identity digital™

Anti-Abuse Report 2022 Q2

Identity Digital takes a multi-faceted approach to address DNS Abuse (defined below), which includes strong policies and procedures, reviews of each report we receive, sophisticated and state-of-the-art software, a network of Trusted Notifiers (more on this below), and an experienced group of compliance staff.

Each report of DNS Abuse we receive is independently reviewed on a case-by-case basis. To be actionable, DNS Abuse reports should at a minimum include the following factors:

- Well-evidenced abusive activity.
- The action requested (e.g., suspension, redirect, transfer etc.) is proportional to the harm.
- The appropriate party is being asked to mitigate and disrupt, depending on the circumstances.

In Focus > For more information on why we are publishing an Anti-Abuse Report, make sure to take a look at our recent blog post: Introducing the Identity Digital, Anti-Abuse Report

Cases vs. Reports

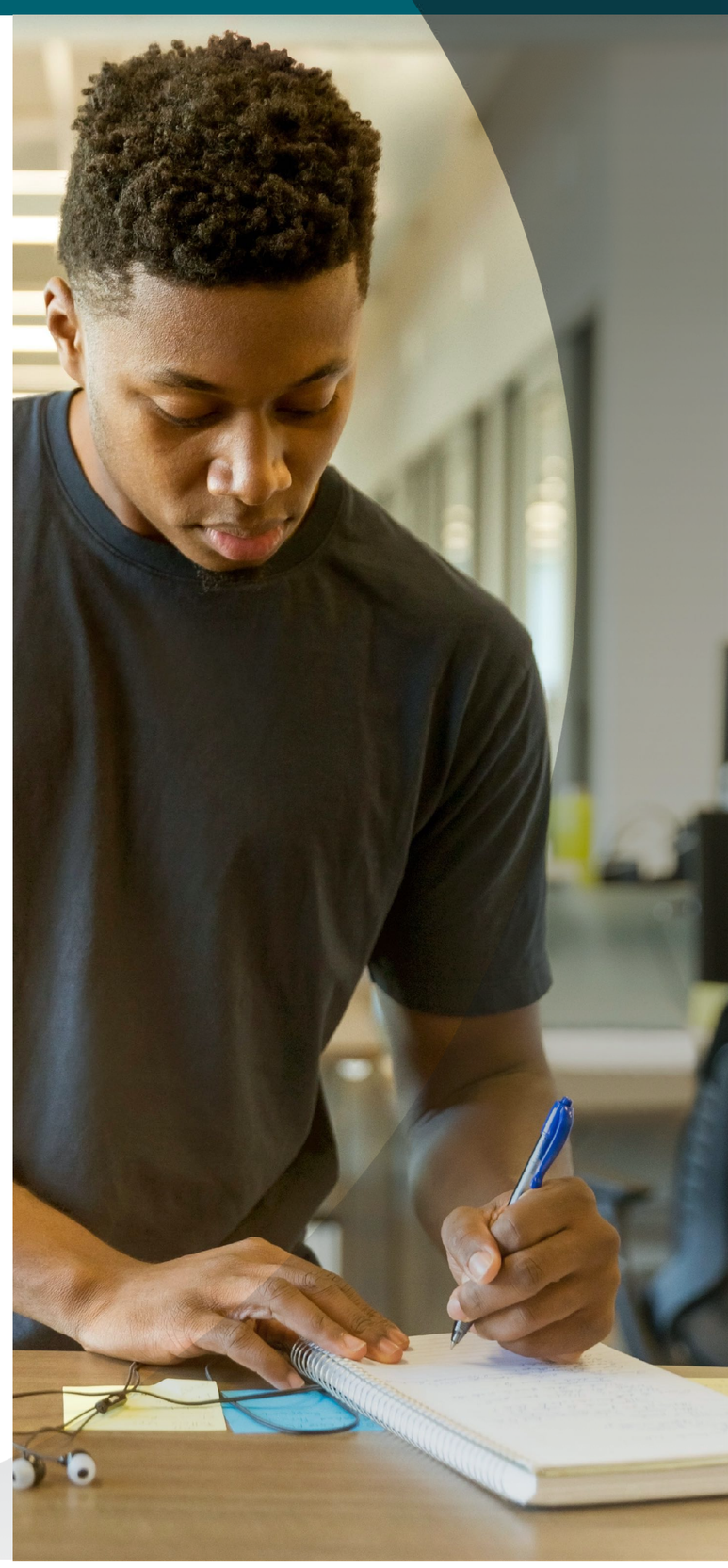
Well-Evidenced Escalations

Given the consequences of the actions we can take on DNS Abuse, for a report of DNS Abuse to escalate to an active "case," the report must be accompanied by evidence of the abuse.

Although what constitutes acceptable evidence remains dependent on the individual circumstances, generally speaking we seek real and contemporaneous evidence of the reported abuse such as screenshots, sample emails, and infrastructure indicators.

Conversely, reports or allegations of abuse alone (e.g., uncorroborated blacklistings) will rarely be considered sufficient to merit any action, whether working with our registrar partners or independently.

Below we present a summary of the abuse report for the second quarter of 2022, broken down by type and action taken.



Abuse Cases Q2

Abuse by type	Cases	% of total cases
Phishing	2794	92.9
Spam (as a delivery mechanism)	124	4.1
Malware	49	1.6
Pharming	11	0.4
Botnet	4	0.1
Other	25	0.9

3007
Cases

3816
Unique domains affected

0.024%
of all Identity Digital domains

Website Content Abuse Q2

Although our primary focus remains on DNS Abuse, we also believe there are other forms of abuse that, although falling outside the definition of “DNS Abuse,” are so egregious that when provided with specific and credible notice, the registry should act. This should not be confused with actions taken under court order or official authority of Law Enforcement, which is covered later in this report.

These forms of abuse include:
(1) child sexual abuse materials (“CSAM”);
(2) online illegal distribution of opioids;
(3) human trafficking; and
(4) specific and credible incitements to violence.

In **Q2 2022**, Identity Digital intervened in **one (1)** case specifically relating to website content abuse.

In this instance, the abuse was reported related to a targeted and credible threat of incitement to violence.

Although escalations were made to both registrar and registrant, the registry received no response and as such we suspended the domain. We have not received any query or follow up on the matter since suspension.

Key Definitions

DNS Abuse is composed of five categories of harmful activity insofar as they intersect with the DNS: *malware, botnets, phishing, pharming*, and *spam* (when it serves as a delivery mechanism for the other forms of DNS Abuse).

Phishing occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g., account numbers, login IDs, passwords), whether through sending fraudulent or “look-alike" emails, or luring end users to copycat websites.

Malware: Malicious software, installed on a device without the user’s consent, which disrupts the device’s operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.

Botnets: Collections of Internet-connected computers that have been infected with malware and commanded to perform activities under the control of a remote administrator.

Child Sexual Abuse Material (CSAM):
For this definition and further information regarding the work of the Internet Watch Foundation (IWF), please see https://www.iwf.org.uk/about-us/

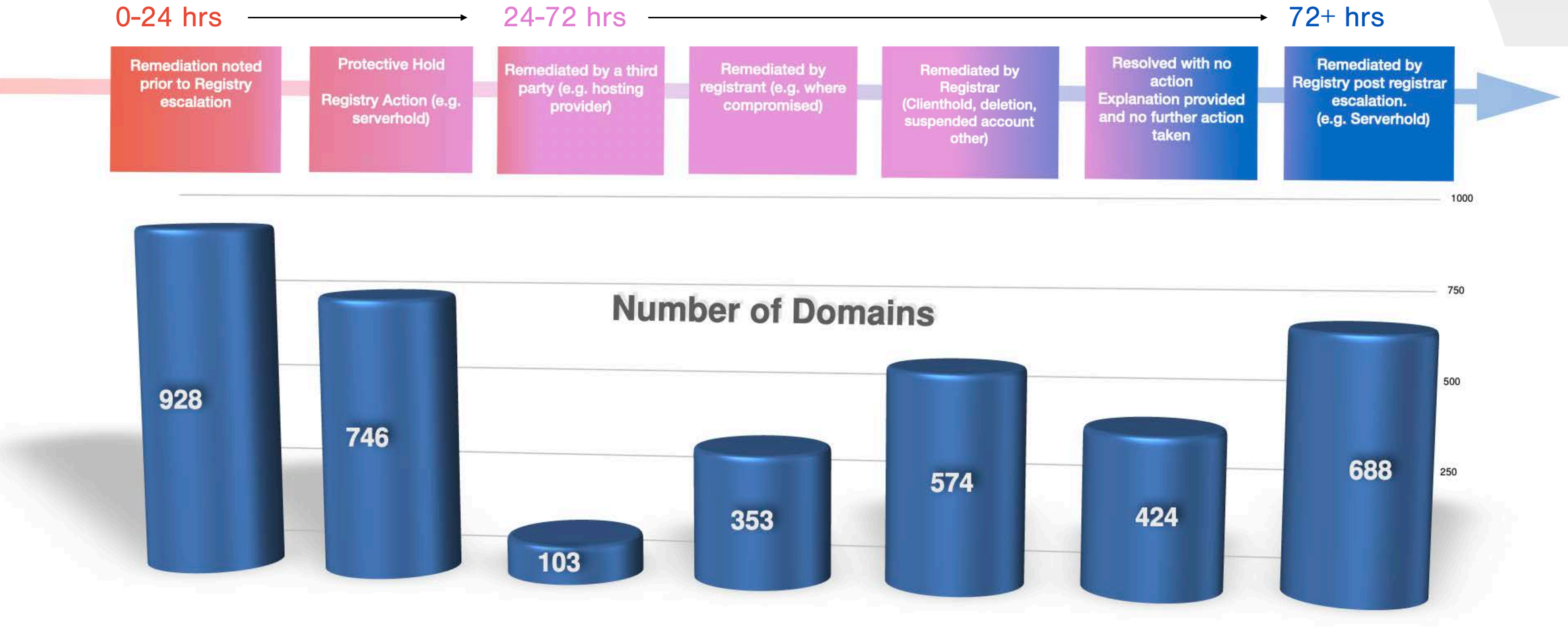
Pharming: the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning.

Protective Holds: Where evidence gathered relating to an allegation of DNS Abuse objectively demonstrates a high likelihood of potential harm to an end user, and that harm outweighs the potential impact to the registrant, then Identity Digital will take immediate suspension action to prevent, as best as possible, any further impact.

Spam: Unsolicited bulk email, where the recipient has not granted permission for the message to be sent, and where the message was sent as part of a larger collection of messages, all having substantively identical content. While Spam alone is not DNS Abuse, we include it in the five key forms of DNS Abuse when it is used as a delivery mechanism for the other four forms of DNS Abuse. In other words, generic unsolicited email alone does not constitute DNS Abuse, but it would constitute DNS Abuse if that email is part of a phishing scheme.

Action Timeline Q2

The chart is intended to help visualize the registry escalation process and timeline.



Action Taken	Cases	%	Domains*	%
Registrar took action pre-registry escalation	920	**31**	928	**24**
Registry took action pre-escalation to registrar (e.g., Protective Hold)	735	**24**	746	**20**
Remediated by a third party (e.g., hosting provider)	74	**2**	103	**3**
Remediated by registrant (e.g., compromised domain)	347	**12**	353	**9**
Registrar took action post-registry escalation (e.g., Clienthold, deletion, suspended account, other)	222	**7**	574	**15**
Explanation provided and no further action taken	320	**11**	424	**11**
Registry took action post-registrar escalation (e.g., Serverhold)	389	**13**	688	**18**
	3007		**3816**	

*Some cases may contain multiple domains in a single escalation.

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."

Generally these are organizations with whom we have an active, formal relationship. For more information on "trusted notifiers" in general please see the Contracted Party House Trusted Notifier Framework.

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

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 the second quarter of 2022, we received the following reports:

		IWF	MPA	RIAA
Reports received (URLs)		101	6	0
Domains suspended	Registrar	3	0	0
	Registry	0	6	0
Remediation confirmed by registrar		26	0	0
Unique domains reported		26	6	0
Closed / remediated other		0	0	0

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

Law Enforcement Authority (LEA) Requests Q2

In addition to Trusted Notifiers, Identity Digital also works directly with various law enforcement authorities to help mitigate or eliminate DNS Abuse. Law enforcement requests come in broadly three forms, including judicial orders, administrative orders, and requests for information on the registrants directly. Identity Digital reviews each request on an individual basis.

In the second quarter of 2022, we received the following requests:

4	1	3	3
Received Requests*	Actioned Requests	Declined Requests**	Affected Domains

* Note: Requests for disclosure of registrant information by LEA are not included here. These are included, if any, in the “Disclosure” section below.

**Same request received 3 times.

Court Orders Q2

This category contemplates orders we have received from courts of suitable jurisdiction, directing the Registry to take specific actions.

4	16	0	16
Valid Court Orders Received	Affected Domains	Suspended Domains	Transferred Domains

Data Disclosure Requests

https://identity.digital/policies/whois-layered-access/

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 and whether those persons may enjoy strong legal protections in their home country.

As noted above, we review each request received and only disclose the requested information where such disclosures are justified, necessary, proportional, and in line with our legal obligations. The following two tables display both the number of disclosure requests received by the Registry, as well as the closure reason for requests received during the second quarter of 2022.

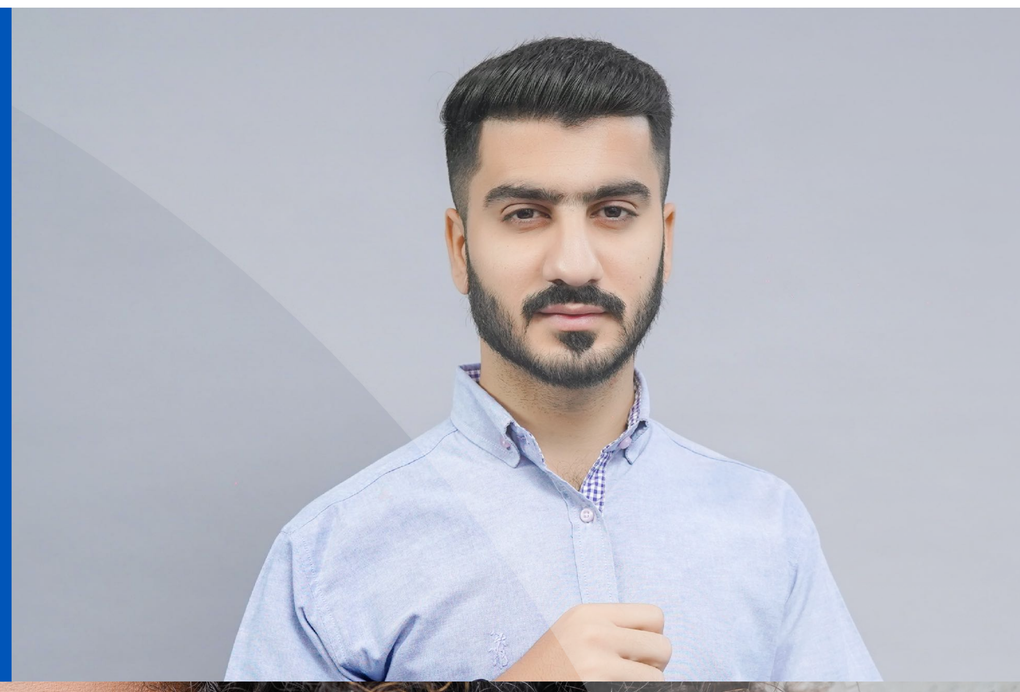
Overview

44	18	3	23
Affected Domains	No Data Processed*	Decisions to Disclose	Decisions to Not Disclose

*Request did not pass a basic completeness review

Category of Data Disclosure Requests Received

Intellectual Property Related	2
Domain Purchase — existing domain	12
Domain Purchase — domain does not exist	2
DNS Abuse Allegation	1
Website Abuse Allegation	3
Incomplete / Incorrect (insufficient explanation, missing information, wrong registry etc.)	18
Other — requests outside of our remit	6



identity digital™