Anti-Abuse Report Q3 2025

Combating Fake Online Shops

We've all been there, wondering if the deal offered on new designer sunglasses can possibly be legitimate. These fake online shops often appear in prominent search engine results, creating a false impression of credibility that can mislead even experienced internet users. Understanding the nature of these online shops and implementing appropriate protective measures is essential for consumers and legitimate businesses.

What are Fake Online Shops?

Fraudulent online shops are deceptive websites designed to impersonate established brands and legitimate retailers. These operations are constructed to replicate the appearance and functionality of those brands. Their goal is to obtain the customer's sensitive personal and financial information.

How to Protect Yourself?

As fake online shops grow more prevalent, it is important to stay vigilant. When conducting online transactions, watch out for these key indicators:

- **URL Analysis:** Inspect the search bar and web address - does that look like an oddly placed hyphen, or a different TLD from the page you used previously?
- **Pricing and Discounts:** Does the deal seem too good to be true? Does this brand's product usually go on sale like this? Is the price unreasonably low compared to other sites?
- **Payment Processor:** Are you getting redirected to an unrecognized credit card processing site?

While it is important to protect yourself, brands should be proactively protecting their digital identities through comprehensive domain security and ongoing monitoring.

Our Approach

As a Registry Operator, we offer homographic blocking that identifies and blocks visually similar domains from being registered in our TLDs. Brand owners should go one step further and utilize the Domains Protected Marks List (the "DPML") and the Global Block Service, both powerful shields against brand impersonation across a myriad of TLDs.

Under ICANN policy, a "fake shop" is not a defined category of DNS Abuse. Therefore, when a fake shop is reported, it's treated through an actionable lens of phishing. Our team analyzes reports of phishing with two main questions:

1. Is the website impersonating a legitimate brand?
2. Is it actively trying to steal sensitive information through a login, fake checkout page, or other means?

We also utilize hosting patterns and other forms of data to inform our decisions of intervention. In cases where intervention is not appropriate, filing a dispute with the World Intellectual Property Organization (WIPO) is often a better alternative.

DNS monitoring and AI continuously patrol for emerging threats. Machine learning and automated detection tools analyze registrations patterns in near real time, flagging risks more effectively.

Fake online shops are increasingly prevalent and it's important to understand the threat. Both consumers and businesses should take proactive steps by registering with trusted and secure registrars, and reporting fake shops when they appear.

Thought leadership 1

Abuse Reporting Statistics 2

Action Timeline 3

Our Expertise 4

Trusted Notifiers 5

LEA Requests and Court Orders 6

Data Disclosure Requests 7

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.

106,620
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)	34,806 46,588 115 24,671	35,460	26,854	33.26%	106,180
Malware	Abuse List Report API Submissions Third Party Reports (email or abuse form)	859 1,973 39	1,482	215	1.39%	2,871
Pharming	Any	0	0	0	0%	0
Botnets	Any	1,086	743	25	0.70%	1,086
Spam (as a delivery mechanism)	Spam Traps Third Party Reports (email or form)	0 38	32	12	0.03%	38
Denial-of-service attacks	Any	0	0	0	0%	0
Child Sexual Abuse Material	IWF Third Party Reports (email or form)	457 1	72	45	0.07%	458
Promotion, encouragement, sale, or distribution of prescription medication without a valid prescription in violation of applicable law	Third Party Reports (email or form)	424	129	48	0.12%	424
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	0	0	0	0%	0
Incitement to violence or other unlawful actions	Third Party Reports (email or form)	3	3	0	0%	3
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	906 95,708 382 141	78,125	779	73.27%	97,137

Action Timeline

0hrs

Registrar took action **PRIOR** to registry escalation	383 cases	451 Domains
Registry took action **PRIOR** to registrar escalation (protective hold)	1,933 cases	17,905 Domains

24hrs

Registrant or third party remediation (e.g. compromise fix, hosting etc.)	493 cases	290 Domains
Registrar response provided reasonable explanation (no further action taken)	720 cases	1,377 Domains
Registrar took action **POST** registry escalation	1,179 cases	1,725 Domains

72hrs

Registry took action **POST** registrar escalation	813 cases	9,065 Domains
Compromised / Platform (registry intervention deemed inappropriate)	190 cases	88 Domains

5,752
Cases closed*

30,204
Unique domains affected (closed)**

17,905
Domains placed on protective holds (within 24 hrs of report)

0.22%
Percent of all ID domains

14M
Number of all ID domains in current Q

26,415
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		70	0	0
Domains suspended	Registrar	7	0	0
	Registry	39	0	0
Remediated (confirmed by IWF or registrar)		20	0	0
Closed / remediated other		11	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
Seizure Warrants	USA	2	5	5	0
Court Order	USA	5	13	0	13
Digital Service Act	Italy	1	1	1	0

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.

1	1	0	1
# 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

Data Disclosure Requests

We favor a system that supports freedom of expression, predictability, and safety for the data of all our registrars and their registrant customers, regardless of physical location.

We review each data disclosure request received and only disclose the requested information where such disclosures are justified, necessary, proportional, and in line with our legal obligations. The following table displays the number of disclosure requests received by the registry, as well as the closure reason for requests received during this quarter.

Of note we continue to receive a number of disclosure requests each quarter that are either spam or simply relate to TLDs not administered by our registry.

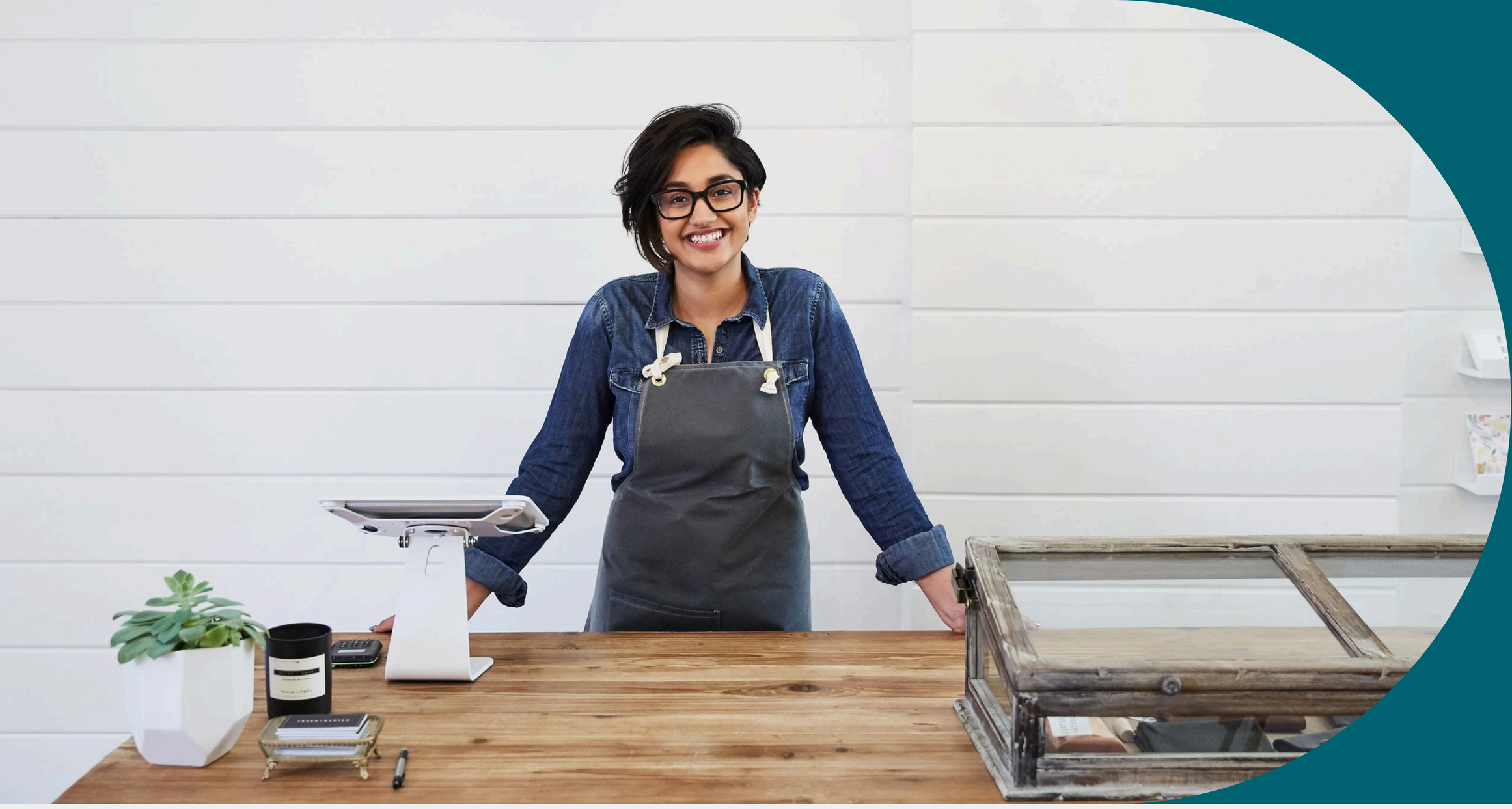
Overview

11	9	1	0
Affected Domains	No Data Processed*	Decision to Disclose	Final Decisions to Not Disclose

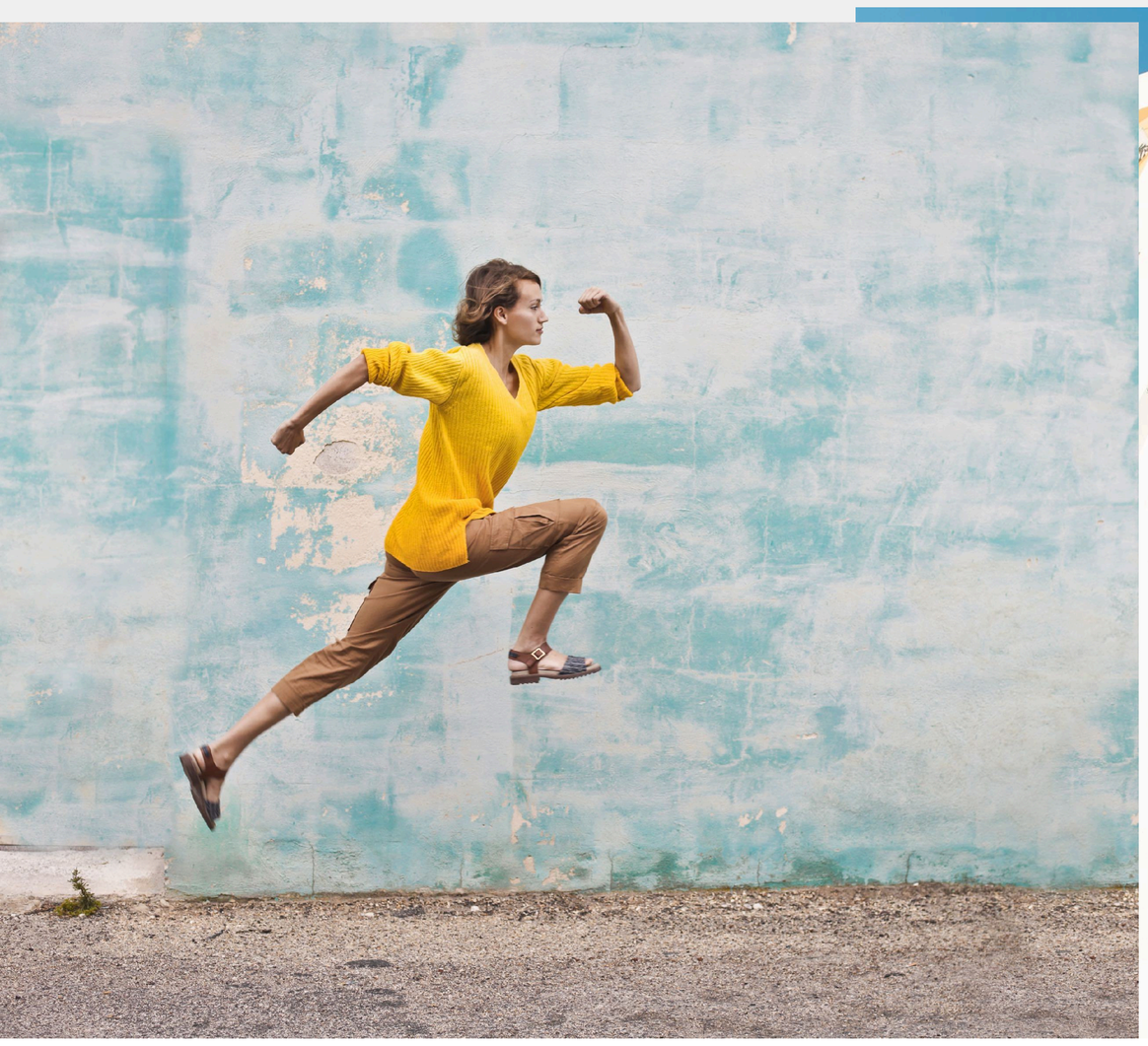
Category of Data Disclosure Requests Received	
Intellectual Property Related	5
Law Enforcement Request	4
Domain Purchase – domain does not exist	1
Not a valid disclosure request (No actual valid request made / unconnected to domains / spam)	0
Incomplete / Incorrect (Incomplete form, missing information, wrong registry etc.)	0

* Underlying registrant data not reviewed as request was not complete / no valid legal basis established

In accordance with ICANN'S Registration Data Policy, Identity Digital no longer retains contact details for domains registered within our gTLDs. We will no longer report on data disclosure requests since there is no data to process. Registrars may be able to provide more information about contact details. You can find the registrar of record for gTLDs by going to lookup.icann.org.



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



identity.digital | compliance@identity.digital

identity digital®