

When it's gone, it's gone!

The value of safeguarding consumer trust in the retail sector



Contents

1. Introduction
2. Trust pays for itself
3. Brand protection: the buck stops with you
4. Email's role in safeguarding trust
5. DMARC: a fundamental layer for retail email security
6. The results are in: how DMARC in the retail sector currently measures up
7. DMARC's role in safeguarding trust in retail
8. Is a lack of trust impacting your email ROI?
9. Logo visibility for consumer trust
10. Start safeguarding your brand reputation and consumer trust



19.5% of total
global retail sales
share comes from
ecommerce⁹



114% rise in global
ecommerce since 2018¹¹



\$4.8 billion worth
of global retail
ecommerce sales
in 2021^{9,10}

1. Introduction

American painter and writer Walter Anderson once said, 'Trust is like a vase, once it's broken, though you can fix it, the vase will never be the same again.' In business, there is a lot of focus on building trust. Consumer-facing sectors will go out of their way to build their brand and bolster reputation, but what are they doing to safeguard and maintain the consumer trust foundational to these? In this whitepaper, we'll focus on the value of safeguarding consumer trust in the retail sector, and how the changing ecommerce landscape amplifies email's role in doing this. We'll also explore how businesses can lock down the basics to secure consumer confidence now and in the future.

Executive summary

1

Trust has real business value, and is widely considered one of the most important factors for buying behavior and brand loyalty

4

90% of consumers agree or strongly agree that seeing a signed logo would improve their confidence in an email

2

We're seeing a shift to ecommerce that demands new ways to build and maintain trust, email plays a pivotal part in this

5

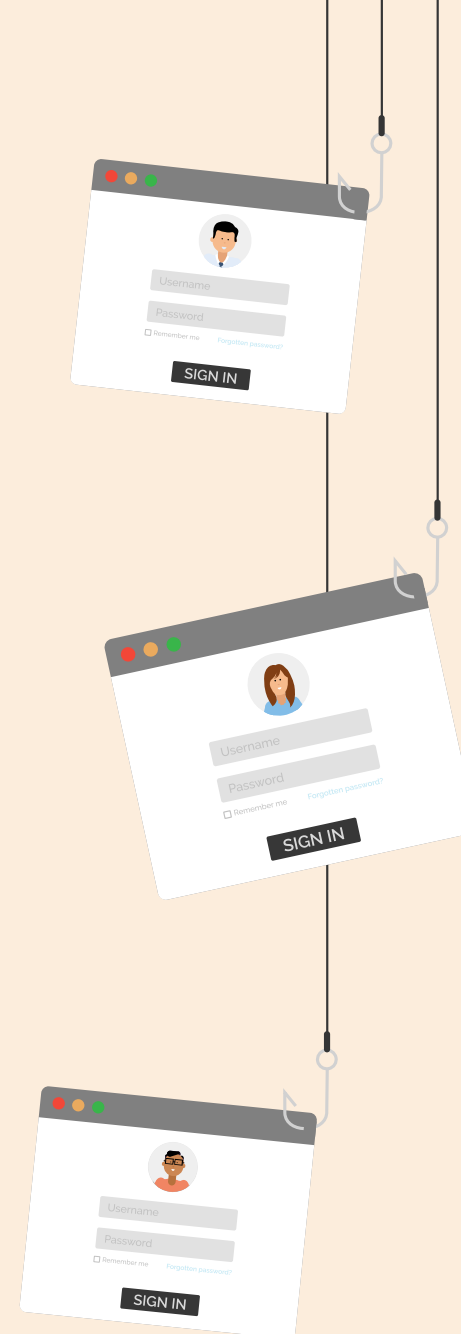
DMARC and BIMI with VMC are essential to locking down email security, vital for retailers' communications with consumers

3

88% of top global retailers are not protected from impersonation attacks

6

Retailers aren't recognizing the importance of fully implementing DMARC at p=reject, with the global policy=none still sitting at 52%



2. Trust pays for itself

In any relationship, trust is the building block that breeds longevity. And the relationship between business and consumer is no different. Being able to rely on a brand, and knowing that it will give us a consistently good product or service that we can rely on is often what makes us choose it over others.



"Trust is the glue of life. It's the most essential ingredient in effective communication. It's the foundational principle that holds all relationships."

Stephen Covey, Author of The 7 Habits of Highly Effective People¹

It's well documented that trust is considered one of the most important factors for consumer buying and loyalty. Edelman ranks brand trust as a top buying consideration, and furthermore found that a staggering 75% are loyal to a brand they trust even if there's a 'trendier' option available, while 59% would spend more on similar products from a brand they trust.² PWC also discovered 35%³ of people consider trust in a brand the most motivating factor to shop at a particular retailer. Add to this that 76% of consumers pay attention to the advertising and communications of brands they have trusted for a long time over just 48%² for those they haven't, and it's clear that trust quite literally pays for itself.



¹Steven Covey

²Edelman

³PWC

⁴Salesforce

The buying habits of loyal customers



76%
of people pay attention to the advertising of brands they have trusted for a long time²



75%
are loyal to a brand they trust even if there's a 'trendier' option available²



66%
will buy from a brand even if a competitor is more innovative²



59%
would spend more on similar products from a brand they trust²



65%
of customers stopped buying from brands that did something they consider distrustful⁴

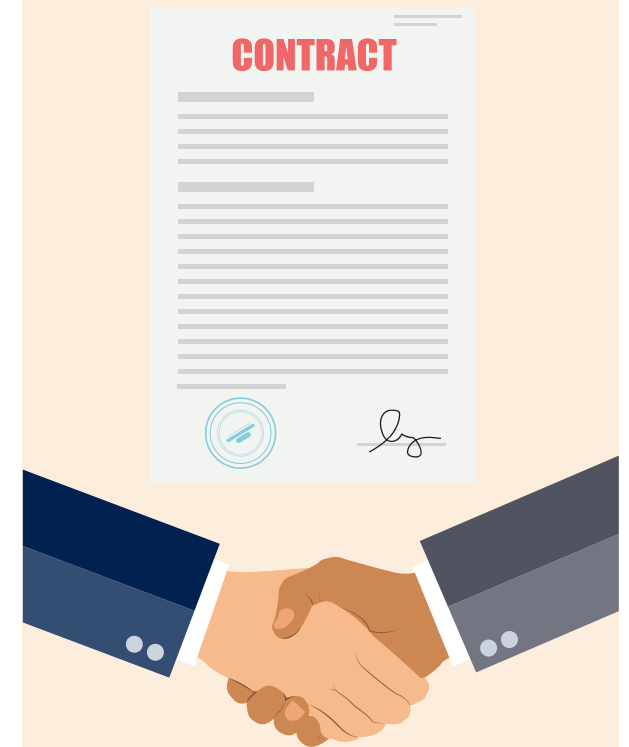
Consumer trust in the time of COVID

In 2019, 73% of consumers said that trust in companies mattered more than it did the previous year, and 54% said it was harder than ever to earn their trust.⁴ Now, in the wake of a global pandemic, we can only imagine how these figures have increased. Research conducted by Deloitte in June 2020 signposted that brand trust is still 'alive and palpable'.⁵ In troubled times consumers look to brands they trust to retain some sense of normality.

"In a time of so much uncertainty, when daily decisions about personal safety and financial wellbeing are made, most consumers are reaching for brands they trust. It may provide comfort to reach for something familiar, and it's one less decision to make."

Deloitte, Brand Power in Times of Covid Report⁵

It is likely that the global impact of the pandemic will be felt for years to come. Given that trust has been a driving force in protecting consumer buying in recent times, it will only become more important for businesses to safeguard it once they have earned it.



54%

of consumers say it's
harder than ever to earn
their trust⁴

3. Brand protection: the buck stops with you

Traditionally, conversations surrounding consumer trust have had product quality, service consistency, and societal commitments at the forefront. But what's becoming increasingly prominent in the age of data breaches, ransomware, and the ever-evolving phishing scam is consumer privacy and data security. Not surprisingly then, consumer trust and brand reputation now hang on how good businesses are at protecting these.

With the shift to digital, data is like a form of currency in itself, and businesses worldwide are raring to get their hands on it. However, PWC found that 88%⁶ of consumers base the willingness to share personal information on how much they trust a company. And even once a business does have it, Dusted found an eye-watering 81%⁷ of respondents reported they'd stop engaging with a brand online following a data breach.

Consumers aren't willing to hand out their information to just anyone, and those that do get it need to ensure it stays safe - or suffer the consequences.



88%

of consumers say their willingness to share personal information is based on how much they trust a company⁶



81%

of consumers will stop engaging with a brand online following widespread news of a data breach⁷

⁶PWC

⁷Dusted



Consumers can be unforgiving

RSA found that a groundbreaking 64%⁸ of Americans blame the company - not the hacker - for the loss of personal data. This might seem astounding, but it is understandable considering the limited visibility consumers have. For example, if they are impacted by a data breach, they won't see that it was in fact the outsourced HR company that was responsible. This limited visibility will lead them to leave the blame at the door of the company they know.

In the eyes of the consumer, the buck stops with you. The cold, hard truth is that consumers expect the businesses that handle and store their personal information to take the necessary measures to safeguard it. There's very little margin for error if they don't.



"Compounded by living digitally through a pandemic, consumer awareness surrounding privacy, cookies, and data has strengthened. But ultimately the consumer's view is still limited. So when things do go wrong (i.e. personal data is breached), the consumer will hold the brand they know accountable, even if the mistake has been made by an outsourced party. So, it's never been a more important time for businesses to put the building blocks in place to safeguard their reputation, and in turn solidify consumer trust."

Randal Pinto, CTO at Red Sift

⁸RSA Security

Costly fines for data mismanagement

It's not only the consumer that holds companies to account for the protection of data and privacy. Data protection laws like GDPR and CCPA were created for exactly this reason. Not abiding by these can set businesses back considerably, with fines of up to £20 million (\$28 million) for those that don't put the measures in place to protect consumer information. Times are changing, and the protection of consumer data will be high on the list of priorities for businesses, consumers, and governing bodies for the long term.



4. Email's role in safeguarding trust

The landscape between consumer and business is rapidly changing, and this has only accelerated as the pandemic moved virtually everyone to online buying. Currently, 19.5% of the total global retail sales share comes from ecommerce⁹, and so far this has amounted to a hefty \$4.8 billion in 2021.^{9,10} Since 2018, there's been a 114%¹¹ rise in global ecommerce overall.

The days of face-to-face interactions and brick-and-mortar buying are diminishing. Now, businesses must be creative in the way they build and maintain consumer trust, primarily by utilizing the digital channels that underpin this online-led buying environment.



19.5% of total global retail sales share comes from ecommerce⁹



114% rise in global ecommerce since 2018¹¹



\$4.8 billion worth of global retail ecommerce sales in 2021^{9,10}



Email and ecommerce go hand in hand

Whether logistical, transactional, or promotional, email underpins the online (and oftentimes in store) consumer lifecycle. Like a reverse economy of scale, with more consumers buying online than ever before, comes a need for more emails to be sent.

Every day, hundreds of thousands of businesses worldwide rely on email for their internal and external communications. More than 321 billion emails were sent everyday in 2021, and this figure is set to reach 376 billion by 2025.¹² But the very prevalence of email makes it an attractive target for cybercriminals looking to steal money, data — or both.



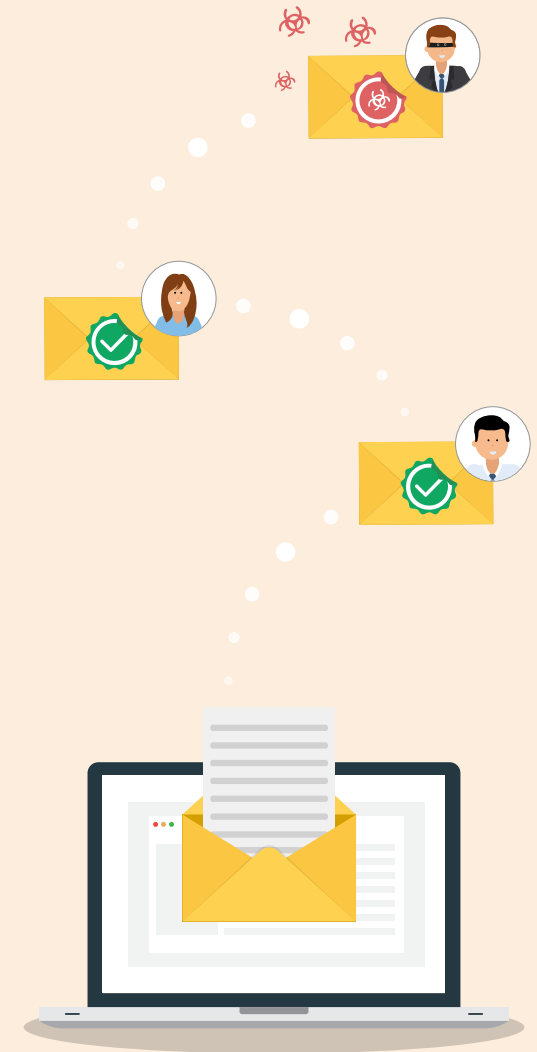
321 Billion

emails were sent everyday
in 2021¹²



376 Billion

emails sent daily by 2025¹²



5. DMARC: a fundamental layer for retail email security

With email being a vital lifeline between retailers and consumers, it's essential that the right measures are in place to protect it. Having DMARC fully-configured is essential for all businesses that use email, but particularly those that hold a lot of sensitive information, payment, and customer data like retail.

What is DMARC?

DMARC stands for Domain-based Message Authentication, Reporting, and Conformance. It's an email security and authentication protocol that protects domains against exact impersonation. Essentially, it ringfences your domain (*www.example.com*) and blocks hackers from being able to use it to impersonate your business and send phishing emails to your customers, employees, and supply chain.

How does DMARC work?

When correctly configured at a policy of p=reject, DMARC works using existing security protocols SPF and DKIM to tell any receiving servers that an email coming from your domain is legitimate. It also instructs receiving servers to reject any emails that don't come from your authorized sending sources. This stops hackers using your domain for phishing and has also been shown to improve email deliverability and placement.

DMARC protects everyone, and is a foundational tool for safeguarding trust:

- **Your employees** won't receive emails from your company's domain, pretending to be the CEO, accounts department or other senior members. This means money, data, and employee wellbeing are protected.
- **Your customers** won't receive emails pretending to be from your business with bogus links or attachments, so your customers stay safe, your reputation stays intact, and trust in your brand is secure.
- **Your suppliers** can be confident that emails are coming from you, and they're protected from phishing scams using your domain.

Benefits of DMARC



Stops hackers impersonating your brand and domain to send phishing emails



Improves email deliverability and inbox placement



Makes you eligible for BMI, showing your registered logo in email

6. The results are in: how DMARC in the retail sector currently measures up

Retailers race to provide the best experience possible for their customers online. From fast user experience to order tracking, and personalization, there are numerous flashy ways to try and stick out in the crowd. But are these businesses putting the basic measures in place to secure email, the channel that facilitates so much of their business volume and consumer communication?

Red Sift carried out some analysis looking at current DMARC adoption across 287 top global retailers

DMARC Status	Explanation	# of retailers	% of retailers
P=reject	Full protection	34	12%
P=quarantine	Partial protection	21	7%
P=none	No protection, reporting only	148	52%
N/A	No DMARC record published	83	29%

88% of top retailers not protected

Retail is one of the most vulnerable sectors when it comes to data breaches, credential theft, and financial loss. Yet we found that just 12% of the globe's top retailers are fully protected from domain impersonation, meaning 88% are highly vulnerable to impersonation attacks and their damaging effects.

2021 DMARC status of the top global e-commerce & retailers



■ Reject	12%
■ Quarantine	7%
■ Reporting only mode	52%
■ No DMARC in place	29%

A policy of p=none is never enough

Compared to data gathered earlier this year, we can see that adoption of both p=quarantine and p=reject policies are slowly creeping up. However, the percentage of retailers sitting at p=none hasn't changed. This suggests that retailers aren't recognizing the importance of fully implementing DMARC, and while a basic policy of p=none offers visibility into your sending sources, it does nothing to protect your brand from being used for phishing scams.

How each DMARC policy works

Your DMARC policy is essentially the instruction you give to receiving servers, telling them what to do with emails that come from your domain. There are three DMARC policies to choose from:



None policy

p=none

This policy tells the recipient server to accept all emails from your organization's domain, regardless of whether they pass authentication or not.



Quarantine policy

p=quarantine

This policy tells the recipient server to send any emails from your organization's domain that fail authentication to spam.



Reject policy

p=reject

This policy tells the recipient server to reject any emails coming from your organization's domain that fail authentication.

Adoption of p=reject has doubled

While 12% is still a meager amount considering the breadth and scale of these businesses, it is an uplift from the 6% we saw in March 2021.¹³ These businesses appear to be recognizing the importance of full DMARC protection, and the more this figure increases, the more pressure there will be on their competitors not to get left behind.



¹³<https://go.redsift.com/retail-whitepaper.html>

7. DMARC's role in safeguarding trust in retail



DMARC protects consumer data

Business Email Compromise (BEC) is an umbrella term used to describe phishing attacks that target an organization by impersonating its domain and/or employees. BEC poses an ever-increasing threat to brand reputation and consumer trust because if a brand's employees can be tricked into divulging sensitive information, then customer data is leaked and trust in the brand is lost. By implementing DMARC, retailers are not only stopping their customers from being phished, but they're also blocking hackers from being able to masquerade as a member of the business and trick employees into handing over sensitive information, money, and credentials.



By not implementing DMARC, retailers are taking a big risk

The businesses we analyzed are large, global corporations, and so have already invested time, money, and effort into building up trust within their network. Yet as we've seen already, trust is precious, and once it's gone it can be very hard to get back. By not configuring DMARC at p=reject, these retail businesses are leaving the door wide open for criminals to impersonate their domain to send scam emails and wreak irreversible havoc on their reputation.



Brand impersonation: the bigger the better

Hackers don't pick businesses to impersonate by chance. Instead, they spoof organizations with strong, reputable brands that carry a lot of weight. This is because they're likely to have more contacts to phish, and will have already established trust with their customers. If a retailer doesn't have the right measures in place, cybercriminals will pounce on the chance to leverage its hard-earned brand trust for their own gain, no matter the damage to its reputation.



DMARC promotes a safer email ecosystem

The email ecosystem is a global network that stretches far and wide, and it's important we all play our part to keep it secure. The more businesses that adopt DMARC as the standard way to authenticate emails and block hackers from impersonating their domains and brands, the safer the global email channel will become as a whole.

8. Is a lack of trust impacting your email ROI?

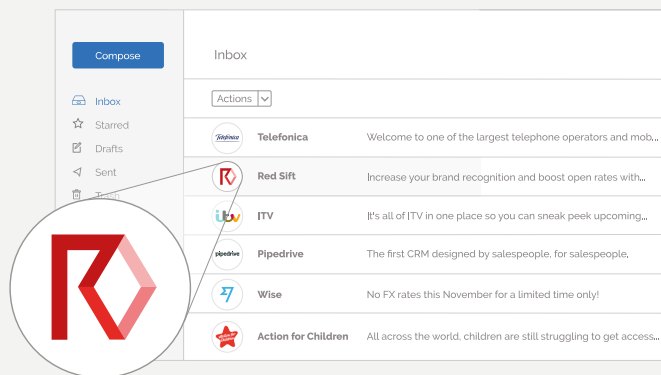
For many retailers, the mountain that is brand building has already been scaled. But with the current global email open rate sitting at just 18%, and click-throughs at just 2.6%¹⁴, are organizations failing to appeal to their target base effectively via email, and could trust - or rather a lack of it - have something to do with it?

The average person receives around 121 emails every day¹⁵ and the typical person's attention span is just 8 seconds¹⁶. So when it comes to email marketing, it's likely that many of these trusted brands are failing to stand out from the crowd. But with the continued rise in cybercrime and phishing attacks, it's also possible that consumers are finding it increasingly difficult to trust the authenticity of the emails they're receiving, and therefore are reluctant to click.

How can retailers reassure recipients?

A survey conducted by GoDaddy found that 75%¹⁷ of people believe having a domain-based email that matches your website is a very to extremely important factor in trusting an email. But without full DMARC configuration, that 'legitimate' email address could be a hacker impersonating that brand.

In addition to DMARC, retailers can leverage BIMl to show their registered logo on their emails. This protocol provides a tangible way of reassuring recipients that the emails they're receiving are legitimate, and ultimately helps retailers stand out in an increasingly oversaturated inbox.



18% global average
open rate¹⁴



2.6% global average
click-through rate¹⁴



121 average number of
emails sent to a person
per day¹⁵



8 seconds average
human attention span¹⁶

¹⁴Campaign Monitor

¹⁵Review42

¹⁶Microsoft

¹⁷GoDaddy

9. Logo visibility for consumer trust

Earlier this year, we carried out research¹⁸ looking at how showing a verified logo in email using Brand Indicators for Message Identification (BIMI) impacts consumer interaction with and confidence in emails.

What is BIMI?

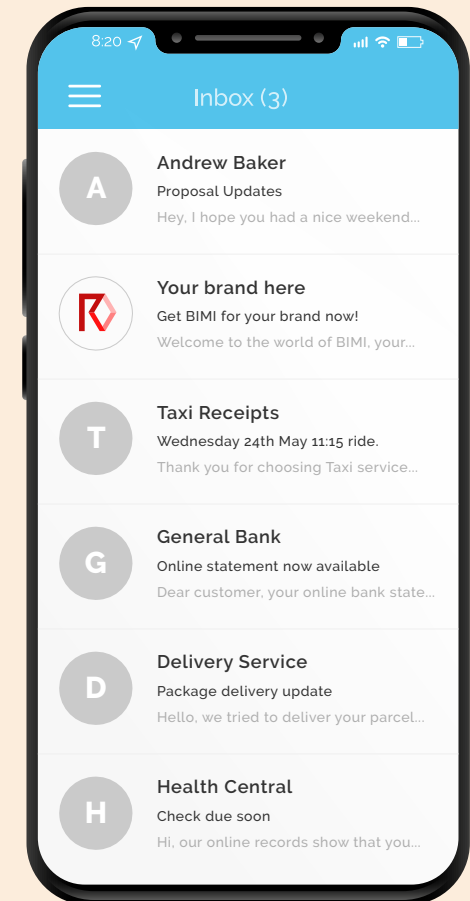
BIMI stands for Brand Indicators for Message Identification. This new standard allows businesses to display registered, trademarked logos on DMARC-authenticated emails using a Verified Mark Certificate (VMC). BIMI with VMC helps you stand out in the inbox, and has been shown to improve consumer interaction and confidence in emails.

What is a Verified Mark Certificate? (VMC)

A Verified Mark Certificate (VMC) is a digital certificate created by Entrust, Red Sift's partner, in conjunction with the AuthIndicators working group. A VMC can only be issued by an approved Certificate Authority (CA) such as Entrust. To qualify for a VMC, a business must be DMARC compliant. Implementing BIMI with VMC is the only way a brand can confirm that its logo is authentic, as DMARC is the authentication mechanism it uses.



BIMI



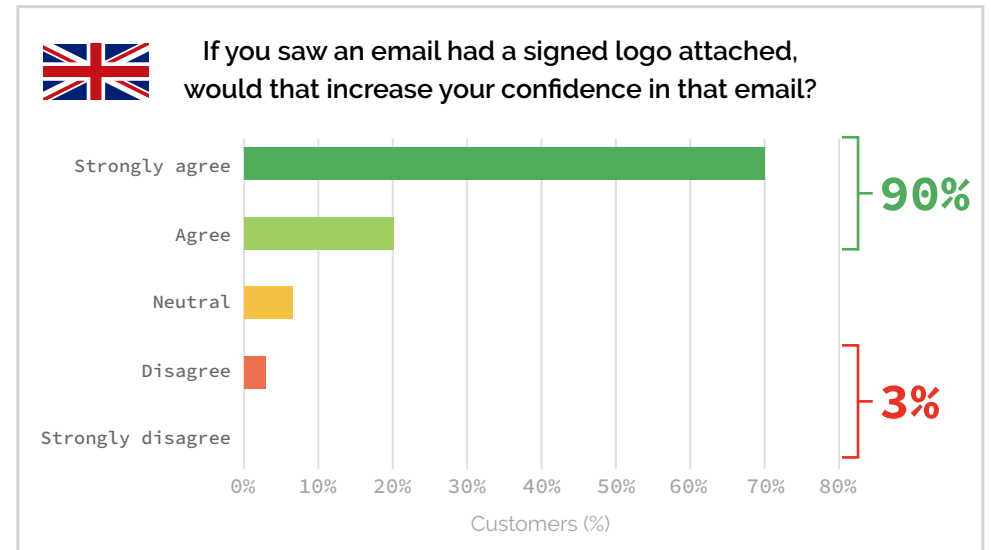
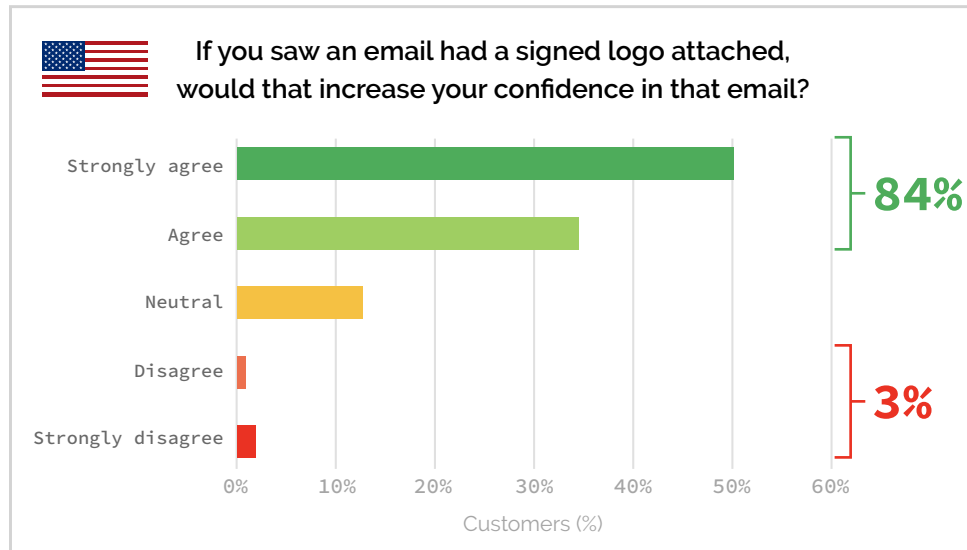
**Brand Indicators for
Message Identification**

¹⁸<https://go.redsift.com/bimi-whitepaper.html>

Does showing a logo in the inbox increase confidence in that email?

If three quarters of people believe the key to trusting an email is if it comes from a domain that matches the company's website, then surely the presence of a trademarked logo - which in itself confirms full DMARC authentication - is an even stronger incentive for trust? DMARC and BIMl with VMC could be the key to unlocking success rates of email by ensuring consumer confidence, while enabling businesses to get more return on investment for their campaigns.

To investigate this, we carried out research looking at whether showing a registered logo in email does impact consumer confidence in an email's legitimacy.



At least 84% of participants in either country agreed or strongly agreed that seeing a signed logo would improve their confidence in an email

BIMl with VMC solidifies consumer trust in a brand's emails

When asked if a signed logo attached to an email would increase their confidence in that email, 84% in the US group and 90% in the UK said they either agreed or strongly agreed that it would. While this doesn't imply direct buying behavior, trust is valuable for organizations, and these findings further strengthen the case for logo visibility and the value it brings businesses.

BIMl with VMC is something that requires serious consideration by all businesses, not just to ensure their email efforts continue to deliver ROI, but to give consumers confidence that their email communications can be trusted, and safeguard trust in this vital channel now and for the future.

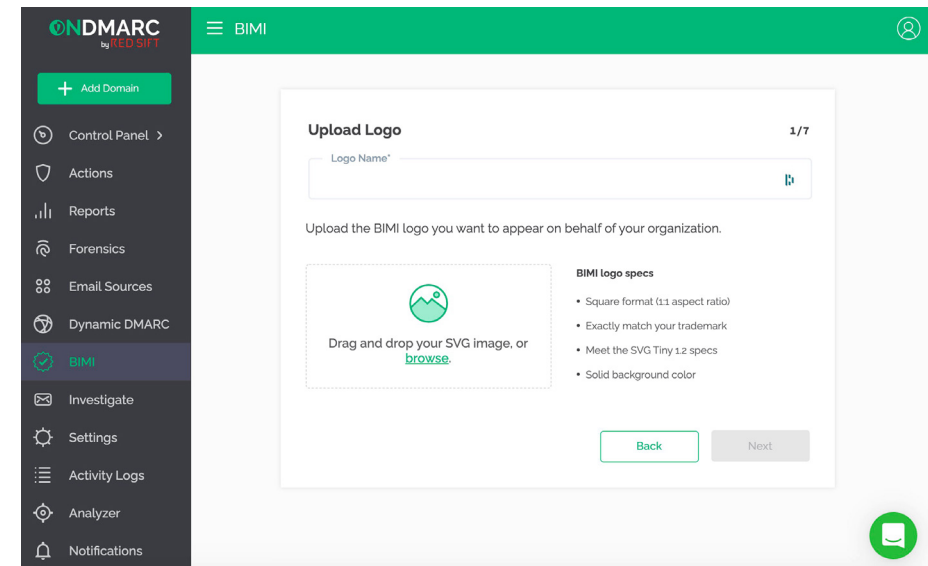
10. Start safeguarding your brand reputation and consumer trust

DMARC, and BIMi with VMC, are two essential and foundational components all retailers should be using to protect trust in their brand, and they're not as difficult to implement as you might think. In partnership with Entrust, we offer the first and only end-to-end DMARC and BIMi solution, enabling businesses to both improve their email security strategy and create a more consistent email experience for email recipients.

How Red Sift can help

Red Sift's award-winning product OnDMARC, which helps brands block phishing attempts using their domain, combined with Entrust's new Verified Mark Certificate, provides businesses with a proven method for showing a registered brand logo on their email communications. This is a simple yet cost-effective way to secure your outbound email strategy, consumer confidence, and brand presence.

We've helped a number of global businesses through the DMARC and BIMi implementation process, and now they're reaping the benefits. So why not [contact us](#) to get started on your journey to safer and more effective email today?



Contact us to book your free consultation today

Contact us

Methodology

In November 2021, Red Sift analyzed the DMARC status of 287 top retailers worldwide. In June 2021, Red Sift surveyed 1,026 participants across the US and UK to assess the impact that logo visibility has on consumer interaction and confidence. To learn more about the results of individual retailers, please get in touch with the Red Sift team.

About Red Sift

Founded in 2015, Red Sift is a global cybersecurity company whose clients include organizations such as Domino's, Telefonica, Pipedrive, Rentokil, Wise, and top global law firms. The Red Sift data analysis platform is purpose-built for the challenges of cybersecurity. Products on the Red Sift platform include OnDMARC and OnINBOX, SaaS applications that work together to close the net on the phishing problem by blocking outbound phishing attacks and analyzing the security of inbound communications for company-wide email threat intelligence.

References

1. The 7 Habits of Highly Effective People, Stephen Covey
2. https://www.edelman.com/sites/g/files/aatuss191/files/2019-06/2019_edelman_trust_barometer_special_report_in_brands_we_trust.pdf
3. <https://www.pwc.com/gx/en/industries/consumer-markets/consumer-insights-survey/consumer-trust.html>
4. <https://www.salesforce.com/news/stories/state-of-the-connected-customer-report-outlines-changing-standards-for-customer-engagement/>
5. <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consumer-business/us-cb-brand-power-in-times-of-covid-19.pdf>
6. <https://www.pwc.com/gx/en/industries/consumer-markets/consumer-insights-survey/consumer-trust.html>
7. <https://www.dusted.com/insights/why-brand-trust-is-so-important>
8. <https://www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf>
9. <https://www.statista.com/statistics/534123/e-commerce-share-of-retail-sales-worldwide/>
10. <https://www.forrester.com/Consumer+Technographics+COVID19+Survey+Wave+2/-/E-sus5652>
11. <https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/>
12. <https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/>
13. <https://go.redsift.com/retail-whitepaper.html>
14. <https://www.campaignmonitor.com/resources/guides/email-marketing-benchmarks/>
15. <https://review42.com/resources/how-many-emails-are-sent-per-day/>
16. <https://dl.motamem.org/microsoft-attention-spans-research-report.pdf>
17. <https://aboutus.godaddy.net/newsroom/press-releases/press-release-details/2016/Consumer-Trust-In-Online-Small-Businesses-Strengthened-By-Professional-Email/default.aspx>
18. <https://go.redsift.com/bimi-whitepaper.html>
19. <https://www.verizon.com/business/en-gb/resources/reports/dbir/>
20. <https://www.forbes.com/sites/blakemorgan/2020/06/22/50-stats-showing-why-companies-need-to-prioritize-consumer-privacy/?sh=3a52109537f6>