VAIXUS

Technologies

VAIXUS-CS-002

# Multi-Provider Enterprise Authentication Assessment

*A Laboratory-Engineered Consulting Simulation — Post-Acquisition Email Infrastructure*

Prepared for: Meridian Fintech Group (Synthetic Engagement)
Prepared by: Vaixus Technologies
Publication Date: July 3, 2026
Document Version: 1.0
Classification: Laboratory Simulation — Public Portfolio Use

**LABORATORY-ENGINEERED CONSULTING SIMULATION**

This report is a fictional, laboratory-generated case study prepared for portfolio and methodology-demonstration purposes. It does not describe a real client, a real organization, or an actual engagement.

# Confidentiality Notice

This document is a laboratory-engineered consulting simulation produced by Vaixus Technologies for portfolio, training, and methodology-demonstration purposes. All organization names, personnel, domains, IP addresses, DNS records, SMTP transcripts, authentication results, and engineering findings contained within this document are entirely synthetic and were constructed within a controlled laboratory environment. No portion of this report describes, references, or was derived from any real organization's infrastructure, personnel, or confidential information.

This report does not represent an actual client engagement. Vaixus Technologies has not been retained by, and has no business relationship with, any organization resembling the fictional entity described herein. Any resemblance to an actual organization, domain, or individual is coincidental and unintended.

Where this document is distributed for evaluative purposes (e.g., prospective client discovery, recruiting, or partner review), it should be treated as a demonstration of Vaixus Technologies' consulting methodology, technical documentation standard, and analytical approach — not as evidence of prior client work or measured business outcomes.

If adapted as a template for an actual client engagement, all synthetic evidence contained in this document must be replaced in its entirety with verified production evidence before delivery, and this notice must be revised to reflect the real engagement's confidentiality requirements.

# Document Control

| Field | Value |
|---|---|
| Document Title | VAIXUS-CS-002 — Multi-Provider Enterprise Authentication Assessment |
| Document Version | 1.0 |
| Publication Date | July 3, 2026 |
| Prepared By | Vaixus Technologies |
| Review Status | Final — Approved for Portfolio Publication |
| Classification | Laboratory Simulation — Public Portfolio Use |
| Engagement Type | Laboratory-Engineered Consulting Simulation |

### Revision History

| Version | Date | Author | Summary of Changes |
|---|---|---|---|
| 0.1 | June 15, 2026 | Soorya S V | Initial discovery findings drafted following environment reconnaissance. |
| 0.7 | June 26, 2026 | Soorya S V | Technical findings and remediation roadmap completed; internal engineering review. |
| 1.0 | July 3, 2026 | Soorya S V | Final release following documentation and executive review. |

# Table of Contents

**Confidentiality Notice** ..... 2
**Document Control** ..... 3
**Table of Contents** ..... 4
**1. Executive Summary** ..... 5
**2. Environment Overview** ..... 6
**3. Assessment Scope** ..... 7
**4. Infrastructure Architecture** ..... 8
**5. Assessment Methodology** ..... 9
**6. Executive Findings Summary** ..... 10
**7. Detailed Technical Findings** ..... 11
**8. Risk Prioritization** ..... 22
**9. Business Impact Analysis** ..... 23
**10. Remediation Strategy** ..... 24
**11. Verification Plan** ..... 25
**12. Final Assessment** ..... 25
**13. References** ..... 26
**14. Technical Appendix** ..... 26
**A. Full DNS Record Set (Synthetic Laboratory Environment)** ..... 26
**B. Sample Authentication-Results Header (SES Trace Test)** ..... 27
**C. Command Output — SPF Lint (Post-Remediation, Simulated)** ..... 28
**D. Vendor Configuration Inventory** ..... 28

# 1. Executive Summary

Meridian Fintech Group (“Meridian”) engaged Vaixus Technologies to assess its email authentication posture following three acquisitions completed over the past four years, each of which introduced its own email infrastructure, DNS conventions, and sending platform into the Meridian environment without a unifying integration standard. Meridian's IT leadership sought an independent inventory of what its combined DNS and authentication footprint actually looks like today, following an internal audit finding that no single team could produce a complete list of authorized senders for the organization's root domain.

The assessment covered Meridian's root domain (Microsoft 365, corporate correspondence), the Google Workspace tenant retained from the LedgerPay acquisition, Amazon SES and SendGrid transactional streams, a legacy Mailgun integration inherited from the QuickTerm Lending acquisition, a developer-platform integration on Resend, and HubSpot marketing sending — seven distinct sending identities sharing a single root DNS zone.

Vaixus identified thirteen findings. Two are rated Critical: the root domain's SPF record has accumulated includes from every vendor onboarded since Meridian's first acquisition and now exceeds the RFC 7208 ten-lookup limit, and a Mailgun-authenticated sending stream inherited from the decommissioned QuickTerm Lending platform continues to deliver monthly account statements to a small population of legacy customers with no assigned internal owner, no monitored bounce or complaint dashboard, and a corporate payment method nearing expiration. Both findings are direct consequences of inorganic growth outpacing DNS and vendor governance, a pattern reflected throughout this report.

This assessment finds no evidence of active compromise or unauthorized access. Every finding traces to the absence of a unifying sender-governance model across four merged organizations. Vaixus recommends establishing a centralized authorized-sender inventory as the foundational remediation step, from which the DNS, alignment, and ownership findings in this report can be resolved in a coordinated sequence rather than the ad hoc, per-team basis that produced the current state.

### Infrastructure Maturity Snapshot

| Dimension | Current State | Target State |
|---|---|---|
| Sender Inventory | No centralized record; senders discovered ad hoc per team | Single authoritative inventory covering all sending identities |
| Authentication Coverage | Root SPF in PERMERROR; DKIM alignment inconsistent across streams | SPF valid on all domains; DKIM alignment verified for every stream |
| Post-Acquisition Integration | Subsidiary domains retain pre-acquisition policy and key material | Unified DKIM rotation cadence and DMARC policy across all domains |
| Vendor Ownership | One legacy vendor relationship has no assigned internal owner | Every sending identity has a named owner and review cadence |

# 2. Environment Overview

Meridian Fintech Group is a payments and lending infrastructure provider headquartered in Chicago, Illinois, with approximately 1,200 employees. Meridian's current footprint is the product of three acquisitions completed over the past four years: LedgerPay (payments processing, acquired two years ago and still operating on its pre-acquisition Google Workspace tenant), QuickTerm Lending (a consumer lending platform acquired four years ago and decommissioned eight months ago, with a small residual customer-communication obligation), and a developer-tools acquisition that introduced Meridian's current engineering organization and its independently selected transactional and developer-notification vendors.

Corporate correspondence for the parent organization is served by Microsoft 365 on the root domain, meridianfg.com. Each acquired or newly built business unit layered its own sending platform on top of this shared root DNS zone: LedgerPay retained Google Workspace on a subsidiary domain; Engineering adopted Amazon SES for product notifications and, more recently, Resend for developer-platform alerts; Finance uses SendGrid for billing correspondence; the residual QuickTerm obligation is served by a Mailgun integration; and Marketing uses HubSpot for lifecycle campaigns. All seven identities share Route 53 as the authoritative DNS provider for the root zone, though a subset of legacy subdomains inherited from QuickTerm's original GoDaddy-hosted DNS have not yet been fully cut over (see Finding CS002-08).

### Infrastructure Inventory

| Component | Platform / Vendor | Function |
|---|---|---|
| Root Domain | meridianfg.com | Corporate mail, brand identity, root DNS zone |
| Corporate Mail Platform | Microsoft 365 (Exchange Online) | Employee mailboxes for parent organization |
| Subsidiary Mail — LedgerPay | Google Workspace (ledgerpay.meridianfg.com) | Payments-processing subsidiary correspondence |
| Transactional — Product | Amazon SES (app.meridianfg.com) | Product and account notifications |
| Transactional — Billing | SendGrid (billing.meridianfg.com) | Invoices and payment receipts |
| Legacy Platform Mail | Mailgun (legacy.meridianfg.com) | Residual QuickTerm Lending account statements |
| Developer Platform | Resend (developers.meridianfg.com) | API and developer-platform notifications |
| Marketing | HubSpot (marketing.meridianfg.com) | Lifecycle and demand-generation campaigns |
| DNS Provider | Amazon Route 53 (primary); legacy GoDaddy zone (partial) | Authoritative DNS — migration in progress |

No individual team disputes the legitimacy of its own sending configuration; the risk in this environment arises entirely from the absence of a cross-team view, which is the root cause connecting the majority of findings in Section 11.

# 3. Assessment Scope

## In Scope

- Root domain and all subdomain DNS records across Route 53 and the legacy GoDaddy zone
- SPF, DKIM, and DMARC configuration and alignment for all seven identified sending identities
- Post-acquisition integration state of the LedgerPay Google Workspace tenant
- Ownership and monitoring status of the legacy Mailgun (QuickTerm) sending stream
- DKIM key age and rotation cadence across all platforms
- DMARC organizational-domain and subdomain policy interaction
- Vendor onboarding governance for recently added sending platforms (Resend)

## Out of Scope

- Application security of Meridian's payments or lending platforms
- PCI-DSS or other regulatory compliance certification activity
- Internal network security and corporate firewall configuration
- Endpoint security of employee workstations
- Mail content or campaign messaging review
- Data residency or cross-border transfer analysis

This assessment is architectural and configuration-focused. It does not constitute a penetration test, a regulatory compliance audit, or a review of any Meridian product's transaction-processing security.

# 4. Infrastructure Architecture

Meridian's email architecture reflects the accretive nature of its growth: rather than a single designed system, it is seven independently configured sending identities layered onto one shared root DNS zone. Figure 1 illustrates the current relationship between these platforms and the root zone.

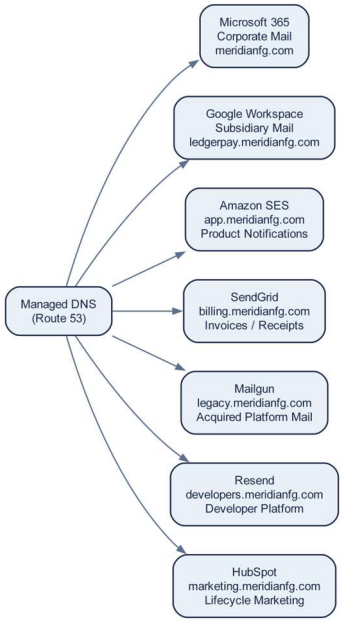


*Figure 1 — Enterprise Email Architecture*

### Domain-to-Service Mapping

| Domain / Subdomain | Sending Service | Purpose |
|---|---|---|
| meridianfg.com | Microsoft 365 | Corporate correspondence |
| ledgerpay.meridianfg.com | Google Workspace | Subsidiary correspondence |
| app.meridianfg.com | Amazon SES | Product notifications |
| billing.meridianfg.com | SendGrid | Invoices and receipts |
| legacy.meridianfg.com | Mailgun | Acquired platform mail |
| developers.meridianfg.com | Resend | Developer platform alerts |
| marketing.meridianfg.com | HubSpot | Lifecycle marketing |

Figure 2 shows the ownership overlay across these platforms: no two sending identities share the same internal owning team, which is a primary contributor to the governance findings detailed in Section 11.

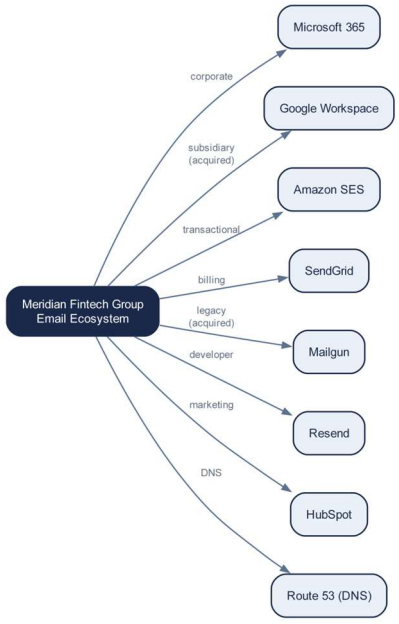


*Figure 2 — Vendor Relationship Diagram*

# 5. Assessment Methodology

Vaixus applied its standard five-stage methodology, adapted for a multi-entity, post-acquisition environment.

- Discovery Workshop — structured interviews across IT, Engineering, Finance, and Marketing to reconstruct an as-built sender inventory, since no consolidated record existed at engagement start.
- Passive DNS Reconnaissance — authoritative-record enumeration across the Route 53 zone and residual GoDaddy-hosted legacy zone to establish the complete as-built configuration.
- Authentication Trace Testing — controlled test messages sent through each of the seven identified sending identities, with full header capture and Authentication-Results inspection, including explicit SPF/DKIM alignment analysis under both relaxed and strict DMARC modes.
- Vendor and Ownership Review — direct review of Microsoft 365, Google Workspace, Amazon SES, SendGrid, Mailgun, Resend, and HubSpot configuration, cross-referenced against internal ownership records (or their absence).
- Findings Synthesis and Executive Readout — consolidation into severity-rated, business-impact-aligned recommendations presented to Meridian's CTO and Head of IT Governance.

All engineering evidence referenced in this report was captured during reconnaissance and trace-testing and is reproduced in the Technical Appendix.

# 6. Executive Findings Summary

Vaixus identified thirteen findings: two Critical, two High, six Medium, two Low, and one Informational.

| ID | Finding | Category | Severity |
|---|---|---|---|
| CS002-01 | Root domain SPF exceeds 10-lookup limit (6 vendor includes) | DNS / Authentication | Critical |
| CS002-02 | Orphaned Mailgun stream from decommissioned QuickTerm platform | Vendor Governance | Critical |
| CS002-03 | LedgerPay subsidiary DMARC (p=none) overrides parent policy | Post-Acquisition Integration | High |
| CS002-04 | SES transactional mail has no SPF alignment path (DKIM-only) | Authentication | High |
| CS002-05 | Marketing subdomain has no explicit DMARC record | Authentication | Medium |
| CS002-06 | Resend onboarded without vendor review; root-domain SPF include | Vendor Governance | Medium |
| CS002-07 | SendGrid Return-Path not customized; SPF alignment DKIM-only | Authentication | Medium |
| CS002-08 | Legacy GoDaddy NS delegation incomplete for subset of subdomains | DNS | Medium |
| CS002-09 | DMARC organizational record omits explicit sp= directive | Authentication | Medium |
| CS002-10 | No enterprise-wide DKIM key rotation cadence | Authentication | Medium |
| CS002-11 | SES no-reply stream lacks bounce/reply handling | Operational Risk | Low |
| CS002-12 | SES bounce/complaint visibility not shared with security | Operational Risk | Low |
| CS002-13 | No centralized authorized-sender inventory | Governance | Informational |

# 7. Detailed Technical Findings

Findings are presented in descending order of severity.

## CS002-01 — Root Domain SPF Record Exceeds RFC 7208 Ten-Lookup Limit

| | |
|---|---|
| **Severity** | **Critical** |
| **Category** | DNS / Authentication |
| **Reference** | RFC 7208 §4.6.4 |

**Evidence.**

The SPF record published at the root of meridianfg.com now includes six separate vendor mechanisms, accumulated across four years of independent onboarding by different teams, resolving to eleven total DNS lookups.

```
$ dig TXT meridianfg.com +short | grep spf1
"v=spf1 include:spf.protection.outlook.com include:amazonses.com include:sendgrid.net
  include:mailgun.org include:_spf.hubspotemail.net include:spf.resend.com ~all"

Lookup expansion:
  spf.protection.outlook.com  -> 2 nested lookups (Microsoft 365)
  amazonses.com               -> 1 nested lookup
  sendgrid.net                 -> 2 nested lookups
  mailgun.org                  -> 2 nested lookups (legacy, see CS002-02)
  _spf.hubspotemail.net        -> 2 nested lookups
  spf.resend.com                -> 2 nested lookups (see CS002-06)
  TOTAL                           = 10 nested + 1 base lookup = 11
```

**Technical Analysis.**

No single team added an unreasonable number of mechanisms; each of the four organizations now merged into Meridian added exactly one include when it onboarded its own sending platform, and the root domain accumulated all of them because no team isolated its sending onto a dedicated subdomain with its own scoped SPF record — the pattern that would have kept the root domain's lookup count low regardless of how many vendors the broader organization used.

**Business Impact.**

Every message sent from the root domain — including all Microsoft 365 corporate correspondence — is subject to unpredictable PERMERROR evaluation by strict validators, independent of which specific vendor a given recipient's mail gateway is stricter about. This is a shared-fate risk: the least-isolated sending pattern (Marketing's HubSpot mail, in this case) directly threatens the deliverability of the most business-critical stream (executive and customer correspondence via Microsoft 365).

**Recommendation.**

Migrate every non-corporate sending identity onto its own dedicated subdomain with its own scoped SPF record (a pattern already correctly followed for app.meridianfg.com, billing.meridianfg.com, legacy.meridianfg.com, developers.meridianfg.com, and marketing.meridianfg.com at the DNS-record

level) and remove all non-Microsoft-365 includes from the root domain's SPF record entirely, since root-domain mail is only ever sent via Microsoft 365.

**Verification Method.**

Confirm via SPF lint validation that the root domain resolves to two or fewer lookups following remediation, and confirm each subdomain's independently scoped SPF record continues to validate for its respective vendor.

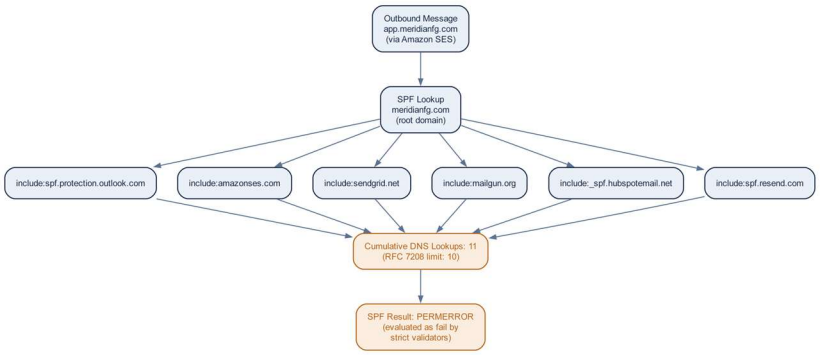


*Figure 3 — Authentication Flow: Root-Domain SPF Evaluation*

## CS002-02 — Orphaned Legacy Sending Stream From Decommissioned Acquisition

| Severity | Critical |
|---|---|
| Category | Vendor Governance |
| Reference | M3AAWG Sender Best Common Practices |

**Evidence.**

legacy.meridianfg.com remains actively authenticated via Mailgun and is used by a scheduled job, running on infrastructure predating the QuickTerm Lending acquisition, that emails monthly account statements to approximately 40 legacy customers whose loans remain in a grandfathered servicing status.

```
$ dig MX legacy.meridianfg.com +short
10 mxa.mailgun.org.
10 mxb.mailgun.org.
$ dig TXT legacy.meridianfg.com +short | grep spf1
"v=spf1 include:mailgun.org ~all"
```

**Technical Analysis.**

Interviews confirm the QuickTerm engineering team that originally built and monitored this job was dissolved following the platform's decommissioning eight months ago. No individual at Meridian currently owns the Mailgun account, monitors its bounce or spam-complaint dashboard, or has visibility into whether the scheduled job is functioning correctly beyond the absence of customer complaints. The Mailgun account's billing is charged to a corporate card set to expire within the next billing cycle, with no owner positioned to act on a renewal notice.

**Business Impact.**

Approximately 40 real customers depend on this stream for account statements; an unmonitored failure (billing lapse, bounce accumulation triggering a Mailgun account suspension, or DNS record drift) would interrupt a genuine customer-communication obligation with no internal team positioned to notice or respond quickly. The unmonitored nature of the stream also means any anomalous sending behavior (e.g., a compromised credential misusing the domain) would likely go undetected.

**Recommendation.**

Assign explicit ownership of the legacy.meridianfg.com sending stream to a named team (recommended: Customer Operations, given the customer-facing nature of the obligation), update the Mailgun account's payment method to a monitored corporate account, and enable bounce/complaint dashboard alerting to that team. In parallel, evaluate migrating the remaining 40 accounts onto a currently supported platform to allow full decommissioning of the legacy Mailgun integration.

**Verification Method.**

Confirm named ownership is documented in Meridian's service catalog, confirm updated billing method via Mailgun account review, and confirm at least one team member has active dashboard access and a defined alerting threshold within 30 days of remediation.

## CS002-03 — Subsidiary DMARC Policy Overrides and Conflicts With Parent Organization

| | |
|---|---|
| **Severity** | **High** |
| **Category** | Post-Acquisition Integration |
| **Reference** | RFC 7489 §7.1 |

**Evidence.**

ledgerpay.meridianfg.com, the Google Workspace tenant retained from the LedgerPay acquisition, publishes its own DMARC record at p=none, which — per RFC 7489's subdomain policy resolution — takes precedence over the parent organizational domain's policy for mail claiming to be from that subdomain.

```
$ dig TXT _dmarc.ledgerpay.meridianfg.com +short
"v=DMARC1; p=none;"
$ dig TXT _dmarc.meridianfg.com +short
"v=DMARC1; p=quarantine; pct=100; rua=mailto:dmarc@meridianfg.com;"
$ dig TXT google._domainkey.ledgerpay.meridianfg.com +short
"v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArP7K...[truncated]"
```

**Technical Analysis.**

This DMARC record, along with the subsidiary's original pre-acquisition DKIM selector, has not been reviewed or updated since the acquisition closed two years ago. The result is a brand-critical inconsistency: Meridian's parent domain enforces DMARC at p=quarantine, while a subsidiary domain still carrying the Meridian brand in its name is fully unenforced, with no visibility (no rua present) into its authentication posture.

**Business Impact.**

A subsidiary domain sharing Meridian's brand identity is meaningfully more exposed to spoofing than the parent organization believes its overall DMARC posture provides, directly undermining the intent of the parent domain's enforcement policy for any recipient who cannot distinguish between the two domains by name alone.

**Recommendation.**

Bring ledgerpay.meridianfg.com's DMARC policy into alignment with the parent domain's enforcement level following a monitoring period with rua reporting enabled, and rotate the subsidiary's DKIM key as part of the broader key-rotation program addressed in CS002-10.

**Verification Method.**

Confirm updated DMARC record via `dig TXT`, confirm rua reports are being received, and confirm policy alignment (or an explicitly documented, deliberate exception) with the parent domain within the next quarterly review cycle.

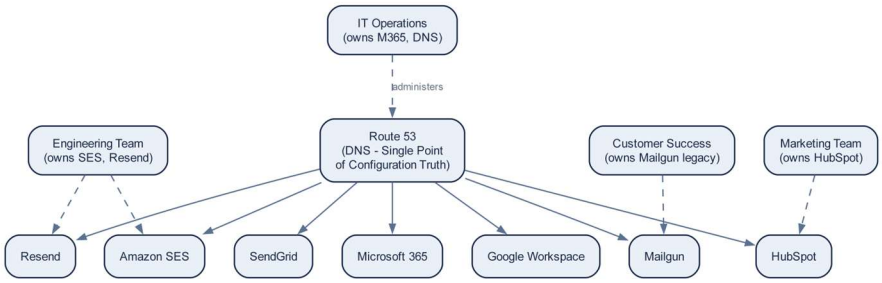


*Figure 4 — Infrastructure Dependency Map (Ownership Overlay)*

## CS002-04 — SES Transactional Mail Has No SPF Alignment Path

| | |
|---|---|
| **Severity** | **High** |
| **Category** | Authentication |
| **Reference** | RFC 7489 §3.1 |

**Evidence.**

Amazon SES for app.meridianfg.com was configured without a Custom MAIL FROM domain, meaning the envelope-sender (Return-Path) address used for SPF evaluation resolves under an Amazon-owned subdomain rather than any meridianfg.com domain.

```
$ dig TXT app.meridianfg.com +short | grep spf1
"v=spf1 include:amazonses.com ~all"

Sample envelope sender observed in trace test:
  Return-Path: <0000018d-example@bounces.us-east-1.amazonses.com>

SPF evaluates against bounces.us-east-1.amazonses.com (PASS),
but this domain shares no organizational relationship with meridianfg.com,
so SPF provides no DMARC alignment under relaxed or strict mode.
```

**Technical Analysis.**

DMARC requires either SPF or DKIM to be in alignment with the visible From-header domain. Because SES's default MAIL FROM was never replaced with a custom subdomain (e.g., bounce.app.meridianfg.com), SPF authenticates an Amazon-controlled domain entirely outside Meridian's organizational domain and can never contribute to alignment, regardless of DMARC's relaxed-mode tolerance. DKIM, which is correctly configured with a custom domain identifier, is the sole mechanism currently carrying DMARC for this stream.

**Business Impact.**

Product notification mail — a customer-facing, trust-sensitive stream for a fintech platform — has no redundancy in its DMARC alignment path. Any future DKIM misconfiguration, key rotation error, or signing outage would cause this entire stream to fail DMARC with no fallback, a materially higher risk profile than the redundant SPF+DKIM alignment present on Meridian's other properly configured domains.

**Recommendation.**

Configure a Custom MAIL FROM domain for the SES identity (e.g., bounce.app.meridianfg.com), publish the resulting SPF record under Meridian's own DNS zone, and re-verify that the new domain is included in future DMARC alignment testing.

**Verification Method.**

Confirm via SES console that a custom MAIL FROM domain is configured and verified, confirm the resulting SPF record resolves under meridianfg.com, and confirm a trace test shows SPF alignment (not merely SPF pass) in the DMARC evaluation result.

## CS002-05 — Marketing Subdomain Has No Explicit DMARC Record

| Severity | Medium |
|---|---|
| Category | Authentication |
| Reference | RFC 7489 §6.6.3 |

**Evidence.**

marketing.meridianfg.com, used for HubSpot campaign sending, has valid SPF and DKIM but no _dmarc TXT record of its own.

```
$ dig TXT _dmarc.marketing.meridianfg.com +short
(no record found)
```

**Technical Analysis.**

In the absence of its own record, this subdomain falls back to the organizational domain's policy per the tree-walk defined in RFC 7489 — which, following remediation of CS002-09, will be explicit. Until that remediation lands, the subdomain's effective policy is ambiguous in exactly the manner CS002-09 describes.

**Business Impact.**

Low standalone impact once CS002-09 is remediated; flagged separately here because Marketing, as the subdomain's operational owner, should have explicit visibility into its own authentication posture rather than depending entirely on an organizational-level record it does not directly control.

**Recommendation.**

Publish an explicit DMARC record at _dmarc.marketing.meridianfg.com with its own rua address, giving Marketing direct reporting visibility independent of the organizational-level record.

**Verification Method.**

Confirm via `dig TXT` that the new record resolves, and confirm Marketing begins receiving aggregate reports within the following reporting period.

## CS002-06 — Developer Platform Onboarded Without Vendor Review

| Severity | Medium |
|---|---|
| Category | Vendor Governance |
| Reference | Internal Vendor Onboarding Standard (informal, pre-engagement) |

**Evidence.**

Resend was integrated for developers.meridianfg.com by an engineering team lead three months ago; the corresponding SPF include was added directly to the root domain's SPF record (contributing to CS002-01) rather than isolated to a dedicated subdomain.

**Technical Analysis.**

No record of IT or security review exists for this integration. While Resend's configuration itself is not misconfigured, its onboarding illustrates the recurring pattern underlying CS002-01: individual teams can independently add root-domain SPF includes with no checkpoint requiring subdomain isolation or centralized review.

**Business Impact.**

Directly contributes to the Critical root-domain SPF finding, and represents a repeatable process gap that will recur with the next vendor onboarded by any team absent a corrective control.

**Recommendation.**

Formalize a lightweight vendor-onboarding checklist requiring any new sending platform to be isolated to a dedicated subdomain with its own SPF record, reviewed by IT prior to DNS changes taking effect.

**Verification Method.**

Confirm the developers.meridianfg.com SPF record is isolated (no longer via root-domain include) following the CS002-01 remediation, and confirm the new onboarding checklist is documented and referenced in the next vendor addition.

## CS002-07 — SendGrid Return-Path Not Customized — Alignment Relies Solely on DKIM

| Severity | Medium |
|---|---|
| Category | Authentication |
| Reference | RFC 7489 §3.1 |

**Evidence.**

SendGrid's automated domain-authentication wizard for billing.meridianfg.com completed the two required DKIM CNAME records but the optional custom Return-Path (automated security) CNAME was never added, leaving the bounce domain on a default sendgrid.net-hosted subdomain.

```
$ dig CNAME s1._domainkey.billing.meridianfg.com +short
s1.domainkey.u1234567.wl123.sendgrid.net.
$ dig CNAME s2._domainkey.billing.meridianfg.com +short
s2.domainkey.u1234567.wl123.sendgrid.net.
$ dig TXT billing.meridianfg.com +short | grep spf1
(no result — SPF only published on default sendgrid.net bounce domain, not on
billing.meridianfg.com)
```

**Technical Analysis.**

This mirrors the structural issue in CS002-04 but at lower severity: DKIM is correctly configured and aligned for this stream, so DMARC currently passes reliably. The gap is the absence of a redundant SPF alignment path should DKIM ever fail.

**Business Impact.**

Billing and invoice correspondence — financially sensitive communication — shares the same single-point-of-alignment-failure characteristic as the SES stream, at lower likelihood given SendGrid's DKIM has been stable historically.

**Recommendation.**

Complete the remaining automated security CNAME in SendGrid's domain authentication wizard to establish a custom Return-Path under billing.meridianfg.com, providing redundant SPF alignment.

**Verification Method.**

Confirm via `dig TXT billing.meridianfg.com` that an SPF record is now present, and confirm both SPF and DKIM alignment in a trace-test Authentication-Results header.

## CS002-08 — Legacy DNS Delegation Incomplete for Subset of Subdomains

| | |
|---|---|
| **Severity** | **Medium** |
| **Category** | DNS |
| **Reference** | RFC 1034 §4.2 |

**Evidence.**

Meridian's DNS migration from the QuickTerm-era GoDaddy account to Route 53 remains incomplete for legacy.meridianfg.com and two related historical subdomains, which still delegate to GoDaddy nameservers rather than Route 53.

```
$ dig NS legacy.meridianfg.com +short
ns1.quickterm-legacy-dns.com.
ns2.quickterm-legacy-dns.com.
$ dig NS meridianfg.com +short
ns-1.awsdns-00.com.
ns-2.awsdns-01.net.
```

**Technical Analysis.**

Split-authority DNS — where different zones of the same organization are managed in two separate systems with two separate access-control models — increases the likelihood of configuration drift and complicates any organization-wide DNS change (such as the SPF remediation recommended in CS002-01) that needs to be applied consistently.

**Business Impact.**

Increases operational complexity and risk during the remediation program recommended in this report, and represents an ongoing access-control inconsistency: it is unclear which team currently retains access to the legacy GoDaddy account.

**Recommendation.**

Complete the Route 53 migration for all remaining legacy subdomains as a prerequisite step before other DNS remediations in this report, and formally decommission GoDaddy account access once cutover is verified.

**Verification Method.**

Confirm via `dig NS` that all Meridian subdomains resolve to Route 53 nameservers, and confirm GoDaddy account access has been revoked or transitioned to a documented owner.

## CS002-09 — Organizational DMARC Record Omits Explicit Subdomain Policy

| Severity | Medium |
|---|---|
| Category | Authentication |
| Reference | RFC 7489 §6.3 |

**Evidence.**

The DMARC record at _dmarc.meridianfg.com does not specify an sp= (subdomain policy) tag.

```
$ dig TXT _dmarc.meridianfg.com +short
"v=DMARC1; p=quarantine; pct=100; rua=mailto:dmarc@meridianfg.com;"
```

**Technical Analysis.**

Per RFC 7489, when sp is absent, subdomains inherit the value of p unless they publish their own explicit DMARC record — which, as documented in CS002-03, at least one subdomain does. While technically well-defined, the absence of an explicit sp value makes the intended policy for the many subdomains without their own DMARC record less discoverable during audit and increases reliance on institutional knowledge rather than a self-documenting record.

**Business Impact.**

Primarily an auditability and clarity concern rather than an active authentication gap; it compounds the difficulty of the sender-inventory problem described in CS002-13.

**Recommendation.**

Add an explicit sp=quarantine (or stricter) tag to the organizational DMARC record to make the intended subdomain policy self-documenting, independent of whether a given subdomain has been audited recently.

**Verification Method.**

Confirm updated record via `dig TXT _dmarc.meridianfg.com` showing an explicit sp= value consistent with organizational policy.

## CS002-10 — No Enterprise-Wide DKIM Key Rotation Cadence

| Severity | Medium |
|---|---|
| Category | Authentication |
| Reference | RFC 6376 §8.14 |

**Evidence.**

DKIM key age varies significantly across Meridian's sending identities with no consistent rotation policy: Microsoft 365's key is 14 months old, the LedgerPay Google Workspace key is 22 months old (see CS002-03), and Amazon SES's key is 6 months old, each rotated only when the respective platform's default behavior or an unrelated migration prompted it.

**Technical Analysis.**

The variance itself is evidence that key rotation is incidental rather than policy-driven across Meridian's sending identities — each platform's key age simply reflects when it was last touched for an unrelated reason.

**Business Impact.**

Increases long-term cryptographic risk exposure inconsistently across sending streams, with the oldest key (LedgerPay) also being the one with the weakest current DMARC enforcement (CS002-03), compounding rather than offsetting that finding's risk.

**Recommendation.**

Adopt a standard 12-month DKIM rotation cadence across all sending identities, tracked centrally as part of the authorized-sender inventory recommended in CS002-13.

**Verification Method.**

Confirm rotation schedule is documented with next-due dates for all seven sending identities, and confirm the LedgerPay and Microsoft 365 keys are rotated within the first cycle following remediation.

## CS002-11 — SES No-Reply Stream Lacks Defined Bounce/Reply Handling

| Severity | Low |
|---|---|
| Category | Operational Risk |
| Reference | RFC 5321 §4.5.5 |

**Evidence.**

Product notifications sent from app.meridianfg.com use a no-reply sender address, but no auto-response or documented handling exists for messages sent in reply; such replies currently bounce with a generic SES-default rejection.

**Technical Analysis.**

This is a customer-experience gap rather than a security or deliverability finding: customers who reply to a legitimate notification (a common behavior despite no-reply framing) receive an unhelpful, unbranded bounce message rather than guidance toward the correct support channel.

**Business Impact.**

Minor but avoidable customer-experience friction for a fintech platform where customers may reasonably expect a responsive channel for account notifications.

**Recommendation.**

Configure a branded auto-response for replies to the no-reply address, directing customers to the appropriate support channel, or evaluate whether a monitored reply-to address better serves the customer experience for this stream.

**Verification Method.**

Send a test reply to a notification message and confirm a branded, helpful auto-response is received rather than a generic SES bounce.

## CS002-12 — SES Bounce and Complaint Data Not Shared With Security Team

| | |
|---|---|
| **Severity** | **Low** |
| **Category** | Operational Risk |
| **Reference** | M3AAWG Sender Best Common Practices |

**Evidence.**

Amazon SES bounce and complaint notifications for app.meridianfg.com are routed to an Engineering-owned SNS topic with no subscription or dashboard access granted to Meridian's security team.

**Technical Analysis.**

Bounce and complaint rate anomalies are a useful early signal for both deliverability issues and potential account-takeover-driven abuse of the notification system; without security visibility, this signal is currently monitored only from an operational-reliability perspective, not a security one.

**Business Impact.**

A gap in cross-functional monitoring coverage rather than an active gap in the underlying data collection, which is otherwise correctly configured.

**Recommendation.**

Grant the security team read access to the existing SNS topic or forwarded dashboard, with a lightweight alerting threshold agreed jointly with Engineering.

**Verification Method.**

Confirm security team access is provisioned and confirm at least one joint review of bounce/complaint trends occurs within 60 days of remediation.

### CS002-13 — No Centralized Authorized-Sender Inventory

| Severity | Informational |
|---|---|
| Category | Governance |
| Reference | M3AAWG Sender Best Common Practices |

**Evidence.**

At engagement start, no team at Meridian could produce a complete list of the organization's authorized sending identities; this report's own inventory (Section 6) was assembled through cross-team interviews conducted specifically for this engagement.

**Technical Analysis.**

This finding is the structural root cause connecting the majority of findings in this report — CS002-01, CS002-02, and CS002-06 in particular are each a direct consequence of no team having visibility into the sending identities other teams had already established.

**Business Impact.**

Ongoing risk of recurrence: absent a structural fix, the next vendor onboarded by any team will likely reproduce the same pattern of un-isolated DNS changes and un-owned vendor relationships documented throughout this report.

**Recommendation.**

Adopt the sender inventory produced in Section 6 of this report as a living document, owned jointly by IT and Security, updated as a required step in any future vendor onboarding or offboarding.

**Verification Method.**

Confirm the inventory is stored in a centrally accessible location with a named owner, and confirm it is referenced as a required step in the vendor-onboarding checklist established under CS002-06.

## 8. Risk Prioritization

Findings are prioritized below by severity and remediation effort, establishing the sequencing basis for the Remediation Strategy in Section 14.

| Priority | Finding ID | Severity | Effort | Rationale |
|---|---|---|---|---|
| 1 | CS002-08 | Medium | Medium | Must precede other DNS changes to avoid split-authority conflicts |
| 2 | CS002-02 | Critical | Medium | Requires ownership assignment before technical remediation is meaningful |
| 3 | CS002-01 | Critical | Medium | Requires coordinated subdomain migration across four teams |
| 4 | CS002-06 | Medium | Low | Bundled with CS002-01 remediation |

| Priority | Finding ID | Severity | Effort | Rationale |
|---|---|---|---|---|
| 5 | CS002-04 | High | Low | Single SES console configuration change |
| 6 | CS002-07 | Medium | Low | Single SendGrid console configuration change |
| 7 | CS002-03 | High | Medium | Requires monitoring period before policy change |
| 8 | CS002-09 | Medium | Low | Single DNS record edit |
| 9 | CS002-05 | Medium | Low | Single DNS record edit |
| 10 | CS002-10 | Medium | Medium | Requires cross-platform coordination for rotation cadence |
| 11 | CS002-13 | Informational | Medium | Process/documentation effort, foundational for recurrence prevention |
| 12 | CS002-11 | Low | Low | Single SES configuration change |
| 13 | CS002-12 | Low | Low | Access-provisioning change only |

# 9. Business Impact Analysis

### Shared-Fate Deliverability Risk

CS002-01 demonstrates a shared-fate risk pattern common in post-acquisition environments: the least security-conscious onboarding decision (an un-isolated SPF include) threatens the deliverability of the most business-critical mail stream (Microsoft 365 corporate correspondence), because all sending identities share one root DNS zone's authentication record.

### Customer Communication Continuity

CS002-02 represents a direct, if narrow, customer-facing risk: a real communication obligation to a legacy customer population persists on unmonitored infrastructure with no assigned owner, a pattern that is easy to overlook precisely because the affected population is small and the platform it depends on is otherwise scheduled for full decommissioning.

### Brand and Trust Inconsistency

CS002-03 and CS002-04 together illustrate that Meridian's overall DMARC enforcement posture is meaningfully less consistent than its parent-domain policy alone suggests: a Meridian-branded subsidiary is fully unenforced, and the primary customer notification stream has no redundant alignment path. Both increase brand and phishing-impersonation exposure beyond what Meridian's IT leadership currently believes their DMARC investment provides.

### Recurrence Risk

CS002-13 is the structural finding underlying the others: without a centralized sender inventory and onboarding checkpoint, each future acquisition or new vendor relationship is likely to reproduce the same category of finding documented in this report.

# 10. Remediation Strategy

Remediation is organized into three phases sequenced by dependency and urgency.

### Phase 1 — Immediate (Weeks 1–3)

| Action | Addresses | Expected Result | Operational Considerations |
|---|---|---|---|
| Complete Route 53 migration for remaining legacy subdomains | CS002-08 | Single authoritative DNS provider for all zones | Prerequisite for subsequent DNS changes |
| Assign named ownership and monitoring to legacy Mailgun stream | CS002-02 | Customer-communication obligation is actively monitored | Coordinate with Customer Operations leadership |

### Phase 2 — Near-Term (Weeks 4–8)

| Action | Addresses | Expected Result | Operational Considerations |
|---|---|---|---|
| Isolate all vendor sending onto dedicated subdomains; correct root SPF | CS002-01, CS002-06 | Root domain SPF resolves to ≤ 2 lookups | Coordinate change window across four teams |
| Configure custom MAIL FROM for SES; complete SendGrid Return-Path CNAME | CS002-04, CS002-07 | Redundant SPF alignment for both transactional streams | No sending downtime required |
| Add explicit sp= to organizational DMARC; add explicit DMARC to marketing subdomain | CS002-09, CS002-05 | Self-documenting, unambiguous subdomain policy | DNS-only change |

### Phase 3 — Governance Hardening (Weeks 9–14)

| Action | Addresses | Expected Result | Operational Considerations |
|---|---|---|---|
| Align LedgerPay DMARC policy with parent; rotate subsidiary DKIM key | CS002-03, CS002-10 | Consistent enforcement across parent and subsidiary | Monitoring period required before policy change |
| Adopt 12-month enterprise DKIM rotation cadence | CS002-10 | Predictable, policy-driven key hygiene | Coordinate across all seven platforms |
| Publish and adopt centralized authorized-sender inventory | CS002-13 | Standing governance artifact prevents recurrence | Requires joint IT/Security ownership |
| Provision security-team access to SES bounce/complaint data; configure reply handling | CS002-11, CS002-12 | Cross-functional monitoring coverage; improved customer experience | Low effort, can proceed independently of other phases |

# 11. Verification Plan

| Finding | Verification Method | Success Criterion |
|---|---|---|
| CS002-01 / CS002-06 | SPF lint validation on root and all subdomains | Root domain ≤ 2 lookups; each subdomain independently valid |
| CS002-02 | Service catalog review + Mailgun dashboard access audit | Named owner documented; dashboard access confirmed active |
| CS002-03 | DMARC record + DKIM key inspection | Subsidiary policy aligned with parent; key rotated |
| CS002-04 / CS002-07 | Trace test with full alignment analysis | Both SPF and DKIM show alignment in Authentication-Results |
| CS002-05 / CS002-09 | DNS record inspection | Explicit DMARC/sp= values present and correct |
| CS002-08 | NS record inspection across all subdomains | All subdomains resolve to Route 53 nameservers |
| CS002-10 | Central rotation schedule review | All seven identities have documented next-rotation dates |
| CS002-11 | Test reply to no-reply address | Branded auto-response received |
| CS002-12 | Access provisioning confirmation | Security team has active dashboard access |
| CS002-13 | Inventory document review | Inventory accessible, owned, and referenced in onboarding checklist |

# 12. Final Assessment

Meridian's email infrastructure reflects the well-known challenge of inorganic growth: four organizations' worth of independently reasonable decisions have combined into a shared environment none of the constituent teams individually designed. Vaixus rates Meridian's current infrastructure maturity as Developing (Level 2 of 5 on Vaixus's internal maturity scale), consistent with organizations that have not yet completed post-acquisition infrastructure integration.

The two Critical findings warrant the most immediate attention, but neither can be resolved instantly: CS002-02 requires an ownership decision before any technical change is meaningful, and CS002-01 requires coordination across four teams to isolate sending correctly. Vaixus recommends treating the centralized sender inventory (CS002-13) as a parallel, foundational workstream rather than a final-phase afterthought, since it directly supports the coordination that Phase 2 remediation requires.

No finding in this report indicates active compromise. Every finding is a configuration, alignment, or governance gap consistent with unintegrated post-acquisition infrastructure, and all are remediable without a change of vendor or an interruption to any active business communication stream.

# 13. References


- RFC 1034 — Domain Names — Concepts and Facilities
- RFC 5321 — Simple Mail Transfer Protocol
- RFC 6376 — DomainKeys Identified Mail (DKIM) Signatures
- RFC 7208 — Sender Policy Framework (SPF) for Authorizing Use of Domains in Email
- RFC 7489 — Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- M3AAWG Sender Best Common Practices, Messaging, Malware and Mobile Anti-Abuse Working Group
- Amazon SES Developer Guide — Custom MAIL FROM Domains and Authentication
- SendGrid Domain Authentication Documentation


# 14. Technical Appendix

## A. Full DNS Record Set (Synthetic Laboratory Environment)

**meridianfg.com (Root Domain)**

| Record Type | Name | Value |
|---|---|---|
| MX | @ | 0 meridianfg-com.mail.protection.outlook.com |
| TXT (SPF) | @ | v=spf1 include:spf.protection.outlook.com include:amazonses.com include:sendgrid.net include:mailgun.org include:_spf.hubspotemail.net include:spf.resend.com ~all |
| CNAME (DKIM) | selector1-meridianfg-com._domainkey | selector1-meridianfg-com._domainkey.meridianfg.onmicrosoft.com |
| CNAME (DKIM) | selector2-meridianfg-com._domainkey | selector2-meridianfg-com._domainkey.meridianfg.onmicrosoft.com |
| TXT (DMARC) | _dmarc | v=DMARC1; p=quarantine; pct=100; rua=mailto:dmarc@meridianfg.com; |
| NS | @ | ns-1.awsdns-00.com / ns-2.awsdns-01.net |

**ledgerpay.meridianfg.com (LedgerPay Subsidiary — Google Workspace)**

| Record Type | Name | Value |
|---|---|---|
| MX | @ | 1 aspmx.l.google.com / 5 alt1 / 5 alt2 / 10 alt3 / 10 alt4 |
| TXT (SPF) | @ | v=spf1 include:_spf.google.com ~all |

| Record Type | Name | Value |
|---|---|---|
| TXT (DKIM) | google._domainkey | v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArP7K...[truncated] |
| TXT (DMARC) | _dmarc | v=DMARC1; p=none; (overrides parent — see CS002-03) |

**app.meridianfg.com (Amazon SES) / billing.meridianfg.com (SendGrid)**

| Record Type | Domain | Value |
|---|---|---|
| TXT (SPF) | app.meridianfg.com | v=spf1 include:amazonses.com ~all |
| CNAME (DKIM) | app.meridianfg.com | 3 CNAMEs to *.dkim.amazonses.com (Easy DKIM) |
| MAIL FROM | app.meridianfg.com | Not configured — default bounces.us-east-1.amazonses.com (see CS002-04) |
| CNAME (DKIM) | billing.meridianfg.com | s1/s2._domainkey → sendgrid.net (see CS002-07) |
| TXT (SPF) | billing.meridianfg.com | Not present — default sendgrid.net bounce domain in use |

**legacy.meridianfg.com (Mailgun) / developers.meridianfg.com (Resend) / marketing.meridianfg.com (HubSpot)**

| Record Type | Domain | Value |
|---|---|---|
| MX / SPF | legacy.meridianfg.com | mxa/mxb.mailgun.org; v=spf1 include:mailgun.org ~all |
| NS | legacy.meridianfg.com | ns1/ns2.quickterm-legacy-dns.com (see CS002-08) |
| SPF | developers.meridianfg.com | Authorized via root-domain include (see CS002-06) |
| SPF / DKIM | marketing.meridianfg.com | v=spf1 include:_spf.hubspotemail.net ~all; valid DKIM |
| DMARC | marketing.meridianfg.com | Not present (see CS002-05) |

## B. Sample Authentication-Results Header (SES Trace Test)

```
Authentication-Results: mx.receivingtest.example;
  spf=pass (sending domain bounces.us-east-1.amazonses.com designates
    23.251.x.x as permitted sender) smtp.mailfrom=bounces.us-east-1.amazonses.com;
  dkim=pass header.i=@app.meridianfg.com header.s=abc123 header.b=k9Lm2p;
  dmarc=pass (p=QUARANTINE dis=NONE) header.from=app.meridianfg.com
  ; NOTE: dmarc=pass achieved via DKIM alignment only — SPF domain
  (bounces.us-east-1.amazonses.com) does not align with header.from
```

## C. Command Output — SPF Lint (Post-Remediation, Simulated)

```
$ spf-lint meridianfg.com
Record: v=spf1 include:spf.protection.outlook.com ~all
Total DNS lookups: 2
Result: VALID (within RFC 7208 limit)
```

## D. Vendor Configuration Inventory

| Vendor | Role | Domain(s) Serviced | Admin Owner |
|---|---|---|---|
| Microsoft 365 | Corporate mail | meridianfg.com | IT |
| Google Workspace | Subsidiary mail (LedgerPay) | ledgerpay.meridianfg.com | LedgerPay Operations |
| Amazon SES | Product notifications | app.meridianfg.com | Engineering |
| SendGrid | Billing correspondence | billing.meridianfg.com | Finance |
| Mailgun | Legacy account statements | legacy.meridianfg.com | Unassigned (see CS002-02) |
| Resend | Developer platform alerts | developers.meridianfg.com | Engineering |
| HubSpot | Marketing campaigns | marketing.meridianfg.com | Marketing |
| Amazon Route 53 | Authoritative DNS (primary) | meridianfg.com and subdomains | IT |
| GoDaddy (legacy) | Authoritative DNS (residual) | legacy.meridianfg.com and 2 related subdomains | Unassigned (see CS002-08) |