongoing investigations, arrests already made and permanent coordination between the FBI, the Department of Justice and the Treasury, which indicates a pipeline, not an isolated event. Third: the asymmetry. Getting on the list is immediate and without notice; getting off, through OFAC's own reconsideration procedure, is slow and discretionary. Whoever prepares after the problem does not prepare, they manage a loss.

The minimum move any company can make this week costs zero: measure its own exposure, check its counterparties against the official lists, write a one-page response protocol and define who answers for this subject. The complete move, the specialized intelligence unit, formed or hired with people of proven experience in the field, is the natural evolution of that first step.

WHAT TO TAKE FROM THIS TEXT

The first sanctions linked to the designation of the PCC and CV have already reached companies and individuals, 26 days after the FTO designation took effect. The regime that produced them sees third parties: the 50% Rule, strict liability and secondary sanctions mean no company can declare itself off the radar in advance. There is an official guide for those who find evidence, with defined channels, deadlines and documents, and it is in this article. What there is not is spare time: the difference between the company that gets through this cycle well and the one that does not is the preparation done **before** the first alert.

Sources and reliability classification

Classification by the NATO (Admiralty) code, from the most reliable source (A1) to the least. A1 indicates an official source and confirmed information; A2, an official source and probably true information; B2, a usually reliable source and probably true information; C3, a fairly reliable source and information to be confirmed. All links were accessed and checked on July 1, 2026.

[A1] U.S. Department of the Treasury, official statement of July 1, 2026: "Treasury Sanctions Brazilian Criminal Network Exploiting U.S. Financial System to Launder Drug Proceeds". Names of the designated parties, amounts, legal bases (E.O. 14059 and E.O. 13224) and implications of the sanctions.
home.treasury.gov/news/press-releases/sb0549

[A1] OFAC, recent action of July 1, 2026 with the entries added to the SDN list.
ofac.treasury.gov/recent-actions/20260701

[A1] U.S. Department of State, statement by the Secretary of State on the designation of the CV and PCC as SDGT and the intent to designate them as FTO effective June 5, 2026 (May 28/29, 2026).
state.gov (statement) · official mirror at br.usembassy.gov

[A1] Federal Register, FTO designation of the PCC and CV, published and effective on June 5, 2026 (91 FR 34267, doc. 2026-11323, Public Notice 13030, signed on May 28, 2026); SDGT designations published the same day (doc. 2026-11324).
federalregister.gov/d/2026-11323 · federalregister.gov/d/2026-11324 · official PDF at govinfo.gov

[A1] Duty to block and report within 10 business days, mandatory content of the reports and the ORS system: 31 C.F.R. §501.603 (blocked property) and §501.604 (rejected transactions).
ecfr.gov · §501.603 · ecfr.gov · §501.604

[A1] OFAC Reporting System (ORS), official page with forms and registration via email OFACReport@treasury.gov; annual report of blocked property due by September 30.
ofac.treasury.gov/ofac-reporting-system

[A1] OFAC official channels: Compliance Hotline, Self Disclosure Portal (self-disclosure as a mitigating factor, per the Enforcement Guidelines, Appendix A to 31 C.F.R. Part 501) and reconsideration procedure for removal from a list.
ofac.treasury.gov/contact-ofac · ofac.treasury.gov/disclosure · Enforcement Guidelines (eCFR) · removal petition

[A1] Official OFAC tool for checking the sanctions lists (Sanctions List Search).
sanctionssearch.ofac.treas.gov

[A1] FinCEN: Suspicious Activity Reports (SAR); hotline for terrorist activity, 1-866-556-3974, 24 hours, whose use does not replace the SAR; reward program for whistleblowers of sanctions violations.
fincen.gov · SAR · fincen.gov · hotline · fincen.gov · whistleblower

[A1] FBI, public reporting channel, including anonymous and from abroad; phone 1-800-CALL-FBI.

tips.fbi.gov · fbi.gov/contact-us

[A1] Brazil: Law No. 9,613/1998, Articles 9 and 11 (obligated sectors, reporting to COAF and protection of the good-faith reporter); Law No. 13,260/2016 (terrorism, investigation by the Federal Police, Art. 11); Law No. 13,810/2019 (compliance with UN Security Council sanctions); COAF and the SISCOAF portal.

planalto.gov.br · Law 9,613 · planalto.gov.br · Law 13,260 · planalto.gov.br · Law 13,810 · gov.br/coaf

[A2] January 2026 arrests in Florida and indictment in the U.S. Federal Court for the Southern District of Florida, as described in the Treasury statement; the specific court documents were not individually checked by this article.

home.treasury.gov/news/press-releases/sb0549

[B2] Specialized legal analyses on the effects of the designation for companies with operations in Brazil. Secondary sources, useful for interpretation, subject to case-by-case verification.

White & Case · Hogan Lovells · DLA Piper

[B2] Press coverage of the July 1, 2026 sanctions, used only for context; all central facts of this article were checked against the primary sources above.

Exame · Terra · The Rio Times

[C3] Institutional assessment by INCC and CNC on the level of preparedness of Brazilian institutions and on the need for proven experience in the intelligence unit, based on the field experience of the institutes; it is neither a statistic nor a formal survey. The statement about INCC's direct connection to the U.S. government database is an institutional declaration by INCC itself.

Own assessment, flagged as such in the body of the text

The dates, names and legal framings cited were checked against official primary sources on July 1, 2026. OFAC designations are administrative acts of the U.S. government and reflect that government's allegations; they do not constitute a judicial conviction.

This article is informational and educational and **does not constitute legal advice**. Responding to a concrete case of evidence of a link to a designated organization requires dedicated and immediate 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.

The persons and companies mentioned as designated by OFAC are cited exclusively based on official and public acts and statements of the United States government, referenced in the sources. The designation is an administrative act of that government and does not represent this Institute's judgment on the guilt or responsibility of anyone whatsoever.

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)**
July 2026 · TLP:WHITE · free distribution, citation encouraged with attribution.