Institutional Pressures and Organizational Compliance with Platform Mandates: Longitudinal Evidence from the Adoption of Email Authentication

Francis Davison

Founder, SpamCipher · https://spamcipher.com/insights/platform-mandates-email-authentication

Preprint · SpamCipher Insights · July 2026 · Longitudinal desk study

ABSTRACT

This empirical study examines how organizations respond to compliance requirements introduced by platform operators. In October 2023, Google and Yahoo announced that email authentication practices that had long been recommended would become mandatory for bulk senders from February 2024. Drawing on institutional theory, this study analyzes the adoption of the DMARC authentication standard in a balanced panel of 191,431 organizational domains observed monthly from January 2023 to June 2026, using public DNS measurement data. An analysis of these data was performed using interrupted time series regression and discrete-time event history models. The results revealed a significant increase of 9.6 percentage points in adoption at the enforcement date, and the increase was significantly larger for consumer-facing domains. The results also revealed significant effects of the domain's mail infrastructure and of recent adoption among sector peers on the probability of adoption. Furthermore, this study found that domains adopting after the enforcement date were significantly more likely to adopt in monitoring-only form and significantly less likely to strengthen their configuration afterward, which is consistent with the decoupling of formal from substantive compliance. The findings of this study contribute to the literature on institutional theory and to research on platform governance. This study also has practical contributions to platform operators, infrastructure providers, and marketing organizations.

Keywords: Institutional theory. Platform governance. Coercive pressure. Email authentication. DMARC. Decoupling.

1 Introduction

A growing share of economic activity is conducted through digital platforms whose owners set the rules under which other organizations participate (de Reuver et al. 2018; Rietveld and Schilling 2021; Cennamo 2021). Research on platform governance has shown that platform owners act as private regulators and exercise rule-setting authority over the organizations that participate in their ecosystems (Gorwa 2019; Kretschmer et al. 2022). Organizations that depend on platforms face substantial power asymmetries in these relationships (Cutolo and Kenney 2021). However, little is known about how populations of organizations respond when a platform operator converts a recommendation into a requirement, which organizations comply, how quickly they do so, and whether their compliance is substantive or only formal.

Commercial email provides a suitable setting for studying these questions. Email remains a central channel of digital marketing (Kannan and Li 2017), and a substantial literature has quantified the returns to email campaigns and their design (Chittenden and Rettie 2003; Bonfrer and Drèze 2009; Wattal et al. 2012; Zhang et al. 2017; Sahni et al. 2018). Whether these returns are realized depends on mailbox providers, which filter inbound mail algorithmically (Cormack 2008; Blanzieri and Bryl 2008) and condition acceptance on sender authentication standards such as SPF (Kitterman 2014), DKIM (Crocker et al. 2011), and DMARC (Kucherawy and Zwicky 2015). For organizations that send email at volume, the mailbox provider controls access to the recipient, and its published requirements are a condition of using the channel.

In October 2023, Google announced that senders of bulk email to Gmail accounts would be required, from February 2024, to authenticate their mail, to offer one-click unsubscription conforming to RFC 8058 (Levine and Herkula 2017), and to keep user-reported spam rates below a published threshold, with non-compliant traffic subject to rejection (Google 2023, 2026). Yahoo introduced parallel requirements on the same timetable (Yahoo 2026). These requirements converted practices that had been advisory for roughly a decade into enforced conditions with published effective dates. Because compliance with the DMARC standard is recorded in the public Domain Name System, the response of the affected population of organizations can be observed directly and without self-report.

Institutional theory (DiMaggio and Powell 1983) explains the adoption of organizational practices through coercive, normative, and mimetic pressures in the organization's environment. Quantitative applications of the theory have examined state regulators and powerful trading partners as the source of coercive pressure (Teo et al. 2003; Liang et al. 2007). There is hardly any empirical study that tests the framework where the coercive actor is a platform operator enforcing rules algorithmically over a large population. Moreover, the related prediction that organizations under strong external pressure adopt ceremonially, decoupling formal structure from substantive practice (Meyer and Rowan 1977), has rarely been tested at scale, because researchers seldom observe both the requirement and the compliance state of every organization; the decoupling literature has relied on informant reports and disclosure documents (Westphal and Zajac 2001; Bromley and Powell 2012). The DMARC standard makes both observable. A published record satisfies the formal requirement, and the record's policy field separates monitoring-only configurations, which impose no consequences on unauthenticated mail, from enforcing configurations that quarantine or reject it.

To fill these gaps, this study attempts to answer the following questions: Q1: Did the introduction of mailbox provider sender mandates significantly change the level and trajectory of email authentication adoption among organizational domains? Q2: Do normative carriers and mimetic exposure significantly predict which organizations adopt? Q3: To what extent is post-mandate compliance substantive rather than ceremonial?

Answering these questions helps to extend institutional theory to a setting in which the regulator is a market actor whose enforcement is automated. It also helps to address a gap in the literature on decoupling, which has usually been inferred from surveys or case studies rather than observed across a population. The results of this research can also add to the knowledge of the compliance layer of the email channel, which the email marketing literature has treated as given (Hartemo 2016; Sahni et al. 2018). This research has practical implications that can be of importance to platform operators that design such requirements, to infrastructure and email service providers, and to marketing organizations deciding how to respond to them.

2 Theoretical framework

2.1 Platform gatekeepers as private regulators

Research on digital platforms characterizes them as governance structures (de Reuver et al. 2018). Platform owners set boundary rules, monitor participants, and apply sanctions, and in this way they govern the ecosystems they operate (Gorwa 2019). Kretschmer et al. (2022) describe platform ecosystems as meta-organizations in which the platform owner exercises authority over legally independent complementors through architecture and rules. The degree of control a platform owner retains over participants is a central design choice with documented consequences for ecosystem behavior (Boudreau 2010). Reviews of the platform literature document the breadth of this rule-setting power and its consequences for participants (Rietveld and Schilling 2021).

Mailbox providers fit this characterization. A sender of commercial email depends on the provider for access to recipients, participates under rules the provider publishes, and is subject to enforcement the provider applies unilaterally. In contrast to app stores and marketplaces, there is no onboarding process and no contractual relationship between sender and provider, so the relationship between them is governed by published rules alone. The sender requirements published by Google and Yahoo specify technical authentication, unsubscription functionality, and complaint-rate ceilings, and they attach consequences, including rejection of traffic, to violations (Google 2026; Yahoo 2026).

2.2 Email authentication and the compliance state

The technical background of the mandated practice is codified in open standards. SPF allows a domain owner to publish the servers authorized to send mail for the domain (Kitterman 2014). DKIM allows messages to carry a verifiable domain signature (Crocker et al. 2011). DMARC allows the domain owner to publish a policy stating what receivers should do with mail that fails authentication, and to request aggregate reports (Kucherawy and Zwicky 2015; the specification was standardized in revised form as RFC 9989 during the observation window, Herr and Levine 2026). Measurement studies document the security rationale for these standards and their incomplete adoption (Durumeric et al. 2015; Foster et al. 2015; Hu and Wang 2018).

Two properties of DMARC make it suitable for compliance research. First, the record is public. Any observer can retrieve every domain's DMARC record from the DNS, so the compliance state of a large population can be measured without contacting the organizations. Second, the record encodes the depth of compliance. A policy of none instructs receivers to take no action against failing mail and enables monitoring only, whereas policies of quarantine and reject impose consequences. A domain can therefore satisfy a requirement to publish a DMARC record without enforcing any policy against failing mail. This distinction corresponds to the difference between ceremonial and substantive adoption in institutional theory (Meyer and Rowan 1977).

2.3 Institutional theory and isomorphic pressures

Institutional theory (DiMaggio and Powell 1983) explains the influence of external forces in organizations' environments, including rules, standards, and competitor behavior, on the adoption of practices. Organizations facing the same institutional environment become similar through three mechanisms. Coercive pressures arise from formal and informal demands exerted by organizations upon which the focal organization depends. Normative pressures stem from professionalization, as norms of appropriate practice diffuse through occupational communities and standards. Mimetic pressures operate under uncertainty and lead organizations to model themselves on peers perceived to be successful. The pursuit of legitimacy, the generalized perception that an organization's actions are appropriate within its social system, underlies these mechanisms (Suchman 1995). Meta-analytic evidence confirms that isomorphic pressures are associated with organizational conformity across settings (Heugens and Lander 2009). Prior work has cautioned that the three pressures should be operationalized distinctly (Mizruchi and Fein 1999). Organizations respond to institutional processes strategically rather than uniformly, so that meaningful variance in adoption remains to be explained (Oliver 1991).

The framework has an established place in marketing research, where the institutional environment has been shown to shape the governance of marketing channels (Grewal and Dharwadkar 2002) and marketing actions directed at the social environment (Handelman and Arnold 1999). It has also been validated quantitatively in research on technology adoption. Teo et al. (2003) found that coercive, normative, and mimetic pressures all significantly predicted organizational intention to adopt interorganizational linkages. Liang et al. (2007) showed that institutional pressures shape the assimilation of enterprise systems. Research on interorganizational imitation has further specified the mimetic mechanism, showing that organizations imitate practices in proportion to the frequency of adoption among comparable others (Haunschild 1993; Haunschild and Miner 1997), and that the strength of the isomorphic response depends on organizational context (Dacin 1997).

The present setting differs from previous applications in the identity of the coercive actor. The coercive actor here is a platform operator rather than a state regulator or a trading partner. The mailbox providers control access to recipients, publish explicit requirements, and enforce them algorithmically. The February 2024 sender requirements therefore constitute a dated and publicly observable change in the coercive environment of every organization that sends commercial email at volume, and they motivate the timing of this study.

2.4 Compliance and decoupling

Meyer and Rowan (1977) argued that organizations facing institutional demands often adopt required structures ceremonially and decouple the formal structure from day-to-day practice in order to secure legitimacy at low cost. A substantial literature has developed this prediction. Organizations respond to legal demands by erecting symbolic structures whose relation to practice is loose (Edelman 1992). Organizations announce policies they do not implement (Westphal and Zajac 1994, 2001). Self-regulation often remains symbolic unless the enforcement environment strengthens it (Short and Toffel 2010). The extent of decoupling depends on internal conditions and on the observability of conduct (Crilly et al. 2012; Bromley and Powell 2012). Decoupling has been difficult to observe directly, because the researcher must see both the formal adoption and the substantive practice behind it, and the classic evidence rests on informant reports and case studies. In the email authentication setting, the formal structure is the published DMARC record and the substantive practice is the enforcement policy the record carries, and both are publicly observable. Decoupling can therefore be measured in this setting by comparing the entry policies of mandated and earlier adopters and their subsequent policy changes.

3 Research model and hypotheses

This study models the adoption of email authentication as an organizational response to coercive, normative, and mimetic pressures, and models the depth of the adopted configuration as the observable indicator of substantive versus ceremonial compliance. The research model (Fig. 1) assumes that the platform mandate, the domain's mail infrastructure, and recent adoption among category peers are all important determinants of DMARC adoption, and it distinguishes adoption from the enforcement depth of the adopted policy. The relationships of the proposed research model and the associated hypotheses are discussed in the following sections.

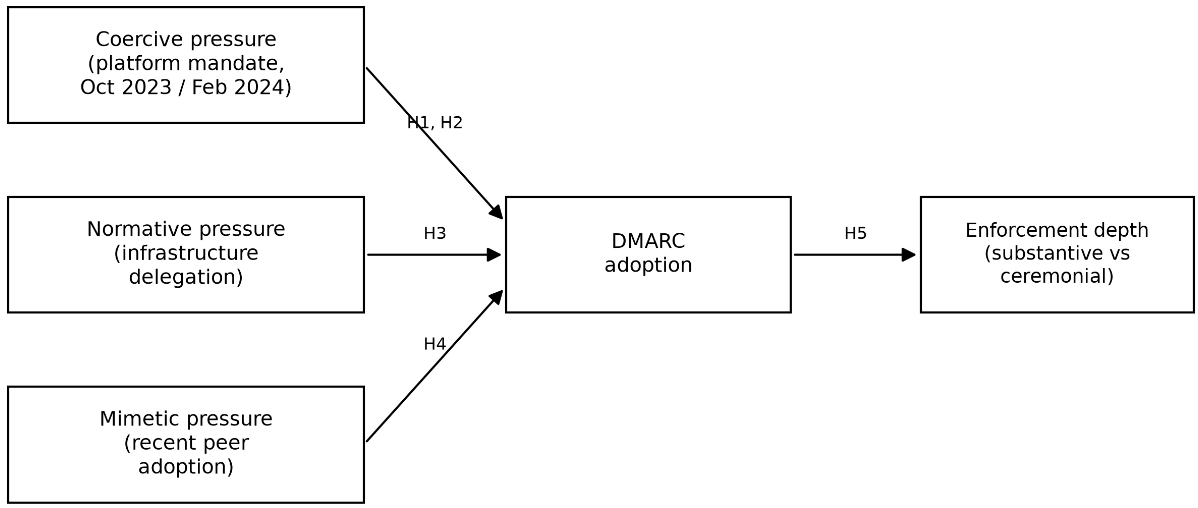

Fig. 1 The research model. The platform mandate (H1), conditioned by audience orientation (H2), infrastructure delegation (H3), and recent peer adoption (H4) relate to DMARC adoption; enforcement depth separates substantive from ceremonial compliance among adopters (H5).

3.1 The impact of the platform mandate

Coercive pressure arises from entities upon which an organization depends and which can attach consequences to non-conformity (DiMaggio and Powell 1983). Senders of commercial email depend on mailbox providers for access to recipients, and a message that a provider rejects does not reach the recipient. The October 2023 announcement and the February 2024 enforcement of the Google and Yahoo sender requirements converted advisory authentication practice into a condition of channel access with published dates and thresholds (Google 2023, 2026; Yahoo 2026). Prior research has found that perceived coercive pressure from resource-dominant partners significantly increases the adoption of technologically mediated practices (Teo et al. 2003; Liang et al. 2007). If coercive pressure operates in this setting, the adoption trajectory of the affected population should exhibit discontinuities aligned with the published dates of the mandate rather than gradual diffusion alone. Therefore, this study proposes:

H1: The announcement and enforcement of mailbox provider sender mandates are associated with significant changes in the level and slope of DMARC adoption among organizational domains.

3.2 The role of audience orientation

Coercive pressure binds in proportion to the organization's dependence on the coercing actor (DiMaggio and Powell 1983; Oliver 1991). The mandates apply to senders of bulk email to consumer mailboxes, and consumer mailboxes are concentrated at the mandating providers. Organizations whose activity is oriented to consumer audiences, such as retail, media, and travel, depend more heavily on reaching those mailboxes than organizations oriented to technical or business audiences. Consequently, consumer-facing organizations should respond more strongly to the mandate. Therefore, this study proposes:

H2: The post-mandate increase in DMARC adoption is stronger for domains in consumer-facing categories than for other domains.

3.3 The impact of normative pressures

Normative pressure stems from professionalization (DiMaggio and Powell 1983). In the email setting, a concrete professionalization decision is the choice of mail infrastructure. An organization that delegates its mail to a major workspace provider or to a dedicated email security gateway enters a professionalized service relationship in which authentication is standard practice. Such providers document and default authentication configurations, and their tooling embodies the norms codified in the standards (Kitterman 2014; Crocker et al. 2011; Kucherawy and Zwicky 2015). Organizations operating their own mail infrastructure, or relying on simple forwarding services, are less exposed to these norms. Prior research has found that normative pressure transmitted through professional relationships significantly predicts adoption (Teo et al. 2003). Therefore, this study proposes:

H3: Domains whose email infrastructure is operated by major providers or security gateways exhibit a significantly higher probability of DMARC adoption than domains with self-operated infrastructure.

3.4 The impact of mimetic pressures

Mimetic pressure operates under uncertainty (DiMaggio and Powell 1983; Mizruchi and Fein 1999). Filtering systems are adaptive and opaque (Cormack 2008; Blanzieri and Bryl 2008), and the consequences of non-compliance are probabilistic and delayed, so the behavior of comparable organizations serves as a guide to appropriate practice. Research on diffusion and interorganizational imitation shows that practices spread through the observation of comparable others (Strang and Soule 1998), that adoption can follow bandwagon dynamics under uncertainty (Abrahamson 1991), and that organizations imitate in proportion to the frequency of recent adoption among comparable others (Haunschild 1993; Haunschild and Miner 1997). In this setting, the relevant comparables are organizations in the same activity category, whose practices circulate through the same professional communities. Therefore, this study proposes:

H4: The probability that a domain adopts DMARC in a given period increases with recent adoption of DMARC among domains in the same category.

3.5 DMARC adoption and enforcement depth

Institutional theory predicts that organizations adopting under external mandate will disproportionately adopt ceremonially (Meyer and Rowan 1977). The diffusion literature has similarly distinguished early adopters, whose adoption tracks technical merit, from late adopters, whose adoption is increasingly driven by legitimacy (Tolbert and Zucker 1983; Kennedy and Fiss 2009). Organizations that adopted DMARC before the mandate did so, on average, for the operational value of the practice. Organizations induced to adopt by the mandate satisfy an external demand, and a monitoring-only record suffices for that purpose. Ceremonial adoption should therefore be more prevalent among post-enforcement adopters at the moment of adoption. In addition, if the difference reflects decoupling rather than the recency of adoption, post-enforcement adopters should also be slower to strengthen their policies afterward. Therefore, this study proposes:

H5: Domains adopting DMARC after the enforcement of the mandate are significantly more likely to adopt in monitoring-only form, and significantly less likely to progress to enforcing configurations, than domains that adopted before the mandate.

4 Research methodology

4.1 Data sources and sample construction

The study draws on the OpenINTEL active DNS measurement infrastructure, which performs daily structured measurements of large domain populations and publishes the results for research use (van Rijswijk-Deij et al. 2016). The analysis uses OpenINTEL's measurement of the Tranco top sites list, a research-oriented domain ranking hardened against manipulation (Le Pochat et al. 2019). One snapshot per month, the first available measurement day, was retrieved for every month from August 2022, the earliest month available in the archive, through June 2026. For each snapshot and each apex domain, three facts were extracted: the presence of the domain in the measurement (via its SOA record), the domain's mail exchanger (MX) records, and the domain's DMARC record at the standard _dmarc location, from which the policy tag (p=), subdomain policy (sp=), percentage tag (pct=), and reporting address presence (rua=) were parsed. Records not beginning with the v=DMARC1 version tag were treated as absent; 0.2% of retrieved policy tags were malformed and treated as missing.

The archive contains no _dmarc measurements before January 2023. The analysis window is therefore January 2023 through June 2026, 42 monthly observations, which provides nine monthly observations before the October 2023 announcement.

Sample construction proceeded in three steps, summarized in Table 1. First, domains present in all 42 monthly snapshots form the balanced cohort (n = 238,736); balancing removes compositional change in the ranking from all longitudinal comparisons. Second, the analysis is restricted to mail-active domains, defined as publishing MX records in at least half of observed months (n = 191,431), since DMARC adoption is only meaningful for domains that participate in email. Third, for the event history analyses, domains that had already adopted DMARC at the window's first observation are left-censored and excluded, leaving a risk set of 110,752 domains at risk of first adoption, among which 57,003 adoption events occur during the window.

Table 1. Sample construction.

Step	Criterion	n
Monthly snapshots retrieved	first measurement day per month, Aug 2022 to Jun 2026	47
Analysis window	months with _dmarc coverage, Jan 2023 to Jun 2026	42
Balanced cohort	domain present in all 42 snapshots	238,736
Mail-active cohort	MX records in at least half of observed months	191,431
Event-history risk set	not adopted at January 2023	110,752
Categorized systematic sample	every twelfth cohort domain	15,953
Firm-level subsample	index constituents matched to cohort domains	450

Domain categories were assigned to a deterministic systematic sample (every twelfth domain of the alphabetically ordered cohort; n = 15,953) in three steps. First, each sample domain's homepage title and meta description were retrieved (75.6% reachable). Second, a large language model (Qwen 2.5 72B Instruct, temperature 0) classified each domain from this metadata into a fixed 21-category taxonomy and made a binary judgment of consumer orientation; domains without retrievable metadata were classified from the domain name alone and flagged, and all analyses using categories are repeated excluding these lower-confidence cases. LLM-based annotation with validation has been shown to match or exceed human crowd annotation quality (Gilardi et al. 2023). Third, the labels were validated against two independent sources: content categories from Cloudflare's domain intelligence service for 353 overlapping domains (consumer-orientation agreement 75.4%), and GICS/ICB sector classifications for the 33 sample domains belonging to S&P 500, FTSE 100, and FTSE 250 constituents mapped to their official domains through Wikidata (agreement 81.8%). Classification succeeded for 15,878 of the 15,953 sampled domains. Domain popularity is measured as the domain's rank decile in a pinned Tranco list (list 94VW2), retained as a control covariate.

4.2 Measures

Table 2 summarizes the study's measures. Adoption is a binary domain-month state: the presence of a syntactically valid DMARC record. Enforcement depth is the published policy: none (monitoring only), quarantine, or reject. Coercive pressure is operationalized by calendar time relative to the mandate's two public dates, the October 2023 announcement and the February 2024 enforcement start (Google 2023, 2026; Yahoo 2026). Coercive exposure (H2) is operationalized by the classifier's binary consumer-orientation judgment described above; the metadata-only variant of the labels supplies the robustness check reported in the analysis. Normative carriage (H3) is operationalized from MX records: each domain's mail infrastructure is classified by suffix rules into Google Workspace, Microsoft 365, dedicated email security gateways, regional consumer providers, hosting providers, forwarding services, cloud email services, and self-operated or other infrastructure, taking the modal class over the domain's observed months. Mimetic exposure (H4) is measured as recent peer adoption activity: the share of the domain's category peers that adopted DMARC during the trailing three months, centered on each month's cross-category mean so that the measure captures a category's position relative to the population trend rather than the common diffusion shock. The stock of peer adoption (lagged prevalence) is reported as an alternative specification; as Section 5.2 documents, the stock measure is confounded in hazard models by risk-set depletion. All measures are derived from public data, and no self-reported data are used.

Table 2. Measures.

Measure	Definition	Source
DMARC adoption	presence of a valid record at _dmarc.domain	OpenINTEL snapshots
Enforcement depth	published policy: none, quarantine, or reject	OpenINTEL snapshots
Coercive timing	announcement Oct 2023; enforcement Feb 2024	Google (2023, 2026); Yahoo (2026)
Consumer orientation	binary classifier judgment from homepage metadata, validated against two external sources	Section 4.1
Infrastructure class	modal MX provider class over observed months	OpenINTEL MX records
Recent peer adoption	trailing three-month category adoption share, centered on the monthly cross-category mean	derived from panel
Popularity	rank decile in pinned Tranco list	Le Pochat et al. (2019)

4.3 Estimation

H1 and H2 are tested with segmented regression interrupted time series models (Wagner et al. 2002; Lopez Bernal et al. 2017) on the monthly cohort adoption rate, with level and slope terms at both the announcement and enforcement dates and heteroscedasticity and autocorrelation consistent standard errors with four lags (Newey and West 1987). H2 is tested by segmented regression on the difference between the consumer-facing and other monthly adoption series, which yields a single time series on which the autocorrelation-consistent errors are well defined; the stacked stratum-interaction model is reported descriptively alongside it. H3 and H4 are tested with discrete-time event history models (Allison 1982): a logit of first adoption on domain-months in the risk set, with period controls, rank decile, and standard errors clustered by domain; the H4 specification runs on the categorized subsample and adds category fixed effects and the recent peer adoption measure described above. Peer-effect estimates in observational data face the reflection problem (Manski 1993); the month-centered flow measure, category fixed effects, and period controls limit, but cannot fully eliminate, the resulting identification concerns, and the H4 estimate is read as an association consistent with imitation rather than a causal peer effect. H5 is tested in two parts: a logit contrasting monitoring-only adoption between pre-enforcement and post-enforcement adopter cohorts with infrastructure and popularity controls, and a discrete-time model of progression from monitoring-only to enforcing policies with time-since-adoption controls, which accounts for the shorter follow-up time of recent adopters. Robustness checks comprise exclusion of the two transition months, a placebo breakpoint within the pre-announcement period, and an equal-follow-up variant of the progression analysis. All effect estimates are reported with 95% confidence intervals. Analyses use Python (DuckDB for data assembly; statsmodels for estimation).

5 Data analysis

5.1 Adoption over time and the mandate

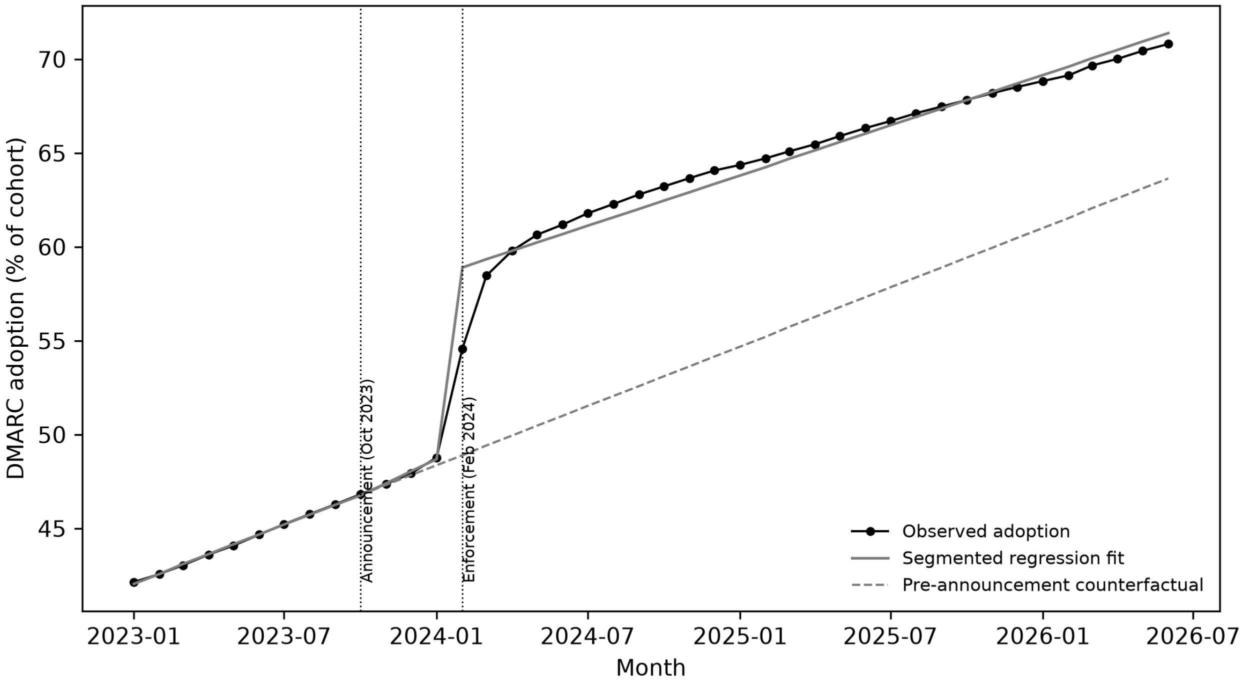

Fig. 2 Monthly DMARC adoption in the balanced mail-active cohort (n = 191,431), with the segmented regression fit and the pre-announcement counterfactual. Dotted vertical lines mark the October 2023 announcement and the February 2024 enforcement date.

Fig. 2 plots the monthly DMARC adoption rate in the balanced mail-active cohort together with the fitted segmented regression and the counterfactual continuation of the pre-announcement trend. Adoption rises from 42.1% in January 2023 to 70.8% in June 2026. Table 3 reports the segmented regression estimates. Before the announcement, adoption grew at 0.53 percentage points per month (95% CI 0.51 to 0.54). The October 2023 announcement is associated with no level change (-0.03 points, 95% CI -0.10 to 0.03) but with a significant slope increase of 0.12 points per month (95% CI 0.07 to 0.17). The February 2024 enforcement date is associated with a level increase of 9.56 percentage points (95% CI 8.10 to 11.02), after which the slope declines by 0.20 points per month (95% CI -0.26 to -0.13) relative to the notice period, settling at approximately 0.45 points per month. The model accounts for 99.4% of the variance in the series. By the end of the window, observed adoption exceeds the pre-announcement counterfactual by 7.2 percentage points. These results support H1: the announcement is associated with a slope change and the enforcement date with a large level change, while the announcement level term is not significant. The post-enforcement slope is slightly below the notice-period slope, which is consistent with the mandate having accelerated adoption that diffusion would otherwise have produced later.

Table 3. Segmented regression estimates for monthly DMARC adoption (H1). HAC standard errors, four lags. n = 42 months, cohort n = 191,431 domains.

Term	Estimate (pp)	95% CI	p
Intercept	42.049	41.984 to 42.114	<.001
Baseline slope (per month)	0.527	0.514 to 0.539	<.001
Announcement level change	-0.032	-0.099 to 0.034	.339
Announcement slope change	0.118	0.071 to 0.166	<.001
Enforcement level change	9.562	8.102 to 11.022	<.001
Enforcement slope change	-0.199	-0.264 to -0.134	<.001

Stratifying the categorized subsample by consumer orientation tests whether coercive exposure conditioned the response (H2). Fig. 4 plots the two adoption series. The primary test is a segmented regression on the monthly difference between the two series. The consumer-facing minus other adoption gap widens by 5.67 percentage points at the enforcement date (95% CI 4.95 to 6.38, $p < .001$), and the two series do not differ significantly at the announcement. Descriptively, domains classified as other than consumer-facing ($n = 7{,}627$) exhibit an enforcement level change of 6.68 percentage points (95% CI 5.58 to 7.77), while consumer-facing domains ($n = 8{,}251$) respond with approximately 12.3 points. Consumer-facing domains entered the window with lower adoption than other domains (40.5% against 43.3% in January 2023) and overtook them in the enforcement month, as shown in Fig. 4. Restricting the strata to domains classified from homepage metadata leaves the difference estimate essentially unchanged (5.68 points, 95% CI 5.04 to 6.33). These results support H2.

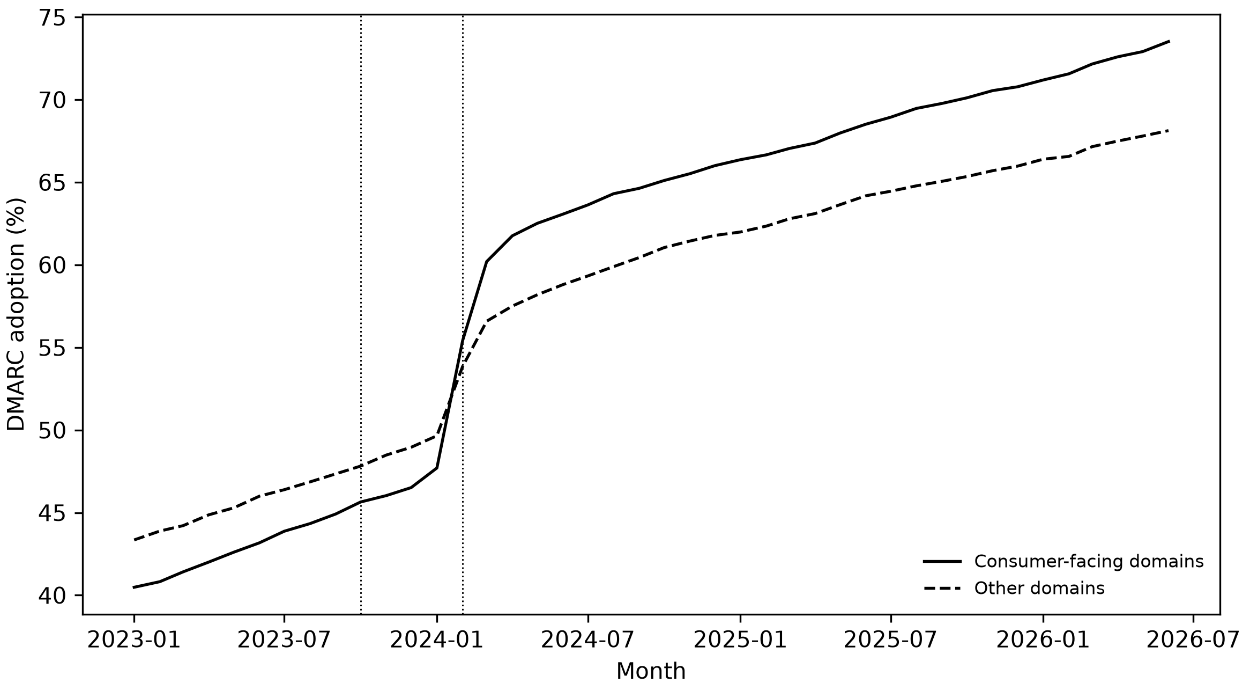

Fig. 4 DMARC adoption among consumer-facing and other domains in the categorized systematic sample. Consumer-facing domains had lower adoption at the start of the window and higher adoption after the enforcement date.

A complementary firm-level analysis examines the top of the firm-size distribution. Constituents of the S&P 500, FTSE 100, and FTSE 250 indices were mapped to their official domains through Wikidata, yielding 450 listed-firm domains within the cohort. These domains had already reached 92.4% adoption in January 2023 and 96.2% in January 2024, and their series exhibits no enforcement discontinuity distinguishable from zero (level change 0.68 percentage points, 95% CI -0.14 to 1.51, among non-consumer sectors; consumer-sector difference 0.09 points, 95% CI -0.69 to 0.88). The aggregate response was therefore concentrated in the part of the population below the large-firm stratum, where adoption was still incomplete when the mandate arrived.

5.2 Infrastructure, peers, and adoption

Table 4 reports the discrete-time event history estimates for first adoption among the 110,752 domains at risk at the start of the window (3,189,384 domain-months; 57,003 adoption events; standard errors clustered by domain). Relative to domains with self-operated or unclassified infrastructure, the adoption hazard is higher by a factor of 1.84 for domains on Google Workspace (95% CI 1.80 to 1.89), 2.83 for domains on Microsoft 365 (95% CI 2.75 to 2.90), and 3.72 for domains behind dedicated email security gateways (95% CI 3.58 to 3.87). Domains on consumer-oriented regional providers (OR 0.59, 95% CI 0.56 to 0.62) and simple forwarding services (OR 0.53, 95% CI 0.49 to 0.58) adopt at significantly lower rates, while generic hosting and cloud email services do not differ significantly from the reference. These results support H3: the more professionalized the mail infrastructure, the higher the adoption hazard. Period effects within the same model are consistent with H1 at the domain level: relative to the pre-announcement period, the adoption hazard is 1.25 times higher during the notice period and 2.56 times higher after enforcement. Adoption probability declines with rank decile (OR 0.96 per 100,000 ranks), indicating that more popular domains adopt earlier.

Table 4. Discrete-time event history of first DMARC adoption (H3). Logit odds ratios; SEs clustered by domain. Reference: self-operated or other infrastructure; pre-announcement period.

Covariate	OR	95% CI	p
Google Workspace	1.844	1.801 to 1.887	<.001
Microsoft 365	2.828	2.754 to 2.903	<.001
Email security gateway	3.720	3.580 to 3.866	<.001
Regional consumer provider	0.591	0.562 to 0.621	<.001
Hosting provider	0.993	0.941 to 1.048	.79
Forwarding service	0.532	0.487 to 0.581	<.001
Cloud email service	1.018	0.935 to 1.108	.69
Rank decile	0.964	0.960 to 0.968	<.001
Notice period (Oct 2023 to Jan 2024)	1.251	1.208 to 1.296	<.001
Post-enforcement period	2.555	2.493 to 2.618	<.001

The mimetic hypothesis is tested on the categorized subsample (9,232 risk-set domains; 265,161 domain-months; 4,790 adoption events) with category fixed effects. The preferred flow specification replicates the infrastructure gradient within the subsample (Google Workspace OR 1.61, 95% CI 1.48 to 1.75; Microsoft 365 OR 2.46, 95% CI 2.24 to 2.70; security gateways OR 2.94, 95% CI 2.57 to 3.37). Recent peer adoption activity is associated with a significantly higher adoption hazard: each additional percentage point of category peers adopting during the trailing three months, relative to the population trend that month, is associated with 4.2% higher odds of adoption (OR 1.042 per point, 95% CI 1.032 to 1.052, $p < .001$). These results support H4 in the form the imitation literature predicts, namely a response to the frequency of recent adoption among comparable others. The alternative stock specification, one-month-lagged peer prevalence, carries a negative coefficient under the same controls. This is the expected signature of risk-set depletion, since categories with high accumulated prevalence retain disproportionately adoption-resistant domains, and it indicates that the flow measure is the appropriate operationalization of mimetic exposure in hazard models.

5.3 Ceremonial versus substantive compliance

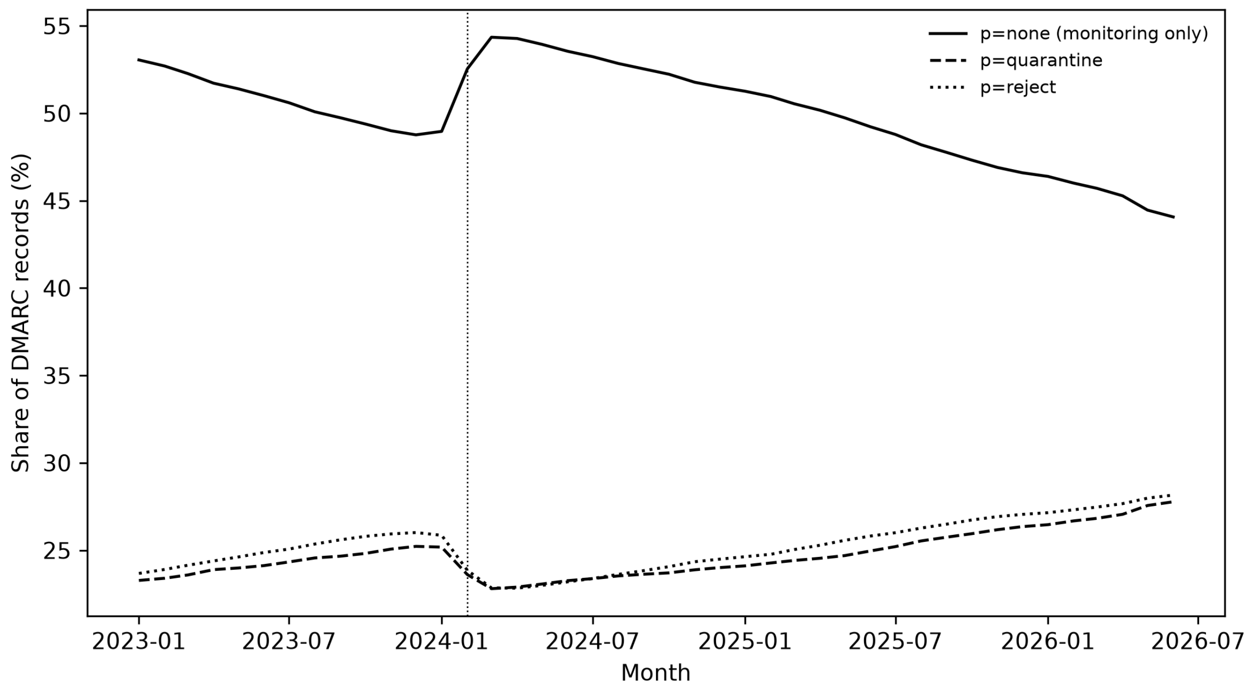

Fig. 3 Composition of published DMARC policies over the window. The monitoring-only share steps up at enforcement as mandated adopters enter at p=none, then declines slowly as a minority strengthen their policies.

Fig. 3 plots the composition of published DMARC policies over the window. Table 5 reports the decoupling estimates. Among domains adopting during the window with a parseable policy at adoption (147 adopters with malformed first policy tags are excluded), 70.1% of pre-enforcement adopters (n = 13,677) published a monitoring-only policy at adoption, against 81.4% of post-enforcement adopters (n = 43,179). Controlling for infrastructure class and rank decile, post-enforcement adoption is associated with 1.91 times higher odds of monitoring-only entry (95% CI 1.82 to 1.99). The progression analysis addresses the possibility that recent adopters merely lack time to strengthen their policies. In a discrete-time model of first movement from a monitoring-only to an enforcing policy, with time-since-adoption controls, post-enforcement adopters progress at 0.63 times the hazard of pre-enforcement adopters (95% CI 0.60 to 0.65). In absolute terms, 45.1% of pre-enforcement monitoring-only adopters progress to an enforcing policy within the window, against 21.4% of post-enforcement adopters; restricting both groups to an identical twelve-month follow-up, the shares are 23.5% and 12.4% (OR 0.46, 95% CI 0.44 to 0.49). Both components of H5 are supported. At the population level this compositional shift is visible in Fig. 3 as a step increase in the monitoring-only share at enforcement, followed by a slow decline as a minority of adopters strengthen their policies.

Table 5. Decoupling estimates (H5).

Quantity	Pre-enforcement adopters	Post-enforcement adopters	Estimate
Monitoring-only at adoption	70.1% (n = 13,677)	81.4% (n = 43,179)	OR 1.91 (1.82 to 1.99)
Progression hazard (monthly)	reference		OR 0.63 (0.60 to 0.65)
Ever progressed within window	45.1%	21.4%	
Progressed within 12 months	23.5%	12.4%	OR 0.46 (0.44 to 0.49)

5.4 Robustness

Excluding the two transition months (February and March 2024), during which the enforcement response was still unfolding, raises the estimated enforcement level change to 10.46 percentage points (95% CI 9.98 to 10.94). A placebo breakpoint placed at June 2023 and fitted on the pre-announcement window alone yields a level change of 0.11 percentage points (95% CI 0.07 to 0.15); the estimate is statistically distinguishable from zero because the pre-period trend is very tight, but its magnitude is roughly one ninetieth of the enforcement effect. The primary series retains residual positive autocorrelation (Durbin-Watson 1.28); re-estimating the model with eight Newey-West lags leaves the enforcement estimate unchanged (9.56 points, 95% CI 8.23 to 10.90). The equal-follow-up decoupling estimate reported above (OR 0.46) is stronger than the primary progression estimate. For the category-based analyses, restricting classification to domains with retrievable homepage metadata, thereby excluding the lower-confidence domain-name-only labels, leaves the H2 difference estimate essentially unchanged, and the H3 infrastructure gradient replicates within the categorized subsample under the preferred flow specification. Table 6 summarizes the hypothesis tests.

Table 6. Testing hypotheses.

H	Test	Estimate	p	The result
1	Enforcement level change (segmented regression)	+9.56 pp	<.001	Supported
2	Consumer-facing difference in enforcement level change (difference series)	+5.67 pp	<.001	Supported
3	Infrastructure class odds ratios (event history)	0.53 to 3.72	<.001	Supported
4	Recent peer adoption (event history, per +1 pp)	OR 1.042	<.001	Supported
5	Monitoring-only entry OR 1.91; progression OR 0.63		<.001	Supported

6 Discussion

The interrupted time series analysis showed a large and durable increase in DMARC adoption aligned with the enforcement date of the mandate. This finding is consistent with prior studies in which coercive pressure from resource-dominant actors significantly predicted the adoption of technologically mediated practices (Teo et al. 2003; Liang et al. 2007). Moreover, the announcement was associated with a modest slope increase only, and the large level change occurred when enforcement began. This asymmetry is consistent with the argument of Oliver (1991) that organizations respond strategically to institutional demands and delay costly compliance until enforcement takes effect. The finding that the post-enforcement slope falls slightly below the notice-period slope suggests that the mandate accelerated adoption that gradual diffusion would otherwise have produced later.

The findings on audience orientation are consistent with the dependence logic of coercive pressure. Consumer-facing domains, which depend more heavily on the mandating providers for access to their audiences, responded to enforcement with an increase nearly twice as large as that of other domains, while the two strata did not differ significantly before the mandate. At the top of the firm-size distribution, constituents of major stock indices had already reached 92.4% adoption in the window's first month and show no enforcement discontinuity distinguishable from zero. These results indicate that the most visible organizations converged early, which is consistent with the effect of visibility and scrutiny on institutional conformity (Dacin 1997), and that the response to the mandate was concentrated in the part of the population where adoption was still incomplete.

The findings affirm that the domain's mail infrastructure has a significant influence on adoption. Domains behind dedicated email security gateways adopt at 3.7 times the hazard of self-operated domains, with major workspace providers in between and consumer-grade forwarding arrangements below the reference. This ordering is consistent with the finding of Teo et al. (2003) that normative pressure transmitted through professional relationships predicts adoption, and it extends that finding to a setting in which the norm is transmitted through the operational defaults and documentation of the organization's chosen infrastructure provider. The result is also consistent with Dacin (1997), in that the strength of the isomorphic response is conditioned by the organization's structural position.

The results validate the influence of mimetic pressure on adoption. Domains adopt at a higher rate when more of their category peers have adopted recently, which is consistent with the frequency-based imitation documented in prior research (Haunschild 1993; Haunschild and Miner 1997). The effect is modest relative to the coercive and normative effects in the same model, which suggests that mimetic pressure played a secondary role in this setting. Accumulated peer prevalence carries a negative conditional association with adoption in the hazard model, which is the expected consequence of risk-set depletion. Therefore, studies that measure mimetic pressure as accumulated prevalence in hazard models may underestimate imitation effects.

The decoupling findings are consistent with the prediction of Meyer and Rowan (1977) that organizations adopting under external demand adopt the required formal structure without corresponding changes in practice, a pattern previously documented for legal structures (Edelman 1992), governance policies (Westphal and Zajac 2001), and self-regulatory programs (Short and Toffel 2010). Post-enforcement adopters disproportionately published the monitoring-only configuration that satisfies the formal requirement, and they subsequently strengthened their configurations at roughly half the rate of earlier adopters. The equal-follow-up estimate shows a larger difference (OR 0.46). The pattern is difficult to attribute to capability differences alone, since infrastructure and popularity controls persist in the entry model and the progression contrast replicates under an identical follow-up window. In this setting, compliance with the requirement is verified automatically through the presence of a published record. The results indicate that ceremonial compliance also occurs when verification is automated, because a monitoring-only record is sufficient to satisfy the verified requirement.

The cohort's 42% baseline adoption in January 2023 and 71% by mid 2026 are consistent with the measurement literature's record of incomplete authentication uptake (Durumeric et al. 2015; Foster et al. 2015; Hu and Wang 2018). The composition results add that a substantial share of measured adoption is monitoring-only in form.

7 Implications and future research

7.1 Theoretical implications

This empirical study aims to fill the existing gap in the literature on organizational responses to platform mandates. The results revealed that the three-pressure framework of institutional theory transfers to a setting in which the coercive actor is a platform operator: coercive pressure produced the dominant discontinuity, normative pressure operated through professionalized infrastructure, and mimetic exposure was measurable as recent peer adoption. The study contributes to institutional theory in two further respects. First, adoption changed mainly at the enforcement date, when consequences began to apply, and only modestly at the announcement, which supports the argument that organizations respond strategically to institutional demands (Oliver 1991). Second, the decoupling results show that ceremonial adoption also arises when compliance is verified automatically. This connects institutional theory to the study of algorithmic regulation, in which standard-setting, monitoring, and sanctioning are delegated to automated systems (Yeung 2018), and it suggests a proposition for platform governance research (Gorwa 2019; Kretschmer et al. 2022): when a mandate is enforced through automated verification of a formal requirement, organizations will comply with the verified requirement at high rates, while adoption of the associated substantive practice will remain lower. For the marketing literature, the study shows that the authentication and filtering infrastructure of the email channel, which the effectiveness literature has treated as given (Sahni et al. 2018; Zhang et al. 2017), can be studied with organizational theory and public data.

7.2 Practical implications

The results of this study have practical implications for platform operators, providers, and marketing organizations. For platform operators, the results indicate that mandates are followed by rapid and large-scale compliance, that notice periods are associated with limited anticipatory compliance relative to enforcement, and that the design of the verification affects the outcome: the mandate verified the presence of a DMARC record, and most mandated adopters published monitoring-only records. Operators that seek substantive outcomes should consider conditioning treatment on enforcing policies. For infrastructure and email service providers, the infrastructure gradient quantifies their role in distributing compliance norms; defaults and managed onboarding are associated with higher adoption than published guidance alone. For marketing organizations, the results show that the majority of mandated adopters stopped at the monitoring-only minimum, so organizations that adopt an enforcing policy differ from the majority on a dimension that mailbox providers observe directly and that provider documentation links to message handling. For policymakers observing private regulation of shared infrastructure, the results show that the mandate was followed by more adoption in one quarter than voluntary diffusion had produced in the preceding year, and that most of the new adoption was monitoring-only in form.

7.3 Limitations and future research

Although the empirical results are based on a large panel, several limitations should be mentioned. The unit of analysis is the domain, not the firm; multi-domain organizations appear multiple times, and the mapping from domains to organizations is not observed. The cohort comprises domains stable in a top-1M popularity ranking across the window, so the findings generalize to established organizational domains rather than to smaller or transient domains. The category measures cover a systematic subsample and derive from an automated classifier whose consumer-orientation labels agree with an independent commercial classification for 75.4% of overlapping domains; the remaining misclassification would generally attenuate the stratum contrast. The categories were also assigned from homepages retrieved after the observation window, so category change between 2023 and the retrieval date is a further source of measurement error. Adoption of DMARC is one observable facet of email compliance practice: DKIM configuration is not measurable at population scale without sender cooperation, and SPF records carry no policy field, so they cannot distinguish ceremonial from substantive compliance; DMARC is also the record whose publication the mandates operationalize. The design is observational; the interrupted time series estimates are associational, and although the alignment of the discontinuity with the enforcement date and the placebo comparisons support an institutional interpretation, unobserved contemporaneous shocks cannot be excluded. The event history models use three coarse period bins rather than a saturated monthly baseline, and adoption is treated as an absorbing first event, abstracting from subsequent record churn. Future research could link domains to firm registries to recover organization-level covariates such as size and industry, exploit the enforcement waves announced through 2025 as repeated events, model the progression from monitoring-only to enforcing configurations as a function of observed enforcement experiences, and extend the decoupling design to other platform mandates whose compliance states are publicly observable.

8 Conclusions

Platform operators set requirements for the organizations that depend on them, and email provides a setting in which the response of a large population of organizations to such requirements is publicly observable. The lack of empirical research on organizational responses to platform mandates inspired this study to pose the following three questions: Q1: Did the mailbox provider sender mandates significantly change the level and trajectory of email authentication adoption? Q2: Do normative carriers and mimetic exposure significantly predict which organizations adopt? Q3: To what extent is post-mandate compliance substantive rather than ceremonial?

On the first question, the February 2024 enforcement date is associated with a 9.6 percentage point immediate increase in DMARC adoption in a balanced cohort of 191,431 organizational domains, over a stable baseline trend of half a point per month, with a modest slope increase after the October 2023 announcement. The increase was concentrated among consumer-facing domains and absent among large listed firms, which had adopted before the mandate. On the second question, the adoption hazard rises with the professionalization of the domain's mail infrastructure, from half the reference rate for forwarding arrangements to 3.7 times the reference rate behind email security gateways, and it rises with recent adoption among category peers. On the third question, mandate-era adopters disproportionately complied in monitoring-only form and were roughly half as likely to progress to enforcing configurations, which is consistent with the decoupling of formal from substantive compliance.

The results show that platform mandates can produce rapid and large-scale compliance, and that a substantial share of this compliance is formal rather than substantive. Future research on platform governance should take the design of compliance verification into account.

Competing interests. The author is the founder of a commercial email deliverability company. This is a material competing interest. The analysis rests entirely on public data and released code, no product is named, evaluated, or recommended by any result, and the findings do not depend on any commercial offering.

Author contributions. Francis Davison is the sole author and is responsible for the conception, the data pipeline and its code, the analysis, and the accuracy of every figure and value. AI tools were used under the author's direction for research and drafting assistance and, as reported in Section 4, as a classification instrument; the author reviewed and takes responsibility for all content.

Data and code availability. The snapshot extraction code, panel construction, categorization pipeline including the classification prompt and validation, estimation scripts, and figure-generation code are released with this paper, together with the pinned Tranco list identifier and the derived series. The OpenINTEL archive and all cited sources are public.

Acknowledgment. The longitudinal analysis was made possible by OpenINTEL (https://www.openintel.nl/), a joint project of the University of Twente, SIDN, NLnet Labs and SURF; OpenINTEL open-access data is licensed CC BY-NC-SA 4.0 and used here for non-commercial research.

Funding. None external.

References

Abrahamson E (1991) Managerial fads and fashions: the diffusion and rejection of innovations. Acad Manag Rev 16(3):586-612. doi:10.2307/258919.

Allison PD (1982) Discrete-time methods for the analysis of event histories. Sociol Methodol 13:61-98. doi:10.2307/270718.

Blanzieri E, Bryl A (2008) A survey of learning-based techniques of email spam filtering. Artif Intell Rev 29(1):63-92. doi:10.1007/s10462-009-9109-6.

Bonfrer A, Drèze X (2009) Real-time evaluation of e-mail campaign performance. Mark Sci 28(2):251-263. doi:10.1287/mksc.1080.0393.

Boudreau K (2010) Open platform strategies and innovation: granting access vs. devolving control. Manag Sci 56(10):1849-1872. doi:10.1287/mnsc.1100.1215.

Bromley P, Powell WW (2012) From smoke and mirrors to walking the talk: decoupling in the contemporary world. Acad Manag Ann 6(1):483-530. doi:10.5465/19416520.2012.684462.

Cennamo C (2021) Competing in digital markets: a platform-based perspective. Acad Manag Perspect 35(2):265-291. doi:10.5465/amp.2016.0048.

Chittenden L, Rettie R (2003) An evaluation of e-mail marketing and factors affecting response. J Target Meas Anal Mark 11(3):203-217. doi:10.1057/palgrave.jt.5740078.

Cormack GV (2008) Email spam filtering: a systematic review. Found Trends Inf Retr 1(4):335-455. doi:10.1561/1500000006.

Crilly D, Zollo M, Hansen MT (2012) Faking it or muddling through? Understanding decoupling in response to stakeholder pressures. Acad Manag J 55(6):1429-1448. doi:10.5465/amj.2010.0697.

Crocker D, Hansen T, Kucherawy M (eds) (2011) DomainKeys identified mail (DKIM) signatures. RFC 6376.

Cutolo D, Kenney M (2021) Platform-dependent entrepreneurs: power asymmetries, risks, and strategies in the platform economy. Acad Manag Perspect 35(4):584-605. doi:10.5465/amp.2019.0103.

Dacin MT (1997) Isomorphism in context: the power and prescription of institutional norms. Acad Manag J 40(1):46-81. doi:10.2307/257020.

de Reuver M, Sorensen C, Basole RC (2018) The digital platform: a research agenda. J Inf Technol 33(2):124-135. doi:10.1057/s41265-016-0033-3.

DiMaggio PJ, Powell WW (1983) The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. Am Sociol Rev 48(2):147-160. doi:10.2307/2095101.

Durumeric Z, Adrian D, Mirian A, Kasten J, Bursztein E, Lidzborski N et al (2015) Neither snow nor rain nor MITM: an empirical analysis of email delivery security. In: Proceedings of the 2015 Internet Measurement Conference, pp 27-39. doi:10.1145/2815675.2815695.

Edelman LB (1992) Legal ambiguity and symbolic structures: organizational mediation of civil rights law. Am J Sociol 97(6):1531-1576. doi:10.1086/229939.

Foster ID, Larson J, Masich M, Snoeren AC, Savage S, Levchenko K (2015) Security by any other name: on the effectiveness of provider based email security. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications

Security, pp 450-464. doi:10.1145/2810103.2813607.

Gilardi F, Alizadeh M, Kubli M (2023) ChatGPT outperforms crowd workers for text-annotation tasks. Proc Natl Acad Sci 120(30):e2305016120. doi:10.1073/pnas.2305016120.

Google (2023) New Gmail protections for a safer, less spammy inbox. blog.google, October 2023. Accessed 8 July 2026.

Google (2026) Email sender guidelines. support.google.com/a/answer/81126. Accessed 8 July 2026.

Gorwa R (2019) What is platform governance? Inf Commun Soc 22(6):854-871. doi:10.1080/1369118x.2019.1573914.

Grewal R, Dharwadkar R (2002) The role of the institutional environment in marketing channels. J Mark 66(3):82-97. doi:10.1509/jmkg.66.3.82.18504.

Handelman JM, Arnold SJ (1999) The role of marketing actions with a social dimension: appeals to the institutional environment. J Mark 63(3):33-48. doi:10.1177/002224299906300303.

Hartemo M (2016) Email marketing in the era of the empowered consumer. J Res Interact Mark 10(3):212-230. doi:10.1108/jrim-06-2015-0040.

Haunschild PR (1993) Interorganizational imitation: the impact of interlocks on corporate acquisition activity. Adm Sci Q 38(4):564-592. doi:10.2307/2393337.

Haunschild PR, Miner AS (1997) Modes of interorganizational imitation: the effects of outcome salience and uncertainty. Adm Sci Q 42(3):472-500. doi:10.2307/2393735.

Herr T, Levine J (eds) (2026) Domain-based message authentication, reporting, and conformance (DMARC). RFC 9989. Obsoletes RFC 7489.

Heugens PPMAR, Lander MW (2009) Structure! Agency! (and other quarrels): a meta-analysis of institutional theories of organization. Acad Manag J 52(1):61-85. doi:10.5465/amj.2009.36461835.

Hu H, Wang G (2018) End-to-end measurements of email spoofing attacks. In: 27th USENIX Security Symposium.

Kannan PK, Li H (2017) Digital marketing: a framework, review and research agenda. Int J Res Mark 34(1):22-45. doi:10.1016/j.ijresmar.2016.11.006.

Kennedy MT, Fiss PC (2009) Institutionalization, framing, and diffusion: the logic of TQM adoption and implementation decisions among U.S. hospitals. Acad Manag J 52(5):897-918. doi:10.5465/amj.2009.44633062.

Kitterman S (2014) Sender policy framework (SPF) for authorizing use of domains in email, version 1. RFC 7208.

Kretschmer T, Leiponen A, Schilling M, Vasudeva G (2022) Platform ecosystems as meta-organizations: implications for platform strategies. Strateg Manag J 43(3):405-424. doi:10.1002/smj.3250.

Kucherawy M, Zwicky E (eds) (2015) Domain-based message authentication, reporting, and conformance (DMARC). RFC 7489.

Le Pochat V, Van Goethem T, Tajalizadehkhoob S, Korczynski M, Joosen W (2019) Tranco: a research-oriented top sites ranking hardened against manipulation. In: Proceedings of NDSS 2019. doi:10.14722/ndss.2019.23386.

Levine J, Herkula T (2017) Signaling one-click functionality for list email headers. RFC 8058.

Liang H, Saraf N, Hu Q, Xue Y (2007) Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. MIS Q 31(1):59-87. doi:10.2307/25148781.

Lopez Bernal J, Cummins S, Gasparrini A (2017) Interrupted time series regression for the evaluation of public health interventions: a tutorial. Int J Epidemiol 46(1):348-355. doi:10.1093/ije/dyw098.

Manski CF (1993) Identification of endogenous social effects: the reflection problem. Rev Econ Stud 60(3):531-542. doi:10.2307/2298123.

Meyer JW, Rowan B (1977) Institutionalized organizations: formal structure as myth and ceremony. Am J Sociol 83(2):340-363. doi:10.1086/226550.

Mizruchi MS, Fein LC (1999) The social construction of organizational knowledge: a study of the uses of coercive, mimetic, and normative isomorphism. Adm Sci Q 44(4):653-683. doi:10.2307/2667051.

Newey WK, West KD (1987) A simple, positive semi-definite, heteroskedasticity and autocorrelation consistent covariance matrix. Econometrica 55(3):703-708. doi:10.2307/1913610.

Oliver C (1991) Strategic responses to institutional processes. Acad Manag Rev 16(1):145-179. doi:10.2307/258610.

Rietveld J, Schilling MA (2021) Platform competition: a systematic and interdisciplinary review of the literature. J Manage 47(6):1528-1563. doi:10.1177/0149206320969791.

Sahni NS, Wheeler SC, Chintagunta PK (2018) Personalization in email marketing: the role of noninformative advertising content. Mark Sci 37(2):236-258. doi:10.1287/mksc.2017.1066.

Short JL, Toffel MW (2010) Making self-regulation more than merely symbolic: the critical role of the legal environment. Adm Sci Q 55(3):361-396. doi:10.2189/asqu.2010.55.3.361.

Strang D, Soule SA (1998) Diffusion in organizations and social movements: from hybrid corn to poison pills. Annu Rev Sociol 24:265-290. doi:10.1146/annurev.soc.24.1.265.

Suchman MC (1995) Managing legitimacy: strategic and institutional approaches. Acad Manag Rev 20(3):571-610. doi:10.2307/258788.

Teo HH, Wei KK, Benbasat I (2003) Predicting intention to adopt interorganizational linkages: an institutional perspective. MIS Q 27(1):19-49. doi:10.2307/30036518.

Tolbert PS, Zucker LG (1983) Institutional sources of change in the formal structure of organizations: the diffusion of civil service reform, 1880-1935. Adm Sci Q 28(1):22-39. doi:10.2307/2392383.

van Rijswijk-Deij R, Jonker M, Sperotto A, Pras A (2016) A high-performance, scalable infrastructure for large-scale active DNS measurements. IEEE J Sel Areas Commun 34(6):1877-1888. doi:10.1109/jsac.2016.2558918.

Wagner AK, Soumerai SB, Zhang F, Ross-Degnan D (2002) Segmented regression analysis of interrupted time series studies in medication use research. J Clin Pharm Ther 27(4):299-309. doi:10.1046/j.1365-2710.2002.00430.x.

Wattal S, Telang R, Mukhopadhyay T, Boatwright P (2012) What's in a "name"? Impact of use of customer information in e-mail advertisements. Inf Syst Res 23(3):679-697. doi:10.1287/isre.1110.0384.

Westphal JD, Zajac EJ (1994) Substance and symbolism in CEOs' long-term incentive plans. Adm Sci Q 39(3):367-390. doi:10.2307/2393295.

Westphal JD, Zajac EJ (2001) Decoupling policy from practice: the case of stock repurchase programs. Adm Sci Q 46(2):202-228. doi:10.2307/2667086.

Yahoo (2026) Sender best practices. senders.yahooinc.com/best-practices/. Accessed 8 July 2026.

Yeung K (2018) Algorithmic regulation: a critical interrogation. Regul Gov 12(4):505-523. doi:10.1111/rego.12158.

Zhang X, Kumar V, Cosguner K (2017) Dynamically managing a profitable email marketing program. J Mark Res 54(6):851-866. doi:10.1509/jmr.16.0210.

Competing interest: the author is the founder of SpamCipher, a commercial cold email and deliverability platform. This analysis is grounded only in primary and peer-reviewed sources. Canonical version: https://spamcipher.com/insights/platform-mandates-email-authentication