

Authentication, Accreditation & Reputation – for Marketers!

June 2005

Prepared by



and





Abstract

By now, the words “authentication, accreditation and reputation” (AAR) are staples of every email marketer’s vocabulary. Generally speaking, marketers understand that these solutions are aimed at reducing spam and phishing. Unfortunately, however, much of the discussion around these developments has been technically dense, leaving many feeling hopelessly “on the outside looking in.”

For the most part, the technological implementation of authentication is the responsibility of an organization’s IT department and/or its email service and technology partners. But at its core, successful email delivery under an AAR regime necessitates adherence to various ISP/Web-based email client delivery requirements, careful monitoring, and sending consumers the most relevant and wanted communications. This places the onus for deliverability success right back on the shoulders of those in charge of their organization’s email campaigns – marketers.

This white paper takes the clutter out of the confusing AAR story and focuses squarely on what marketers need to know to be successful **in language that marketers can understand**, and answers:

- Why are mailbox providers developing and implementing AAR solutions?
- What are the leading AAR solutions, how do they work, and how will they benefit legitimate marketers?
- How can I navigate AAR successfully?



Table of Contents

| | |
|------------------------------------------------------------------------------------|-----------|
| Why are ISPs Developing and Implementing AAR? | 3 |
| What are the Leading Solutions and How Do They Work? | 4 |
| Authentication | 4 |
| The Leading Authentication Solutions | 5 |
| Sender Policy Framework (SPF) | 5 |
| Sender ID Framework (SIDF) | 6 |
| DomainKeys (DK) and Identified Internet Mail (IIM) | 7 |
| Moving Authentication Forward | 9 |
| Whitelisting, Accreditation & Reputation Solutions | 9 |
| AOL's Enhanced Whitelisting | 10 |
| Practical Advice for Marketers - How Can I Navigate AAR Successfully? | 12 |
| The Three Keys to Success | 12 |
| AAR Success Checklist | 13 |
| Resources | 16 |
| About the Authors | 17 |
| Appendix A – Short-Term AAR Process | 18 |
| Appendix B – Authentication: USPS Analogy | 19 |
| Appendix C – eNewsletter Best Practices | 20 |
| Appendix D – Phishing Example | 21 |



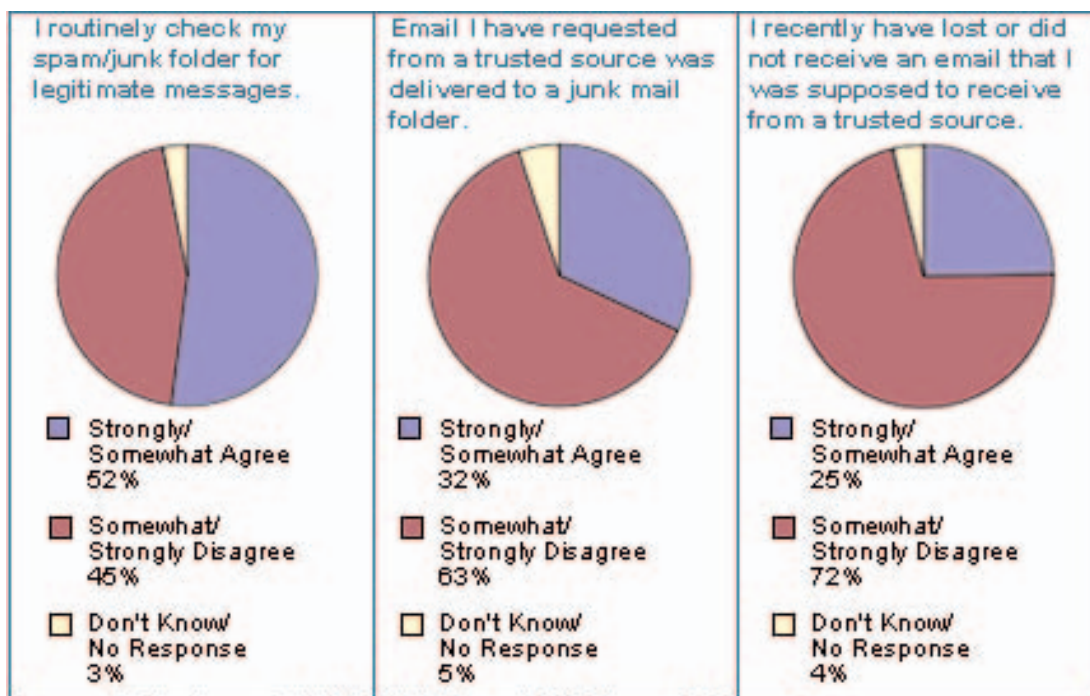
Why are ISPs Developing and Implementing AAR?

ISPs/Web-based email clients (mailbox providers) like America Online (AOL), Yahoo and MSN/Hotmail are developing and implementing AAR solutions to more effectively and more efficiently protect their customers from spam.

Like any other company, mailbox providers' primary obligations are to their customers, and ultimately their shareholders. Efforts to combat spam and phishing have become a costly burden for mailbox providers – significant resources continue to be expended to fight the problem and spam-related customer attrition persists. By implementing effective AAR solutions, they intend to mitigate these costs.

Furthermore, in a fiercely competitive marketplace, blocking spam has become a major selling point in mailbox providers' own advertising campaigns – doing so has become a core differentiator and service, and they believe it is central to attracting and retaining customers. According to the latest Epsilon Interactive/RoperASW consumer survey, 22 percent of American adults switched or considered switching their mailbox provider in the last six months¹ – so the stakes are, indeed, very high.

AAR solutions have been developed to enable more reliable, sophisticated and high-tech email delivery processes so that mailbox providers can better identify and ultimately reduce the amount of spam and phishing email that reach their users. In the process, mailbox providers are less likely to misidentify permission-based email as spam, reducing the incidences of “false-positives” that have been plaguing the email ecosystem in recent years.²



Source: Epsilon Interactive/ NOP World/Roper ASW, February 2005

¹Epsilon Interactive/RoperASW, “Email and Spam: Consumer Attitudes and Behaviors,” February 2005

²According to JupiterResearch, erroneous filtering of permission email cost U.S. businesses approximately \$322 million in 2004. “JupiterResearch Email Model,” sDecember 2003



What are the Leading Solutions and How Do They Work?

Authentication, accreditation and reputation are typically mentioned in the same breath for a very good reason – they are fundamentally linked. Implementing authentication without at least one of the other solutions would be unproductive, as they contribute to the ultimate success of each other. Here's why:

Authentication

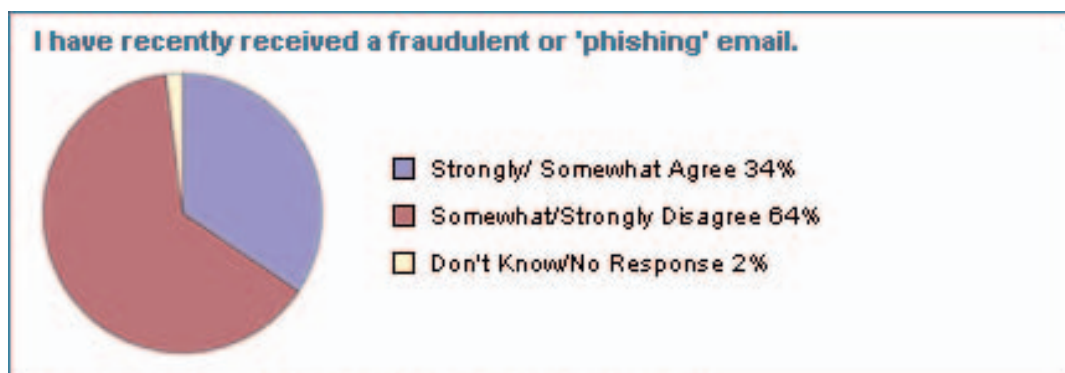
Whether IP-based (e.g., Sender ID Framework and SPF) or cryptographic (e.g., DomainKeys), authentication does not reveal the true identity of the sender – it simply verifies that a computer server/IP address or a specified sender is authorized to send email that purports to be from that sender and/or domain-name. This is all it does – *verify* authorization to send messages – and not, as is commonly assumed, inherently reveal the *identity* of a “real-world” sender.

The way verification is accomplished varies in each of the proposed and implemented authentication solutions, but all are bound by the common purpose of being employed for verification-only.

In IP-based “domain-level” authentication (e.g., Sender ID Framework and SPF), email recipients query an Internet registry called the Domain Name System (DNS) to verify that when email they receive claims to be from a certain domain-name, e.g., “@yourcompany.com,” that the computer server/IP address that actually sent the message is an IP address that is listed as authorized to do so in the DNS for the domain “@yourcompany.com.”

Meanwhile, in cryptographic-based “message-level” authentication (e.g., DomainKeys), public/private key pairs are generated by email senders, with one of the keys stored in the DNS or another Internet registry, and its matching key being used to generate unique message signatures that are embedded in outbound email headers. Mailbox providers then authenticate emails received by querying the DNS/registry to determine that the signature in the header matches the key stored in the DNS/registry.

While spammers have shown aptitude at forging certain aspects of email messages – for example, altering the domain name in the visible “From” field of an email message to make it look like it's coming from a different source, or graphically feigning a legitimate brand's identity in the body of an email (as occurs in “phishing” schemes, see Appendix E for an example) – forging IP addresses or cryptographic signatures is distinctly more difficult to accomplish.



Source: Epsilon Interactive/ NOP World/Roper ASW, February 2005



In addition, mailbox providers like AOL have testified in the past that as much as 90 percent of spam contains falsified header and/or routing information.³ Therefore, it is believed that by using authentication solutions, mailbox providers will be able to more easily identify and block a significant number of spam emails.

As can be expected, spammers are following “spam news” as much as legitimate email marketers, and one of the largest providers of consumer email accounts, Microsoft, reports that domain spoofing attempts have been detected in nearly a quarter of all email purportedly sent from SPF-publishing domains.⁴

This is why it is fundamentally necessary for authentication to be tied to accreditation and/or reputation – because even though a computer server/sender is verified as authorized to send a specific message, that doesn’t automatically mean that a message isn’t fraudulent and/or spam. Many spammers are actually trying to work around authentication by simply purchasing and setting up new domain names from which they are, in fact, authorized to send email.

For this reason, some sort of assessment must be made to determine whether an authenticated message should be passed along to its intended recipient, should be looked at again, or should be blocked outright. This is where solutions like accreditation and reputation step in (often used to help mailbox providers determine whether a sender should be added to and kept on their “whitelists”). Today, and even more so in the future, by using these solutions in tandem with each other, authenticated spam should have a reduced likelihood of making it to the inbox.

Note that the word “authenticated” is highlighted here because, in the short-term – where the majority of email senders have not yet complied with email authentication – mailbox providers will in most cases subject non-authenticated email to traditional spam filtering processes (e.g., volume and content-based filters), which spammers have shown a degree of prowess at navigating (this also means that non-authenticated spam won’t be rejected outright either). See Appendix A for a graphical representation of how most mailbox providers will use AAR in concert with legacy spam filtering solutions – at least until a critical mass of email senders have adopted authentication.

The Leading Authentication Solutions

Sender Policy Framework (SPF)

Developed by Meng Wong, chief technology officer and co-founder, Pobox, SPF – which is open-source – is the most simple of the authentication solutions currently being tested and deployed in the marketplace.

How it works: For senders, SPF compliance entails publishing an “SPF record” into the existing DNS. The DNS can be thought of as a universal Internet directory, and is the backbone of today’s World Wide Web. When an Internet user types in a domain name, for example “www.yourcompany.com,” the DNS is used to look-up the right server for a computer to connect to in order to receive the requested Web page.

An “SPF record” is basically a list of computer servers/IP addresses that IT professionals and email partners add to their existing corporate DNS records as servers which are authorized to send email that claim to be coming from their or their clients’ domains. Publishing these records is cost-free, simple to do, and remarkably “low-tech.”

³Jennifer Carrol Archie of Latham & Watkins LLP, Washington, DC, on behalf of her client, America Online, before the Pennsylvania State Senate Communications and Technology Committee, September 23, 2003.

⁴Microsoft press release, “Sender ID Framework Demonstrates Positive Results for E-Mail Authentication,” March 2, 2005



While spammers often forge “FROM” lines and “MAIL FROM” addresses that appear in email message headers, it is extremely difficult for them to forge/conceal the true IP address from which the message was sent.

On the receiving-side, SPF authentication checks verify that the MAIL FROM address in an email header maps to a computer server/IP address that is authorized to send email on behalf of the domain it says it's from. If the IP addresses listed as authorized to send email for that domain in the DNS are different from what appears to be the actual originating IP address, the message “fails” the SPF authentication check. If they match, it passes and is considered authenticated.

SPF is most effective at combating “joe-jobs” and the “you sent me a virus” phenomena – which occur when spammers spoof MAIL FROM addresses. If thought of in terms of a piece of traditional mail sent through the U.S. Postal Service (USPS), SPF only validates the authenticity of the outer envelope, but not the contents inside per se.

Marketplace Adoption & Challenges: As mentioned before, SPF is the most simplistic of all authentication solutions, and is considered an important first step in the authentication process, especially because so much spam contains falsified MAIL FROM information.

Because it is virtually cost-free and is so easy to comply with, many believe that SPF will be embraced by more email senders than any other authentication solution. And because it is also “open-source,” SPF also has the fewest hurdles to widespread testing and implementation on the mailbox provider side. However, it is regarded as a weaker email authentication approach compared to cryptographic solutions like DomainKeys.

Sender ID Framework (SIDF)

SIDF is the result of combining SPF with Microsoft's proprietary authentication solution, “Caller ID for Email” (SPF is, therefore, a component technology of SIDF). Microsoft implemented SIDF earlier this year for MSN Hotmail and has announced availability in Outlook 2003, Outlook Express and Exchange 2003 before year-end. Recently the Internet Engineering Task Force (IETF) approved SIDF and SPF as experimental.

How it works: The Caller ID aspect of the solution authenticates the “Purported Responsible Address” or PRA, which is often the visible “FROM” portion of an email header. Consequently, the complete solution, SIDF, adds an extra layer of protection against visibly forged domain-names in phishing scams, in addition to the MAIL FROM protection provided by SPF.

SIDF is backward compatible with SPF, and only requires email senders to publish SPF records. The only difference is that mailbox providers who implement SIDF can verify either or both the “MAIL FROM” or “PRA” portions of an email header, with both of these being tied to the list of authorized sending IP addresses contained in the SPF record.

Using the USPS analogy again, SIDF is akin to verifying the authenticity of both the outer envelope and the letterhead on the document inside of the envelope. While this presents a slightly stronger solution than SPF by itself, it is still possible for the content of the message to be altered during transmission, and it isn't considered as strong as cryptographic solutions.



Marketplace Adoption & Challenges: According to Microsoft, more than 1 million domains have published their SPF records, the method used within SIDF to identify a sender's authorized outbound email servers, and it is estimated that more than 1 billion e-mail messages worldwide are sent each day that include SPF records.⁵

SIDF appears to be yielding positive early results. In just the first few months since the company implemented SIDF for Hotmail, Microsoft already recorded a 6 percent reduction in false positives, and, together with its other various anti-spam measures, the solution has helped achieve an average 70 percent reduction in the volume of spam delivered to its members' inboxes year-over-year. In addition, on June 22, 2005, Microsoft implemented visual warnings in the MSN Hotmail user interface on email in which the Sender ID Framework (SIDF) cannot verify authentication.

Microsoft plans to license SIDF in perpetuity at no cost to anyone who wants to use it. In addition, it is worth remembering that for senders, complying with SIDF only requires publishing SPF records.

For the most part, mailbox providers agree that IP-based solutions like SIDF and SPF are complementary to stronger, cryptographic solutions like DomainKeys. Because they are easier to implement and do not necessarily require the purchasing of additional hardware or software, IP-based solutions should be viewed as a foundational layer for building greater accountability into email, and, as such, clearly more work needs to be done to encourage continued SIDF/SPF authentication compliance by email senders.

DomainKeys (DK) and Identified Internet Mail (IIM)

DK and IIM are more advanced, cryptographic/signature-based solutions developed by Yahoo and Cisco, respectively.

Yahoo has already implemented DK, whereas no mailbox providers have implemented IIM. However, on June 1, 2005, Yahoo and Cisco formally announced that they are collaborating to merge the IIM specification with DK in order to create a stronger and more scalable cryptographic authentication solution that will be called DomainKeys Identified Mail (DKIM). Furthermore, they said it would be made available to the industry-at-large royalty free.⁶

How it works: DK requires email senders to generate "public/private key pairs" and then publish the public keys into their DNS records. The matching private keys are stored in a sender's outbound email servers, and when those servers send out email, the private keys generate message-specific "signatures" that are added into additional, embedded email headers.

Mailbox providers that authenticate incoming messages using DK query the DNS for the public key, which is then used to verify that the signature was generated by the matching private key in order to authenticate the message. According to Yahoo, this not only will ensure that an authorized sender sent the message, but also that its headers and content weren't altered in any way during its trip from the original sender to its intended recipient (these represent some of the technological concerns posed by IP-based solutions like SPF and SIDF).

IIM works in a similar fashion, except the public key is stored in the sender's outbound email headers along with the signature generated by the public key. The authentication process involves checking the integrity of the message using the public key included in the signature header, in addition to verifying whether the public key used to sign the message

⁵Microsoft Web site, "Q&A: MSN Hotmail Adds Safety E-Alerts for Email Authentication," June 22, 2005

⁶Yahoo/Cisco press release, "Yahoo! and Cisco Drive Industry Toward a Unified E-Mail Authentication Standard to Combat E-Mail Forgery," June 1, 2005



is authorized for use with the sender's email address. This step involves querying either a to-be-developed Key Registration Server (KRS) or the DNS of the sending domain. The authorization records in the KRS or DNS contain information about the binding between a specific key and email address. Some believe this approach to message signing could make cryptographic authentication less computing resource intensive for email senders than the current DK specification.

Cisco also postulates that it might be appropriate for cryptographic authentication to reside stand-alone/apart from the DNS because of "wildcard DNS limitations" (e.g., it's not entirely clear that the existing DNS infrastructure wouldn't be overwhelmed by the demands placed on it by cryptographic authentication verification) and because this would be "consistent with the typical organizational separation of the groups that manage email and DNS."⁷ While this point of view certainly is meritorious from a technological perspective, establishing a new and separate Internet lookup system such as a KRS would likely create a new set of costs of doing business for both senders and receivers who decide to implement such a solution.

In the end, Yahoo and Cisco say that the merged specification, DKIM, will use the DNS in the same manner as DK, while leveraging IIM's approach to header-signing. This could make the final combined solution more palatable to the sending community for adoption than either solution is standalone. In addition, the companies plan to submit the combined specification for consideration by the Internet Engineering Task Force (IETF) to become the cryptographic standard later this year.

Key-based solutions like DK, IIM, and the combined DKIM solve many of the shortcomings associated with SPF and SIDF because they authenticate messages themselves, rather than examining only sending IPs. Using the USPS analogy one last time, cryptographic authentication is akin to verifying a unique signature – which is valid regardless of the envelope or letterhead it was written on. See Appendix B for a graphical representation comparing the various leading authentication solutions using the USPS analogy.

Marketplace Adoption & Challenges: As mentioned before, Yahoo has implemented DK, however, as of the publication of this document, approximately 200 domains have implemented DK compliance on the sending side, representing a fraction of a percent of all email sending domains worldwide (which means this is dwarfed by SPF compliance).

The adoption of DK has been impeded by the fact that it may require more computing resources than SPF or SIDF, and could slow down email delivery speed. Also, many senders will probably wait for the final version of DKIM to be made available to the marketplace rather than implementing DK standalone and then making any necessary upgrades.

That said, cryptographic authentication is the next step toward an end-to-end authentication solution. Additional technological barriers to sending spam may be critical to meaningfully address the problem, but at the same time, the industry is cognizant of the need for an authentication solution that is accessible to large and small email senders and receivers alike. From an ideological perspective, the largest mailbox providers and other key industry stakeholders generally agree that there should be a level playing field when it comes to the delivery of legitimate email – the promise of e-commerce must not be squashed and should be accessible to all legitimate businesses that play by the rules.

⁷Cisco whitepaper, "Cisco Identified Internet Mail: A Network-Based Message Signing Approach To Combat Email Fraud," http://www.identifiedmail.com/IIM%20WP_v3.pdf



Moving Authentication Forward

Mailbox providers continue to test and implement authentication solutions. However, the Internet Engineering Task Force (IETF), the Internet standards body, has not yet endorsed any authentication proposal, which has somewhat impeded widespread marketplace adoption of any solution on both the email sending and receiving sides. However, it should be noted that it isn't unusual for industry to move forward with standards before the IETF completes its review and approval process, which can take years (similar to the patent approval process).

Despite the lack of one standard, the industry and its key stakeholders are continuing along a path of unprecedented collaboration to devise the strongest, most scalable authentication solution(s) that hopefully will make email a more reliable and spam-free communications medium. And while an IETF endorsement would probably spur quicker and broader marketplace adoption, the leading mailbox providers, email service providers and many others continue to move forward with the testing and implementation of SPF, SDF, and DKIM.

Industry is also requesting the active involvement of marketers and other legitimate email senders in the continuing discussion around authentication compliance and implementation. Accordingly, it is strongly recommended that all marketers/senders carefully audit and monitor their e-mail deployment infrastructure in order to support and comply with existing solutions. In addition, it has been noted that even at major national brand name companies, there are legacy email, CRM and DNS systems that cannot support even the most basic technological requirements required for authentication compliance. Furthermore, there are some organizations that have published inaccurate or incomplete SPF records.

Much of the discussion regarding the ongoing development of AAR solutions and automated feedback loops centers around establishing unified but robust additions to email message headers, with authentication compliance required as a baseline. For example, in the future, authenticated messages might be categorized and treated differently based on whether a message was sent for "transactional" or "promotional" purposes, and many other criteria that could potentially be added into email headers.

Authentication records and email headers will also increasingly be used as mechanisms for mailbox providers to deliver valuable, real-time automated feedback – e.g., user complaints, reasons for blocks, etc. – back to email senders/marketers (Note: AOL already uses SPF records to maintain a dynamic version of its whitelisting program called the "dynamic senders list"). Therefore, businesses that don't have the necessary system capabilities in place will be disadvantaged and face substantial challenges as the email delivery landscape continues to evolve in such a direction.

Whitelisting, Accreditation & Reputation Solutions

By now it should be clear that authentication compliance alone is not sufficient for mailbox providers to make deliver/non-deliver decisions. All authentication does is verify authorization to send, but it doesn't tell mailbox providers anything about whether the authorized sender is legitimate or a spammer. This is where solutions like whitelisting, accreditation and/or reputation steps in, and they often work in concert with each other to do so.

AOL officially introduced the industry's first accreditation and reputation-based solution, the enhanced whitelisting program, more than a year ago. Similar proprietary and/or licensed whitelisting, accreditation and reputation-based systems are now in place at virtually all of the major mailbox providers (e.g., Yahoo, Earthlink, and MSN Hotmail) and enterprise spam filtering companies (e.g., CipherTrust and Symantec Brightmail).



Third-party whitelists, accreditation and reputation vendors have surfaced in recent months, but none has yet achieved a critical mass of senders adopting their solutions, nor have a critical mass of mailbox providers implemented them. Of course, whether or not a large number of mailbox providers eventually do enter into agreements with these vendors would likely have a dramatic effect in terms of spurring email sender adoption.

Meanwhile, it is more productive to examine the current implementation of AOL's enhanced whitelisting program as an example of how these types of solutions are being applied in the marketplace today.

AOL's Enhanced Whitelisting

Senders who wish to be placed on AOL's enhanced whitelist must submit a certification application (a form of "accreditation") beforehand in which they attest that they meet and will abide by the program's requirements. The agreement relates to areas such as CAN-SPAM compliance, list hygiene, email deployment infrastructure capabilities including bounce acceptance, and others. After they have submitted their application, AOL tracks and makes assessments of senders' reputations based on dynamically observed marketing behavior and complaint-rates against senders at the IP-address level.

Pursuant to the successful completion of a 30-day "evaluation period" – in which a sender adheres to AOL's whitelisting policy and receives a very low complaint rate (as reported by AOL's members) – a sender is rewarded by being added to the enhanced whitelist, where they receive deliverability benefits including bypassing certain levels of filtering (e.g., volume filters), inbox placement, and guaranteed full image and link rendering/display.

Senders are automatically included in AOL's Enhanced Whitelisting program if their complaint rate falls below AOL's preset complaint threshold. But in addition, AOL also allows an incremental percentage of senders to participate in the program on a daily basis based on a low complaint rate compared to the rolling average of all senders calculated and updated each day. AOL reserves the right to change this complaint rate threshold and formula at any time and has not publicly disclosed the actual figure.

However, in all cases, if a sender on the enhanced whitelist subsequently violates the requirements and/or receives too many complaints, they can be subjected to short or long term blocks, and even be kicked out of the program, forcing them to prove their good reputation and worthiness from scratch. In addition, end-users have final control, and even if a sender qualifies for the enhanced whitelist and maintains a miniscule complaint rate, if an end-user clicks the spam complaint button, all future email from that sender will be routed to the individual user's junk folder.

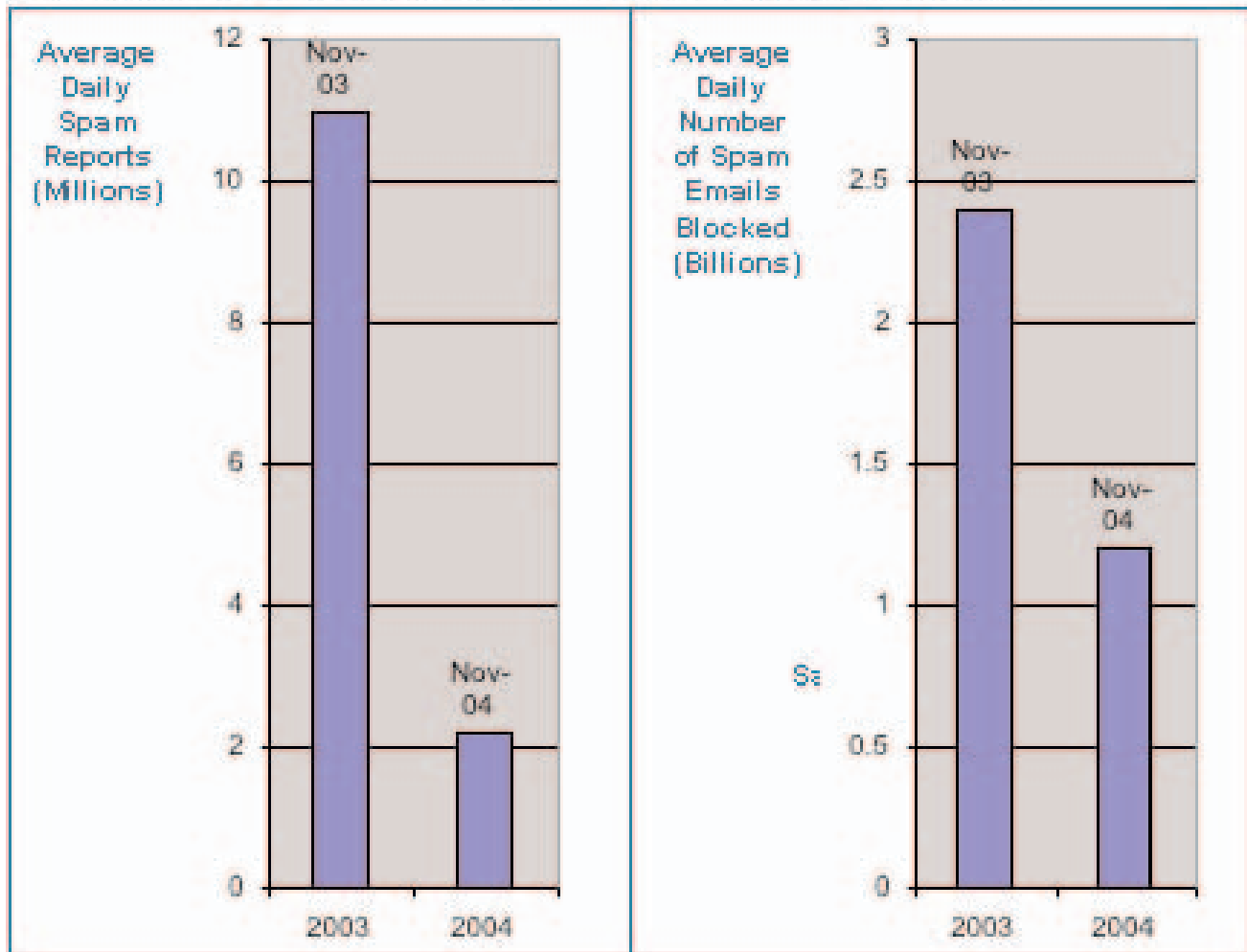
By using enhanced whitelisting with accreditation and reputation in concert with legacy filtering for all non-whitelisted senders, AOL has achieved anti-spam success and recorded a substantial, year-over-year decline in spam sent to and received by its members from Nov. 2003 – Nov. 2004.⁸

Having enhanced whitelisting in place also enabled AOL to establish the industry's first feedback loops with trusted email senders, providing marketers with invaluable intelligence about how consumers react to their campaigns and with complaint rate information. Undoubtedly, the greater communication and processing efficiency of unwanted email between senders/marketers and AOL has also made a positive impact on the anti-spam success of the nation's largest mailbox provider.

⁸AOL press release, "America Online Announces Breakthroughs in Fight Against Spam," December 27, 2004.



America Online Announces Breakthroughs In Fight Against Spam



Source: America Online - December 27, 2004



Practical Advice for Marketers – How Can I Navigate AAR Successfully?

Now that you've learned how these solutions work, the following educates marketers about what is required to have a "good reputation" in the email world, and then provides a bullet-point checklist that gives a more holistic view of what marketers need to keep in mind and manage in order to effectively navigate AAR.

The Three Keys to Success

Reputation in the email world is calculated differently than in the offline world, and often requires adherence to whitelisting/accreditation standards and what is considered ever-evolving email marketing etiquette. Essentially, there are three areas that marketers need to master:

1. Good List Hygiene. Sending email to too many addresses that don't exist isn't only a trait of spammers – it is a trait of any entity that is considered to have poor marketing practices and is sending spam. Mailbox providers acknowledge that there is a lot of churn in terms of consumers changing email addresses, and because of that, they do allow for some margin of error. However, it is generally accepted that marketers should aim to keep "invalid" addresses at less than 10 percent of each mailing. Of course, reducing these types of errors isn't just good for deliverability, but for email ROI as well.

2. Sound Email-Sending Infrastructure. Another common trait of spamming is to redirect email bounces and replies to spoofed, non-functional or non-existent return addresses. Therefore, legitimate senders are expected to be capable of receiving the volume of bounces that typically accompany any high-volume email campaign, and most mailbox providers require that email senders are capable of receiving at least 90 percent of messages that are "bounced" back to them when they attempt to send email to invalid or "unknown" addresses. Most automated reputation systems and mailbox provider abuse desk professionals consider not accepting their "bounce back" error replies as suspicious. Furthermore, from time to time, mailbox providers might ask high-volume email senders to adjust the number of simultaneous connections to their networks and/or to institute mail volume "throttling" (spreading out the number of emails sent over a longer period of time).

3. High Relevance/Low Complaint Rate. Having good list hygiene and a sound delivery infrastructure are the foundation to having a good reputation – but keeping complaint rates low is where reputation gets its real juice. The key to having a low complaint rate is making sure that your email is relevant and delivers value to the recipient.

At the same time, companies that embrace and leverage the unique sense of consumer empowerment in the email channel enjoy good "email world" reputations, already experience minimal complaint rates, achieve the greatest email marketing ROI, and will continue to be poised for success in the developing landscape.

In general, mailbox providers believe there should be little to no reason for a consumer to complain about legitimate email. And in light of this ultra consumer sensitive framework, complaint rate thresholds before mailbox providers institute blocks are often miniscule. Marketers should aim to keep that rate below 0.1 percent. A mere two or three complaints out of a thousand emails delivered could result in dynamic short-term blocking by mailbox providers that employ reputation systems, and severe, long-term blocking if not demonstrably brought under control.



Marketers should view emerging accreditation and reputation solutions, as well as authentication solutions, as highly positive developments. They bring to the table clearly defined parameters for email delivery and much more assurance that your messages will be delivered as long as you stay within those boundaries.

Reviewing the *Three Keys to Success* highlights how critical it is for marketers to work collaboratively with a best-in-class email deployment partner. Sending from a platform that has powerful automated hygiene capabilities is a foundational requirement for marketers who care about their email performance. In addition, marketers should pay close attention to factors such as compliance with mailbox provider specific demands, connection and delivery speed management, and opt-out processing capabilities – all of which play a role in achieving the highest delivery rates.

But keeping complaints low is all about best practices, and resides entirely on decisions made by the people in charge of their company's email campaigns. Monitoring and managing complaints is essential.

As Forrester Research's Principal Analyst, Jim Nail, advised in his opening remarks at a recent event, always ask yourself "How can email support the consumer's goal?"

Always keep in mind that email is fundamentally changing the way people communicate with each other all across the world, and take time to monitor and study the nuances of consumer behavior and how people interact with the channel – using one's own personal experiences with the medium can often help identify areas for improvement.

The bottom line is that, more than with any other medium, consumers feel entitled and empowered to control the content that is delivered to their email inboxes. The email communication stream that a company establishes with a consumer can last a lifetime or a day, so the choices to consider when it comes to implementing privacy best practices should be obvious. Making the right decisions here will be essential both for deliverability and overall email success as reputation systems continue to gain momentum in the marketplace.

AAR Success Checklist

The following provides a checklist summary of what is required for deliverability success as AAR continues to replace legacy spam filtering systems at mailbox providers around the world.

- **Publish Your SPF Record and Implement Cryptographic Solutions.** For more information on the latest authentication technologies and helpful guides and wizards designed to make compliance as easy as possible, visit: www.emailauthentication.org/resources.
- **Audit Your Email Infrastructure & Monitor Published Records.** Depending on the size and complexity of your organization, you can be sending email from multiple IP addresses and using various domain and sub-domain names in your messages (e.g., "@yourcompany.com," which is a domain, or info.yourcompany.com," a sub-domain). Email service providers are usually charged with sending only specific messaging streams for their clients, but it's important for marketers to have a solid understanding of what type of email is emanating from their organization, from where, and who is in control/hitting the send button.



It is also critical for marketers to be aware of and account for all new email-sending platforms and make sure that the people in charge of their DNS and publishing authentication records account for these as well. By the same token, if marketers discontinue using certain servers for sending email, this should also be noted.

- **Audit System Capabilities.** Companies whose email infrastructure doesn't support AAR cannot derive its benefits, and could even be hurt by AAR if they don't adapt to its requirements. There are several legacy email, CRM and DNS systems observed in the marketplace which are unable to support the most basic technological requirements and header additions required for authentication and feedback loop automation and processing.

Much of the discussion regarding the ongoing development of authentication solutions and automated feedback loops centers around establishing unified but robust additions to email message headers.

In addition, headers and authentication records stored in the DNS will likely be increasingly used as mechanisms to deliver valuable, real-time automated mailbox provider feedback (e.g., user complaints, reasons for blocks, etc.) back to email senders/marketers. Therefore, businesses that don't have the necessary system capabilities in place will be disadvantaged and face substantial challenges as the email delivery landscape continues to evolve in such a direction.

Furthermore, it is critical to have the technological flexibility to adapt to constantly evolving ISP requirements. Your email deployment platform should, at the very least, include automated hygiene, spam-trap address removal and opt-out processing, high-volume bounce-acceptance capability and effective SMTP connection/throttling management, as these features and functionality will continue to play a role in achieving strong delivery rates.

- **Control Your Domain-Name.** It is important to review all registrations and internal and external uses of your brand's domains and sub-domains. Increasingly, ISPs will make every effort to reject email that comes from fraudulent, derivative "cousin" domains (domains that are registered by spammers/phishers in an attempt to feign a company's brand identity, for example, a spammer/phisher might try to register and send email from "@yourcompany-email.com"). But at the end of the day, it is your responsibility to reign-in and control uses and misuses of your brand identity – from within and without your organization. After all, it is your brand that's on the line.
- **Always Ask to Be Added to the Address Book.** Asking to be listed in a consumer's "Address Book" will help ensure delivery of requested and critical communications. Use registration pages on your Web sites and all subsequent email communications to ask consumers to add you to their address books. Benefits vary, but may include special icon designation, full image content/link rendering, bypassing personal adaptive filtering and challenge-response systems, and guaranteed folder placement. According to the latest Epsilon Interactive/RoperASW consumer research, 56 percent of consumers strongly/somewhat strongly agreed that they always add legitimate, trusted senders to their address book, and 42 percent of consumers strongly/somewhat strongly agreed that legitimate email they subscribe to usually encourages them to add the company to the address book at the time of subscription or in each message.⁹ This is positive news, but indicates that there is still a lot more work to be done on this critical, consumer education front.

⁹Epsilon Interactive/RoperASW, "Email and Spam: Consumer Attitudes and Behaviors," February 2005



- **Standardize “From” Lines For “Add to Address Book” Benefits.** Many ISPs will/do add a “positive weight” – improving one’s email reputation score – to email that comes from senders whose email addresses are listed in their members’ address books.

Therefore, in most cases it is desirable to send email from as few different addresses in the “From” line as possible. Depending on one’s organizational complexity, lines of business, or other challenges, it is important to carefully consider and manage your company’s “From” line strategy. The key is to keep it standardized, consistent, and under your control to optimize the benefits of Add to Address Book across multiple messaging streams.

- **Monitor Mailbox Provider Bounce-Backs/Replies.** Understanding the specific reasons for email bounce-backs is critical in maintaining and enhancing strong delivery rates. By monitoring and understanding the reasons for mailbox provider bounce-backs, marketers have the opportunity to audit their practices for potential issues and identify areas for improvement. For example, a high rate of unknown or invalid “user errors” might point to the need for improvements in your company’s email collection processes.
- **Empower the Consumer/Recipient.** Provide easy and conspicuous access to preference pages and your privacy policy, allowing recipients to understand and control their preference information, including the ability to opt-out or change messaging frequency and content. Incorporate email change of address links and preference-selection information in all messaging and on Web site registration pages and preference centers.
- **Adhere to Whitelisting and Privacy Best Practices and Monitor Complaints.** Abiding by leading mailbox providers whitelisting policies is essential. Moreover, keeping complaints to a minimum is required for AAR success, and is the one area of AAR management that rests entirely on the shoulders of the people in charge of their organization’s email campaigns. Minimizing complaints requires taking every step to ensure that when consumers receive your permission-based email, they receive what they expect to receive. Make sure to set up feedback loops with ISPs that maintain them (currently AOL, MSN Hotmail and Juno/NetZero). ISPs will send complaints (as reported by their users) back to trusted senders in order to safely opt-them out. In the process, this also enables marketers to determine their aggregate complaints per campaign, and average complaint rates, which can help marketers identify when improvements are in order.
- **Test Your Creative.** While the email landscape is still in flux and many mailbox providers (especially small- and enterprise-level providers) have not yet implemented AAR solutions, continue to pretest creative elements and content with legacy anti-spam filtering software to avoid words, phrase, coding, punctuation, and design common to spam.
- **Follow AAR News.** Developments in the AAR space continue to unfold and impact deliverability. Experts ranging from Meng Wong to Bill Gates predict that a much different looking inbox is only two or three years away. This white paper was written specifically to take the confusion out of AAR and the rapidly evolving email delivery landscape. Follow the news and participate in The DMA’s IMAB councils, committees, and educational programs.



Resources

The Direct Marketing Association Anti Spam Page & Resources

www.the-dma.org/antispam

Email Authentication.org News & Resources (DMA IMAB is a steering committee member supporter of this Web site designed as a central information clearinghouse to help marketers and IT pros move authentication forward and to stay abreast of the latest developments in this space)

www.emailauthentication.org

Sender Policy Framework (SPF)

www.spf.pobox.com

Microsoft Sender ID Framework (SIDF)

www.microsoft.com/senderid

Yahoo DomainKeys (DK)

antispam.yahoo.com/domainkeys

AOL Postmaster Homepage

postmaster.aol.com

MSN Hotmail Postmaster Homepage

postmaster.msn.com

E-Mail Authentication Implementation Summit June 12, 2005 • New York, NY

The Direct Marketing Association and Epsilon Interactive, along with a host of other organizations and industry leaders will host the Email Authentication Implementation Summit 2005, to be held at the New York Marriott Marquis hotel on July 12, 2005. The summit will provide marketers with actionable information and recommendations on how to create and publish SPF records and implement authentication. In addition, noted industry experts will discuss the challenges and lessons learned that can help save time and resources while improving overall e-mail deliverability. Organizers expect more than 300 IT professionals, business leaders, and e-commerce executives to attend the summit. More information and online registration can be found at:

www.emailauthentication.org/summit2005



About the Authors



The **Direct Marketing Association** (www.the-dma.org) is the leading trade association for businesses and organizations interested in direct, interactive, and database marketing, which in 2004 generated more than \$2.3 trillion in US sales, including \$143.3 billion in catalog sales and \$52.5 billion in Web-driven sales. In addition to catalogs and the Web, DMA members employ a wide variety of marketing media, including mail, e-mail, telephone, newspapers and magazines, interactive television, and radio, among others. Founded in 1917, The DMA today has more than 5,200 corporate, affiliate, and chapter members from the US and 44 other nations, including 55 companies listed on the Fortune 100.

Reflecting the significant and growing role that direct marketing plays in today's advertising mix, The DMA's membership represents marketers from every business segment, including catalogers, Internet retailers, retail stores, nonprofit organizations, advertising agencies, financial services providers, book and magazine publishers, book and music clubs, industrial manufacturers, and a host of other vertical segments, as well as the service industries that support marketers.



Epsilon Interactive (www.epsiloninteractive.com) is the leading provider of strategic, ROI-focused email communications solutions and marketing automation technologies. Through its combination of innovative technologies, professional services and vertical market expertise, Epsilon Interactive helps marketers acquire, grow and retain profitable customer relationships through highly relevant and personalized email communications. The company's end-to-end suite of industry-specific products and services includes scalable email campaign technology, delivery optimization, marketing automation tools, turnkey integration solutions, strategic consulting, and creative expertise to produce email programs that generate measurable results throughout the customer lifecycle.

Since 1997, Epsilon Interactive has developed successful permission-based email programs for more than 150 top companies, including Expedia, American Honda Motor Co. and The Washington Post/Newsweek Interactive. Privately held and based in New York, the company's investors include JPMorgan Partners, Flatiron Partners, Hudson Ventures, Mitsui & Co., Grey Ventures, HPJ Media Ventures and Syndicat Technologies.



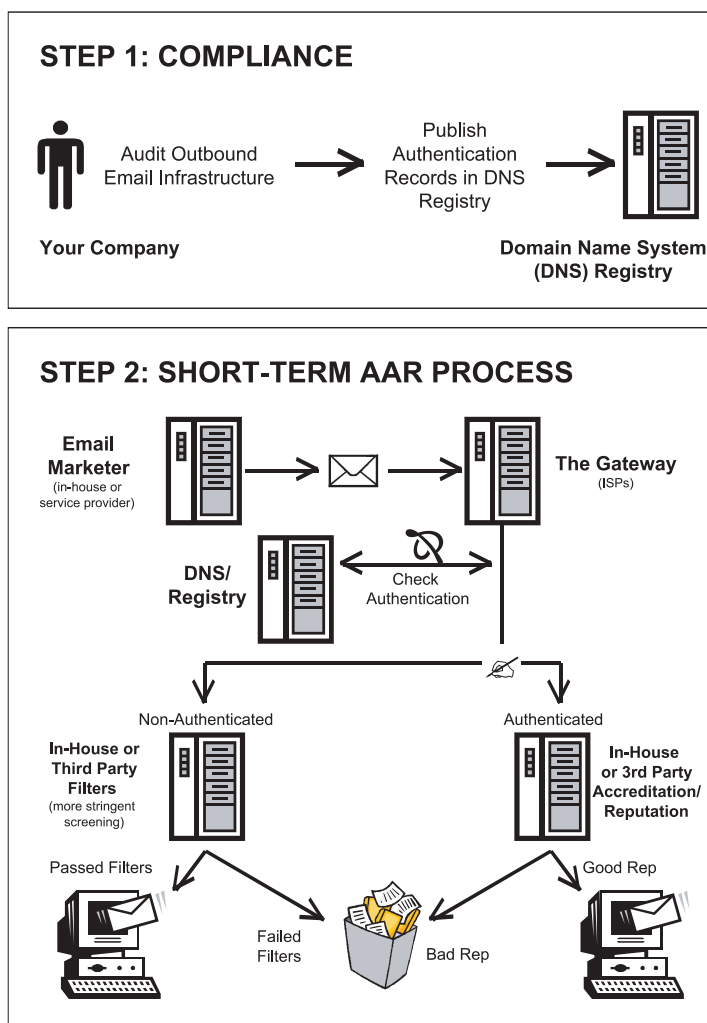
Appendix A – Short-Term AAR Process

As seen in “Step 1: Compliance,” authentication compliance requires auditing your company’s outbound email infrastructure and then publishing information about it in the form of “authentication records” that are published in the existing DNS or into another, to-be-established authentication registry.

“Step 2: Short-Term AAR Process” demonstrates how ISPs will filter email in the short term by employing AAR in concert with legacy filtering systems.

Email that passes authentication checks will not be guaranteed delivery straight to the inbox. In most cases, authenticated email will bypass legacy filters, but then be subjected to more modern email accreditation and reputation solutions (which is desirable from a legitimate sender’s perspective).

Email that fails authentication checks may not be discarded outright either – at least in the current environment – where still only a small percentage of domains have authenticated their email. Non-authenticated email will, in most cases, be subjected to existing, legacy filtering systems, and email that “passes” will still be able to land in the inbox.





Appendix B – Authentication: USPS Analogy

SPF

Dear Email Marketer,
Are you really at
315 Park Ave South
New York, NY 10010?

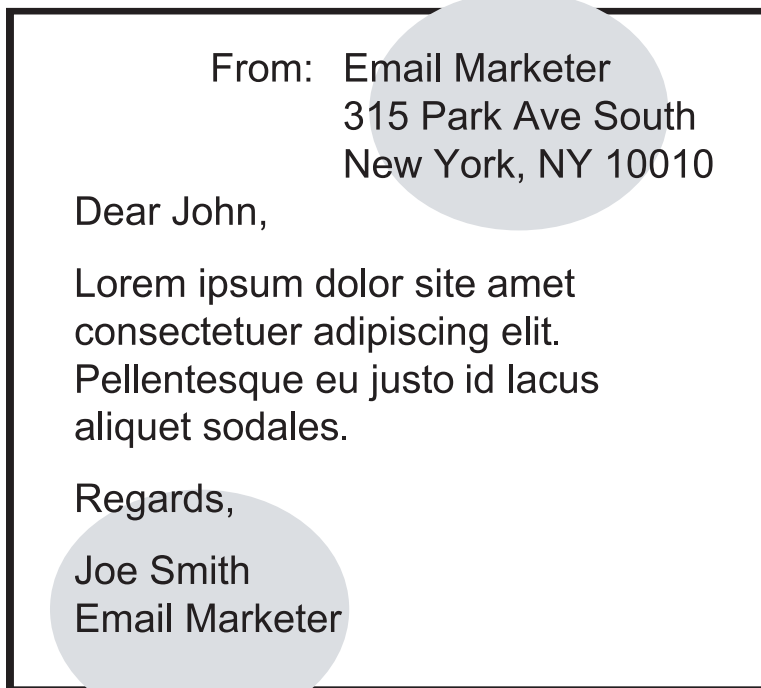


Yahoo DomainKeys

Dear Joe,
Is this really your signature?

Microsoft Caller-ID for Email

Dear Email Marketer,
Are you really at
315 Park Ave South
New York, NY 10010?





Appendix C – eNewsletter Best Practices

From

Company name is prominently featured in “From” for instant brand recognition.

Viral

Include “Forward To A Friend” functionality for increased reach.

In This Issue

Quick links summarize content for easy navigation.

Customer Service

Summarize services offering users convenient organized content.

Layout

Utilize wireframe layout — crisp, clean and scaleable for dynamic content generation.

From: MP3Mart.com

Subject: Your weekly newsletter - Great deals and sweepstakes

To ensure proper delivery of email communications from MP3mart, please add mail@mp3mart.com to your address-book. [Click here](#) for step-by-step instructions.

Opt-out language
Pellentesque luctus diam quis nulla. Maecenas consequat. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Quisque id tellus id tellus interdum posuere. [Nam diamssim](#) libero et ligula.

[Privacy policy.](#)

Duis [tempor pellentesque](#) wisi. Quisque nisi urna, eleifend placerat, rhoncus non, vestibulum et, wisi. Donec ornare elit ut lorem. Nam malesuada, tortor at rhoncus ultrices, lacus maunis adipiscing ipsum, nec ullamcorper dui eros quis velit. Nam ultrices felis ac nunc.

Phasellus commodo:
123 Franklin Street
New York, NY 10010

Subject Line

Consistent for recognition while also communicating value.

Header

Reminds user to “Add To Address Book” to ensure future delivery.

Sweepstakes

Promotional offering above the fold.

Feature

Featured products are based on past purchase history.

Call-To-Action

Response mechanisms in text and image format to ensure readability when images are blocked.

Body Content

Content is dynamically generated based on purchase behavior and preferences.

CAN SPAM Compliance

Footer must include opt-out, physical address, link to email preference center and privacy policy.



Appendix D – Phishing Example

The diagram shows a phishing email with several red flags highlighted by callouts:

- Spelling Error:** Points to the word "Billing" in the subject line, which is misspelled as "Biling".
- Forged Domain:** Points to the email address "mailto:art(fraud.ref.num7329@citi@bank.com)", which is a forged domain.
- Brand Theft:** Points to the "citi" logo, which is used without the "Bank" part of the name.
- No Personalization/Account ID:** Points to the salutation "Dear CitiBank customer," which is generic and lacks a specific account ID.
- Asks For Personal Info:** Points to the text "confirm your banking details", which is a common phishing tactic.
- Links To Fraudulent Web Site:** Points to the URL "https://web-da-us.citibank.com/signin/scripts/login/user_setup.jsp", which is a fraudulent website.

The email content is as follows:

From: CITIBANK [mailto:art(fraud.ref.num7329@citi@bank.com)]
Sent: Saturday, October 02, 2004 8:01 AM
To: John Doe
Subject: Ct Bank Biling Department: Important Information

citi

Dear CitiBank customer,

Recently there have been a large number of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

To securely confirm your Citibank account details please go to:

https://web-da-us.citibank.com/signin/scripts/login/user_setup.jsp

Thank you for your prompt attention to this matter and thank you for using CitiBank!

Citi® Identity Theft Solutions
Do not reply to this email as it is an unmonitored alias

A member of citigroup
Copyright © 2004 Citicorp