

Anti-Abuse Report

Q2 2026



We make the integrity of our top-level domains (TLDs) a primary focus. We publish these quarterly Anti-Abuse Reports because we believe transparency helps inform our stakeholders on the performance of our TLDs and related abuse mitigation efforts, but also because that transparency furthers the integrity of what we do. This quarter's report focuses on TLD security.

Domain Abuse Remains Rare in Identity Digital TLDs

DNS Abuse is an important issue that we take very seriously. Due to the wide spectrum of harms it can cause, DNS Abuse as a topic draws significant attention. And this attention in public discourse often encourages exaggeration, lacks statistical discipline, and often relies on unsupported, biased, or duplicated third-party reports. This is why we require documentation on our abuse forms, such as screenshots, which provides us the evidence we need to act swiftly while maintaining the integrity of our secure and stable TLDs. As just one statistic, throughout 2025 we identified just 0.15% of domains across our TLDs as abusive, which aligns with our historical trends.

Monitoring Abuse Patterns

We monitor several patterns across our TLDs to keep DNS Abuse in check. This pattern recognition enables us to spot these registrations early, investigate, and act before the DNS Abuse spreads. While no registry can completely eliminate DNS Abuse, we believe early detection, strong partnerships with our registrar partners, and intervention are key to maintaining the integrity of a TLD and a healthy namespace.

Among other metrics, we review domain renewal activity on a TLD-by-TLD basis. Understanding whether registrants renew domains helps us distinguish between normal lifecycle trends and potentially suspicious behavior. Some view low renewal rates in a TLD as a de facto sign of DNS Abuse. Based on the data we have compiled over multiple decades, we believe that conclusion lacks nuance and connection is not conclusive. Renewal rates naturally vary across our TLDs because the underlying users and uses are varied; some organizations have longer online needs while others are more temporary, and a lower renewal rate alone does not indicate higher levels of DNS Abuse.

Promotions Help Registrants Try New TLDs

We run promotions to encourage registrants to explore new TLDs and establish and grow their online identities. Promotions often bring a wave of new registrations, and that growth often includes users looking to exploit a domain and the users who access it. We maintain a vigilant stance, responding with precision to discourage malicious behavior and preserve the reliability of our network.

Furthermore, if specific registrar partners consistently demonstrate high spikes in DNS Abuse during promotional windows, we reserve the right to suspend or disable their eligibility for future promotional pricing. This targeted enforcement ensures that our promotional incentives support genuine growth without compromising our security standard. Mitigating DNS Abuse requires a great deal of time and other resources, and doing a close review of our registrar partners' domain abuse history helps limit those costs while maintaining the trust and integrity of the underlying TLD.

Lower Abuse Rates Take Steady Work

Our 2025 abuse rate of 0.15% reflects consistent investment in monitoring and enforcement across every TLD we operate. We hold ourselves to a high standard and keep looking for better ways to stop abusive registrations. Anyone who finds DNS Abuse in one of our TLDs can [report it here](#).

Thought Leadership 1

Abuse Reporting
Statistics 2

Action Timeline 3

Our Expertise 4

Trusted Notifiers 5

LEA Requests
and Court Orders 6

!

Abuse Reporting Statistics

The table below includes information about the number of reports Identity Digital has received in the last quarter about domain names in our TLDs. We may receive multiple reports about the same domain name, and multiple reports are often consolidated into one case.

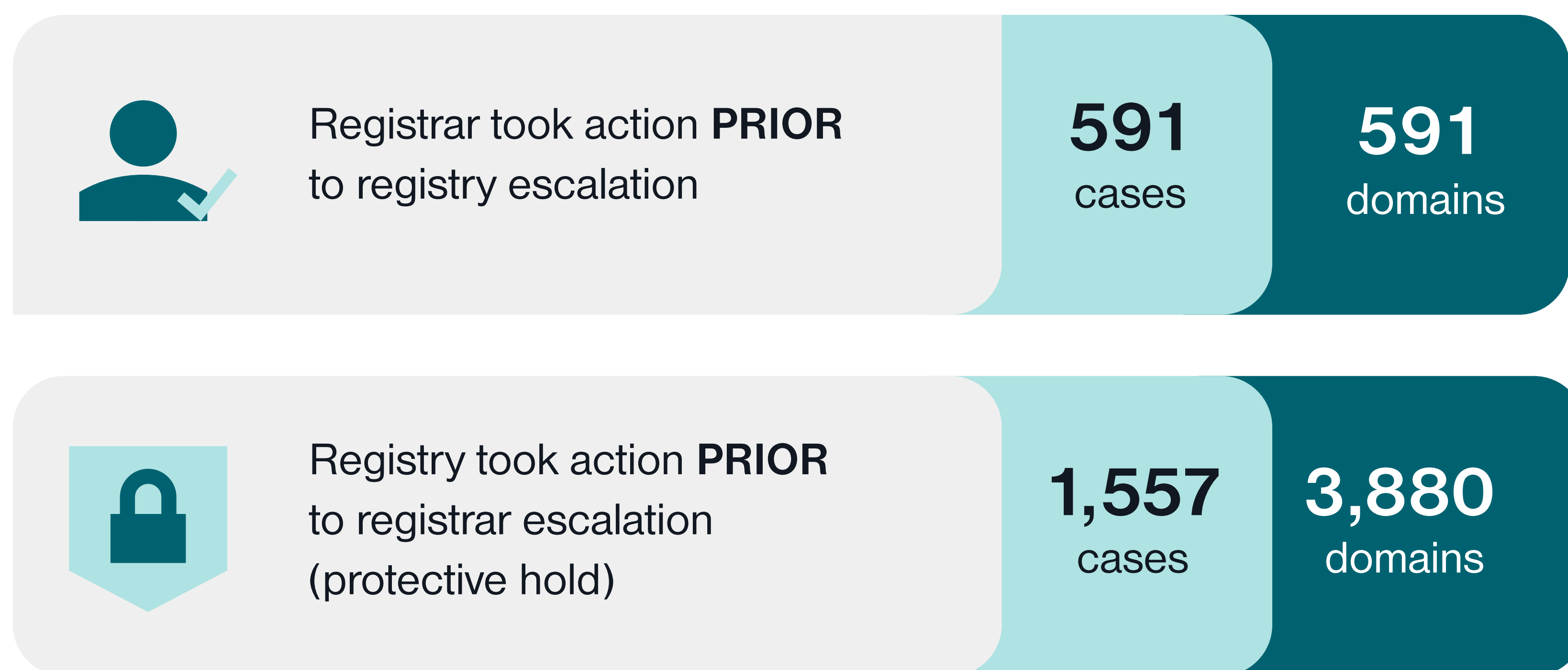
87,165

Total Domains Reported

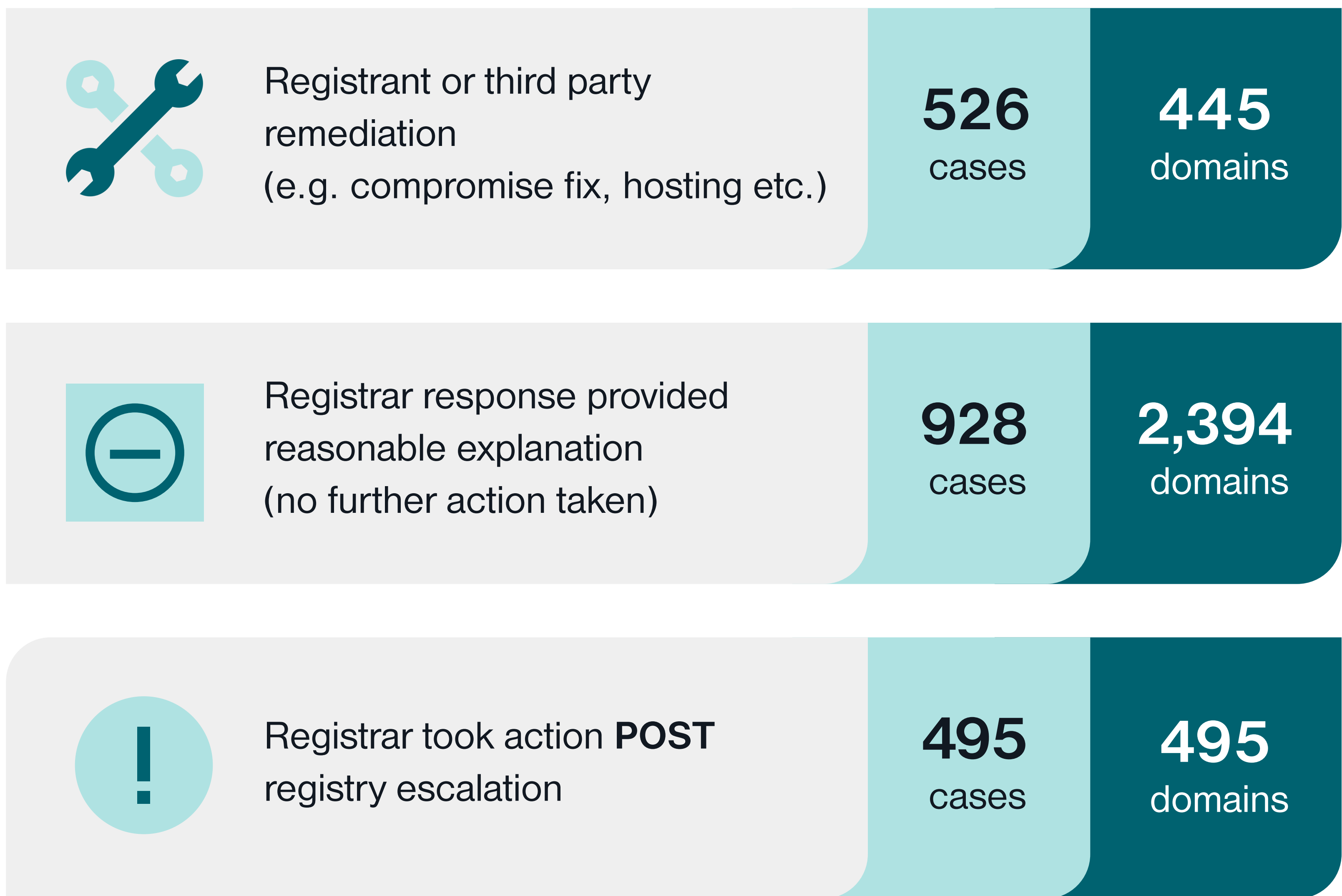
Type of Abuse	Detection Method	Number of Reports	Number of Domains Reported	Number of Domains on serverHold	% of Total Domains Reported	Number of Reports by Abuse Type
Phishing	Abuse List	39,531	23,427	5,747	26.88%	78,779
	Report API Submissions	30,388				
	Manual Submissions	2,372				
	Third Party Reports (email or abuse form)	6,488				
Malware	Abuse List	3,599	1,546	334	1.77%	5,257
	Report API Submissions	855				
	Third Party Reports (email or abuse form)	803				
Pharming	Any	0	0	0	0%	0
Botnets	Any	73	43	10	0.05%	73
Spam (as a delivery mechanism)	Report API Submissions	250	277	7	0.32%	383
	Third Party Reports (email or form)	133				
Denial-of-Service Attacks	Any	13	13	6	0.01%	13
Child Sexual Abuse Material	IWF	704	32	7	0.04%	704
	Third Party Reports (email or form)	0				
Promotion, encouragement, sale, or distribution of prescription medication without a valid prescription in violation of applicable law	Third Party Reports (email or form)	547	188	121	0.22%	547
Illegal access of computers or networks	Any	0	0	0	0%	0
Cyber-bullying, harassment, or other forms of abuse to individuals or groups	Any	1	1	0	0%	1
Incitement to violence or other unlawful actions	Third Party Reports (email or form)	91	56	13	0.06%	91
Failure by registrant of a two-character SLD to take steps to ensure against misrepresenting or falsely implying that it is affiliated with the corresponding government or country-code manager, if such affiliation, sponsorship or endorsement does not exist	Any	0	0	0	0%	0
Holding oneself out as a licensed medical practitioner in a .doctor domain name when such license doesn't exist	Any	0	0	0	0%	0
Other	Report API Submissions	3,408	62,882	139	72.14%	65,485
	Manual Submissions	60,127				
	Third Party Reports (email or abuse form)	460				
	Abuse List	1,490				

Action Timeline

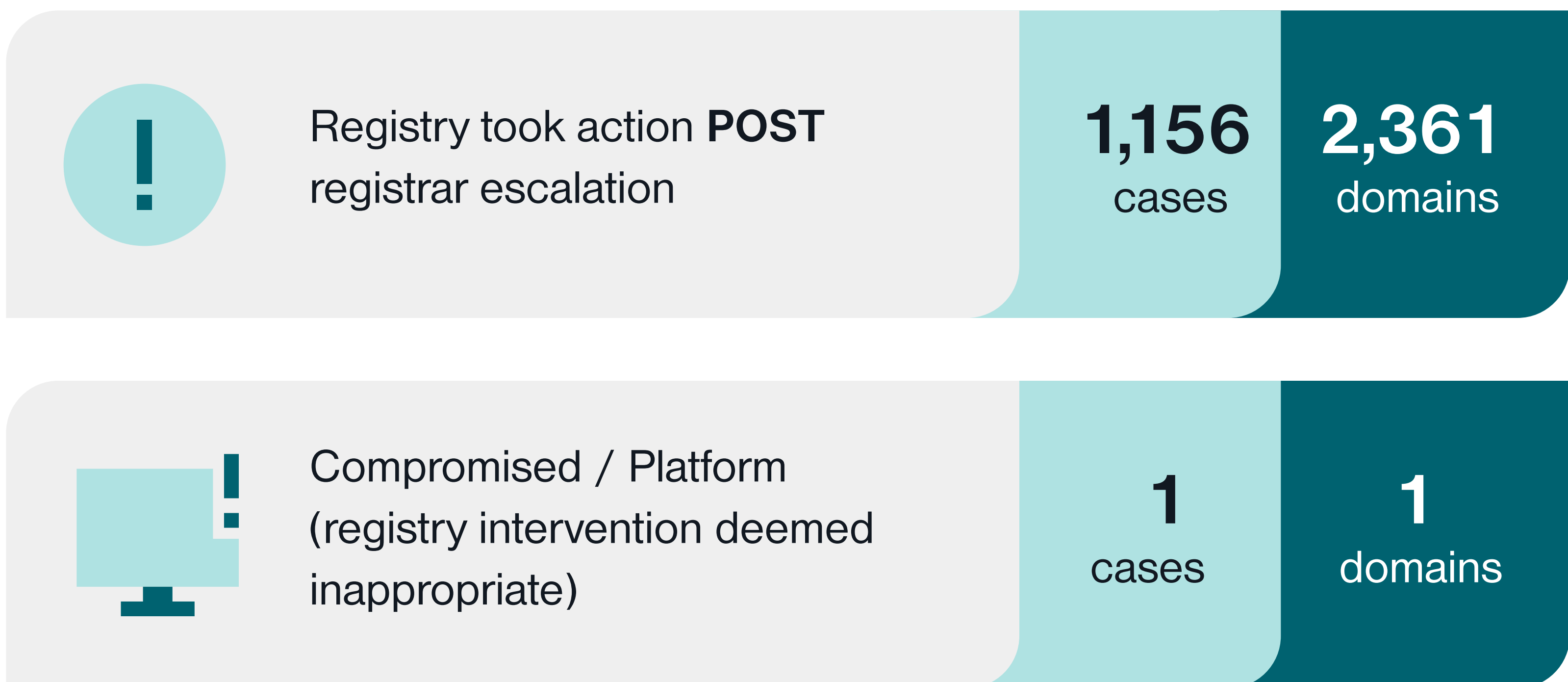
0hrs



24hrs



72hrs



5,912

Cases closed*

10,872

Unique domains affected (closed)**

3,880

Domains placed on protective holds (within 24 hrs of report)

0.07%

Percent of all ID domains

15.5M

Number of all ID domains in current Q

6,145

Total number of domains reported on serverHold status

* Statistics for “cases opened” vs. “cases closed” can ordinarily differ in the same measurement period

** Cases often contain multiple domains in a single escalation

Our Expertise

Detection methods, training given to staff, use of automated decision making when creating abuse cases and suspending domains

Identity Digital Abuse Team members complete continuing professional education (CPE) at least once per month, focused on topics related to anti-abuse and cybersecurity. Monthly performance audits, conducted by subject matter experts, evaluate the quality of escalations and takedowns. These audits aim to identify areas for improvement and determine additional CPE opportunities to enhance staff performance. Additionally, all staff participate in annual or quarterly security training.

We continuously evaluate abuse submissions and automatically create a case if the available evidence meets threshold standards. A team of analysts then reviews these cases and manually escalates the reports for investigation.





Trusted Notifiers

Identity Digital considers reports made to it via a number of avenues; however, there is a small category of reporters we consider “Trusted Notifiers.”

In addition to the other sources of reports described in this report, Identity Digital works with a small category of reporters we consider “Trusted Notifiers.” Identity Digital maintains formal, contractual relationships with our Trusted Notifiers.

Although each Trusted Notifier relationship is subjective and unique, the formal arrangements establish accepted standards of due process, including evidential expectations, due diligence, and ensuring reports are made to the appropriate and proximate service providers, prior to the registry being asked to intervene.

For more information on Trusted Notifiers in general please see the Contracted Party House Trusted Notifier Framework.

If you would like to discuss a potential trusted notifier relationship with Identity Digital, please contact us at compliance@identity.digital.

Identity Digital currently maintains formal trusted notifier relationships with:

Internet Watch Foundation (IWF)

The IWF securely provides us with reports of URLs using Identity Digital domains, which have been verified and confirmed as being used to access Child Sexual Abuse Material.

Motion Picture Association (MPA)

Recording Industry Association of America (RIAA)

Identity Digital receives reports of domains associated with pervasive and patently apparent copyright infringement. All reports must come with clear evidence of this pervasive infringement, and all reports must have already been made to the more proximate and appropriate service providers, such that any consideration of the registry is appropriate at that time.

In this quarter, we actioned the following reports:

		IWF	MPA	RIAA
Unique Domains Affected		32	0	0
Domains Suspended	Registrar	10	0	0
	Registry	7	0	0
Remediated (confirmed by IWF or registrar)		15	0	0
Closed / Remediated Other		0	0	0



LEA Requests and Court Orders

Orders from Competent Jurisdictions**

This table details the requests received by Identity Digital from courts or other government agencies of competent jurisdictions. These requests usually ask Identity Digital to take specific actions, such as redirecting nameservers, transferring domains to different registrars, or suspending the subject domain names.

Report Category (abuse or illegal activity)	Country	Number of Requests	Number of Affected Domains	Number of Domains Suspended	Number of Domains Transferred
Court Order	USA	2	4	4	3
Court Order	Germany	1	1	1	1

LEA Requests*

In addition to working with our Trusted Notifiers to combat abuse in our TLDs, Identity Digital collaborates directly with law enforcement authorities to help mitigate or eliminate online harms. These requests address reports of ongoing violations of registration terms such as our Acceptable Use Policy.

4

of requests received

4

of requests actioned

0

of requests declined

36

of affected domains

*This is taking down/transferring domains due to court orders

**This is requests to help mitigate DNS Abuse



.zone .travel .ride .plus .guru .cool .life .world .social

