Rethinking email signatures

See how Exclaimer revolutionizes how IT controls email signatures

Exclaimer

Contents

Introduction

Despite all the new options for digital communications — messaging apps, video chats, texts, and more — the business world still runs on email. Personal, non-automated emails are one of the most effective ways to interact with customers, partners, and other business contacts. In fact, research shows that the return on investment (ROI) for email marketing can be as high as 44 times the investment.[1]

But what does this *mean* for IT?

> More often than not, IT professionals are the unsung heroes of an organization, working to keep email systems up and running.
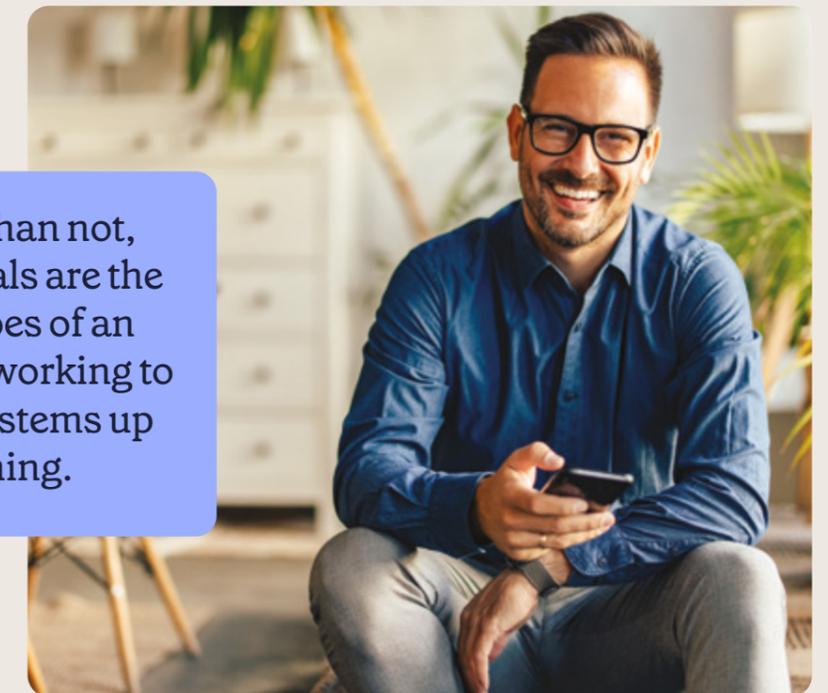
The consistency of corporate email signatures is the least of their worries. In the "2025 State of IT" report from Spiceworks Ziff Davis, 50% of technology professionals reported working overtime on a regular basis, with an average of eight additional hours per week. This is primarily due to project deadlines and unexpected technical issues.[2]

Yet the task of email signature management comes with many challenges.

For IT professionals, managing email signatures is an operational burden. Manual updates, security vulnerabilities, compliance risks, and the constant influx of marketing requests make maintaining consistent signatures a frustrating and time-consuming process.

This whitepaper explores how Exclaimer automates email signature management, enabling IT teams to:

- **Enforce** security & compliance standards

- **Eliminate** manual updates, saving thousands of IT hours annually

- **Integrate** with Microsoft 365, Google Workspace, and Exchange Online

- **Reduce** time and operational costs by up to $100K annually for large enterprises

Traditional IT methods for *updating* email signatures

Just one signature change a quarter for 100 employees could end up costing an organization $9,000 and 50 hours in lost time.

Deploying professional email signatures across an organization can take up a lot of an IT team's time.

In a small office, IT staff might go from desk to desk, manually copy-and-pasting a signature into each employee's email client.

But this method is hugely inefficient. On average, IT administrators are paid $45 per hour.[3]

If it takes half an hour to update and test a user's signature, just one signature change a quarter for 100 employees could end up costing an organization $9,000 and 50 hours in lost time. This equates to $43,200 and 200 hours per year. For an enterprise with 1,000 employees, this can exceed $432,000 and 2,000 hours per year in lost productivity.

Emailing out a template is also problematic because it's up to employees to deploy the design themselves — and not make their own changes. This opens up security risks, such as unauthorized signature modifications, outdated legal disclaimers, or a lack of encryption in email clients. Employees may also be out of the office, overlook the instructions, or simply forget to make an update.

Centrally *managing* email signatures: The IT approach

Traditionally, there are two ways to centrally manage email signatures from an IT perspective.

Approach 1

Apply server-side mail transport rules to ensure signatures are added after an email is sent, but before it leaves the corporate network. The signature is essentially "stamped" onto the message, allowing for signatures on email sent from any device.

Approach 2

Use client-side scripts to add a designed signature to the client settings of assigned users. From within their email client, users can see the signature as they type an email message.

Common IT *challenges* with standardizing email signatures

Although an IT professional can enforce a signature policy using a script and custom HTML code, the following challenges complicate that approach:
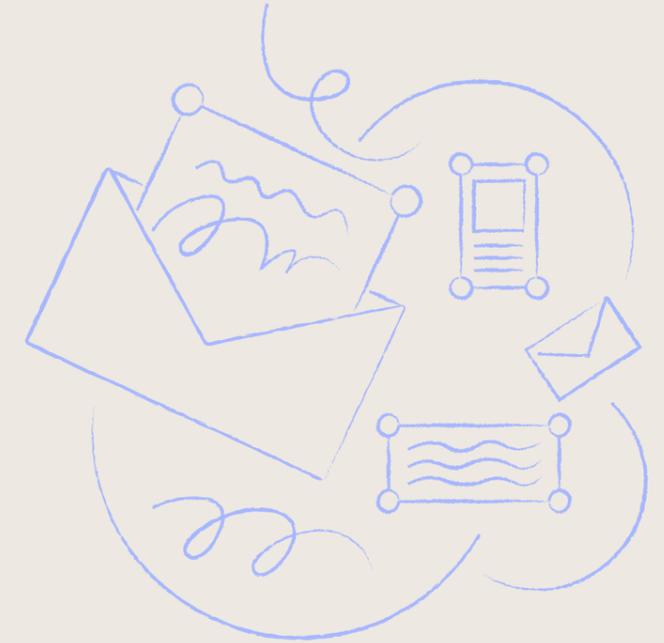
01
Signatures render differently on different devices:

Rules need to be created so that a signature template is applied correctly based on the device type. Design variations also need to be considered. For example, iOS emails use plain text, so designs that look good on desktop may not appear on iPhones or iPads.

02
Issues with client-side scripts:

Client-side scripts are typically not supported on mobile devices and non-standard clients. This means 100% design conformity is impossible.

Meanwhile, using client-side scripts with server transport rules isn't an effective work-around because the two methods will compete with each other.

03
Incomplete or inaccurate contact details:

When creating email signatures using directories like Active Directory or Google Directory, missing contact details can lead to blank fields. Since employees often can't update these themselves, IT is left to fix the errors.

04
HTML design limitations:

Creating an HTML email signature is time-consuming and often requires after-hours testing, even with a great design. Microsoft 365's disclaimer function isn't built for high-quality HTML, and Google Workspace's "Append footer" option doesn't support HTML and limits text to 10,000 characters, requiring links from a web server.

05
Constant requests from non-IT teams:

Non-IT teams like marketing, HR, legal, and sales increasingly want IT to make various email signature updates. Marketing teams, for example, often want to add banners to promote offers, events, or product launches. These updates are usually time-sensitive, leading to urgent IT requests to add them and then remove them once the campaign is over.

06
Signature stacking:

Native email signature functionality in Microsoft 365 and Google Workspace are designed for adding disclaimers. This means signatures are always added to the bottom of emails when using server-side rules, with no options for customization.

07
Images appear as attachments or get removed:

By default, many email clients automatically block any externally hosted images as a security measure. Recipients must mark emails as from a safe sender or click a "Download Images" button before they can see any images.

08
Compliance & security risks:

Organizations in finance, healthcare, and legal sectors must navigate strict regulations on email communication. However, manually managing email signatures can create serious compliance risks. Inconsistent legal disclaimers can lead to violations of regulations like GDPR, HIPAA, or SOX. Unauthorized changes to email signatures can expose companies to reputational and legal issues, while emails sent without proper security measures increase the risk of phishing and fraud.

Exclaimer to the *rescue*

Professional email signature solutions make it easy for IT teams to:

1

Ensure consistent signatures on every device and control signatures from a web browser, even while working remotely.

2

Eliminate the need for manual signature design updates.

3

Empower marketing professionals and relinquish day-to-day responsibility.

The power in Exclaimer is in the centralized control, which can be both robust and straightforward. Every employee can have a signature appended to their emails from whatever device they're using.

1. Automate signature management & save IT hours

With Exclaimer, IT teams eliminate the manual burden of email signature management. Exclaimer's cloud-based platform automates updates, ensuring real-time deployment across all users. This guarantees brand consistency and legal compliance across the organization.

– No need for manual scripting, policy adjustments, or one-off template updates.

– Signatures update instantly across all employees and devices.

– Specific signatures can be created for email replies or forwarded messages, saving time.

– Signatures can be scheduled for campaigns, events, or seasonal updates.

Example time & cost savings for a 100 user organization

– Estimated time per update: 15 minutes (0.25 hours).

– Total annual time spent: 0.25 hours × 4 updates = 1 hour per year.

– Time saved per year: 200 hours (manual process) – 1 hour (automated process) = 199 hours saved annually.

– Time saved as a percentage: (199 hours / 200 hours) × 100 = 99.5% time saved.

– Cost savings at $45/hour: 199 hours × $45 = $8,955 saved annually.

2. Enterprise-grade security & compliance

Exclaimer enforces strict security policies and regulatory compliance for IT-managed email signatures.

– Compliant with top cloud security standards like ISO/IEC 27001 and SOC 2.

– Prevents unauthorized signature edits with centralized control.

– Enforces GDPR, HIPAA, and industry-specific disclaimers automatically.

– Supports 99.99% uptime while conforming to data privacy requirements.

3. Seamless integration with leading email platforms

Exclaimer syncs in real-time with IT environments, ensuring accurate and up-to-date employee information.

– Microsoft 365 & Google Workspace compatibility ensures signatures render correctly across all email clients.

- User directory integrations keep contact details synced, hiding unpopulated fields to avoid errors.

- Exclaimer works in both cloud and on-premises environments, so email signatures migrate when organizations move to the cloud.

4. Cross-functional collaboration

Exclaimer bridges the gap between IT and marketing, making email signature management smarter and more efficient.

– IT can delegate signature updates to marketing using role-based access control (RBAC), freeing up time for strategic projects while retaining oversight.

– Marketing teams can customize branding, add promotional banners, and manage templates.

– Email signatures evolve through CRM integrations, social feeds, rotating banners, and enhanced analytics, transforming them into a marketing channel.

Ready to *transform* the way you manage email signatures?

IT professionals worldwide trust Exclaimer for email signature management.

- ⊘ Guarantee 100% brand consistency across all corporate emails

- ⊘ Reduce IT workload by automating signature updates

- ⊘ Eliminate compliance risks with tamper-proof, policy-driven signatures

About *Exclaimer*
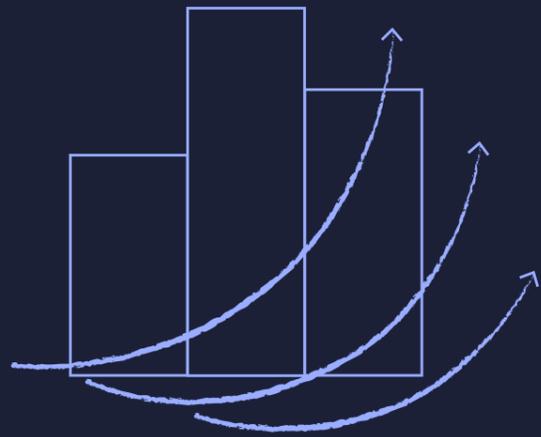
Exclaimer is the industry's leading provider of email signature solutions, empowering businesses to unlock the potential of 1:1 email as a marketing channel.

With its award-winning platform, organizations can simplify the management of email signatures to deliver consistent branding, deliver marketing campaigns and company news, gather real-time customer feedback, and much more.

Over 65,000 organizations in 160+ countries rely on Exclaimer for their email signature solutions. Its diverse customer base includes Sony, Mattel, Bank of America, NBC, the Government of Canada, and the BBC.

Sources

1. Jordie van Rijn, "Email Marketing ROI Statistics: The Ultimate List for 2025", Emailmonday, January 12, 2025. https://www.emailmonday.com/email-marketing-roi-statistics/

2. Spiceworks, "The 2025 State of IT", November 11, 2024. https://www.spiceworks.com/research/it-report/

3 Salay.com, "Hourly Wage for IT System Administrator Salary in the United States", March 01, 2025, https://www.salary.com/research/salary/listing/it-system-administrator-hourly-wages

Start *centrally* managing email signatures

See for yourself how Exclaimer lets you update and manage email signatures without the hassle.

Get a free trial

Book a demo

exclaimer.com