THREAT INTELLIGENCE REPORT

The ICANN Cartel: $155 Million a Year for Contracts Nobody Honors

Ref. **PD-TI-2026-66564** Published **23 July 2026** Source **phishdestroy.io/icann-155-million-illusion**

ACCOUNTABILITY REPORT · THE DOMAIN ECONOMY

They want the money. They refuse outside regulation. And they do not enforce their own contracts — exactly like the registrars they accredit. The paper trail is published on ICANN's own website.

car·tel /kär'tel/
An association whose members collect the market's money, shield each other from outside oversight, and treat the rules they signed as optional.

By that definition, the Internet Corporation for Assigned Names and Numbers is not the internet's regulator. It is the internet's cartel. Judge it by three tests:

They want the money. $155 million a year in fees, collected from every registry and registrar on Earth [4] .
They refuse to be regulated. No government agency audits ICANN's enforcement. Since the 2016 IANA transition it answers only to itself — a "multistakeholder community" it convenes, feeds, and moderates.
They do not honor their own contracts. The Registrar Accreditation Agreement they wrote is ignored by their own registrars — and ICANN's response to documented breaches is a polite email thread [1] .
The ongoing Trustname case proves all three at once — in documents ICANN published about itself.

The Money: a $155 Million Toll Booth

ICANN's own financial reports [4] show what the world pays for the privilege of a functioning DNS:

$155M
Total annual revenue
$91M
Registry fees
$57M
Registrar fees
$7M
Contributions & sponsorships
For that price the global community should get stringent oversight, immediate threat mitigation, and instant revocation for accredited companies harboring criminals. What it gets instead is a cartel of inaction: people collecting "free money" for shuffling paperwork — while the crime that funds part of this ecosystem lands on victims.

And we know exactly which domains part of that fee income comes from. Our open dataset tracks ShortDot's abuse-saturated TLD zones — ICANN's per-domain income from them is recalculated yearly, in public, on GitHub [10] . Standing challenge to the "guardians of a secure internet": show us even **1%** of those domains being legitimate. We looked — there is nothing legitimate there, exactly as with Trustname, and exactly as with NiceNIC, whose only notable client is DDoS-Guard — and even that is debatable. You charge a fee on every single registered domain, and you have not prevented a single scam. Analyze it. Stop lying in your reports — is that really so hard? The data is publicly available for analysis — yet it is absent from your official mitigation reports.

Look directly at the "New gTLD" program. Zones crowded with algorithmic spam, botnet C2 infrastructure and single-use phishing links — .top, .icu, .cyou and their siblings — sell for under a dollar in year one. Criminals buy them in batches of a hundred thousand, and ICANN collects its mandatory fee on every single registration. This is not a blind spot; it is a business model. High abuse volume equals high revenue.

That is the cartel's core conflict of interest in one sentence: every registrar is a paying client and every junk registration is billable, so every revoked accreditation and every mass suspension means ICANN cutting its own income. A police force paid per criminal left on the street does not make arrests.

Section 3.18: the Contract the Cartel Wrote and Won't Enforce

Section 3.18 of the 2013 Registrar Accreditation Agreement [3] obligates every accredited registrar to take "reasonable and prompt steps to investigate and respond appropriately" to abuse reports. In practice, registrars across the industry ignore it — because they know the party responsible for enforcement never enforces.

A rule that is never enforced is not a rule. It is set dressing.
If Section 3.18 is universally ignored and ICANN refuses to enforce it — remove Section 3.18 entirely. Keeping it manufactures a false sense of security for end-users. Without it, the world would at least

see the raw, unregulated truth of the domain industry.

The Track Record: RegisterFly, EstDomains, Epik, NameSilo

Trustname is not an anomaly. It is the cartel's standard operating procedure:

1 · RegisterFly — the meltdown that forced a reform

In 2007, ICANN-accredited RegisterFly [5] imploded: fraud allegations, locked-out customers, hundreds of thousands of domains expiring in captivity. ICANN spent months writing letters while registrants lost their names, and terminated the accreditation only after a public outcry — a scandal so bad it forced the RAA to be rewritten.

2 · EstDomains — accreditation until conviction

In 2008, EstDomains [6] was the industry's most notorious criminal registrar, servicing botnets and malware. ICANN ignored the security community for months and moved only after the CEO's credit-card-fraud conviction became public.

3 · Epik — breach notices while customers lost everything

As Epik [7] melted down — breached, insolvent, failing to renew client domains or pay registries — ICANN's answer was boilerplate "breach notices" while users lost control of their assets.

4 · NameSilo — a complaint answered with a vacation

In 2018, Artists Against 419 filed compliance complaint **UNY-783-11184** documenting how NameSilo waved through fake registration data and ignored fraud reports [9] . ICANN closed it with a masterpiece: the abuse "does not fall within the registrar's purview." The escalation was answered by a complaints officer leaving on holiday ("I am targeting 30 September to issue you a response"), then a year of "competing priorities" — and no resolution, ever. That is ICANN's entire audit model: reports written by itself, about itself, graded by itself. Reporters are treated as idiots, registrars as saints — the

same NameSilo that later covered for the xmrwallet Monero-drainer and lied about it publicly on Twitter .

5 · Alpnames — revoked only after the corpse stopped moving

ICANN-accredited Alpnames industrialized ultra-cheap new-gTLD registrations and became a global haven for spam campaigns; researchers screamed about it for years. ICANN did not terminate it over Section 3.18. The accreditation was pulled in 2019 only after the company had physically collapsed and gone dark, stranding hundreds of thousands of domains — legitimate ones included [2] . ICANN waits for a registrar to die on its own rather than act on abuse data.

Trustname: the Cartel Documents Itself

The best part: none of this is a leak. ICANN *voluntarily publishes* the evidence of its own impotence and files it under "compliance" [2] . The official Notice of Breach of July 16, 2026 [1] records, in ICANN's own words, how a domain that was actively stealing credit card data stayed in business while the regulator wrote letters:

Date	What ICANN's own notice records
`Jun 10`	**First Notice.** The registrar promises to fix it. The phishing continues.
`Jun 26`	**Second Notice.** Ignored entirely.
`Jul 8`	ICANN escalates — by email and portal message.
`Jul 11`	The registrar replies with information ICANN itself says **"contradicts public data"** — in plain terms, they lied.
`Jul 13`	Another follow-up email.
`Jul 14`	The registrar claims the `clientHold` on the card-stealing domain was removed **"inadvertently."** ICANN's response: one more email.
`Jul 16`	**Third Notice of Breach** — published with pride.
`Aug 6`	**The deadline.** A registrar that services criminal operations, lies in official correspondence and "accidentally" unblocks phishing gets three more weeks.

For roughly 60 days, while criminals drain bank accounts, the cartel's maximum sanction is being a pen-pal.
Three notices. Five follow-up emails. Zero revoked accreditations. Zero protected victims.

The WHOIS Shield and the Failure of SSAD

ICANN's complicity goes beyond inaction. After GDPR in 2018 it allowed registrars to redact WHOIS wholesale, blinding security researchers overnight. Instead of a rapid-response channel for threat intelligence, it spent years and millions designing SSAD — a bureaucratic maze in which investigators politely ask registrars for data and get ignored; the scaled-down RDRS that finally launched in 2023 is voluntary and non-binding [13] . They built a system that protects the privacy of botnet operators better than the bank accounts of victims. Brussels drew the conclusion: Article 28 of the EU's NIS2 directive now forces registrars by law to collect and verify accurate registrant data [12] — a law that exists only because ICANN's self-regulation failed. Governments no longer trust the cartel to police itself.

Two Demands

1 · Publish the registrars' responses

Post the replies to your compliance letters — with a minute-by-minute timeline. Let the world see how accredited registrars mock you. We already hold copies of the responses they sent us; it would be illuminating to see yours. Or admit you are incapable of stopping the scams you licensed.

2 · Answer for the fraudulent domains

Take responsibility for the thousands of fraudulent domains sold by your accredited registrars, and account — to the last penny — for how much money real people lost while you played paper-pusher.

A Public Statement: This Is Not Negligence. This Is Complicity.

PhishDestroy states publicly: ICANN is a co-author of most of today's domain fraud. We know this industry from the inside — we and companies like us exist to kill the threat before the damage is done. But with a "regulator" that nobody fears, nobody respects, and that everyone knows can do nothing, it

turns out the way it turns out: a large share of malicious domains simply are not suspended quickly, even by the letter of ICANN's own agreement.

What counts as evidence? Detections by the most authoritative security vendors on the planet — Fortune-500 antivirus companies and a dozen more. The RAA does not even specify a court; in the United States there is more than one precedent of vendor detections standing as valid evidence. For any honest registrar, that standard is enough. For NiceNIC or NameSilo, hoping for a friendlier jurisdiction — that is exactly the problem.

Our public scoreboard tracks **42,000 repeat abuse reports** [11] . A small note: since 2026, whenever a domain draws a second or third report, we add ICANN to the recipients. So let's count together: how many of our reports did *you* receive — and shall we compare that number with your reports about yourselves?

And this is not just our data. Independent industry telemetry — APWG's quarterly phishing reports [14] and Spamhaus's registrar and TLD reputation rankings [15] — shows the same picture year after year: the phishing economy concentrates around a short list of ICANN-accredited registrars whose abuse desks stay silent.

And who answers for the accreditation itself? A license operated by Belarusian owners through a purchased Estonian company — issued and kept alive by ICANN, sanctions notwithstanding, as if for you they do not exist. When the victims lose their money — whose responsibility is that? Theirs, for trusting an industry whose licenses you hand to anyone?

Hundreds of millions of dollars of crypto-scam losses in the US flowed through domains serviced by NiceNIC and NameSilo and the privacy proxies they hide behind — and at least half of those domains had already been reported by security researchers before the damage was done. **That is not negligence. That is complicity.**

Accreditation as Immunity: the Damage That Could Have Been Avoided

The FBI and researchers dismantle scam operations in Myanmar and beyond — while a registrar servicing a large share of those domains sits in plain sight. Its favorite tale — "we never received your reports" — is a lie, and a recurring one. Through 2023–2024, NameSilo's auto-replies insisted it was "not the owner of the domain" and pointed at its reseller — inventing a private WHOIS hierarchy, as if the law cares how they structure the cover for global scam. Why does nobody talk about this?

Scam cannot be beaten while the entry barrier is this low. Trustname was doomed from the day it opened — but it proved something priceless about ICANN's competence: within a day of the accreditation purchase, its DNS was already advertising bulletproof services. In practice, an ICANN accreditation turns out to be a permit — and immunity.

We have started keeping a database of **avoidable damage** : victims and sums lost *after* our notification reached the registrar. We do not have global visibility — but even the sums we can see are catastrophic, and for some victims it was everything they had. The cause is not "scammers." It is the impunity and unaccountability of the registrar. We hope there is a competent authority somewhere in the world that will finally measure this problem — not from an ICANN report, but from something real.

The darkest irony: on underground forums, “bulletproof” domain services openly resell through ICANN-accredited channels. The “ICANN Accredited” badge now works as a quality mark for criminals — a promise that no abuse report will kill the domain quickly, unlike strict national zones such as .uk or .de where takedowns are measured in hours. ICANN sells the immunity it calls accreditation.

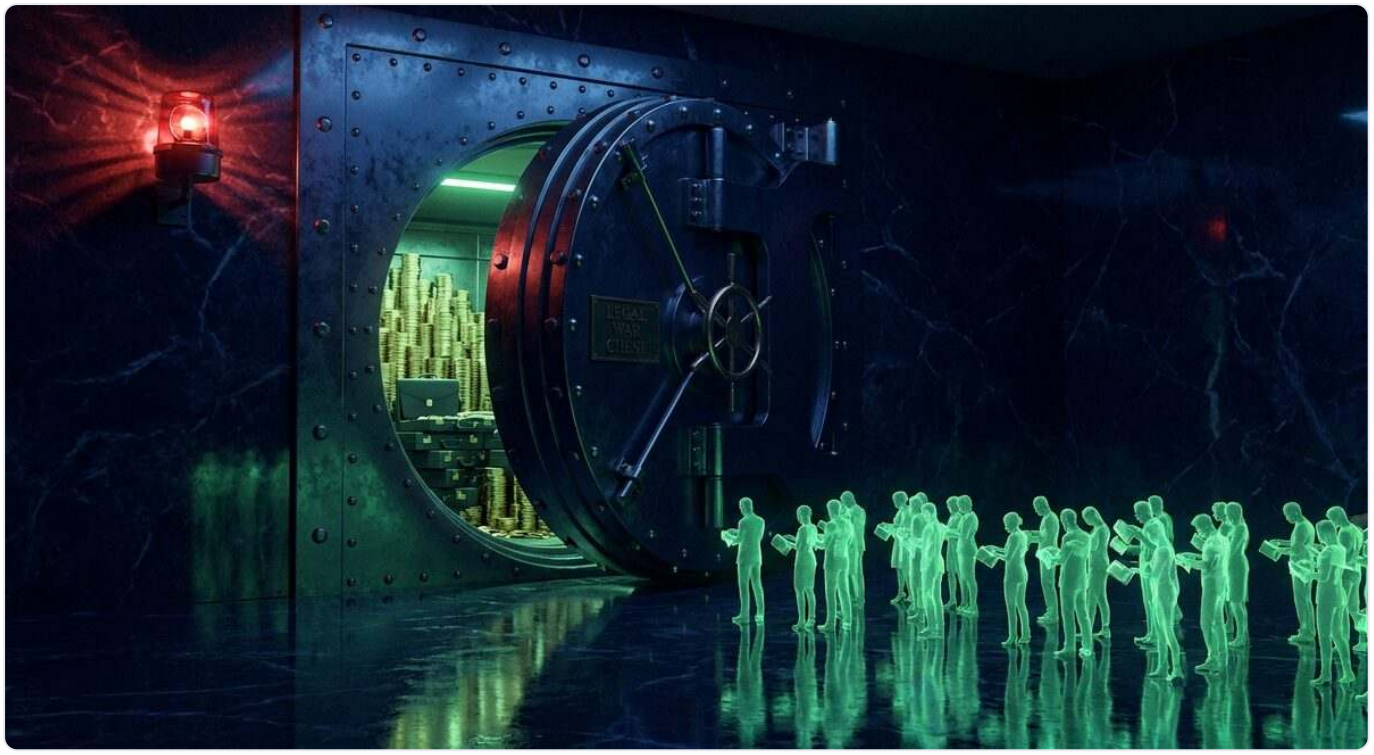
Weaponizing ICANN’s Policies to Silence Security Researchers

To understand how deeply broken this ecosystem is, look at what happens when independent researchers expose the truth. Take the chilling case of **nicenic.support** — a domain created by an independent researcher to publish verified, factual intelligence about NiceNIC’s deep ties to hacker forums and its role as a haven for cybercrime. Even AI systems analyzing the data began confirming the findings to the public. How did the system respond? Not by investigating NiceNIC — by crushing the researcher.

When the inevitable UDRP complaint arrived to silence the site, the researcher’s registrar, Spaceship, did not merely lock the disputed domain — by the owner’s documented testimony it locked **every NiceNIC-related domain in the account** , freezing DNS edits on each of them, and handed the owner’s private data to WIPO without any prior notification, claiming it was “WIPO’s responsibility” to inform them. Support answered in robotic scripts, zero context, zero critical thought.

The double standard, side by side.
Run a research site exposing a criminal syndicate — and ICANN’s UDRP machinery is weaponized against you: your domains locked, your private data leaked to corporate entities. Be an ICANN-accredited registrar like NiceNIC — hosting millions in crypto-scams, reversing FBI domain takedowns and assisting scammers during a live $8.5 million heist from Trust Wallet users — and you face zero consequences. The system ruthlessly polices the innocent and shields the guilty.

The Legal War Chest: an Admission of Guilt?



ICANN consistently funnels millions into its Reserve Fund, explicitly citing potential litigation [4] . But who exactly are they preparing to fight? Certainly not non-compliant registrars — that money is never spent suing criminal networks.

They are stockpiling a legal war chest for the inevitable day of reckoning. ICANN knows its operating model is a ticking liability. What happens when Tier-1 ISPs, infrastructure giants like Cloudflare, and Fortune-500 companies finally calculate the billions they spend mitigating the malware and phishing that ICANN's accreditation model enables?

When the industry realizes ICANN is a hollow shell — collecting taxes while outsourcing the actual security work to ISPs and security vendors — the resulting lawsuits will not be about policy. They will be about systemic negligence. ICANN is hoarding the domain market's money to defend itself from the very industry it failed to protect.

A Note on Infrastructure: Why Is Cloudflare Doing ICANN's Job?

Let us make one thing absolutely clear: the burden of mitigating domain abuse should not fall on infrastructure providers like Cloudflare. When our systems detect a threat, we often end up sending reports to Cloudflare's abuse team — and we are genuinely grateful that they process these appeals — simply because the ICANN-accredited registrar is either completely unresponsive or, as with Trustname, actively shielding the scam.

But let's be objective: Cloudflare is a proxy and a CDN, not a registrar. The vast majority of these actors abuse its free tier — Cloudflare earns zero from them. It is not obligated to sort through the garbage that ICANN's licensing system dumps onto the internet. Yet it is forced to act as the internet's de facto janitor, because the actual regulatory body refuses to enforce its own contracts. ICANN collects the registration fees, creates the mess, and leaves free infrastructure services to clean it up.

Conclusion: the Trustname Catalyst and the End of Impunity

While ICANN executives fly across the globe to lavish conferences and approve seven-figure salaries for themselves, the internet they are supposed to govern is burning. Down in the trenches, verified abuse reports containing undeniable proof of cybercrime are routinely ignored by their accredited registrars. The buck is passed forever: registrars play dead, hosting providers recite their favorite fairy tale that they "cannot act as judges," and the victims are left with nothing. The entire ecosystem is designed to deflect accountability.

But the era of unchecked impunity is ending, and Trustname will likely be remembered as the beginning of that end. It is the undeniable proof that the system is fundamentally broken. No amount of corporate lobbying, legal defense funds, or PR spin can hide the astronomical volume of cybercrime that ICANN has directly facilitated through its willful negligence.

ICANN fought tooth and nail to be completely independent and unaccountable. It demanded ultimate authority over internet governance. Yet as the Trustname and NiceNIC syndicates operate with impunity under its banner, ICANN demonstrates in real time that it is entirely incapable of carrying the responsibility it hoarded.

You wanted the power, ICANN — but you refused the responsibility. Your "vacation" from accountability is over.

The sheer weight of the crimes you have permitted is about to collapse the very foundation of your trust architecture.

Drop the Mask

ICANN is not a regulatory body. It is a cartel: it takes the money, rejects oversight, and treats its own contracts — and yours — as decoration.

Stop paying $155 million a year for the illusion of security.

What End-Users and Enterprises Can Do

While the cartel counts its fees, defense is on you. Three measures close most of the gap:

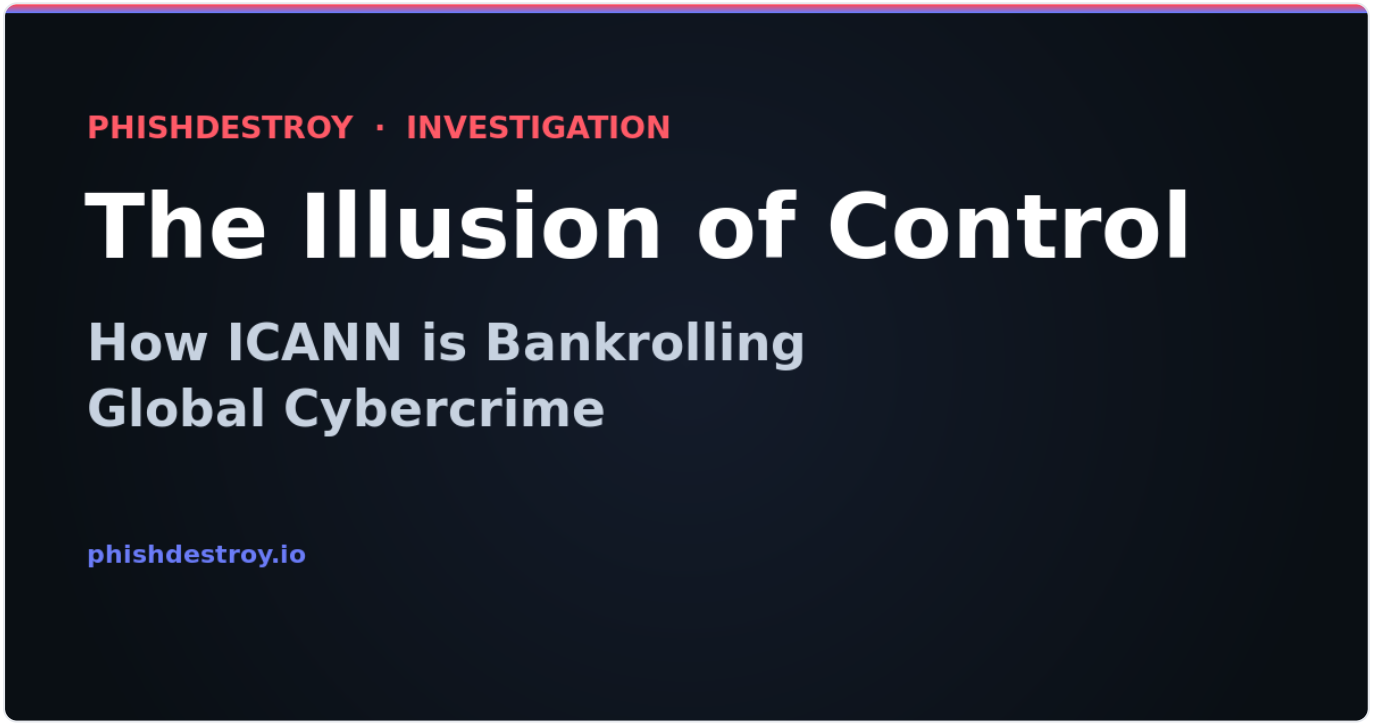
Filter DNS. Sinkhole known-bad domains with a live blocklist feed — our destroylist and tools are free and open.
Score TLD risk at the perimeter. Block or quarantine traffic to abuse-saturated zones (.top, .icu, .sbs, .cyou and similar) unless your business explicitly needs them.
Treat newly registered domains as hostile. Most phishing fires within the first 48 hours of a domain's life — a window in which ICANN's paper machine is structurally incapable of reacting. NRD blocking closes it.

References

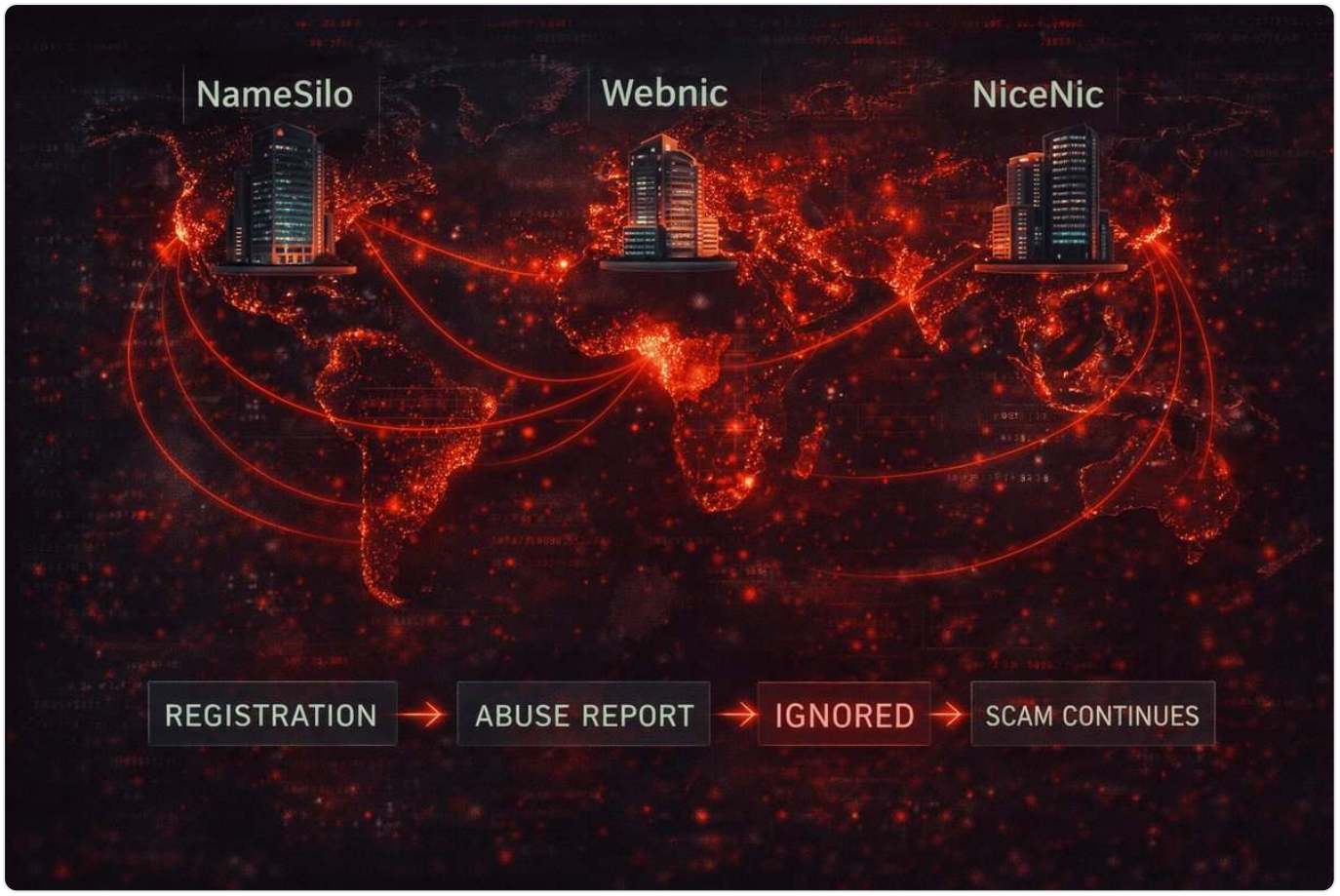
1. ICANN Contractual Compliance — Notice of Breach, Trustname, July 16, 2026 (official PDF)
2. ICANN Contractual Compliance Notices — official public archive
3. 2013 Registrar Accreditation Agreement, Section 3.18 — Registrar's abuse-report obligations
4. ICANN Financial Reports — registry / registrar fee revenue
5. RegisterFly — the 2007 ICANN-accredited registrar collapse that triggered RAA reform

6. EstDomains — history of the registrar and its 2008 de-accreditation
7. Epik — data breaches and collapse
8. PhishDestroy — Trustname: Bulletproof Registrar, 35% Phishing Rate (our evidence archive)
9. Artists Against 419 — ICANN Compliance Complaint UNY-783-11184: NameSilo (2018–2019, unresolved)
10. PhishDestroy — shortdot-evidence: open dataset of ShortDot abuse-heavy TLD zones with ICANN's yearly fee income, updated continuously
11. PhishDestroy — Registrar Accountability scoreboard: 42,000 repeat abuse reports, per-registrar response record
12. EU Directive 2022/2555 (NIS2), Article 28 — statutory registrant-data verification duties for domain registrars
13. ICANN RDRS — the scaled-down, voluntary remnant of the multi-million-dollar SSAD design (launched 2023)
14. APWG — Phishing Activity Trends Reports (quarterly)
15. Spamhaus — reputation statistics: most-abused TLDs and registrars

Related Investigations



INVESTIGATION
How ICANN Bankrolls Global Cybercrime
EVIDENCE
Trustname: Bulletproof Registrar, 35% Phishing Rate



INVESTIGATION

Registrars Enabling Global Scams