The “regulator” was registered one day before the broker

Galidix, 10 sister brands and 11 invented financial watchdogs

Open source fraud infrastructure report | Research sample

PEIS

Research: 26–27 October 2026
English edition: 6 November 2026

> Public-source research sample. Domains are written in a non-clickable form (`example[.]com`) so that nobody lands on a fraudulent site by accident. Regulator warnings are linked in full.

Galidix presents itself as an international online broker for forex, indices, shares, commodities and crypto assets. It is translated into 14 languages, including Slovak, Czech, Hungarian and Polish. This report traces who stands behind it, how it is built and what links it to other brands. Method: passive OSINT only — public websites, regulator databases, RDAP, Certificate Transparency, the Wayback Machine, urlscan.io and static analysis of publicly served JavaScript. No account was opened, no form was submitted and no login was attempted.

1. Key findings

- **No identifiable legal entity.** The website never names a company, registration number, country of incorporation or licence — not even in its terms and conditions.
- **At least five European regulators have warned against it** (Belgium, Sweden, Italy, France, Norway) between December 2025 and September 2026. Sweden’s Finansinspektionen states that it could not verify that Galidix is a real company.
- **A made-to-measure fake regulator.** The site displays a “membership” badge from `cryptomonitoringauthority[.]com`, a domain registered **one day before** `galidix[.]com`. Its member list places Galidix next to real, regulated brokers to borrow their credibility.
- **A rotating trading platform.** Clients trade on `trading-area.galidix-vN[.]com`. At least six versions (v2–v7) serve an identical build, and v8 is registered in reserve — consistent with replacing domains as authorities block them.
- **Built-in “operator” and “dealer” roles** plus login by a token in the URL: staff can open a client’s session and act inside it. This is typical equipment of call-centre investment fraud (“boiler rooms”).
- **Still online** on 27 October 2026, with active Slovak and Czech versions and no warning yet from the Slovak (NBS) or Czech (ČNB) central banks.

2. Identifiers

Type	Value	Note
Brand	Galidix	
Main website	`galidix[.]com`	Behind Cloudflare, PHP back end

Trading platform	`trading-area.galidix-v2[.]com` … `v7[.]com`	Identical build `index-BBEFitQI.js`
Email domains	`galidix[.]finance`, `galidix[.]team`	The Slovak page shows a machine-translated “podpora@…” address
Phone numbers	+44 7459 742814 (UK mobile); +65 3159 0473 (Singapore)	Sweden’s March 2026 warning lists +65 3159 0597 — the number has changed
Stated addresses	London EC4R (serviced offices shared by many firms); Singapore	No sign of an actual office
“Regulator”	`cryptomonitoringauthority[.]com`	Invented authority, see section 5
Translation key	Linguise `pk_9swR29lv`…	Pivot to other sites run by the same operator

3. Infrastructure

Domain	Registered	Registrar	Name servers	Status 27 Oct 2026
`cryptomonitoringauthority[.]com`	**2025-08-06**	Tucows	hk3/hk4.koddos.com	online
`galidix[.]com`	**2025-08-07**	Internet Domain Service BS Corp	irma / kayden (Cloudflare)	online
`galidix[.]finance`	2025-08-07	TLD Registrar Solutions	stanley / kelly (Cloudflare)	email domain
`galidix[.]team`	2025-08-22	TLD Registrar Solutions	cris / bingo (Cloudflare)	email domain
`galidix-v2…v5[.]com`	2025-08-22	Internet Domain Service BS Corp	irma / kayden	trading area online
`galidix-v6[.]com`	2025-09-08	Internet Domain Service BS Corp	irma / kayden	trading area online
`galidix-v7[.]com`	2025-11-28	Internet Domain Service BS Corp	irma / kayden	trading area online
`galidix-v8[.]com`	2025-11-28	Internet Domain Service BS Corp	irma / kayden	registered, not yet used

- The main domain and every `galidix-vN` domain share the same Cloudflare name-server pair (irma/kayden). Cloudflare assigns name-server pairs per account, so these domains are very probably managed from one Cloudflare account.
- The fake regulator runs on different hosting (Koddos name servers) but was registered one day before the brand — a strong timing link.
- First TLS certificate for `galidix[.]com`: 22 August 2025 (crt.sh). First Wayback Machine capture: 23 December 2025.
- `galidix[.]net` and `galidix[.]io` are not linked to the operation by any evidence; they may be unrelated or defensive registrations.

4. What the website does

- **Redirects by country and language:** a visitor from Slovakia lands on `/sk`. Fourteen languages through the Linguise service.
- **Terms and conditions** mention only “Galidix (the Company)”: no legal entity, address, registration number, governing law or licence. The company reserves the right to charge inactivity and low-balance fees “at its discretion”, and accepting a bonus binds the client to separate bonus rules — a common tool for blocking withdrawals.
- **Account ladder:** Standard 250, Bronze 3,500, Gold 25,000, Platinum 50,000. Each step promises a “more senior” personal consultant, “insured contracts” and “company funding”. This ladder is a sales script of call-centre brokers.
- **Filler content:** live news feeds (Business Wire, Cointelegraph, CNBC) make the site look active.

5. The fake regulator: “Crypto Monitoring Authority”

The site poses as an independent supervisory body with a dispute committee, a “compensation fund of €100,000 per complaint”, a list of “fraudulent brokers” and a “File a complaint” form.

- Its **member list of 37 brokers** consists mostly of real regulated firms — and **Galidix**.
- Galidix’s “certificate” is dated **24 February 2025**, six months before the domain `galidix[.]com` existed (registered 7 August 2025). The date is invented.
- No real regulator of that name exists. It has no legal basis and appears on no official list.
- **Risk:** the “complaint” and “compensation” pages are a natural trap for *recovery fraud* aimed at people who have already lost money.

6. The trading platform (static JavaScript analysis)

`trading-area.galidix-vN[.]com` is a React/Vite single-page application. The public bundle (identical on v2–v7) shows:

- **Three user roles: client,** `operator` **and** `dealer`**.** An operator session can place trades (`isOperator` plus one-click trading).
- **Login by URL token:** parameters `tkn`, `user_id` / `operator_id` and `tknlnd` (a landing-page token). A staff member or a landing page can open a client session directly through a link.
- **Built-in chat** between client and staff, a websocket “user stream” and notifications.

Interpretation: a white-label “broker in a box” in which call-centre staff can see into client accounts and act in them, while a “dealer” controls trade execution — consistent with simulated trading rather than real market access. This is a conclusion drawn from the code, not a confirmed finding.

7. Regulatory action

Date	Authority	Action
2025-12-18	FSMA (Belgium)	Warning — no authorisation (IOSCO I-SCAN)
2026-03-27	Finansinspektionen (Sweden)	Investor alert; could not verify that Galidix is a real company

2026-08-04/05	CONSOB (Italy)	Blocking order, including galidix.com and the galidix-v2 trading area
2026-09-04	AMF (France)	Blacklist — crypto-asset derivatives
2026	Finanstilsynet (Norway)	Republished the AMF warning

A search summary mentioned an Australian ASIC listing for the v3 trading area; it **could not be verified**. No warning from Slovakia's NBS or the Czech ČNB existed at the time of research, although the site is fully translated into both languages.

8. Following the leads: a network of sister brands

Following the technical leads uncovered a network of **at least 10 broker brands and 11 fake "regulators"** built to the same recipe.

How the network was found

1. **A byte-identical trading app.** Searching urlscan.io for the SHA-256 fingerprint of Galidix's trading bundle returned the trading areas of UmexGain. The same bundle is served by the trading areas of Fintradix and LotmentCapital.
2. **A shared block of phone numbers.** UmexGain lists +65 3159 0475, Galidix +65 3159 0473 (previously 0597) — neighbouring numbers from one Singapore VoIP block.
3. **A second fake regulator.** UmexGain links to `digitaloversightcommission[.]com`, set up exactly like the first one: registrar Tucows, Koddos hk3/hk4 name servers, the same WordPress template, the same "€100,000 compensation fund" text.
4. **Reverse name-server lookup** on the Koddos servers (HackerTarget, 92 domains) revealed **11 fake "authorities"** with the same naming pattern. Each lists 32–40 real brokers as "members" plus **one unknown brand** — the scheme it was built for.
5. The brand domains were then confirmed through the pattern `trading-area.<brand>-vN[.]com`, `<brand>.team` and live websites.

The fake "regulators" (all on Koddos name servers)

Fake authority	Registered	Unknown brand among the "members"
`cryptoassetscontrol[.]com`	2024-01-08	(no member list)
`digitalfinanceauthority[.]com`	2025-02-28	MulfinTrade
`cryptoregulationcommission[.]com`	2025-04-03	FinoForge
`digitalcryptocommission[.]com`	2025-04-15	Fintradix
`cryptofinancecommission[.]com`	2025-05-20	VelorGain
`cryptomonitoringauthority[.]com`	2025-08-06	**Galidix**
`cryptoregulationauthority[.]com`	2025-08-06	MaxfulEdge
`cryptooversightauthority[.]com`	2025-12-10	Chain4Coins

`internationalcryptoauthority[.]com`	2025-12-10	LotmentCapital
`digitaloversightcommission[.]com`	2026-04-15	UmexGain
`cryptoregulatoryaffairscommission[.]com`	2026-04-15	Deon Markets

The fake authorities appear in pairs on the same day (2025-08-06, 2025-12-10, 2026-04-15), usually **0–25 days before** the brand's own domains. VelorGain's fake certificate carries **the same invented date as Galidix — 24 February 2025**.

The sister brands

Brand	Website (27 Oct 2026)	Trading areas	Platform generation	Regulator warnings found
Galidix	online	v2–v7	A (identical bundle)	FSMA, FI, CONSOB, AMF, Finanstilsynet
UmexGain	online	v3/v4/v5/v9	A (identical bundle)	CONSOB (July 2026), FSMA
LotmentCapital	online	v3–v7	A (identical bundle)	FSMA via I-SCAN (April 2026)
Fintradix	main site not found	v3–v6	A (identical bundle)	An FSMA entry from 2021 may concern an older firm with the same name
VelorGain	online	v2–v5	B (Vue white label)	none found
FinoForge	online	v2	B	none found
MaxfulEdge	online	v2–v5	C (API proxy shell)	German SGK list (Feb 2026)
Deon Markets	online	v2–v5	C	none found
Chain4Coins	offline	v2–v5	C	German SGK list (Jan 2026)
MulfinTrade	online	—	—	German SGK list (July 2025)

Shared traits: rotating `trading-area.<brand>-vN` domains; email domains `<brand>.team` / `<brand>.finance`; main and trading domains at Internet Domain Service BS Corp (Bahamas) or NameSilo, email domains at TLD Registrar Solutions; everything behind Cloudflare; a separate Linguise translation key per brand. Generation B exposes its settings in `/config.js`: brand name, API and socket addresses, 12 languages including Czech and Polish, withdrawals by bank, BTC, ETH and USDT, and `MINIMUM_WITHDRAWAL: 0`.

9. Assessment

High confidence: Galidix, UmexGain, LotmentCapital and Fintradix run on the same platform deployment (identical code), and Galidix and UmexGain share a block of phone numbers — pointing to one operator or one service provider.

Medium confidence: VelorGain, FinoForge, MaxfulEdge, Deon Markets, Chain4Coins and MulfinTrade belong to the same network, based on the shared fake-regulator infrastructure, matching templates, invented dates and the same domain routine. They use other versions of the trading platform, so a common “fraud as a service” supplier working for several call centres is also possible.

10. Recommended next steps

- Report the live brands — especially those **without any warning** (VelorGain, FinoForge, Deon Markets) — to NBS, ČNB, FSMA and AMF.
- Report the 11 fake authorities to the abuse contacts of the hosting provider and registrar, and to IOSCO members (impersonation of supervisory bodies).
- Check whether the brands’ `api.` and `socket.` hosts share a common back-end IP (passive DNS).

Sources

- Finansinspektionen (Sweden): investor alert on Galidix
- IOSCO I-SCAN entry 47977 and entry 51187
- Finanstilsynet (Norway): investor alert
- AMF (France): blacklists (data.gouv.fr export, 26 October 2026)
- CONSOB (Italy): website blocking orders and latest warnings; Teleborsa report of 6 August 2026
- FSMA (Belgium): companies operating unlawfully
- SGK e.V. (Germany): warnings
- RDAP (rdap.org), crt.sh, Wayback Machine CDX and urlscan.io queries, 26–27 October 2026; HackerTarget reverse name-server lookup (hk3/hk4.koddos.com), 27 October 2026

Independent research sample. Findings reflect public sources and passive checks completed on 27 October 2026. Websites and domains in this network change frequently; check the current regulator warnings before relying on any status shown here.