Stopping Scammers From Impersonating Your Business

Email Authentication in ABA: Findings from 740 Providers

Prepared by ABAOps.ai in collaboration with Anchor Networks

In plain language: why this matters for ABA providers

For most ABA organizations, email is how you:

- Communicate with parents about schedules, progress, and concerns
- Coordinate with schools and payers about services and authorizations
- Share reports, assessments, and documentation

If someone can send emails that look like they came from your organization, three things can happen:

- Families may share sensitive information (PHI) with a scammer who looks like "you"
- Fake cancellation or schedule emails can disrupt children's routines and therapy
- Schools and payers can receive misleading or fraudulent messages under your name

This whitepaper looks at how well 740 ABA providers are protected against that kind of impersonation, what the numbers show, and what practical steps you can take with your IT partner to reduce that risk over time.

Executive Summary

This report presents findings from an analysis of email authentication practices across 740 Applied Behavior Analysis (ABA) provider domains. The analysis examined the implementation of three core email security protocols:

- SPF (Sender Policy Framework) – specifies which servers are allowed to send email for a domain
- DKIM (DomainKeys Identified Mail) – adds a digital signature to outgoing messages
- DMARC (Domain-based Message Authentication, Reporting & Conformance) – tells receiving systems how to handle unauthenticated email

At a glance, the most important points are:

- 65% of ABA provider domains have no DMARC policy in place, meaning there are no published instructions for how to handle suspicious messages that appear to come from their domain.
- 45% of domains fall into a high-risk category for email impersonation, with overall security scores below 5 out of 10.
- 20% of providers have missing or misconfigured SPF records, making it harder for receivers to verify legitimate senders.
- Among providers with DMARC policies, most (about 71%) use monitoring-only settings rather than active protection.
- Approximately 20% of ABA organizations have implemented comprehensive email authentication, showing that effective protection is achievable in this sector.

In practical terms, this means:

- It is often technically possible today for someone to send emails that appear to come from an ABA provider's domain.

- A significant number of ABA organizations have already closed most of these gaps, using well-understood steps and without large budgets.

These findings suggest that ABA providers—who regularly exchange sensitive behavioral, medical, and educational information via email—face a meaningful level of avoidable risk from email impersonation. At the same time, the data shows that many peer organizations have successfully addressed these gaps using a methodical, stepwise approach.

Key numbers at a glance

- 65% of domains have no DMARC
- 45% of domains are high risk
- 20% have comprehensive protection

Why Email Security Matters in ABA

ABA organizations occupy a distinct place in the broader healthcare and education landscape. They work directly with children with autism and their families while coordinating services across multiple stakeholders:

- Parents and caregivers
- School districts and IEP teams
- Insurance companies and funding sources
- Referring physicians and clinical partners

Email remains a primary communication channel for:

- Treatment plans and progress updates
- Scheduling and session changes
- Authorization requests and claims documentation
- Sharing assessment results and behavioral data

When email authentication is not properly configured, it becomes easier for unauthorized parties to send messages that appear to come from an ABA provider's domain. In practice, this can lead to scenarios such as:

Information exposure

A spoofed email requesting updated insurance information or medical history may look routine. A parent who trusts the sender name and logo may respond with protected health information (PHI) to someone who is not connected to the provider.

Service disruption

Fraudulent emails about session cancellations or schedule changes can confuse families and disrupt carefully planned routines. For many children with autism, sudden changes in schedule can be especially challenging.

Strained professional relationships

Schools and insurance companies depend on accurate information from providers. Spoofed emails containing incorrect treatment details or billing information can create confusion and erode trust—even if the provider was not responsible for the message.

Payment and internal fraud

In addition to external messages, attackers sometimes imitate internal emails from leaders or managers. For example, a spoofed message that appears to come from a CEO or clinical director might instruct finance staff to "urgently" pay an invoice, change bank details, or purchase gift cards. If email authentication is weak, these messages can be difficult to distinguish from legitimate internal requests, increasing the risk of unauthorized payments or financial loss.

It is important to emphasize that these risks exist not because ABA organizations are careless, but because email standards and attack patterns have evolved quickly, while many providers have rightly focused their limited resources on delivering clinical services.

Dataset and Methodology

What We Analyzed

The analysis examined email security configurations for approximately 740 ABA provider domains collected from public provider directories and related sources. For each domain, we assessed:

- The presence and configuration of SPF, DKIM, and DMARC records
- Overall email security posture using a 0–100 scoring system
- Risk levels categorized as:
  - Low risk: scores 8–10
  - Medium risk: scores 6–7
  - High risk: scores 0–5

These scores are intended as a practical indicator of how well each domain is protected against impersonation, not as a formal certification.

How Scoring Works

Each domain receives component scores based on the implementation of:

- SPF score – whether the domain has an SPF record and how comprehensively it covers legitimate senders
- DKIM score – whether outgoing emails are signed and verifiable
- DMARC score – whether the domain has a DMARC policy and whether that policy is enforcing or monitoring-only

An overall score combines these elements into a single measure of email authentication strength.

Important Limitations

This analysis represents a point-in-time snapshot and has several limitations:

- Sampling considerations
  Domains were identified primarily from publicly listed ABA providers. The dataset may not include all private practices or newly established organizations, and larger entities may be overrepresented.
- Technical limitations
  The analysis is limited to publicly visible DNS records. It does not capture internal measures such as secure email gateways, endpoint protections, or staff training programs.
- Organizational context
  The data does not distinguish between environments managed entirely in-house and those managed by MSPs or third-party IT providers.

These limitations do not reduce the usefulness of the findings, but they should be kept in mind when interpreting percentages and trends.

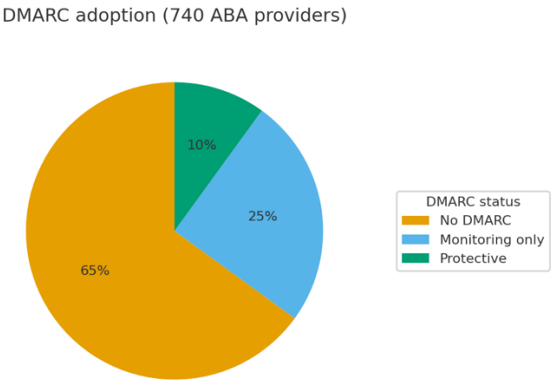
Key Findings Across 740 ABA Providers

DMARC Implementation

DMARC acts as a published policy that tells receiving email systems what to do with messages that fail authentication checks.

What we observed:

- 65% of ABA provider domains have no DMARC record
- 25% use monitoring-only DMARC (policy p=none)
- 10% have protective DMARC policies (p=quarantine or p=reject)



In practical terms:

- Domains with no DMARC are not providing guidance to receivers about how to handle messages that fail SPF/DKIM checks. Suspicious messages may still be delivered to inboxes.
- Domains with monitoring-only DMARC receive reports about email activity but are not yet instructing receivers to block or quarantine unauthenticated messages.
- Domains with protective DMARC are better positioned to prevent spoofed messages from reaching end users.

SPF Configuration

SPF records specify which servers are authorized to send email on behalf of a domain.

What we observed:

- 20% have missing or broken SPF records
- 45% have basic SPF covering their primary email system
- 35% have more comprehensive SPF that appears to include multiple legitimate senders (for example, practice management, billing, and marketing tools)

Without a functioning SPF record, receivers have no published way to verify whether a sending server is legitimate. Even with basic SPF in place, gaps can appear if new services are added but not reflected in the record.

DKIM Status

DKIM adds a digital signature to outgoing emails that can be verified by receivers.

What we observed:

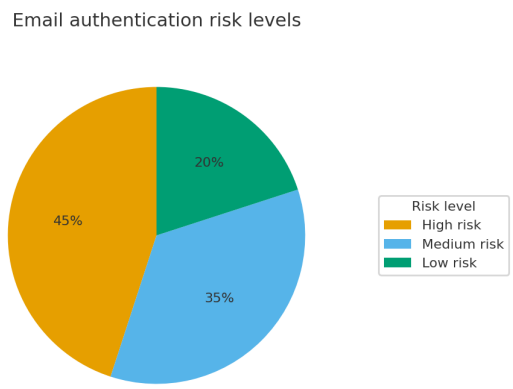
- 70% of domains appear to lack DKIM signing
- 20% have partial DKIM implementation
- 10% have more complete DKIM coverage

DKIM is often configured through the organization's email provider (such as Microsoft 365 or Google Workspace). When not enabled, messages do not carry this additional cryptographic assurance.

Overall Risk Distribution

Combining SPF, DKIM, and DMARC, we categorized domains into risk levels:

- High Risk – 45%
  - Scores 0–5
  - Minimal or no email authentication in place
- Medium Risk – 35%
  - Scores 6–7
  - Partial protections, but gaps remain (for example, monitoring-only DMARC, incomplete SPF)
- Low Risk – 20%
  - Scores 8–10
  - Comprehensive email authentication with protective DMARC, working SPF, and DKIM



This distribution shows that many ABA providers would benefit from improved email authentication. It also shows that a significant minority have already achieved strong protections, demonstrating that better security is achievable even with the constraints common in ABA organizations.

Implications for ABA Organizations and Their IT/MSP Partners

Clinical Operations

The observed gaps in email authentication have several practical implications for ABA operations:

- Protected Health Information (PHI)
  Spoofed emails requesting updated forms, assessment results, or behavioral data can lead families to share sensitive information with unauthorized recipients.
- Scheduling and consistency
  Therapy schedules are important not just for logistics, but for clinical outcomes. Fraudulent messages about cancellations or rescheduling can disrupt routines that many clients depend on.
- Billing and authorizations
  Email is often used to transmit claims-related information, authorization forms, and documentation for payers. Misleading or unauthorized messages in this space can cause delays, confusion, or disputes.

Stakeholder Trust

ABA providers maintain relationships built on trust:

- Families rely on timely, accurate updates about care
- Schools require reliable information for educational planning
- Payers depend on correct documentation and clear communication

Email impersonation, even if rare, can damage these relationships and create uncertainty about which messages can be trusted.

Resource Constraints

Most ABA organizations face real constraints:

- Limited internal IT resources
- Heavy reliance on MSPs or generalist technology vendors
- Limited time and budget to investigate technical topics in depth

Given these realities, email authentication work needs to be structured as a phased, manageable effort, not a one-time overhaul.

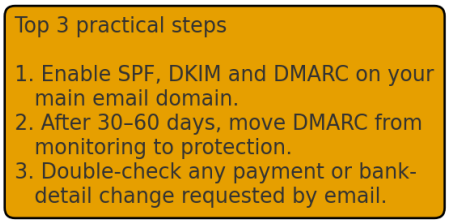
Recommended Actions

Based on the data and typical ABA constraints, we recommend that ABA organizations and their IT or MSP partners follow a practical sequence of steps. In most cases, these steps are implemented together with an existing IT services provider or internal IT team. Where no such partner exists, it can be helpful to discuss options with a provider experienced in ABA organizations before making changes.

1. Establish the current state
    - Inventory all domains used for ABA communication:
        - Main organizational domain
        - Domains used for billing systems
        - Domains used for marketing or outreach
    - Many organizations discover they are actively using more domains than they initially realized.
2. Implement basic SPF records
    - Work with your email provider or IT partner to create SPF records for each domain.
    - Ensure these records include:
        - Primary email platform (for example, Microsoft 365, Google Workspace)
        - Any practice management or billing systems that send email
        - Any messaging or marketing tools used for families or referrers
3. Deploy monitoring-only DMARC
    - Begin with a DMARC policy set to p=none (monitoring mode).
    - This allows you to receive reports about how your domain is being used, without affecting delivery.
    - Use this period to:
        - Identify legitimate senders you may have missed
        - Detect unauthorized or unexpected sources
4. Review and refine configurations
    - After 30–60 days, review DMARC reports with an IT or MSP partner.
    - Update SPF and DKIM settings to cover all legitimate senders and reduce noise in the reports.
5. Move to protective DMARC policies
    - Once there is confidence that legitimate email passes authentication, gradually strengthen DMARC:
        - Begin with p=quarantine to send suspicious messages to spam or quarantine folders.
        - When comfortable, move to p=reject so clearly unauthenticated messages are rejected outright.

6. Implement ongoing monitoring
    - Email configurations can drift as services are added or changed.
    - Establish a cadence (for example, quarterly checks) to confirm that SPF, DKIM, and DMARC remain correctly configured.

This path allows organizations to make meaningful progress without taking on more change than their teams can manage at one time and fits naturally into the kind of work most ABA providers already do with their IT services partner.



How ABAOps.ai and Anchor Networks Support This Work

ABAOps.ai and Anchor Networks work together to support ABA organizations and the IT partners who serve them.

- ABAOps.ai provides tools that allow ABA organizations to check and monitor email authentication across their domains. The goal is to make it straightforward to see where gaps exist and what they mean in practical terms, without requiring deep technical expertise.
- The platform is designed so organizations can:
    - Run a free baseline check of their domains
    - Review clear, non-technical explanations of findings
    - Share those findings with their existing IT services provider or MSP and decide together how to address them

Anchor Networks is a managed service provider (MSP) and IT support partner focused on ABA organizations. Using insights from ABAOps.ai, Anchor Networks can:

- Help inventory all domains used for communication
- Configure or refine SPF, DKIM, and DMARC with existing email providers
- Set up ongoing monitoring and periodic reviews
- Support MSPs and in-house IT teams that want a second set of eyes on ABA-specific questions

In many cases, ABA organizations will work through the recommendations in this report with their current IT provider, using ABAOps.ai as a shared reference point. For organizations that do not have a dedicated IT

partner, or that would like to discuss what a remediation plan might look like, Anchor Networks is available to have an initial conversation without obligation.

The central goal is not to replace existing relationships, but to make progress on closing avoidable email authentication gaps in a way that fits ABA operations.

Conclusion

This analysis of 740 ABA provider domains indicates that email authentication is an area where many organizations can make practical security improvements.

- A majority of domains currently lack DMARC, or use monitoring-only policies.
- A meaningful portion have gaps in SPF and DKIM coverage.
- At the same time, roughly one in five providers have already achieved comprehensive protection, showing that strong email authentication is realistic within typical ABA constraints.

The sensitive nature of ABA services—working with vulnerable populations, handling PHI, and maintaining trust with families, schools, and payers—makes it particularly important to reduce avoidable risks from email impersonation. Fortunately, the steps required to do so are well understood and can be implemented gradually.

ABA organizations do not need to solve everything at once. A practical path is to:

1. Understand the current state of all domains used for communication
2. Implement basic SPF and monitoring-only DMARC
3. Refine configurations based on real-world data
4. Move toward protective DMARC policies
5. Maintain light but consistent monitoring over time

By following this approach, providers can support the trust-based relationships that are central to effective ABA services, while better protecting the families and partners they serve.

For more information about interpreting your organization's email authentication status or planning a phased improvement effort, visit www.abaops.ai or contact the team at support@abaops.ai.