Anti-Abuse Report Q3 2026



Strong Domain Names Are Becoming a Bigger Part of How People Build Trust Online

Domains and the DNS give the internet its foundation for identity and trust. As AI and AI-driven search agents change how people search for and evaluate businesses online, domain names are taking on increased importance. A recent survey of 1,120 professionals found that 77% of respondents expect the importance of a strong domain name to matter more because of AI.[1] Forty percent are registering keyword-rich domains to improve visibility in answers that large language models generate. Appearing in those answers can be an early trust signal.

The same trust that makes a strong domain valuable also makes a lookalike domain convincing. AI has made it easier to write a persuasive message and build a website that closely mirrors a trusted brand. Helping people recognize a genuine web address on their own protects the trust that strong domains earn.

To protect against these threats, users can follow several practical steps when navigating new websites:

- Pause before clicking a link and find the actual registered domain.
- Remember that a familiar brand name placed earlier in the address, such as in a subdomain, does not confirm where the link leads.
- When a message asks for money or personal information, type the address from memory or use a saved bookmark.

A check like this takes only seconds and works well alongside the safeguards that registries, registrars, technology platforms, and security providers built into the domain system to catch lookalike domains early. Everyday habits combined with a more secure domain system build a foundation of trust for everyone online.

We Act Quickly on Abuse in Our TLDs

The same habits work best alongside the monitoring we do every day. No registry can operate with zero abusive registrations, so we aim to keep abuse as low as possible.

We track abuse patterns within and across Identity Digital TLDs and investigate each one as it emerges. Catching abuse early keeps more than half of those cases from needing further review. Here is how that work performed: This quarter, we closed 20,948 abuse cases, taking action on 19,250 unique domains. We placed 8,922 domains on temporary hold this quarter and completed 6,230 of those holds, about 70%, within 24 hours of receiving the report.

Every Domain Receives the Same Level of Monitoring

Promotional periods bring a wave of new registrations and give more people the chance to build something new. We apply the same monitoring standards to every domain, regardless of when registration happens. We design our promotions to entice registrants to try new TLDs and grow their businesses, and the monitoring behind each registration stays the same.

We Believe in Constant Process Improvement

Our Abuse Team completes continuing professional education monthly and additional security training quarterly or annually, and subject matter experts audit escalation and takedown quality each month to identify ways we can improve.

Beyond our own team, we work with outside partners to strengthen this work. We responded to all four law enforcement requests we received this quarter, addressing 100 domains, and worked with the Internet Watch Foundation on 26 unique domains, remediating 21 of them. We aim to keep improving how we address abusive registrations.

Anyone who encounters an abusive website in one of our TLDs can report it through our abuse form.

Thought Leadership 1

Abuse Reporting Statistics 2

Action Timeline 3

Our Expertise 4

Trusted Notifiers 5

LEA Requests and Court Orders 6

[1]Name.com, The Empowered Builder: Digital Identity in the Age of AI, published via BusinessWire, May 27, 2026. Verified live and covered independently by SecurityBrief UK and IT Brief UK, June 1, 2026. Name.com is an affiliate of Identity Digital.

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.

67,038
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 Report API Submissions Manual Submissions Third Party Reports (email or abuse form)	44,518 78,188 785 8,091	32,994	11,462	49.22%	131,582
Malware	Abuse List Report API Submissions Third Party Reports (email or abuse form)	5,016 419 1,982	1,823	845	2.72%	7,417
Pharming	Any	0	0	0	0%	0
Botnets	Any	31	21	4	0.03%	31
Spam (as a delivery mechanism)	Report API Submissions Third Party Reports (email or form)	20 176	160	516	0.24%	196
Denial-of-Service Attacks	Any	13	5	0	0.01%	13
Child Sexual Abuse Material	IWF Third Party Reports (email or form)	11,237 2	28	1	0.04%	11,239
Promotion, encouragement, sale, or distribution of prescription medication without a valid prescription in violation of applicable law	Third Party Reports (email or form)	666	340	169	0.51%	666
Illegal access of computers or networks	Any	23	13	2	0.02%	23
Cyber-bullying, harassment, or other forms of abuse to individuals or groups	Any	2	2	0	0%	2
Incitement to violence or other unlawful actions	Third Party Reports (email or form)	114	75	10	0.11%	114
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 Manual Submissions Third Party Reports (email or abuse form) Abuse List	697 29,998 1,556 3,444	31,889	190	47.57% 100.47%	35.695

Action Timeline

0hrs

Registrar took action **PRIOR** to registry escalation	832 cases	913 domains
Registry took action **PRIOR** to registrar escalation (protective hold)	2,917 cases	6,230 domains

24hrs

Registrant or third party remediation (e.g. compromise fix, hosting etc.)	831 cases	736 domains
Registrar response provided reasonable explanation (no further action taken)	1,306 cases	2,266 domains
Registrar took action **POST** registry escalation	8,861 cases	8,197 domains

72hrs

Registry took action **POST** registrar escalation	6,198 cases	5,547 domains
Compromised / Platform (registry intervention deemed inappropriate)	0 cases	0 domains

20,948
Cases closed*

19,250
Unique domains affected (closed)**

6,230
Domains placed on protective holds (within 24 hrs of report)

0.12%
Percent of all ID domains

15.6M
Number of all ID domains in current Q

8,922
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		26	0	0
Domains Suspended	Registrar	4	0	0
	Registry	1	0	0
Remediated (confirmed by IWF or registrar)		21	0	0
Closed / Remediated Other		1	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	1	1	0	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.

5	5	0	100
# of requests received	# of requests actioned	# of requests declined	# 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





identity.digital | compliance@identity.digital

identity digital®