Lost money to a scam? These “lawyers” are coming for the rest

Recovery-fraud ads aimed at Slovakia and the Ukrainian call-centre playbook they match

Open source fraud advertising report | Research sample

PEIS
Status checked: 30 October 2026
Media context added: 6 November 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. Names of advertising pages that look like personal names, and payer names, are left out.

The research started with a single Instagram ad from a “European Consumer Helpdesk” that promised to get money back for victims of online fraud. It then mapped similar ads shown in Slovakia and Czechia. “Recovery” offers are a second-wave fraud: people who have already lost money are asked to pay again — a “fee”, a “tax” or a “deposit” — to an invented lawyer, agency or authority that will never recover anything.

1. Key findings

- **Two faces for every link.** The ad links are cloaked: Facebook’s and Instagram’s automated reviewers are shown a harmless page (a travel blog, a “legal services in Germany” page), while a real visitor from a phone sees a fake helpdesk or law firm with a contact form.
- **Fake authority.** One page imitates an INTERPOL “Silver Notice” to look like an official asset-tracing service.
- **Industrial set-up.** The same traffic-distribution software (Keitaro), the same PHP version, shared lead-collection systems and shared Cloudflare name-server pairs link domains that look unrelated.
- **Five clusters.** 16 live domains sort into five groups that very probably share a Cloudflare account, plus several standalone sites.
- **Russian is the working language, not proof of who is behind it.** The victim-facing pages are written in Russian and aim at Russian speakers living in Slovakia and Czechia. The same “fake law firm will recover your money” scheme was raided by Ukrainian police in Kharkiv in 2026, and Europol-backed raids in Kyiv, Dnipro and Ivano-Frankivsk hit call centres that targeted Slovakia (section 5). The technical evidence in this dataset does not by itself tie these specific sites to a country.
- **Fast rotation.** Most domains were registered or first certified between June and October 2026; some ads from 2022–2023 are still listed as active but point to dead domains.

2. What the reviewer sees vs. what the victim sees

Ad domain	Shown to the platform’s bot	Shown to a real visitor
`topnews[.]my`	A travel blog	“European Consumer Helpdesk” with a lead form
`x.clarentix[.]info`	“Legal services in Germany”	A fake INTERPOL “Silver Notice” asset-recovery page

assistantwork[.]top	The same page, shorter	A “legal company” offering recovery
conc-supp[.]info	The same page	Another “legal company” with a contact form
brokerverif[.]live	The same page	Testimonials thanking “experts” for getting money back
lidermylaw[.]com	The same page	A “European centre for the return of funds”

The switch is done by a traffic-distribution system (Keitaro). It decides by device, referrer and network whether the visitor is a reviewer or a target. Some sites returned an empty page to direct visits and only answered visitors who came from the ad.

3. Infrastructure clusters

Cloudflare assigns a pair of name servers to each account. Domains that share a pair are very probably managed from the same account, even when their brands differ.

Cluster	Cloudflare name-server pair	Domains	Notes
A	connie / pranab	topnews[.]my, x.clarentix[.]info	Keitaro, PHP 7.4.33; leads go to lead.sharkleads[.]app; fake INTERPOL notice
B	alberto / hazel	assistantwork[.]top, concordialegal[.]online, conc-supp[.]info, easyref[.]site	Keitaro; forms post to post.php; ads in Slovakia and Czechia from 2 October 2026
C	rayden / angela	startexo[.]pro, jurexhelp[.]info, stone-sterling[.]com	Pages empty to direct visits; new ads on 28 October 2026
D	adaline / stan	help-bws-limited[.]info, concorde-slctrs[.]info	New ads on 28 October 2026
Standalone	separate pairs	brokerverif[.]live, lidermylaw[.]com, infobase[.]help, sitefinlaw[.]info, engelber-tink[.]com	brokerverif sends leads to an API on yurpomosh[.]ru; lidermylaw continues older “Lider” domains from 2023; engelber-tink poses as a Dutch law firm, uses +31 numbers and targeted Czechia and nine other EU countries, ages 45–64

4. Related funnels found in the same sweep

- acrisvault[.]com (ads from 28 October 2026, Czechia) impersonates Meta: a “Facebook AI” platform promising €1,600 a month, with a six-step quiz and a contact form.
- offchannelarbitrax[.]com (ads from 29 October 2026) pushes visitors into a Telegram “arbitrage” channel with about 9,500 members.
- jt-community[.]space redirects to a crypto and gold “trading” site that moves the conversation to Telegram.

5. The same scheme in Ukrainian police files

Public enforcement records from 2025–2026 describe call centres in Ukraine running exactly this kind of second-wave fraud against Europeans:

- **Kharkiv, May 2026 — fake “legal company”.** Operators bought contacts of people already hit by fake-investment schemes, posed as employees of a legal company and promised to recover the lost money. They then asked for payments, had victims install remote-access software “for verification”, took over online banking and took out loans in the victims’ names. Victims in Latvia lost more than €116,000. Eurojust reports four arrests and 14 searches. (Eurojust, 29 May 2026; From-UA, 25 Aug 2026)
- **Nationwide, August 2026 — 94 call centres in one week.** Ukrainian police, the SBU and prosecutors carried out more than 400 searches; some victims “were promised help in returning money that they had previously lost to scammers”, and EU citizens were among the targets. (Help Net Security, 14 Aug 2026)
- **Kyiv, Dnipro and Ivano-Frankivsk, December 2025 — Slovakia among the victims.** A Europol-supported operation searched 72 sites and detained 12 people in a network with more than 400 known victims and over €10 million in losses; Slovakia is named among the countries hit. (Vosveteit.sk, 21 Dec 2025)
- **September 2026 — a Slovak worker inside.** A 23-year-old Slovak woman was lured to Ukraine with a job offer and forced to work in a fraudulent call centre until Polish police freed her in Warsaw. (STVR, 30 Sep 2026)

Assessment: the method seen in these ads matches schemes that Ukrainian and European authorities have documented in Ukrainian call centres targeting victims across Europe, including Slovakia. That makes a Ukrainian base a plausible working hypothesis. It is **not proven** for these particular domains: none of the sites, trackers or lead back ends examined here carries a technical trace to a specific country, and one lead back end sits on a `.ru` domain. A phone number, a payment account or a caller’s details from a victim would be the evidence that settles it.

6. How the ads were found

1. The original Instagram ad link was resolved and compared as seen by a normal phone browser and as seen by platform crawlers.
2. Meta’s public Ad Library was searched with country = Slovakia and Russian-language keywords about recovering money; this was the most productive method.
3. Each landing domain was checked with RDAP/WHOIS, Certificate Transparency (crt.sh), DNS and HTTP responses, and grouped by Cloudflare name servers, tracker software and form back ends.
4. Some advertisers collect data with Meta’s own lead forms and have no website at all; those can only be reported through the ad itself.

7. Indicators (status 30 October 2026)

Domain	Status	Registered / first certificate	Cluster
`topnews[.]my`	live	2026-10-22	A
`x.clarentix[.]info`	live	cert 2026-02-12	A

assistantwork[.]top	live	2026-07-21	B
concordialegal[.]online	live	2026-07-17	B
conc-supp[.]info	live	cert 2026-07-23	B
easyref[.]site	live	2026-10-01	B
startexo[.]pro	live	cert 2026-06-25	C
jurexhelp[.]info	live	cert 2026-10-02	C
stone-sterling[.]com	live	2026-01-26	C
help-bws-limited[.]info	live	cert 2026-04-22	D
concorde-slctrs[.]info	live	cert 2026-09-29	D
brokerverif[.]live	live	cert 2026-10-09	—
lidermylaw[.]com	live	2026-07-25	—
sitefinlaw[.]info	live	cert 2025-11-14	—
engelber-tink[.]com	live	2026-04-21	—
infobase[.]help	origin down (HTTP 521)	2026-01-09	—
lead.sharkleads[.]app, yurpomosh[.]ru	lead back ends	—	—
trust-plus[.]online, save-trust[.]pro, cap-return[.]org, liderlaw-eu[.]com, lider-law[.]com, lawbladesolutions[.]net	dead (NXDOMAIN), ads still listed	2022–2023	—

8. If you lost money and someone offers to get it back

- Real police, regulators and INTERPOL do not advertise on social media, and do not ask victims for fees to release funds.
- A real lawyer can be checked in the bar association’s register of the country they claim; in Slovakia that is the Slovak Bar Association (SAK).
- Any request for an upfront “fee”, “tax”, “insurance” or crypto payment to unlock recovered money is the fraud itself.
- Report the ad inside Facebook or Instagram, report the fraud to the police, and keep every message, payment record and phone number.

Scope and limits

Passive checks only: public ad listings, normal page loads, DNS, RDAP/WHOIS and certificate logs. No form was submitted, no one was contacted and no attempt was made to get around bot checks. Status is as of 30 October 2026; these domains rotate weekly. Shared infrastructure shows common management of websites, not the identity, nationality or location of the people behind them.

Independent research sample, 30 October 2026. Check current status before relying on any indicator shown here.