



Imposter Website Takedown Toolkit

Imposter websites targeting FINRA member firms and their registered representatives have become increasingly prevalent, serving to defraud investors and potentially damage the reputations of impersonated firms and individuals. This toolkit provides member firms and individuals with actionable strategies for quickly identifying and combating these fraudulent sites, including step-by-step guidelines for detection and response.

Preventive Measure: Register your firm's trademarks and logos with the U.S. Patent and Trademark Office. This strengthens your legal basis for requesting suspension of imposter websites and protects your brand identity.

STEP 1: IDENTIFY IMPOSTER SITES

1.1 Set up Monitoring and Alerts

- Set up automated alerts for your firm's name using free internet monitoring services (such as Google Alerts) to detect new mentions online.
- Encourage your firm's registered representatives to **set up personal alerts for their names** in combination with common industry terms such as "broker," "investment adviser" or "financial consultant."
- Consider subscribing to third-party brand protection services that specialize in detecting imposter sites.

1.2 Conduct Regular Searches

- Regularly search for your firm's name and, to the extent possible, your registered representatives' names combined with industry-related terms.
- To the extent possible, also monitor social media platforms, since threat actors often post fake testimonials or impersonator profiles. A social media mention, even without a direct domain link, may suggest the existence of an imposter site.
- Encourage your registered representatives to conduct their own periodic searches and to monitor for potential impersonation.

1.3 View Suspected Sites Safely

Important: **Avoid accessing suspected sites directly** by clicking links or entering web addresses into your browser, as sites may contain malware or allow threat actors to track your activity.

Use safe viewing methods:

- **Sandbox browser:** An isolated virtual environment that lets you browse websites without risk to your system. Companies typically use vendor-provided services or built-in enterprise tools for this purpose. Consult your IT department, as your

organization may already have sandbox capabilities through existing security tools or operating system features.

- **Cached site:** A stored snapshot of a webpage previously indexed by a search engine. Some search engines provide access to cached versions through their search results. Look for a "Cached" link or option near search results. Note that this feature has become less consistently available.
- **Archived site:** A historical snapshot of a webpage. The Wayback Machine (web.archive.org) is a widely used resource that allows you to enter a URL to search for saved versions. Note that recently created sites or sites that existed only briefly may not be archived.

1.4 Document the Imposter Website

- Capture full-page screenshots of a suspected imposter site before it changes or is suspended. Most browsers offer free screenshot extensions that easily capture full website screenshots. Conduct your due diligence before downloading one.
- Preserve additional evidence, such as:
 - the domain name and URL;
 - screenshots of associated social media profiles;
 - any communications with the imposters;
 - reports from victims or potential victims; and
 - dates when the site was first discovered.

STEP 2: REQUEST SUSPENSION OF IMPOSTER WEBSITES

2.1. Identify and Contact the Domain Registrar

- Look up the domain registrar using the ICANN Lookup tool at lookup.icann.org (the website of the Internet Corporation for Assigned Names and Numbers, or ICANN).
- Under **Registrar Information**, find the **abuse contact email address**.
- **Email the abuse contact** with a suspension request, such as one or both of the examples provided at the end of this document.¹ Registrars typically respond within 24 to 48 hours.

2.2. Contact the Hosting Provider (if necessary)

- If the registrar refuses to take down the site, conduct an internet search for the name of the site's web hosting provider.
- If the hosting provider is different from the domain registrar, report the site to the hosting provider's abuse reporting contact. A hosting provider is the company that stores and serves the website's content. To find abuse contact information, search for "[hosting provider name] report abuse" or check the hosting provider's website for an abuse contact, typically found on their terms of service or "Contact Us" pages.

2.3. Request Suspension of Associated Social Media Accounts

- If you discover fake social media accounts associated with the imposter websites, use reporting tools such as the following to request those accounts' suspensions:
 - [Facebook](#)
 - [Instagram](#)
 - [LinkedIn](#)
 - [Telegram](#)
 - [WhatsApp](#)
 - [X](#)

2.4. Escalate if Needed

- If the registrar does not respond and the domain remains active, [submit an abuse complaint to ICANN using their Domain Name System \(DNS\) Abuse Reporting process](#). Provide evidence of the site's DNS abuse and the registrar's inaction.
- Consult with legal counsel about sending **cease-and-desist letters** to the domain registrar or hosting provider, or pursuing other legal remedies if suspension efforts are unsuccessful.

STEP 3: SHARE INFORMATION ON IMPOSTER WEBSITES

- **Submit a [tip](#) to FINRA.** Depending on the imposter site's content, FINRA may also be interested in requesting suspension of the domain.
- **Report the imposter site and any associated fake social media profiles to the [FBI](#), [FTC](#) and the [SEC](#).** Sharing this information is key to law enforcement action.
- **Report the imposter site to web browsers**, such as [Google Chrome](#), **and search engines**, such as [Microsoft Bing](#), **as an unsafe site**.
- As long as an imposter site or social media profile is active and targeting your firm or broker, **consider posting a warning banner** on your firm's site about the impersonation.

Suspension Request Sample Letter 1 (from a member firm):²

Subject: Trademark Infringement and Demand for Action Regarding Infringing Domain

To Whom It May Concern:

I am writing on behalf of [Insert Your Member Firm's Name], a registered broker-dealer and the lawful owner of the registered trademark [Your Trademark] (Registration No. [Insert Trademark reg number]), which is used in commerce and protected under applicable federal and state trademark laws, including the Lanham Act (15 U.S.C. § 1051 et seq.).

It has come to our attention that the domain name [Insert Domain Name/URL] ("Domain"), which is registered through your services, appears to use our trademark without authorization.

This Domain violates [Insert Your Member Firm's Name]'s trademark rights. [Insert Your Member Firm's Name] holds a registered trademark with the United States Patent and Trademark Office under registration number [Insert Trademark reg number]. The misuse and infringement of our trademark is likely to cause consumer confusion, mislead the public, and falsely suggest an affiliation or endorsement by our firm.

[Describe specific instances of infringement, including: (a) how the domain name incorporates the trademark; (b) how the website content uses or references the trademark; (c) specific examples of potential consumer confusion; and (d) any evidence of actual confusion if available.]

Attached is a screenshot of the Domain and a link to the Domain [Insert link]. [Attach screenshot and any other relevant evidence, such as WHOIS records, to the letter.]

In addition to trademark infringement, this Domain appears to be used in bad faith, as it trades on the goodwill and reputation associated with [Insert Your Member Firm's Name]'s brand.

We respectfully request the following actions, including but not limited to:

1. Investigate the infringing domain name;
2. Take appropriate remedial action, including transfer or cancellation of the domain, as warranted;
3. Provide the name of the Domain's hosting provider and abuse contact information; and
4. Provide written confirmation of the actions taken in response to this notice.

Please direct all correspondence regarding this matter to [Insert contact name, title, phone number, and email address].

We reserve all rights and remedies available under federal and state law, including the right to pursue legal action if this matter is not resolved promptly.

We appreciate your prompt attention to this matter.

Sincerely,

[Insert Your Authorized Representative's Name]

[Insert Title]

[Insert Phone Number]

[Insert Email Address]

[Insert Member Firm's Name]

[CRD Number (optional): Insert CRD#]

Suspension Request Sample Letter 2 (from a registered representative):³

Subject: Impersonation, Identity Theft, and Fraudulent Misuse of Name, Likeness, and Credentials – Demand for Immediate Action

To Whom It May Concern:

I am writing regarding the domain name [Insert Domain Name/URL] ("Domain"), which is registered through your services. I am [Insert Your Full Name], a registered representative associated with [Insert Member Firm Name], holding CRD Number [Insert CRD#] and licensed in [Insert relevant states/Series licenses].

It has come to my attention that the Domain is being used to falsely impersonate me and fraudulently misuse my name, likeness, professional credentials, and reputation to deceive investors and facilitate fraud.

Nature of the Violation

The Domain and associated website content unlawfully misappropriate my identity and professional standing by:

[Describe specific instances of impersonation and fraudulent use, including: (a) use of your name, photograph, or other likeness without authorization; (b) false claims of affiliation with your member firm or other legitimate entities; (c) unauthorized display of your professional credentials, licenses, or registrations; (d) specific examples of how the site is being used to solicit investors or facilitate fraudulent schemes; and (e) any evidence of actual investor confusion or harm if available.]

Attached are screenshots of the Domain, a link to the Domain [Insert link], and supporting documentation evidencing my legitimate identity and credentials. [Attach screenshots, WHOIS records, copies of registration documents, and any other relevant evidence.]

This fraudulent impersonation violates federal and state laws related to identity theft and fraud. This Domain poses an imminent threat to investors and causes substantial harm to my personal and professional reputation. The fraudulent use of my identity may expose innocent investors to financial loss and undermines public confidence in the securities industry.

Demand for Immediate Action

Given the serious nature of this activity, I respectfully request the following actions, including but not limited to:

1. Immediately suspend or disable the infringing domain name to prevent further harm to investors and my reputation;
2. Investigate the domain registration and associated account;
3. Provide the registrant's contact information, including name, address, email, and phone number;

4. Provide the name of the Domain's hosting provider and abuse contact information;
5. Preserve all records related to the domain registration, payment information, and account activity for potential law enforcement investigation; and
6. Provide written confirmation of the actions taken in response to this notice.

Please direct all correspondence regarding this matter to [Insert your contact information].

I reserve all rights and remedies available under applicable law. Thank you for your immediate attention to this urgent matter.

Sincerely,

[Insert Your Full Name]

[Insert Professional Title]

Registered Representative, CRD# [Insert CRD#]

[Insert Member Firm Name]

[Insert Phone Number]

[Insert Email Address]

[Insert Mailing Address]

This tool does not create any new legal or regulatory obligations for firms or other entities. This optional tool is provided to assist member firms in fulfilling their regulatory obligations. This tool is provided as a starting point and you must tailor this tool to reflect the size and needs of your firm. Using this tool, or the template letters, does not guarantee compliance with or create any safe harbor with respect to FINRA rules, the federal securities laws or state laws, or other applicable federal or state regulatory requirements.

¹ The template letters are provided for informational purposes only as examples and do not constitute legal advice. The use of these templates does not create an attorney-client relationship between you and FINRA.

The template letters are intended as examples and should be tailored to a member firm's or registered representative's particular and unique facts and circumstances. Member firms or registered representatives who choose to use the template letters, in whole or in part, should not imply that FINRA is representing them or their request. **The Terms of Use available at FINRA.org (<https://www.finra.org/terms-of-use>) apply to the use of these templates.**

Each situation involving trademark infringement, impersonation, or fraudulent misuse of identity is unique and may involve complex legal issues that require professional legal analysis. Before sending any cease and desist letter or taking legal action:

- Consult with qualified legal counsel to ensure the letter is appropriate for your specific circumstances and complies with applicable federal and state laws;

- Review the matter with your member firm's compliance or legal department to ensure consistency with firm policies and regulatory obligations;
- Consider reporting the matter to appropriate regulatory authorities and/or law enforcement agencies as warranted; and
- Obtain professional guidance regarding evidence preservation, documentation requirements, and potential legal remedies.

The information contained in these templates should not be relied upon as a substitute for legal advice from a licensed attorney familiar with your specific facts and circumstances. Laws and regulations vary by jurisdiction and change over time.

By using these templates, you acknowledge that you have been advised to seek independent legal counsel and that no warranty or guarantee is made regarding the legal sufficiency, effectiveness, or appropriateness of these templates for your particular situation.

Any reference to specific commercial products, processes, or services does not constitute or imply their endorsement, recommendation or favoring by FINRA.

² Ibid

³ Ibid