identity digital™

Anti-Abuse Report 2022 Q4

Overview Q4

In Q4 of 2022, we saw a decrease in the overall number of cases escalated by the registry while the overall number of affected domains increased. While this may sound contradictory, the number of cases and their underlying domains are not always correlated. In some instances, once case may contain multiple related domains stemming from the investigation of a single abuse report. Escalation of multiple domains within a single case actually makes things more efficient for us, though the case-domains ratio is not in our control. Regardless, each case and underlying domain is reviewed independently for evidence of abuse. In short, abuse happens and our goal is to deal with it quickly, effectively and transparently.

DNS Abuse campaigns vary over time, and patterns may take time to materialize. Continuing in the vein of efficiency, we also note that registry early intervention surpassed 50% of our total mitigation actions in Q4. To be clear, we remain a strong proponent of primary escalation to our registrar partners; however, we remain confident in our “Protective Holds” as an effective tool to combat DNS Abuse. These holds are intended to target domains primarily engaged in DNS Abuse, and our process strives for little or no potential for collateral damage. We continue to learn from this process, and hope our actions help streamline our registrar escalations, allowing us to work together to investigate and mitigate less straightforward incidents of DNS Abuse.

In Focus > As Identity Digital continues to enhance our ability to decisively disrupt and mitigate DNS abuse. Learn more about the platform that helps power our abuse management on our partner CleanDNS’s blog.

Cases vs. Reports

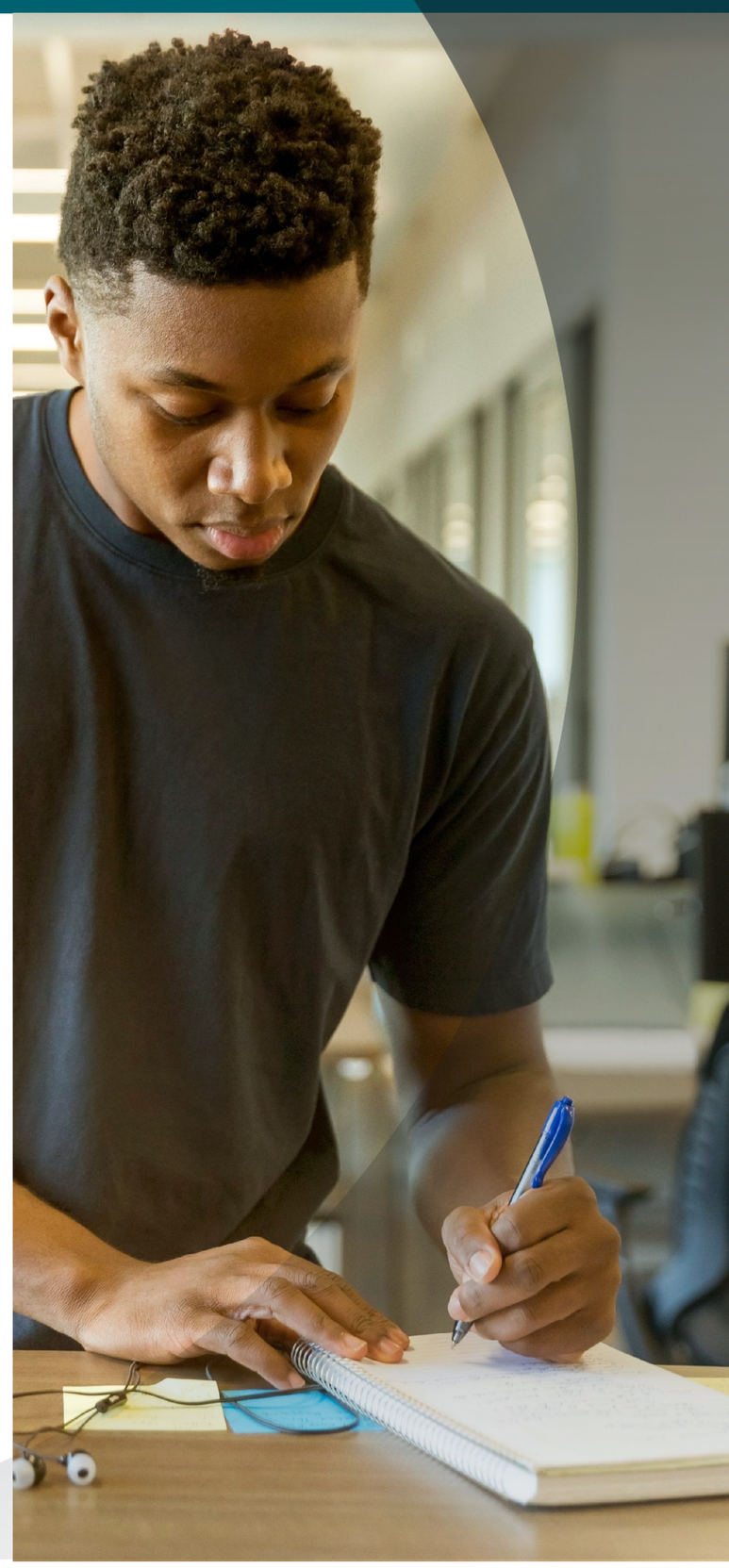
Well-Evidenced Escalations

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 Q4 2022, broken down by type and action taken.



Abuse Cases Q4

Cases by abuse type	Cases (opened)	% of total cases
Phishing	2487	93.3
Spam (as a delivery mechanism)	66	2.5
Malware	77	2.9
Pharming	0	0.0
Botnet	0	0.0
Other	35	1.3

2665
Cases Opened

93.3%
Percentage of phishing cases (of total)

17%
Fewer cases opened in Q4 vs Q3

Website Content Abuse Q4

Although our primary focus remains on DNS Abuse, we also believe there are other forms of abuse that, while 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 **Q4 2022**, Identity Digital intervened in five (5) cases of CSAM. After the escalation of an IWF-confirmed instance, the registry contacted the relevant registrar but did not receive a satisfactory response (if any). Given the severity of CSAM, and noting the minimal risk of unintended or collateral damage relating to these domains, Identity Digital intervened directly.

The registry also received a request to suspend a domain enabling access to an alleged terrorist/doxxing website. Following review, the registry did not find sufficient or corroborating evidence of the abuse, and therefore did not intervene at that time.

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.

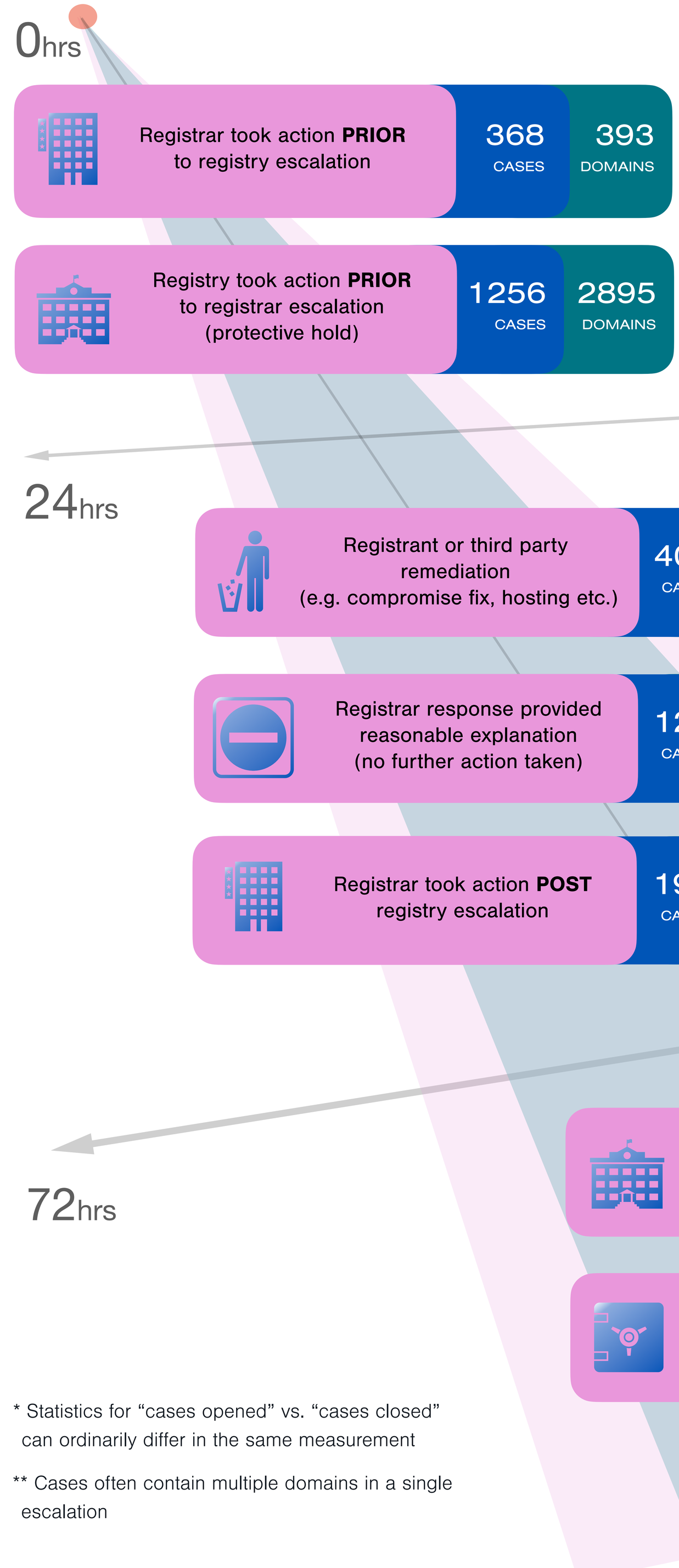
Child Sexual Abuse Material (CSAM):
For this definition and further information regarding the work of the Internet Watch Foundation (IWF), please see https://www.iwf.org.uk/about-us/

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 Q4



2665
Cases Closed*

7329
Unique domains affected (Closed)**

0.098%
Of all Identity Digital domains

2714
Additional unique domains escalated vs. Q3

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

** Cases often 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 fourth quarter of 2022, we actioned the following reports:

		IWF	MPA	RIAA
Unique domains affected		34	4	0
Domains suspended	Registrar	11	0	0
	Registry	5	4	0
Remediated (confirmed by registrar)		18	0	0
Closed / remediated other		0	0	0

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

Law Enforcement Authority (LEA) Requests Q4

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. Like other cases, Identity Digital reviews each LEA request independently.

In Q4 of 2022, we received the following requests:

1	1	0	19
Received Requests*	Actioned Request	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.

Court Orders Q4

This category contemplates orders we have received from courts of suitable jurisdiction, directing the Registry to take specific actions such as suspension, or transferring domains to different registrars.

5	5	0	5
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 fourth quarter of 2022.

Of note the registry received a number of spam / frivolous requests in Q4.

Overview

20	20	0	11
Affected Domains	No Data Processed*	Decision to Disclose	Final Decisions to Not Disclose

Category of Data Disclosure Requests Received

Intellectual Property Related	2
Law Enforcement Request	1
Domain Purchase — domain does not exist	2
Not a valid disclosure request (No actual valid request made / unconnected to domains / spam)	7
Incomplete / Incorrect (Incomplete form, missing information, wrong registry etc.)	6
Other — No clear categorization	2

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

identity digital™