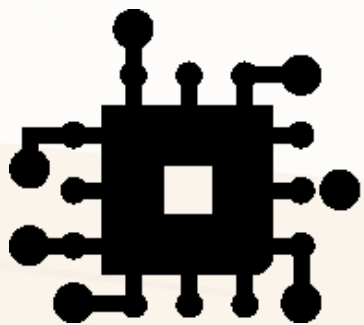
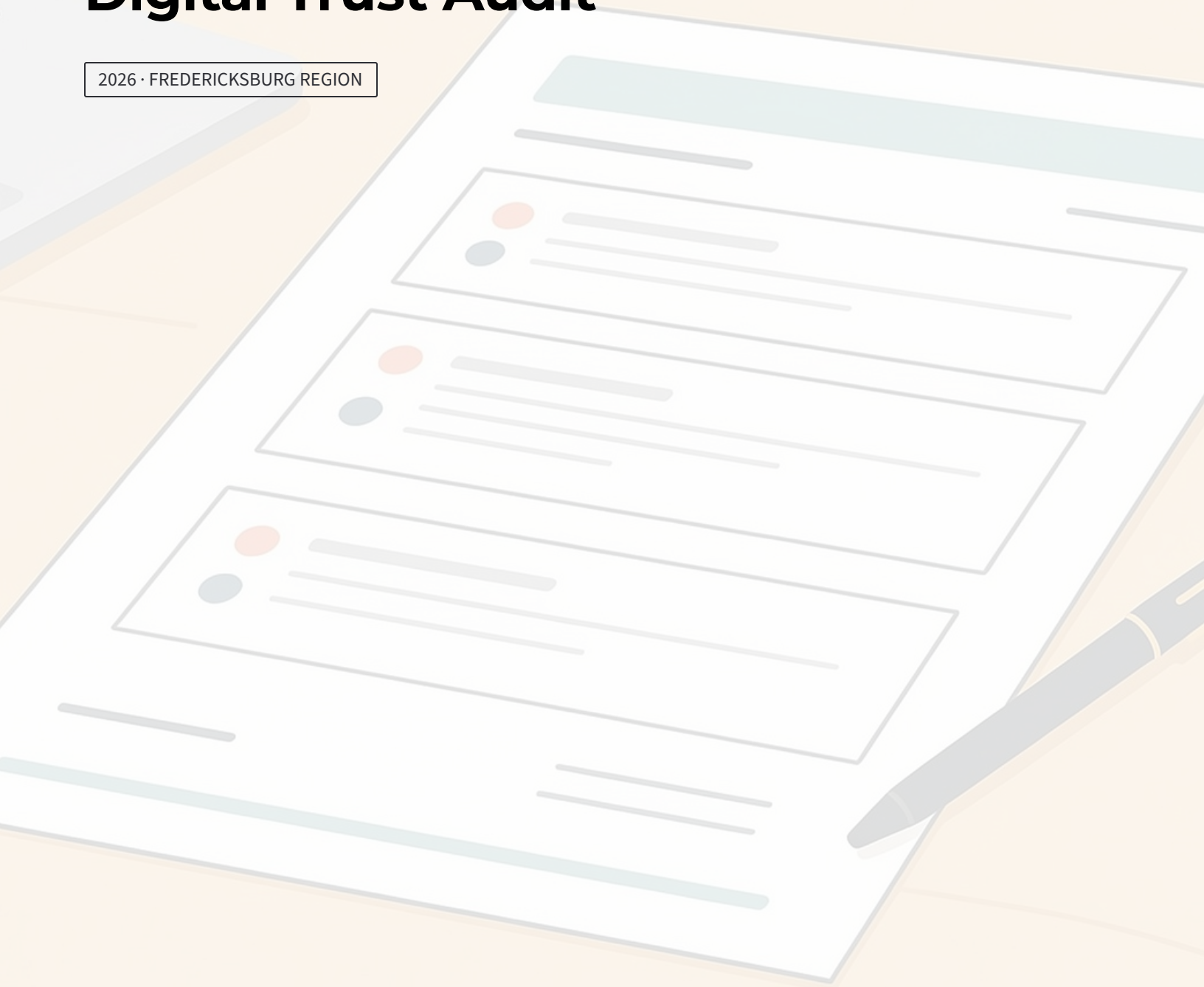




ENUCLEA

Digital Trust Audit

2026 · FREDERICKSBURG REGION



What was measured

This briefing reports public email-authentication posture across 629 unique local small-to-midsize businesses in the Fredericksburg region. Fortune 500 chains, duplicate regional-bank branches, and government agencies were separated from the community scorecard. Each entity is bound to one primary sending domain. The unit of analysis is the published DNS identity of that domain, not an internal network review.

UNIVERSE

629 unique local SMBs

SOURCE

Chamber regional list

CONTROLS

SPF · DKIM · DMARC · DNSBL

ACCESS

Public DNS only

Acronym Definitions

SPF (Sender Policy Framework) — publishes which mail servers are authorized to send on behalf of a domain

DKIM (DomainKeys Identified Mail) — cryptographically signs outbound mail so recipients can verify it was not altered in transit

DNSBL (DNS Blocklist) — a real-time list of IP addresses known to send spam or malicious mail; a hit indicates reputation damage

DMARC (Domain-based Message Authentication, Reporting & Conformance) — ties SPF and DKIM together and tells receiving servers what to do with mail that fails both checks

p=none — monitoring mode only; failing mail is still delivered

p=quarantine — failing mail is sent to spam/junk

p=reject — failing mail is blocked entirely; the strongest enforcement level

How the scores are read

Scoring methodology

Scores come from non-intrusive interrogation of public DNS: SPF authorization, DKIM selector presence, DMARC policy, and — in this run — DNSBL / IP reputation (blocklist checks) where an outbound identity was visible. 'Enforced' means a DMARC policy of p=quarantine or p=reject. A record of p=none is monitoring, not protection. No mail was sent to or from audited domains. No mailbox was accessed. No private system was in scope. This is intentional — the audit is bounded by public DNS and respects the line between observable identity and private infrastructure. The snapshot is point-in-time. Where no DKIM selector was advertised, domains were checked against a common selector dictionary — results reflect an educated estimate, not a confirmed absence.

How to read a sector page

Each sector page holds the same instruments: headcount, mean, median, enforcement rate, missing DMARC, missing DKIM, and the fault that defines the vertical. "Why it matters" is the business-risk path for that vertical. "Why the data looks different" is the operating reason the numbers diverge from the regional mean — vendor mix, tenant type, who owns DNS, and whether the firm's real sending fleet is aligned. Individual private businesses are not named.

Grade scale

Score Range	Grade	Trust Classification
95–100	A+	Precise (High Trust)
90–94	A	Robust (High Trust) *Recommended Goal
75–89	B	Good (Moderate Protection)
60–74	C	Vulnerable (Basic Only)
45–59	D	At Risk (High Exposure)
0–44	F	Critical (No Spoofing Protection)

Scores are derived from a 100-point rubric across five weighted pillars — see the **Scoring Rubric addendum** at the end of this document for the full breakdown.

Community posture is a C+.

Basic authentication is present. Spoof protection is not yet the regional default.

629

ENTITIES

unique local SMBs · providers held out

68.1

MEAN / MEDIAN

Mean 68.1 · Median 67.0 · -11.9 vs Good (80)

C+

GRADE

basic auth / monitoring

27.2%

ENFORCED

72.8% open or inactive

What the region shows

Across 629 unique local entities the community mean is 68.1 and the median is 67.0. That is a tight center: most firms are neither catastrophically unconfigured nor fully enforced. Only 27.2% publish an enforcing DMARC policy. The rest can still be impersonated with a lookalike From line that surviving filters will treat as ordinary local mail.

The sector spread is orderly, not random. Technology & Defense and Financial Services sit above the line because tenant quality and regulatory pressure pull authentication forward. Construction, professional services, and hospitality sit below it because DNS is nobody's job and extra senders are unsigned. General Commercial, at 313 firms and a 68.0 mean, is the gravitational center of the study.

Providers were measured on the same instruments and kept out of the community mean so they would not inflate it.

How to use the pages that follow

Read each sector as an operating system, not a leaderboard. The interesting question is not "who scored lowest." It is why a vertical with the same public DNS toolkit produces a different enforcement rate. Those reasons — field-first admin, donated tenants, unsigned vendor senders, unclicked M365 DKIM — are what make a community grade movable.

IT Providers & MSPs

77.3

MEAN / MEDIAN

Mean 77.3 · Median 78 · +9.2 vs 68.1

42%

ENFORCING

8 of 19 quarantine or reject

26%

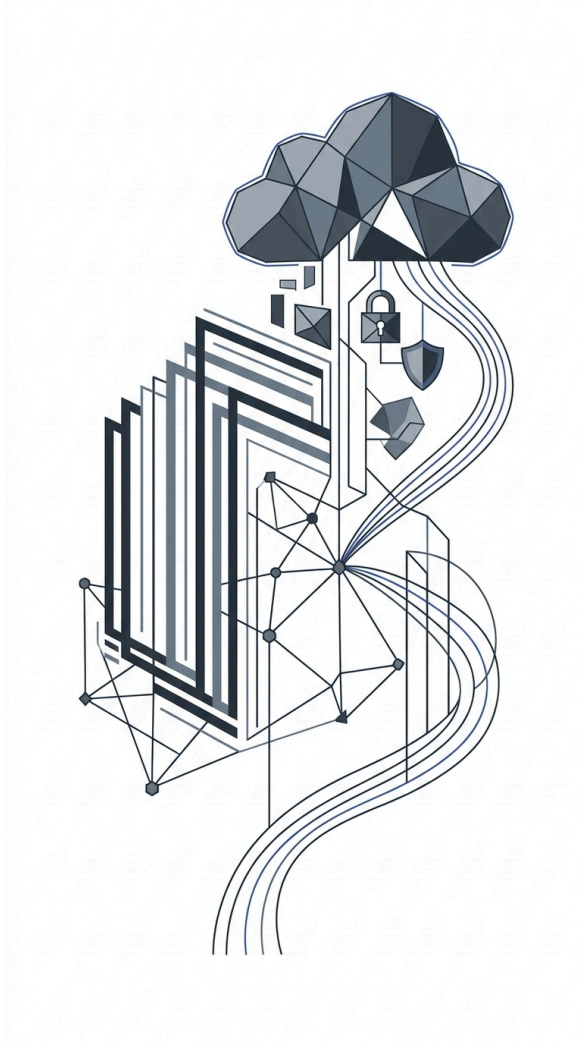
NO DMARC

5 of 19 no policy published

11 of 19

OPEN TO SPOOF

p=none or no DMARC



Why it matters

- Every business in this study is a downstream client of an IT provider — their posture sets the floor for the region
- A spoofed or impersonated MSP domain is a master key: clients accept email from their provider without question
- Fake invoices, remote-access requests, and credential resets sent from a trusted IT domain convert at the highest rate of any vertical

Why the data looks different

- Highest mean in the region (77.3) — providers who sell security tend to practice it
- 42% enforcement rate is strong but leaves 11 of 19 domains open to impersonation
- Gap is not tooling: MSPs live on M365 or similar — DMARC enforcement is a policy decision, not a product gap

Technology & Defense

76.0

MEAN / MEDIAN

Mean 76.0 • Median 80 • +7.9 vs 68.1

40%

ENFORCING

10 of 25 quarantine or reject

32%

NO DMARC

8 of 25 no policy published

16%

DNSBL LISTED

reputation hits observed



Why it matters

- Proximity to Quantico, Dahlgren, and federal primes makes email a high-value attack surface
- Spoofed domains mimic familiar program managers, not spam
- Invoices, visit requests, and CUI-adjacent files routinely exchanged over email

Why the data looks different

- Most firms on M365 or Google Workspace — tooling is already present
- Gap is enforcement, not capability: 32% publish no DMARC; 16% show DNSBL hits
- High mean coexists with an open impersonation window due to uneven policy

Financial Services



73.1

MEAN / MEDIAN

Mean 73.1 · Median 77 · +5.0 vs 68.1

47.5%

ENFORCING

29 of 61 quarantine or reject

27.9%

NO DMARC

17 of 61 no policy published

41%

MISSING DKIM

unsigned outbound mail

Why it matters

- Wiring details, tax documents, and "updated banking" notes routinely exchanged over email
- BEC in this vertical is a funds-out problem, not a brand problem
- Local wealth managers, credit unions, and accounting firms are prime targets

Why the data looks different

- Regional enforcement leader at 47.5% — regulatory culture and core processor pressure pull the mean up
- 41% still send without DKIM; secondary senders (newsletters, billing portals) often never aligned to firm domain
- Ahead on policy, behind on complete sender inventory

Non-Profit & Community



68.5

MEAN / MEDIAN

Mean 68.5 · Median 65 · +0.4 vs 68.1

18.2%

ENFORCING

6 of 33 quarantine or reject

45.5%

NO DMARC

15 of 33 no policy published

45.5%

MISSING DKIM

unsigned outbound mail

Why it matters

- Forged appeal mail and fake board messages convert because audiences want to help
- Lookalike invoice requests target food banks and civic groups
- Donor, volunteer, and grant-officer trust makes the domain a moral credential — and a high-value target

Why the data looks different

- Only 18.2% enforce DMARC; 45.5% have no policy at all
- Many orgs inherit donated Workspace tenants, volunteer DNS admins, or email "set up in 2018"
- Score is average because the mailbox works — nobody owns the DNS records that make it trustworthy

Healthcare & Medical



68.1

MEAN / MEDIAN

Mean 68.1 · Median 68 · +0.0 vs 68.1

36.8%

ENFORCING

21 of 57 quarantine or reject

42.1%

NO DMARC

24 of 57 no policy published

56.1%

MISSING DKIM

unsigned outbound mail

Why it matters

- Spoofed clinic domains used for payment diversion and billing fraud
- Patients cannot distinguish a real clinic from a lookalike domain
- Medical mail creates HIPAA-adjacent confusion even without PHI in the body

Why the data looks different

- 56.1% lack DKIM; 42.1% have no DMARC despite high domain ownership
- Practice-management and patient-messaging vendors send as the clinic without aligned signatures
- DNSBL at 21.1% (second-worst in study) reflects mixed sending infrastructure

General Commercial

68.0

MEAN / MEDIAN

Mean 68.0 · Median 67 · -0.1 vs 68.1

25.9%

ENFORCING

81 of 313 quarantine or reject



39.3%

NO DMARC

123 of 313 no policy published

49.5%

MISSING DKIM

unsigned outbound mail

Why it matters

- Quotes, invoices, and shipping updates sent from unprotected domains
- First point of contact for most customers in the region — community trust is set here
- Lookalike domains indistinguishable from legitimate local businesses

Why the data looks different

- 49.5% missing DKIM reflects domains stood up once and never revisited
- DNS treated as a website setting rather than an identity control
- Distribution is residue, not strategy — moving this cohort moves the regional grade

Construction & Trades

65.5

MEAN / MEDIAN

Mean 65.5 • Median 65 • -2.6 vs 68.1

13.6%

ENFORCING

6 of 44 quarantine or reject

52.3%

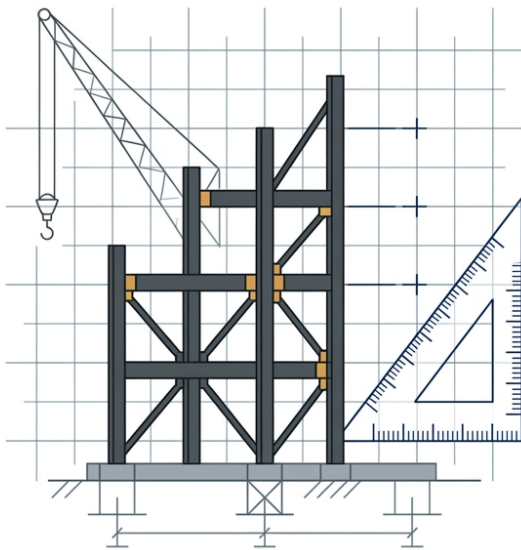
NO DMARC

23 of 44 no policy published

22.7%

DNSBL LISTED

worst rate in the study



Why it matters

- Draw requests, change orders, and supplier invoices are routine wire events
- Invoice-swap and account-takeover fraud thrive on large, expected payments
- Office function often one bookkeeper — minimal oversight on transactions

Why the data looks different

- Lowest DMARC enforcement in the study (13.6%); worst DNSBL rate (22.7%)
- Field-first model: Gmail for the owner, custom domain on the truck wrap, no DNS owner
- Identity layer was never part of the job — payment-heavy process left unprotected

Professional Services (Legal / CPA)



65.0

MEAN / MEDIAN

Mean 65.0 · Median 67 · -3.1 vs 68.1

17.5%

ENFORCING

10 of 57 quarantine or reject

36.8%

NO DMARC

21 of 57 no policy published

61.4%

MISSING DKIM

widest signing gap in high-trust sector

Why it matters

- Attorneys and CPAs sell confidentiality — clients treat firm email as authoritative
- Engagement letters, filings, and settlement instructions accepted on letterhead alone
- Unsealed mail is a professional-identity failure, not a technical footnote

Why the data looks different

- DKIM the critical fault: 61.4% send unsigned despite most firms already on M365
- Control is a checkbox that was never turned on — not a missing product
- DNSBL best in study (12.3%): trusted senders running clean reputation without a seal

Hospitality, Dining & Retail



63.7

MEAN / MEDIAN

Mean 63.7 · Median 65 · -4.4 vs 68.1

20.5%

ENFORCING

8 of 39 quarantine or reject

51.3%

NO DMARC

20 of 39 no policy published

64.1%

MISSING DKIM

widest sealing gap in the study

Why it matters

- Reservations, gift-card, and invoice messages are high-conversion lures against venues
- Lookalike domains easy to believe given public-facing brands and high staff turnover
- Unsigned mail puts customer trust and payment data at risk

Why the data looks different

- Lowest mean in region; 64.1% missing DKIM is the widest sealing gap in the study
- POS, reservation, and marketing platforms often send as the venue without alignment
- Low DNSBL (10.3%) reflects low send volume — an unsigned storefront, not a burned reputation

Free-mail is a second, stable failure.

17.4% of the wider chamber set still use consumer or ISP mail as a public business identity.



What it is

- A separate identity failure from missing DMARC — the domain itself is absent
- Concentrates in trades, salons, and owner-operated services
- Consistent with the March 2026 Stafford baseline of 18.1% — this figure is stable, not improving

728

CHAMBER IDENTITIES

wider set including chains and agencies

127

FREE-MAIL USERS

17.4% of the wider chamber set

79

PURE FREE-MAIL

Gmail, Verizon, or similar as primary

48

SHADOW-MAIL

own a domain, publish free-mail for inquiries

Why it matters

- A DMARC record on a domain nobody uses does not fix a Gmail address on the truck wrap
- Free-mail identities cannot be authenticated, monitored, or enforced against
- The business is invisible to any email-security tooling the recipient deploys

All sectors against the regional mean

IT Providers & MSPs lead the region — and 11 of 19 are still open to impersonation. The top of the table is not a ceiling to aspire to. It is a floor that needs raising.

Sector	Mean Score	vs Regional Mean
IT Providers & MSPs	77.3	+9.2
Tech & Defense	76.0	+7.9
Financial Services	73.1	+5.0
Non-Profit	68.5	+0.4
Regional Mean	68.1	—
Healthcare	68.1	+0.0
General Commercial	68.0	−0.1
Construction	65.5	−2.6
Legal / CPA	65.0	−3.1
Hospitality & Retail	63.7	−4.4

The bulk of the work is in the middle. Five sectors sit within four points of 68.1 — close enough that a single policy change moves the regional grade. But no sector, including the leaders, has closed the impersonation window.

What holds, and what to do with it

The region is configured, not enforced.

A 68.1 mean with 27.2% enforcement means most domains can send mail and most domains can still be forged. Monitoring records and missing DKIM are the common state, not the exception.

Sector gaps follow operations, not slogans.

Construction is a payment-path problem. Legal and CPA is an unclicked DKIM problem. Healthcare is an unaligned vendor-sender problem. Hospitality is an unsigned storefront. Treat them as different jobs.

General Commercial sets the grade.

At 313 of 629 entities, this cohort is the community. If only the regulated and defense-adjacent firms harden DNS, the regional number will not move.

Free-mail is a second, stable failure.

17.4% of the wider chamber set still use consumer or ISP mail as a public identity. That figure matched Stafford's 18.1% in March. It will not be fixed by a DMARC record on a domain nobody uses.

The lift is DNS, not capital.

SPF, DKIM, a DMARC record at p=none, two weeks of reports, then quarantine or reject. The same three steps apply to every page in this book. The sector narratives only change why the owner should care this week.

Domain check enuclea.com/email-security-check

Research Enuclea · Stafford, Virginia

Addendum: Scoring Rubric

Each domain is scored across five positive pillars (max 100 pts) with deductions applied for broad sending scope and blocklist presence. The final score is clamped between 0 and 100.

What adds points

Pillar	Points
Domain Identity ¹	+35
DMARC Enforcement	+25
Reverse DNS / Infrastructure	up to +15
SPF Record & Hygiene	up to +15
DKIM Validity	+10

What removes points

Condition	Penalty
Broad SPF network block (>/28) — more IPs than a typical business needs authorized	−5
Large authorized IP range (>4,096)	−10
Excessive IP range (>65,536)	−20
IP listed on DNSBL blocklist	−15

Partial credit is awarded within each pillar based on configuration quality — e.g. `p=none` with reporting earns +10 of the available +25 for DMARC. The final score is clamped between 0 and 100.

¹ Domain Identity measures whether the business operates on a dedicated custom domain (e.g. `acmeplumbing.com`) or relies on a free consumer address (e.g. Gmail, Yahoo). A custom domain is the prerequisite for all other authentication controls — without it, SPF, DKIM, and DMARC cannot be meaningfully applied.