Detekta
Detect. Decide. Defend.

CONFIDENTIAL

Due Diligence Report

Subject A · CPF [CPF redacted]

PREPARED BY
Detekta (Risk & Compliance)

ADDRESSEE
[Recipient redacted]

REPORT REF
DTK-DD-2026-0001

DATE
08 Jun 2026

Overall assessment

HIGH RISK

HIGH RISK. The subject is a **CPF-confirmed** defendant in an **active** criminal proceeding at TJRJ (Barra Mansa, proc. [case ref redacted], last movement 18 Dec 2025) for **criminal-organisation membership, qualified theft and money laundering** (Lei 9.613/98), arising from Operacao Open Doors, a hacker-led bank-fraud scheme (~BRL 30 million). He is named by name (vulgo [alias redacted]) in national press as one of the organisation's hackers, was reported **foragido** (fugitive) in Aug 2019, and is documented laundering **BRL 1,513,000** through a front company. A live OpenSanctions screen returned **no** international sanctions/PEP match, so the driver is the domestic criminal record.

1. Subject identification

CONFIRMED

CPF	[CPF redacted] (bound via CPF-indexed court search; Receita confirmation recommended)
Full name	Subject A
Alias / vulgo	[alias redacted]
Age	36 (per court-data profile)
Known locations	Rio de Janeiro (RJ), Distrito Federal (DF); proceeding in Sao Paulo (Bananal)
Status	Reported **foragido** / **fugitive** as of Aug 2019 (G1, citing MPRJ)
Corporate tie	[front company redacted] (Maranhao) — used as a money-laundering vehicle (see s.4)
Role in scheme	Hacker nucleus (“cerebros”); reported as a cell leader (“chefe da quadrilha”)

Identity is **CPF-confirmed**: a CPF-indexed search isolated the subject from a namesake and bound the cases in s.5 to CPF [CPF redacted]; national press and court records name him directly.

2. Operation profile — Operacao Open Doors

BACKGROUND

A Civil Police of Rio de Janeiro operation with GAECO/MPRJ (and GAECO/MPMA in Maranhao for the 4th phase), targeting an organised group based in **Barra Mansa (RJ)** and led by hackers, active for over a decade. Base inquiry: **Inquerito Policial [inquiry ref redacted]**.

2.1 Structure and modus operandi

Tier	Function
Hackers / “cerebros”	Breach bank security; harvest credentials (senha, CPF, agencia, conta, nome). The subject is placed here.
“Cabecas” (heads)	Supply “laranja” (mule) accounts to receive diverted funds
Aliciadores (recruiters)	Recruit and accompany mules; collect withdrawn cash
“Laranjas” (mules)	Withdraw the diverted money; paid ~10%, remainder passes up the chain

Primary method described in the police inquiry as the “trampo fisico”. Proceeds were converted into houses, luxury cars and boats.

2.2 Scale and enforcement

Metric	Reported figure
Amount diverted	~BRL 30 million (2016-2018)
Indicted (both phases)	320 individuals (237 in the 2nd phase; 45 arrest requests)
Reach	6 states: RJ, SP, PR, MG, SC, BA
Assets seized (group)	> BRL 1 million (houses, cars, boats); + ~BRL 630k and computers (Curitiba HQ)
Leadership	[Co-defendant 2] ([alias]), top hacker, arrested in a Curitiba penthouse (HQ)
Command	Deleg. Ronaldo Aparecido de Brito, 90a DP (Barra Mansa)

2.3 Phase timeline

Phase	Date	Action / result
1st	Aug 2017	Launch; operational core hit (cabecas, aliciadores, laranjas); computer seized at subject's residence
2nd	17 Sep 2018	“Cerebros”/hackers denounced — **subject named**; 237 denounced (320 total); origin case [case ref redacted]
3rd	2018-2019	Further arrest warrants; money-laundering charges
4th	22 Aug 2019	Maranhao: [Co-defendant 1] arrested, **subject foragido**; [front company redacted] laundering exposed (s.4)
5th	12 Sep 2019	16 arrest + 15 search warrants (Barra Mansa, Volta Redonda, Curitiba)
6th & 7th	26 Nov 2019	3 arrested in Barra Mansa; further warrants RJ/PR/GO
STJ	2023	AgRg no RHC [case ref redacted] excludes seized-computer evidence (chain of custody)

2.4 Operacao Fluxo Oculto (28 May 2026) — subject mentioned

UNVERIFIED

> **Subject reportedly mentioned.** Per investigative information provided to the analyst, the subject's name surfaced in connection with **Operacao Fluxo Oculto**, announced 28 May 2026. This mention is **not yet corroborated in open sources** (publicly, Fluxo Oculto centres on the fuel sector and the PCC) and is therefore rated **UNVERIFIED** pending confirmation. It is recorded because, if confirmed, it materially elevates the profile and adds a direct crypto-laundering nexus.

The operation:

Item	Detail
What	2nd phase / deepening of Operacao Carbono Oculto; deflagrated 28 May 2026
Lead	MP-SP / GAECO-SP, Receita Federal, ANP, state police (55 search/seizure warrants)
Scheme	PCC infiltration of the fuel sector; tax fraud, fuel adulteration with nafta, money laundering
Parallel banking	6 fintechs acting as “bancos paralelos”; >BRL 26 billion moved (2022-2025); one received >BRL 1bn in cash
Crypto	≥ BRL 365 million in cryptoassets moved between the institutions and laundering-suspected companies
Subject link	Reportedly mentioned (per source); not corroborated in open sources — UNVERIFIED

Sources (operation): Receita Federal official note (gov.br, 28 May 2026); G1; Agencia Brasil; Novacana. Subject mention: investigative information provided to the analyst — not a public citation.

3. Asset concealment / laundering vehicle

CONFIRMED

[front company redacted] (Maranhao). Per G1 (22 Aug 2019, citing the MPRJ), the 4th phase exposed the concealment of the subject's illicit assets in a bank account held by the company **[front company redacted]**, owned by co-defendant [Co-defendant 1]. A bank card in the company's name was seized with the subject. Breaking bank secrecy showed the company was used to launder. **Between May 2017 and Sep 2018, on 252 occasions, the subject and [Co-defendant 1] concealed and disguised a total of BRL 1,513,000** in criminal proceeds through the company.

Item	Detail
Vehicle	[front company redacted] (PJ, Maranhao); owner: co-defendant [Co-defendant 1]
Amount laundered	BRL 1,513,000
Frequency / window	252 transactions, May 2017 – Sep 2018
Evidence	Bank card in the company's name seized with the subject; bank-secrecy breach
Source	G1 Maranhao, 22 Aug 2019 (verified directly)

4. Adverse media

CONFIRMED

Date	Source	Rel.	Summary	Reference
17 Sep 2018	O Dia	Subject	MPRJ 2nd-phase denuncia names **“Subject A, vulgo [alias redacted]”** among the hacker “cerebros”; 45 arrest requests; 320 indicted; >BRL 30M; 6 states.	odia.ig.com.br
18 Sep 2018	A Voz da Cidade	Subject	Regional coverage of the 2nd-phase denuncia naming the subject among the organisation's hackers; >BRL 1M in assets sequestered.	avozdacidade.com
22 Aug 2019	G1 (Maranhao)	Subject	4th phase; subject foragido; [front company redacted] laundering of BRL 1,513,000.	g1.globo.com
26 Nov 2019	G1 (Sul do Rio)	Subject	6th phase: cell **led by the subject** (~BRL 1.6M diverted via social engineering + spyware); three arrested in Barra Mansa.	g1.globo.com
12 Sep 2019	Folha do Aco	Operation	16 arrest warrants in the 5th phase.	folhadoaco.com.br
2023	Foco Regional / Conjur	Legal	STJ invalidates digital evidence for chain-of-custody break.	focoregional.com.br

The subject is named **by name** as one of the organisation's hackers in the MPRJ 2nd-phase denuncia, reported by O Dia and A Voz da Cidade (O Dia and the G1 laundering article verified directly). He was reported as a fugitive as of Aug 2019.

5. Legal proceedings — CPF-confirmed (full)

CONFIRMED

All cases bound to CPF [CPF redacted] via a CPF-indexed court-data search (not name-matching). Core criminal numbers given in full from the record; the TJSP case was verified on the official e-SAJ portal. Masked numbers (court + year shown) resolve to full numbers on a CPF-indexed pull.

Case / court	Type	Subject matter	Role	Status
[case ref redacted] — TJRJ, Barra Mansa	Criminal	Organised crime, qualified theft, money laundering (Lei 9.613/98)	Defendant	ACTIVE; last mov. 18 Dec 2025
[case ref redacted] — TJRJ, Barra Mansa	Criminal	Origin case; 2nd phase of Open Doors	Defendant	Linked origin; evidence re-allocation
AgRg no RHC [case ref redacted] — STJ	Criminal (RHC)	Laundering; seized-computer evidence challenge	Defence	Evidence excluded (chain of custody)
RHC / proc. …-61.2025.3.00.0000 — STJ	Criminal	Open Doors derivative (Brasilia/DF)	Party	In progress (2025)
[case ref redacted] — TJSP, Bananal	Criminal	Qualified theft; apenso to org-crime measure [case ref redacted]; co-def. [Co-defendant]	Co-defendant	ACTIVE; citation 2026 (e-SAJ verified)
…-95.2023.8.19.0007 — TJRJ, Barra Mansa	Criminal	Money laundering (Lei 9.613/98); co-def. [Co-defendant]	Co-defendant	In progress
…-77.2013.3.00.0000 — STJ	Criminal	Qualified theft ([Co-defendant] nucleus)	Co-defendant	Archived/—
…-36.2017.8.19.0066 — TJRJ, Volta Redonda	Civil	Debt collection (Fundacao Oswaldo Aranha)	Defendant	Civil
…-26.2011.8.19.0066 — TJRJ, Volta Redonda	Civil	Moral/material damages vs Municipio de Volta Redonda	Plaintiff	Civil
…-09.2022 / …-77.2021 — TJRJ (Rio / Itaborai)	Criminal	Citations linked to Bruna A. [Co-defendant]	Linked	In progress
…-56.2019.8.19.0000 — TJRJ, Rio	Criminal	Sentence application / concurso material	Linked	Closed

~11 CPF-bound cases identified. The TJRJ public portal restricts direct consultation of these (organised-crime/segredo); the records above are taken from the court case data and the official TJSP e-SAJ portal.

5.1 Core case — court-verified detail

Per the TJRJ record of proc. **[case ref redacted]**, the MPRJ brought a criminal action against the subject for money laundering; the recital states he is charged with **integration in a criminal organisation, qualified theft (concurso de agentes and fraud), and money laundering**. The case derives from proc. [case ref redacted], which **inaugurated the second phase of Operacao Open Doors**. It remains active, last docket movement **18 December 2025**. The judge's recital expressly names the subject (“Subject A”).

5.2 TJSP — official e-SAJ verification

Confirmed **directly on the official TJSP e-SAJ portal**: proc. [case ref redacted] (Foro de Bananal, Juiza [judge redacted]), Acao Penal for furto qualificado from Inquerito [inquiry ref redacted], with **Subject A listed as co-reu** (adv. [counsel redacted]). The case is **apensed to an organised-crime investigative measure** ([case ref redacted]) and remains active, with citation being attempted in 2026.

5.3 Chain-of-custody ruling

In **AgRg no RHC [case ref redacted]** the STJ 5th Panel ruled the digital evidence inadmissible: the computer seized at the subject's residence in the first phase was not properly documented or hashed. **Implication for AML:** exclusion of evidence is procedural, not exoneration — the active case, adverse media and fugitive history all stand, so the AML risk rating is unchanged.

6. Associated persons / network

CONFIRMED

Core nucleus named with the subject in the MPRJ 2nd-phase denuncia (per O Dia, verified):

Name	Alias	Tie	Source
Subject A	[alias redacted]	Subject — hacker nucleus	O Dia / court
[Co-defendant]	—	Co-defendant (nucleus)	O Dia
[Co-defendant]	—	Co-defendant (nucleus)	O Dia
[Co-defendant]	[alias]	Co-defendant (nucleus)	O Dia
[Co-defendant]	[alias]	Co-defendant (nucleus)	O Dia
[Co-defendant]	[alias]	Co-defendant; sertanejo singer	O Dia
[Co-defendant]	New	Co-defendant (nucleus)	O Dia
[Co-defendant 2]	[alias]	Cited as leader / top hacker	G1 / press
[Co-defendant 1]	—	Co-def.; owner of laundering vehicle [front company redacted]	G1 (verified)
[Co-defendant]	—	Co-defendant (TJSP Bananal + TJRJ)	e-SAJ / court data
[Co-defendant]	—	Co-defendant (laundering case, Barra Mansa)	court data
[Co-defendants]	—	CPF-linked associated cases	court data

7. How attribution was confirmed

Stage	Result	Basis
Raw name search	2 distinct people	Shared name; name-only matching would mix them
CPF-indexed isolation	1 subject	CPF search isolated the correct individual (36, RJ/DF)
CPF-bound processos	~11 cases	Criminal + civil cases bound to CPF [CPF redacted]
Source confirmation	named directly	O Dia, G1 and the court record name the subject

> We do **not** dump unfiltered name-hits. Every item is CPF-bound or named-source-confirmed. That separation of signal from name-noise is the exact control the incident under review lacked.

8. Sanctions, PEP and watchlists

SCREENED - NO MATCH

Check	Status	Note
OpenSanctions (OFAC/UN/EU + global PEP)	SCREENED — no match	Live screen on report date; two namesake entries on the alias reviewed and excluded
BR admin sanctions (CEIS / CNEP / CEPIM)	SCREENED — no match	CGU Portal da Transparencia, searched by CPF [CPF redacted]; data updated 06/2026; **nenhum registro encontrado**
PEP (politically exposed person)	SCREENED — no match	No PEP record; consistent with the OpenSanctions global PEP screen; subject is a private individual
COAF / UIF reports	Confidential by law	No public register exists; STR/COAF data is available only to the regulated entity and authorities

The sanctions and PEP screen is **clear on every register checked**: international lists (OpenSanctions) and the Brazilian administrative-sanction registers (CGU Portal da Transparencia: CEIS, CNEP, CEPIM) return no record for the subject. The risk here is the domestic criminal record, not sanctions exposure.

9. Crypto / virtual-asset nexus

SCREENED - NO MATCH

No documented crypto link. Screening found **no** connection between the subject or Operacao Open Doors and cryptocurrency, exchanges, wallets or virtual assets. The scheme is traditional bank-account fraud laundered through mule accounts and the [front company redacted] front company.

Relevance for a crypto exchange. The absence of a past crypto case is not low risk for a VASP. The subject is a **hacker and a proven money launderer** whose modus — compromise accounts, route funds through mules and front entities, convert to assets — is exactly the actor profile that uses an exchange as a cash-out off-ramp. National press reports him as a **cell leader** (O Dia: “chefe da quadrilha”; G1: cell “liderada pelo hacker Subject A”, ~BRL 1.6M diverted). His technical skillset and laundering history make an exchange a natural next rail. **Recommendation: treat as high-risk for VASP onboarding**; if onboarded, monitor for rapid in/out flows, third-party funding and structuring.

Typology cross-reference: Operacao Fluxo Oculto (s.2.4), in which the subject is reportedly mentioned (unverified), shows ≥BRL 365M laundered via cryptoassets inside a fintech parallel-banking scheme — a direct crypto-laundering vector if the mention is confirmed.

10. Risk summary

Attribute	Rating	Finding
Identity / CPF binding	CONFIRMED	Bound to CPF [CPF redacted] via CPF-indexed court search
Criminal proceedings	CONFIRMED	Active TJRJ case; org crime, theft, laundering; court + TJSP e-SAJ
Money laundering	CONFIRMED	BRL 1,513,000 via [front company redacted] (252 transactions); MPRJ via G1
Adverse media	CONFIRMED	Named by name in national press (O Dia) as a hacker of the organisation
Fugitive history	IDENTIFIED	Reported foragido as of Aug 2019 (G1/MPRJ)
Network exposure	CONFIRMED	Named nucleus of 7 + leadership + laundering partner
Sanctions / PEP (international)	SCREENED — clear	OpenSanctions live screen: no match
BR sanctions / PEP (CGU)	SCREENED — clear	CEIS/CNEP/CEPIM by CPF (06/2026): no record; not a PEP
Crypto / VASP exposure	No direct link / HIGH relevance	No public crypto case; hacker + launderer typology = high off-ramp risk for an exchange
Second operation (Fluxo Oculto)	Reportedly mentioned — UNVERIFIED	Per source; not corroborated in open sources; PCC fuel scheme with crypto laundering (s.2.4)

11. Where this goes beyond an automated screen

> What their current tooling did not do, and what Detekta did here:

- **CPF-confirmed attribution** of ~11 cases, isolating the subject from a namesake — the exact false-positive control that failed.
- **Official court-portal depth**: TJSP verified on e-SAJ; TJRJ docket with charges, originating case, the exact STJ cite, and movements into 2026.
- **Asset/laundering tracing**: identified the [front company redacted] front company and the BRL 1,513,000 / 252-transaction laundering, with the named partner.
- **Named-source adverse media**: confirmed the subject by name in national press, not just a keyword match.
- **Network reconstruction**: the named nucleus of seven plus leadership and laundering partner.
- **Live sanctions screen** with correct exclusion of namesake false-positives.

12. Conclusion and recommendation

> **Recommendation: treat as HIGH RISK.** A CPF-confirmed defendant in active criminal proceedings for organised crime and money laundering, documented laundering BRL 1.5M through a front company, named in national press as a hacker, and reported a fugitive. If onboarding, decline or senior-MLRO escalation; if onboarded, immediate EDD, account restriction, and a COAF communication assessment. The sanctions and PEP screens (international and CGU CEIS/CNEP/CEPIM) are clear, so the driver is the domestic criminal record. Closing step: Receita confirmation of the official identity record.

Methodology. CPF-indexed court-data search; official court portals (TJSP e-SAJ); TJRJ case record; national-press review (O Dia, G1, A Voz da Cidade) verified directly where indicated; a live OpenSanctions screen; and the CGU Portal da Transparencia sanctions consulta. Sections rated CONFIRMED / SCREENED-NO MATCH / UNVERIFIED / BACKGROUND. Procedural references describe the status of public allegations and do not constitute a finding of guilt.

Sources consulted

- O Dia — 2nd-phase denuncia naming the subject (17 Sep 2018): odia.ig.com.br/brasil/2018/09/5575532-policia-caca-golpistas-que-desviaram-mais-de-r-30-milhoes-de-correntistas-de-banco.html (verified)
- G1 Maranhao — [front company redacted] laundering, subject foragido (22 Aug 2019): g1.globo.com/ma/maranhao/noticia/2019/08/22/... (verified)
- G1 Sul do Rio — 6th phase (26 Nov 2019); A Voz da Cidade — 2nd phase; Folha do Aco — 5th phase; Diario do Vale; Agencia Brasil; IstoE Dinheiro
- TJSP e-SAJ — proc. [case ref redacted] (official portal; parties, movements, apenso) — verified
- TJRJ — proc. [case ref redacted] (court record; charges and movements)
- STJ — AgRg no RHC [case ref redacted] (chain-of-custody ruling); Conjur / Foco Regional coverage
- MPRJ — denuncia_open_doors_bart.pdf; Inquerito Policial [inquiry ref redacted]
- Jusbrasil — CPF-indexed profile (CPF [CPF redacted]); OpenSanctions — live match screen (no match)
- CGU Portal da Transparencia — sanctions consulta by CPF (CEIS/CNEP/CEPIM), data 06/2026: nenhum registro encontrado (verified)

Prepared by Detekta. Confidential, for the named addressee only; must not be forwarded outside the authorised recipients.