BRIDGHAM TECHNOLOGY INSTITUTE
**BTI WORKING PAPER 322-26**

# Email Spoofability Across Credit Unions: A Pre-Registered Passive Measurement of DMARC Enforcement in a Random Draw of 200 Federally Insured Credit Unions

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/322-26

# Email Spoofability Across Credit Unions: A Pre-Registered Passive Measurement of DMARC Enforcement in a Random Draw of 200 Federally Insured Credit Unions

Bridgham Technology Institute*

November 2026

**Abstract:** Members of a credit union act on email that appears to come from the credit union, and the credit union's published DMARC policy determines whether a receiving mail server is told to refuse a message that falsely claims its domain. We measure the published email-authentication records of 200 credit unions sampled at random from the regulator's public roster, using only public DNS and contacting no one. Of the 197 credit unions that were mail-active and on their own domain, 49 (24.9%, 95% Wilson interval [19.4, 31.4]), about 1 in 4, publish no enforcing DMARC policy, which means a message that did not originate with the credit union can still reach a member's inbox appearing to come from it. Strict protection (p=reject) is present at 63 of the 197 credit unions (32.0%). SPF is published at 100.0% and DNSSEC is signed at 19.3%. The method and the sample were set before any data was collected, and the result is published as measured. For the credit unions 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, credit unions, pre-registration, random sample

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

## 1. Introduction

Credit unions hold member account and payment data, and members act on email that appears to come from the credit union: a loan document, a fraud alert, a request to verify an account. Email authentication is the public, checkable control that decides whether a receiving mail server can refuse a message that falsely claims the credit union'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] A credit union that publishes an enforcing DMARC policy instructs receivers to set such a message aside or to refuse it. A credit union 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 credit unions as a group.

In this paper, we measure the share of credit unions that publish no enforcing DMARC policy. We take a random draw of 200 credit unions from the public roster of the National Credit Union Administration (NCUA), limited to federally insured credit unions with total assets of $250 million to $10 billion, and we read each credit union'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 credit union was contacted. Each share is reported with a 95% Wilson score confidence interval (CI).[4]

We document three main findings. First, 49 of the 197 credit unions measured (24.9%, 95% CI [19.4, 31.4]) publish no enforcing DMARC policy. Second, declaring senders is more common than enforcing, and enforcement often stops short of the strictest policy. All 197 credit unions publish SPF (100.0%), 148 (75.1%) publish an enforcing DMARC policy, and 63 (32.0%) publish the strictest policy, p=reject. Third, the interval for credit unions overlaps the interval for community banks, and it does not overlap the intervals for veterinary practices, insurance agencies or registered investment advisers 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 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 a credit union. Section 5 states the limitations, and Section 6 concludes.

## 2. Method

### 2.1. Sampling Frame

The frame holds federally insured credit unions with total assets of $250 million to $10 billion and a published website, located in the 50 states or the District of Columbia. We took it from the NCUA quarterly call-report files, with data as of June 30, 2026.

### 2.2. Draw

We ordered each eligible row by the SHA-256 hash of the seed (20261004) 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 credit union. 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 197 of the 200 credit unions drawn. Three had no MX record, which means they were not mail-active, and they are counted in no denominator.

### 2.6. Independent Reproduction

Two checks agreed with the measurement. 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 agreed with the first on every field for all 197 domains.

## 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 197 credit unions, 49 (24.9%, 95% CI [19.4, 31.4]) publish no enforcing DMARC policy. Four of the 49 publish no DMARC record at all, 44 publish a record at p=none, and 1 publishes a record that does not parse. An enforcing policy is present at 148 of the 197 credit unions (75.1%), and strict protection (p=reject) at 63 of the 197 (32.0%). Among the enforcing records, 6 apply the policy to less than 100% of failing mail.

| Measure | k/n | Share | 95% CI |
|---|---|---|---|
| No enforcing DMARC (spoofable) | 49/197 | 24.9% | [19.4, 31.4] |
| Any enforcing policy | 148/197 | 75.1% | [68.6, 80.6] |
| p=reject | 63/197 | 32.0% | [25.9, 38.8] |
| SPF published | 197/197 | 100.0% | [98.1, 100.0] |
| DNSSEC signed | 38/197 | 19.3% | [14.4, 25.4] |

*Table 1: Email-Authentication Measures Across 197 Credit Unions, with 95% Wilson Score Intervals.*

| DMARC state | Count | Share | Classification |
|---|---|---|---|
| No record | 4 | 2.0% | Spoofable |
| p=none | 44 | 22.3% | Spoofable |
| Unparseable | 1 | 0.5% | Spoofable |
| p=quarantine | 85 | 43.1% | Protected |
| p=reject | 63 | 32.0% | Strictly protected |

*Table 2: Published DMARC Policy Across 197 Credit Unions.*

### 3.2. Declaring Versus Enforcing

SPF, which declares the servers permitted to send for a domain, is universal in this sample (100.0%). An enforcing DMARC policy, which instructs receivers to act on a message that fails that check, is present at 75.1%, and p=reject at 32.0% (Figure 1). More credit unions enforce at p=quarantine (43.1%) than at p=reject.

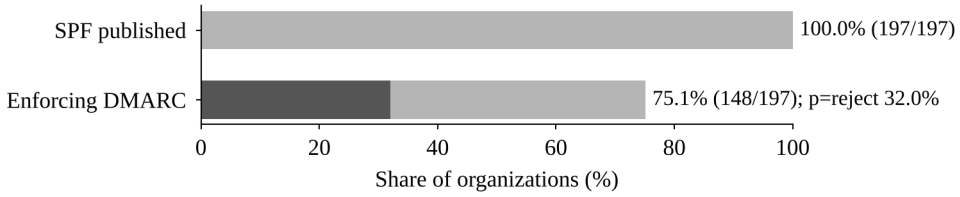



*Figure 1: Declaring Versus Enforcing. SPF published (197/197) against any enforcing DMARC policy (148/197); the darker segment is p=reject (63/197).*

## 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 credit unions overlaps the interval for community banks. It does not overlap the intervals for veterinary practices, insurance agencies or registered investment advisers. 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.

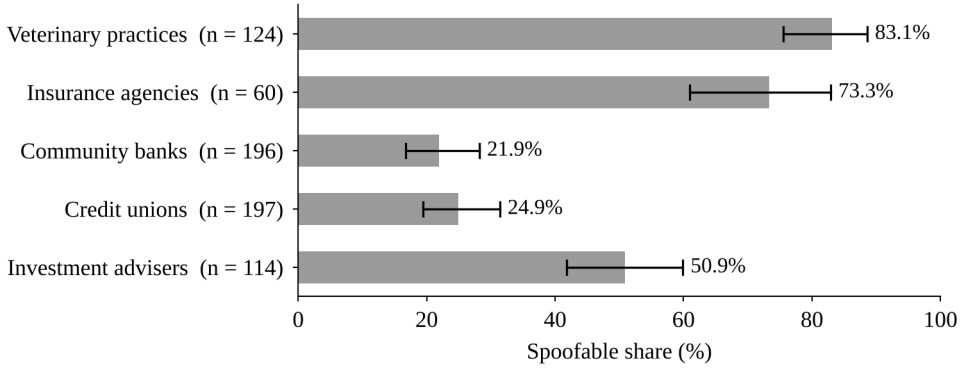



*Figure 2: Spoofable Share Across Five BTI Working Papers, with 95% Wilson Intervals. The veterinary and insurance studies are pooled across their frames.*

### 4.2. Implications for Practice

A credit union 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 core-processor and statement vendors, align. The measurement reported here is the same one that any member, or any attacker, can read from outside the credit union.

## 5. Limitations

Our analysis has four 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 credit union’s domain, not mail the credit union 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 a credit union that sends from a different domain is measured on its website domain. Fourth, the regulator data are as of the dates stated in the frame.

## 6. Conclusion

Members of a credit union act on email that appears to come from the credit union, and a published DMARC policy is the control that tells receiving servers whether to refuse a message that falsely claims the credit union’s domain. In a random sample from the NCUA roster, with the method and the sample set before any data was collected, about one in four credit unions publishes no enforcing DMARC policy, although every credit union measured publishes SPF. The level is close to that of community banks, and most enforcing credit unions stop at p=quarantine rather than p=reject.

These results describe published records and not the handling of mail. For a credit union 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 Registered Investment Advisers. BTI Working Paper 323-26. https://bridghaminstitute.com/research/working-papers/323-26

## 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 institution was contacted. Results are reported in aggregate, and no per-institution 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.