Before the

Federal Trade Commission

Washington, D.C. 20554

In the Matter of	)	
	)	
Trade Regulation Rule on Impersonation of Government and Business	)	Docket No. FTC-2022-0064
	)	

Impersonation NPRM, R207000

COMMENTS OF THE MESSAGING MALWARE MOBILE ANTI-ABUSE WORKING GROUP (M³AAWG) ON THE NOTICE OF PROPOSED RULEMAKING - TRADE REGULATION RULE ON THE IMPERSONATION OF GOVERNMENT AND BUSINESSES

Introduction

The Messaging Malware Mobile Anti-Abuse Working Group (M³AAWG) is pleased to offer comments on the Notice of Proposed Rulemaking (NPRM), Federal Trade Commission, Docket No. FTC-2022-0064, concerning the Trade Regulation Rule on Impersonation of Government and Businesses released on October 17, 2022.

M³AAWG is a technology-neutral global industry association. With more than 200 members worldwide, we are the largest such organization in the online community. We bring together stakeholders in a confidential trusted forum to develop best practices and cooperative approaches for fighting online abuse. As a working body, we focus on operational issues of Internet abuse including technology, industry collaboration and public policy. M³AAWG works to fight online abuse caused by botnets, malware, spam, viruses, DoS attacks and other forms of online exploitation. We commend the Commission for undertaking this initiative and urge that the proposed rule be adopted. M³AAWG responds to several of the key questions raised in the NPRM below.

(1) **Should the Commission finalize the proposed rule as a final rule? Why or why not? How, if at all, should the Commission change the proposed rule in promulgating a final rule?**

The Commission should adopt this rule as part of its critical role in protecting consumers from ongoing and increasing impersonation schemes targeting businesses and governments alike. The Commission's

authority to act is clear and it works in sync with parallel efforts from the private sector.

We suggest the rule make clear that it is not intended to supplant any private right of action or civil remedies or self-help mechanisms that the industry already currently uses to protect businesses and consumers targeted by impersonation schemes. There may be a need for future legislative and regulatory solutions and additional best practices that would further complement the goals in this final rule. If so, M³AAWG would welcome the opportunity to work with the FTC on those refinements.

The scope of the rule should include the use of domain names in impersonation schemes.

Domain names are used for an ever-increasing number of impersonation-related criminal schemes including phishing, online ad fraud, "knock-off" commercial product sales, and more. M³AAWG believes that impersonation as covered under the final rule should specifically include the use of fraudulent domain names in impersonation-related schemes, including:

- both generic top-level domains (gTLDs) and country code top-level domains (ccTLDs), whether nominally tied to the United States (such as dot US) or used in ways that otherwise target U.S. consumers;
- impersonated names registered through blockchain, mobile apps, non-fungible tokens (NFTs);
- impersonated names used on parked websites (a domain name that is registered but not connected to an online service like a website or email hosting), and
- other domain name-related impersonation scams.[1]

M³AAWG does not believe that parody accounts should be considered impersonation unless such accounts are used in a criminal activity.

Although domain name-related issues have long been under debate inside the Internet Corporation for Assigned Names and Numbers (ICANN), the Commission should be aware that ICANN's bylaws prohibit it from acting outside the strict scope of its mission. Issues of unfair or deceptive acts or practices in or affecting commerce lie outside ICANN's mission – but are, fortunately, within the FTC's authority to address.

Application of the final rule here is consistent with the US Department of Commerce's Advance notice of proposed rulemaking (ANPRM). The ANPRM responds to Executive Order (EO) 13984 of January 19, 2021, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities." The EO directs the US Commerce Secretary to implement measures to "deter foreign malicious cyber actors' use of United States Infrastructure as a Service (IaaS) products and assist in the investigation of transactions involving foreign malicious cyber actors." The EO is relevant here with respect to the DNS.

[1] Many fraudulent domain names that resemble the FTC's own already exist. These include: federaltradecommission.com (registered since March 13, 2000); ftcgov.com (registered since August 6, 2003); ftcgov.info (registered since March 18, 2010); ftcgov.legal (registered since December 21, 2021); fraud-ftcgov.com (registered December 22, 2021); and federaltradecommission.online (registered since June 7, 2022).

The Domain Name System (DNS) is a globally-distributed network of servers that provides the means to translate a human-friendly domain name – e.g., m3aawg.org – to the address on the internet where the M[3]AAWG website can be found. Without the DNS, the internet simply cannot scale and flexibly serve the needs of users, organizations and societies worldwide. The DNS is arguably as much a part of our critical infrastructure as the mobile and optical fiber networks that comprise the physical backbone of the internet.

The scope of the rule should include the use of technologies that enable impersonation.

M[3]AAWG also believes that impersonation, as covered under the final rule, should specifically include the use of technologies that promote or enable impersonation via synthetic persona, to include audio, video, pictorial characteristics, and other manipulated media (i.e., deepfakes) intended to pose as an individual associated with a business or governmental entity.

The investigation of impersonation schemes requires cooperation and information from many entities.

In many cases, impersonation involves multiple third parties, providers, platforms, or intermediaries. For example, impersonation might include the use of hosting, Content Delivery Networks, DNS, email-sending infrastructure, social media platforms, and other services. Telephony services are also used at scale for SMS/text-based impersonation attacks as well as call centers specializing in high-volume fraudulent in-person calls to victims. Such multi-faceted attacks have several important implications:

- No single entity may have the "full picture" when it comes to an impersonation scheme.
- Determining whether a potential domain is an innocent/coincidental clash of domain labels or the foundation for an intentional and malicious impersonation attack might require data that isn't readily available to all the specialized providers of niche services used by an attacker.
- Required information known to one or more entities may not be shared or readily available for investigatory purposes.
- The willingness by some entities to take action against an attack may not universally extend to all entities.

To resolve issues of impersonation, it is paramount that these parties cooperate and provide appropriate help and support to investigators, be this by sharing data or resolving ongoing impersonation cases in their relevant infrastructures; e.g., by removing access or making content unavailable.

Below, we address the role of WHOIS specifically, but similar issues apply to other parties and services, where appropriate timelines for a response as well as required mitigations should be considered.

WHOIS information is vital to the investigation of impersonation scams.

The final rule should call out the critical issue of non-available domain "WHOIS" registration data. This data is critical to holding abusers accountable for impersonation schemes and other abuse. The FTC has recognized the need to access such data for its enforcement purposes since the early 2000s. Domain WHOIS access, unfortunately, has become significantly curtailed today, which only serves to emphasize

why this final rule is urgently needed.[2]

WHOIS is a domain name directory service that all registrars must implement. It is used to provide information about a domain to the general public. Brand owners have traditionally relied on this information as a starting point for enforcement efforts against fraudulent domain name schemes. Under current changes in WHOIS rules, however, much of the relevant information is no longer publicly available. This change presents huge challenges to online enforcement efforts. Meanwhile, bad actors continue to proliferate under the new privacy rules, harming the very consumers the privacy laws were intended to protect. Intellectual property assets are leveraged to sell online counterfeit goods, for phishing, and for other fraudulent schemes that dupe internet users. Without the information provided by Domain WHOIS to facilitate online enforcement efforts, brand owners are forced to find other ways to address online abuse—often adding substantial delay and costs.

Former FTC Chair Liebowitz's testimony to Congress in 2006 still rings true today:

> *FTC investigators and attorneys have used WHOIS databases for the past decade in multiple Internet investigations. WHOIS databases often are one of the first tools FTC investigators use to identify wrongdoers. Indeed, it is difficult to overstate the importance of quickly accessible WHOIS data to FTC investigations.*
>
> *There are other legitimate private users of WHOIS databases--businesses, financial institutions, nongovernmental organizations, and intellectual property rights owners--all of which heavily rely on access to accurate WHOIS data. Although the FTC does not represent these entities' interests in the WHOIS debate, their use of WHOIS databases can help consumers. For example, a financial institution concerned about the misuse of its name by "spoofing" its website is not only protecting its own business interests, but it is also protecting its customers from being "phished."*
> …
>
> *Having "real-time" access to WHOIS data is particularly important for a civil law enforcement agency like the FTC. Where a registrar is located in a foreign jurisdiction, the FTC often has no other way to obtain the information it needs. The FTC cannot, in most cases, readily require a foreign entity to provide us with information. Thus, particularly in cross-border cases, WHOIS databases are often the primary source of information available to the FTC about fraudulent domain name registrants.*

The final rule should therefore make clear that domain name registrars, registries, resellers, and privacy/proxy services must collect and maintain accurate WHOIS data and respond promptly to disclosure requests from the Commission, as well as from the targeted impersonated business, government entity or victims. Failure to promptly respond to businesses or victims will only create more enforcement work for the Commission under the final rule. Failure to disclose non-public domain name data promptly in response to credible requests could even be considered evidence of providing the "means and instrumentality" for impersonation schemes.

[2] The application of the EU General Data Protection Regulation (GDPR) significantly restricted the way registration data is handled in the public WHOIS.

The rule should recognize that in the context of a substantiated impersonation scheme, disclosure of domain name registration data is necessary to serve the legitimate interest pursued by the requestor of that data, outweighing any rights of the apparent impersonator. This also serves the public interest by enabling the FTC to better address such impersonation schemes, and by allowing the impersonated business to pursue civil enforcement actions to stop the impersonation schemes. However, the rule should take into account data minimization principles, such as ensuring that the WHOIS data sought by investigators is available from the domain name registries or registrars with a NEXUS, legal, or other contractual requirement to disclose (such as may be found in an ICANN policy or contract).[3]

We note that the final rule should apply where impersonation is achieved through the creation of a subdomain that impersonates a government agency, business, or victim (e.g., "FTC.example.com"). The final rule could also apply to lookalike tricks such as using unicode characters in domain names or "display name impersonation" in account names that are deployed in impersonation scams, such as "support@ftc" in the account name of a website.

M³AAWG's Best Practices papers addressing mitigation of impersonation scams may aid the Commission.

M³AAWG publishes and updates regularly various best common practices and position papers related to business and government impersonation issues. Several of these may be of assistance to the Commission. Our paper on malicious domain names covers a long list of illegal activities that warrant the designation of domain names as malicious, including fraudulent and deceptive schemes.

- M³AAWG Introduction to Addressing Malicious Domain Registrations https://www.m3aawg.org/sites/default/files/m3aawg-maliciousdomainregistratinos-2018-06.pdf.
- M³AAWG Protecting Parked Domains Best Common Practices https://www.m3aawg.org/sites/default/files/m3aawg_parked_domains_bcp-2022-06.pdf

M³AAWG recommends that the FTC consider including best practices for proactive measures to prevent and avoid impersonation attacks. For example:

Validation of Commercial Senders

The FTC could encourage the use of techniques to validate commercial senders of emails in order to avoid impersonation attacks.

[3] See the Comments of the National Telecommunications and Information Administration Regarding Commercial Surveillance ANPR R11004: "[T]ypes of information deemed non-sensitive—or which is deemed less appropriate for privacy protections due to important policy objectives served by making it broadly accessible—may also produce privacy risks that should not be ignored. For instance, while making domain name registration information widely accessible serves important law enforcement, IP rights enforcement, and cybersecurity research objectives, it also contains highly sensitive personal information that can put registrants at enhanced risk of spamming, as well as identity theft, spoofing, doxing (the public dissemination of private and identifying information), online harassment, and even physical harm."

DNS Mitigation

Upon receipt of a credible notice that a maliciously registered domain name is or could be used in an impersonation attack, a registry and/or registrar should promptly investigate and mitigate at the DNS level to prevent the domain name from being used in multiple attacks.[4] This approach is consistent with the approach taken in the proposed S.3399, Domain Reform for Unlawful Drug Sellers Act or the DRUGS Act, which recommends appropriate mitigation actions. The bill "requires a website domain name registrar (or registry operator) to take down a domain name under the registrar's control upon receiving an eligible notification that the domain name is facilitating illegal online drug sales. Upon receiving an eligible notification, the registrar must lock the domain name within 24 hours and suspend the domain name within seven days."

Trusted Notifiers

The FTC should encourage the use of trusted notifier programs by domain name registries or registrars to address maliciously registered domain names. Frequently impersonated businesses or governmental entities should be eligible to become trusted notifiers. Eligible notices from a trusted notifier should include certain information, such as a summary of the alleged illegal activities and a statement that the evidence supporting the allegations is available to be shared with the registrar or registry. In S.3399, the United States Food and Drug Administration (FDA) offered an example of a trusted notifier here. The FDA and the National Telecommunications and Information Administration (NTIA) launched a 120-day pilot in 2020 to help reduce the availability of unapproved opioids illegally offered for sale online. The FTC should consider a similar pilot or approach in which trusted notifiers are identified, subject to appropriate accreditation, accountability, and dispute resolution processes.

Finally, we encourage the FTC to work with its interagency counterparts within the United States government and with international bodies (including ICANN and the European Union) to come up with workable resolutions related to WHOIS.

(2) **Please provide comment, including relevant data, statistics, consumer complaint information, or any other evidence, on each different provision of the proposed rule. Regarding each provision, please include answers to the following questions:**

(a) How prevalent is the act or practice the provision seeks to address?

Impersonation scams such as the recently reported scam regarding the fake Eli Lilly Twitter Account which contained a blue "verified" check mark highlight the need for the proposed rule. In that example, on November 10, 2022, a verified Twitter account posing as Eli Lilly wrote in a viral tweet, "We are excited to announce insulin is free now." By the next day, the drugmaker's shares plunged by about $22 billion.

M[3]AAWG submits the following data and information in support of the additional recommendations described above:

[4] See for example, the recommendations in the EU DNS Abuse Study (2022).

- 2022 DNS Abuse Study Commissioned by the European Commission, and Appendix 1 - Technical Report
- M³AAWG 2021 Study on ICANN, GDPR and WHOIS: A Users Survey - Three Years Later
- Interisle Phishing Landscape 2022: An Annual Study of the Scope and Distribution of Phishing
- Interisle Malware Landscape 2022: A Study of the Scope and Distribution of Malware
- Anti-Phishing Working Group Phishing Trends Reports
- Interisle WHOIS Contact Data Availability and Registrant Classification Study
- Interisle Criminal Abuse of Domain Names: Bulk Registration and Contact Information Access
- 2006 Senate Hearing 109-1152: Internet Governance: The Future of ICANN
- 2022 Akamai Security Research Blog Identifying 13 Million Malicious Domain Names in One Month

Currently, governments and businesses do not have sufficient remedies to tackle impersonation fraud at the scale seen today. For example, the tables below highlight recent trends showing the high volumes of phishing attacks targeting the world's largest brands. These attacks often vary depending on the vertical spaces associated with these brands, as well as the time of year. The proposed recommendations described by M³AAWG above, if adopted, could provide a stronger foundation and tools for the FTC and impersonated businesses and governments to investigate, prevent, and mitigate impersonation scams.

The following table shows the number of phishing attacks of recognized brands, financials, and government agencies for two reporting periods: August–October 2022 and May–July 2022. (The source for this table is the Cybercrime Information Center, https://cybercrimeinfocenter.org.] The Cybercrime Information Center uses three commercial and open-source phishing URL blocklists to identify the targets in the metadata included in their phishing reports.

Targeted Brand	Number of phishing attacks August–October 2022	Number of phishing attacks May–July 2022
Mitsubishi UFJ NICOS	95729	37683
Facebook	28263	43451
KDDI	15019	3196
JCB Co.	14680	232
AEON Financial Service	11066	4422
Microsoft	14411	14377
Credit Saison	8464	60
United States Postal	5632	23972

Service		
Apple	3420	2656
AT&T	2805	1991
Wells Fargo	2607	1197
DHL	2518	2713
Naver	2311	1084
Amazon	2152	2372
Yahoo	2065	464
M&T Bank	1570	3181
Santander	1489	1262
Bank Rakyat Indonesia	1390	31
Netflix	1226	1715
IRS	1187	641

Interisle's "Phishing Landscape 2022" contains a table of most targeted brands listed by annual ranking and phishing attacks, and then their quarterly ranking, from May 2021 through April 2022. See https://interisle.net/PhishingLandscape2022.pdf (p. 40).

A table of the number of phishing domains that include brand names in the domain string during these same periods:

Number of phishing domain names reported that contain well-known brand names		
Brand	**August–October 2022**	**May–July 2022**
Apple	3330	3339
Amazon	2201	5980
Facebook	1882	967
United States Postal Service	888	3976
Citi	849	2189

Chase	890	1152

(b) What is the provision's impact (including any benefits and costs), if any, on consumers, governments, and businesses, both those existing and those yet to be started?

M[3]AAWG does not have the data or expertise to address this question.

(c) What alternative proposals should the Commission consider?

In lieu of § 461.4 (applicable to the provision of means and instrumentalities by secondary businesses), the FTC could identify best practices or safe harbors to incentivize prompt mitigation efforts and sound verification techniques. This would avoid the risk that the rule is inadvertently interpreted to create secondary or intermediary liability against the many legitimate businesses, technologies or services that are misused by bad actors to engage in impersonation scams.

(3) **Does the proposed rule contain a collection of information?**

M[3]AAWG does not have the data or expertise to address this question.

(4) **Would the proposed rule, if promulgated, have a significant economic impact on a substantial number of small entities? If so, how could it be modified to avoid a significant economic impact on a substantial number of small entities?**

M[3]AAWG's focus is not on small businesses; thus, we do not have the data or expertise to address this question.

(5) **The proposed rule contains a one sentence prohibition against impersonation of government in § 461.2 and another against impersonation of businesses in § 461.3. Are these prohibitions clear and understandable? Are they ambiguous in any way? How if at all should they be improved?**

The proposed rule should include a definition of "impersonation." We believe that the definition could track existing laws such as adopting the definition of "criminal impersonation" under 18 U.S. Code § 5-113, and track the groups that are specifically called out under 18 U.S. Code Chapter 43. Adopting this definition of "criminal impersonation" would further clarify that the rule is targeting bad actors with intent to impersonate rather than the businesses, technologies or services that are misused by those bad actors. The definition would focus on those with the clear intent and specific knowledge to commit the prohibited acts. M[3]AAWG is happy to work with the Commission on this development.

(6) **The proposed rule, in § 461.4, prohibits providing the means and instrumentalities to commit violations of § 461.2 or § 461.3. Should any final rule contain this prohibition against providing the means and instrumentalities for violations of the prohibitions against government or business impersonation? Why or why not?**

M³AAWG supports the Commission's clarification that it is not seeking to impose secondary liability under this final rule. But we urge the Commission to clarify when direct liability would arise. To ensure against any unintended expansion of intermediary liability doctrines, the Commission should not link liability to a mere knowledge or reason-to-know test. Rather, the rule should state that primary liability will attach to those who act willfully or in bad faith, with the clear intent and specific knowledge to commit the prohibited acts by providing such means/instrumentalities. Bad faith would include working in active concert with or aiding and abetting the impersonator. This approach would capture a wide scope of bad actors involved in impersonation schemes and is consistent with other regulatory frameworks concerning intermediary liability.

(7) The proposed rule, in § 461.1, defines "business" to include non-profit organizations. Should any final rule keep the prohibition against impersonating non-profit organizations? Why or why not?

M³AAWG supports the final rule covering non-profit organizations and non-governmental organizations; these categories are often the target of harmful impersonation in the same way as for-profit organizations or government(s).

(8) Should the proposed rule be expanded to address the impersonation of individuals or entities other than governments and businesses in interstate commerce?

For example, should the proposed rule be expanded to prohibit impersonation of individuals for the purpose of seeking monetary payment or contribution, such as in romance or grandparent impersonation scams? In your answer to this question, please provide the following information:

(a) How prevalent is the act or practice?

(b) What would be the impact, including benefits and costs, of including individual impersonation in the proposed rule on consumers, governments, and businesses?

(c) What alternative proposals should the Commission consider?

M³AAWG does not have the data or expertise to address this question.

Conclusion

M³AAWG urges the FTC to consider the above comments and suggestions and thanks you for the opportunity to respond to your questions. We will be glad to address any further questions the FTC might have. Please address any inquiries about our comments or work to M³AAWG's Executive Director, Amy Cadagin.

Sincerely,

/s/ Amy Cadagin
Executive Director, Messaging Malware Mobile Anti-Abuse Working Group
P.O. Box 9125

Brea, CA 92822
comments@m3aawg.org