BRIDGHAM TECHNOLOGY INSTITUTE
BTI WORKING PAPER 323-26

Email Spoofability Across Registered Investment Advisers: A Pre-Registered Passive Measurement of DMARC Enforcement in a Random Draw of 200 SEC-Registered Advisers

Bridgham Technology Institute

This work is made available under the rights statement In Copyright - Educational Use Permitted
https://rightsstatements.org/page/InC-EDU/1.0/
Raleigh, NC: Bridgham Technology Institute, November 2026.

Electronic copy available at: https://bridghaminstitute.com/research/working-papers/323-26

Email Spoofability Across Registered Investment Advisers: A Pre-Registered Passive Measurement of DMARC Enforcement in a Random Draw of 200 SEC-Registered Advisers

Bridgham Technology Institute*

November 2026

Abstract: Clients of a registered investment adviser act on email that appears to come from the adviser, and the adviser's published DMARC policy determines whether a receiving mail server is told to refuse a message that falsely claims the adviser's domain. We measure the published email-authentication records of 200 registered investment advisers sampled at random from the regulator's public roster, using only public DNS and contacting no one. Of the 114 advisers that were mail-active and on their own domain, 58 (50.9%, 95% Wilson interval [41.8, 59.9]), about half, publish no enforcing DMARC policy, which means a message that did not originate with the adviser can still reach a client's inbox appearing to come from it. Strict protection (p=reject) is present at 18 of the 114 advisers (15.8%). SPF is published at 94.7% and DNSSEC is signed at 7.9%. The method and the sample were set before any data was collected, and the result is published as measured. For the advisers without an enforcing policy, these results suggest that the exposure may be closed by a single DNS change after a short period of monitoring.

Keywords: DMARC, SPF, DNSSEC, email spoofing, registered investment advisers, pre-registration, random sample

* Bridgham Technology Institute is a division of Bridgham Cyber, LLC, Raleigh, NC. Contact: headofresearch@bridghamcyber.com.

1. Introduction

Registered investment advisers hold client account and identity data, and their clients act on email that appears to come from the adviser: a transfer instruction, a statement, a request to sign. Email authentication is the public, checkable control that decides whether a receiving mail server can refuse a message that falsely claims the adviser's domain.

Domain-based Message Authentication, Reporting, and Conformance (DMARC) lets a domain owner tell receiving mail servers what to do with a message that claims the domain but fails authentication.[1] An adviser that publishes an enforcing DMARC policy instructs receivers to set such a message aside or to refuse it. An adviser that publishes no enforcing policy gives no such instruction, and impersonating mail can pass. Each policy is published in the public Domain Name System (DNS), where any receiving server can read it. A single record does not show how common enforcement is across advisers as a group.

In this paper, we measure the share of registered investment advisers that publish no enforcing DMARC policy. We take a random draw of 200 advisers from the public roster of the Securities and Exchange Commission (SEC), limited to SEC-registered advisers with regulatory assets under management of $500 million to $10 billion, and we read each adviser's published records from public DNS. Alongside DMARC, we record the Sender Policy Framework (SPF) record, which declares the servers permitted to send for a domain,[2] and whether the domain is signed with DNSSEC.[3] No mail was sent and no adviser was contacted. Each share is reported with a 95% Wilson score confidence interval (CI).[4]

We document three main findings. First, 58 of the 114 advisers measured (50.9%, 95% CI [41.8, 59.9]) publish no enforcing DMARC policy. Second, declaring senders is far more common than enforcing. SPF is published by 108 of the 114 advisers (94.7%), an enforcing DMARC policy by 56 (49.1%), and the strictest policy, p=reject, by 18 (15.8%). Third, the interval for advisers overlaps none of the intervals for veterinary practices, insurance agencies, community banks or credit unions reported in four companion papers.[5–8]

These findings describe published records, not the handling of mail. A domain without an enforcing policy may still filter inbound mail, and we do not measure DomainKeys Identified Mail (DKIM), which is outside the scope of a passive measurement. The level describes the 114 advisers whose website on file is their own domain; 79 of the 200 advisers drawn list a shared platform instead and were excluded. The comparison with the companion papers sets different populations and sampling methods side by side, and it does not describe a trend.

The paper proceeds as follows. Section 2 describes the sampling frame, the draw, the measurement and the definitions. Section 3 presents the results. Section 4 compares the result with the companion papers and discusses what it means for an adviser. Section 5 states the limitations, and Section 6 concludes.

2. Method

2.1. Sampling Frame

The frame holds SEC-registered investment advisers with regulatory assets under management of $500 million to $10 billion, a website address on file, and a main office in the 50 states or the District of Columbia. We took it from the SEC's monthly Form ADV data file (October 2026 release).

2.2. Draw

We ordered each eligible row by the SHA-256 hash of the seed (20261005) joined to its regulator key, and we took the first 200, once, without replacement. The draw can be repeated from the saved roster file. No draw was replaced after an exclusion.

2.3. Measurement

The measurement is passive. We read public DNS only, through two public resolver sets, and we sent no mail and contacted no adviser. For each registrable domain we resolved four records: DMARC at the _dmarc label (presence, policy and parseability),[1] the SPF record (presence, as a tri-state, with indeterminate reads excluded rather than counted absent),[2] DNSSEC by the DNSKEY-at-apex definition,[3] and MX as a check that the domain is mail-active.

2.4. Operational Definitions

A domain is *spoofable* when it has no enforcing DMARC policy: the record is absent, set to p=none or unparseable. A domain is *protected* at p=quarantine or p=reject, and *strictly protected* at p=reject. Each share carries a 95% Wilson score interval.[4] We use no significance test and no model.

2.5. Coverage

We measured 114 of the 200 advisers drawn. Two groups were excluded and are counted in no denominator: 79 advisers whose website on file was a shared platform, such as a social-media profile, and not the adviser's own domain, and 7 advisers with no MX record, which means they were not mail-active.

2.6. Independent Reproduction

A second classifier, written from scratch and separately from the measurement code, reproduced every count from the raw answers. A second resolution pass through a different resolver set disagreed with the first on 1 field across all 114 domains. We report the first pass, and the disagreement is logged rather than reconciled.

3. Results

3.1. Aggregate Level

Table 1 reports each measure with its interval, and Table 2 reports the distribution of published DMARC policy. Of the 114 registered investment advisers, 58 (50.9%, 95% CI [41.8, 59.9]) publish no enforcing DMARC policy. Of the 58, 26 publish no DMARC record at all and 32 publish a record at p=none. An enforcing policy is present at 56 of the 114 advisers (49.1%), and strict protection (p=reject) at 18 of the 114 (15.8%). Among the enforcing records, 1 applies the policy to less than 100% of failing mail.

Measure	k/n	Share	95% CI
No enforcing DMARC (spoofable)	58/114	50.9%	[41.8, 59.9]
Any enforcing policy	56/114	49.1%	[40.1, 58.2]
p=reject	18/114	15.8%	[10.2, 23.6]
SPF published	108/114	94.7%	[89.0, 97.6]
DNSSEC signed	9/114	7.9%	[4.2, 14.3]

Table 1: Email-Authentication Measures Across 114 Registered Investment Advisers, with 95% Wilson Score Intervals.

DMARC state	Count	Share	Classification
No record	26	22.8%	Spoofable
p=none	32	28.1%	Spoofable
Unparseable	0	0.0%	Spoofable
p=quarantine	38	33.3%	Protected
p=reject	18	15.8%	Strictly protected

Table 2: Published DMARC Policy Across 114 Registered Investment Advisers.

3.2. Declaring Versus Enforcing

SPF, which declares the servers permitted to send for a domain, is published at 94.7%. An enforcing DMARC policy, which instructs receivers to act on a message that fails that check, is present at 49.1%, and p=reject at 15.8% (Figure 1). Among the three regulator-roster studies, advisers show the widest gap between declaring and enforcing, and the largest share with no DMARC record at all (22.8%).

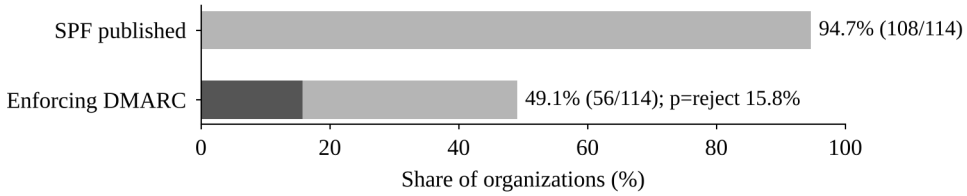


Figure 1: Declaring Versus Enforcing. SPF published (108/114) against any enforcing DMARC policy (56/114); the darker segment is p=reject (18/114).

4. Discussion

4.1. Comparison With Companion Studies

Figure 2 places this result beside four companion papers that report the same measure.[5–8] The interval for registered investment advisers overlaps none of the other four. The earlier veterinary and insurance papers used search-compiled frames of smaller firms, while this paper and its two companions draw at random from regulator rosters. The comparison therefore sets different populations and methods of sampling side by side. It is descriptive, by interval overlap only, and it does not describe a trend.

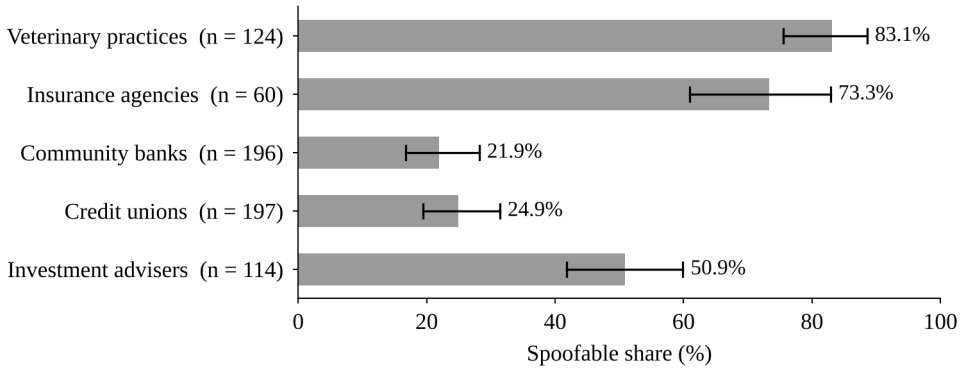


Figure 2: Spoofable Share Across Five BTI Working Papers, with 95% Wilson Intervals. The veterinary and insurance studies are pooled across their frames.

4.2. Implications for Practice

An adviser that has not yet moved to an enforcing policy can do so with a single DNS change, after a short monitoring period at p=none to confirm that its legitimate senders, including custodian and CRM platforms, align. The measurement reported here is the same one that any client, or any attacker, can read from outside the adviser.

5. Limitations

Our analysis has five limitations. First, published DNS is a proxy for deployed behavior. A domain without an enforcing policy may still filter inbound mail, and the measure concerns mail that claims the adviser’s domain, not mail the adviser receives. Second, we do not measure DKIM, which is outside the scope of a passive measurement. Third, we take the registrable domain derived from the website field as the mail domain, so an adviser that sends from a different domain is measured on its website domain.

Fourth, the website field in the frame often holds a social-media profile and not the adviser’s own domain. Under the pre-registered rule we excluded those 79 draws and did not replace them, which leaves 114 advisers measured and a wider interval. If advisers that list a profile differ from those that list their own domain, the level reported here describes the latter. Fifth, the regulator data are as of the dates stated in the frame.

6. Conclusion

Clients of a registered investment adviser act on email that appears to come from the adviser, and a published DMARC policy is the control that tells receiving servers whether to refuse a message that falsely claims the adviser’s domain. In a random sample from the SEC roster, with the method and the sample set before any data was collected, about half of the registered investment advisers measured publish no enforcing DMARC policy, and fewer than one in six has reached p=reject. Advisers sit well above community banks and credit unions on this measure, with an interval that overlaps none of the other sectors studied.

These results describe published records and not the handling of mail, and they describe advisers whose website on file is their own domain. For an adviser without an enforcing policy, they suggest that the exposure may be closed with a single DNS change after a short period of monitoring.

References

1. Kucherawy, M. and Zwicky, E. (2015). Domain-based Message Authentication, Reporting, and Conformance (DMARC). RFC 7489. Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc7489

2. Kitterman, S. (2014). Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1. RFC 7208. Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc7208

3. Arends, R. et al. (2005). DNS Security Introduction and Requirements. RFC 4033, with RFC 4034 and RFC 4035. Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc4033

4. Wilson, E. B. (1927). Probable Inference, the Law of Succession, and Statistical Inference. Journal of the American Statistical Association, 22(158). https://doi.org/10.1080/01621459.1927.10502953

5. Bridgham Technology Institute. (2026). Email Spoofability Across Veterinary Practices. BTI Working Paper 319-26. https://bridghaminstitute.com/research/working-papers/319-26

6. Bridgham Technology Institute. (2026). Email Spoofability Across Insurance Agencies. BTI Working Paper 320-26. https://bridghaminstitute.com/research/working-papers/320-26

7. Bridgham Technology Institute. (2026). Email Spoofability Across Community Banks. BTI Working Paper 321-26. https://bridghaminstitute.com/research/working-papers/321-26

8. Bridgham Technology Institute. (2026). Email Spoofability Across Credit Unions. BTI Working Paper 322-26. https://bridghaminstitute.com/research/working-papers/322-26

Disclaimer

This report is published by Bridgham Technology Institute for informational and analytical purposes only. It does not constitute investment advice, legal counsel, or a solicitation of any kind. The method and the sample were set before any data was collected. The measurement is passive and uses public DNS only; no mail was sent and no adviser was contacted. Results are reported in aggregate, and no per-adviser result is published. The method and aggregate data are open. Reproduction or redistribution of this report, in whole or in part, requires attribution to Bridgham Technology Institute. For questions regarding methodology or data, contact headofresearch@bridghamcyber.com.