Financial Fraud Law Report

VOLUME 3 NUMBER 6 JUNE 2011

The FINANCIAL FRAUD LAW REPORT is published 10 times per year by A.S. Pratt & Sons, 805 Fifteenth Street, NW., Third Floor, Washington, DC 20005-2207, Copyright © 2011 THOMPSON MEDIA GROUP LLC. All rights reserved. No part of this journal may be reproduced in any form — by microfilm, xerography, or otherwise — or incorporated into any information retrieval system without the written permission of the copyright owner. For permission to photocopy or use material electronically from the *Financial Fraud Law Report*, please access www.copyright.com or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For subscription information and customer service, call 1-800-572-2797. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 10 Crinkle Court, Northport, NY 11768, smeyerow@optonline.net, 631-261-9476 (phone), 631-261-3847 (fax). Material for publication is welcomed — articles, decisions, or other items of interest. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.
POSTMASTER: Send address changes to the Financial Fraud Law Report, A.S. Pratt & Sons, 805 Fifteenth Street, NW., Third Floor, Washington, DC 20005-2207. *ISSN 1936-5586*

Authenticating Challenged E-Mails: The Problem of Forgery

ANGELA ZAMBRANO AND RICARDO PELLAFONE

This article addresses the problem of authenticating e-mails amidst allegations of forgery and provides a suggested framework for courts to use when these allegations are present.

E-mail communication is an inescapable part of modern litigation. One marketing research firm that tracks e-mail statistics estimates that there are 2.9 billion e-mail accounts worldwide, 730 million of which are corporate accounts.[1] It is also estimated that the typical corporate user sent and received about 110 e-mails each day in 2010.[2]

As a result of this volume, e-mails are fast becoming the most critical part of discovery involved in litigation.[3] Surprisingly, however, there are few cases examining the methods by which an e-mail may be authenticated for evidentiary use.[4] For example, when considering authentication under Federal Rule of Evidence 901(b)(4) (or a state counterpart thereto), authorities have relied on the generic format of e-mail messages, particularly the presence of e-mail addresses and names in the e-mail "header" fields — the part of an e-mail that contains the "to," "from," and "subject" lines, along with additional information that is typically hidden from view in the default setting of most e-mail clients.[5] These authorities reason that

Angela Zambrano is a partner and Ricardo Pellafone is an associate in the Complex Commercial Litigation section of Weil, Gotshal & Manges, LLP. Based in the Dallas office, the authors may be contacted at angela.zambrano@weil.com and ricardo.pellafone@weil.com, respectively. The authors thank Victoria Neave and Hallie Graves for their assistance in researching this article.

Published in the June 2011 issue of *The Financial Fraud Law Report*.
Copyright 2011 ALEXeSOLUTIONS, INC. 1-800-572-2797.

because these e-mails look like what they are purported to be, they are sufficiently authentic and can be admitted.[6]

In cases where authenticity is not contested, this standard may be fine. But e-mail header data — and particularly the simple header data shown by most e-mail client programs and e-mail print-outs — can be forged by anyone with basic computer skills.[7] This raises the question of what courts should do when specific allegations of forgery are present.[8] The few courts that have attempted to answer this question have arguably confused matters further, and they are so fact-specific that they provide no assistance to a party or court seeking guidance on how to handle a similar fact pattern.

This article addresses the problem of authenticating e-mails amidst allegations of forgery and provides a suggested framework for courts to use when these allegations are present. To that end, the first part discusses the basics of e-mail as a communication medium, including an explanation of how e-mails can be easily forged. The second part of this article discusses the current law on e-mail authentication, both at the initial authentication stage and after an e-mail's authenticity has been challenged. The article then provides a suggested framework for courts to use when faced with a potentially forged e-mail and conclusions.

E-MAILS: MECHANICS AND FORGERY

Not every e-mail is from its purported sender. E-mail can be easily forged; in its simplest forms, forgery takes the shape of a person attempting to create a document in a word processing program that resembles an e-mail[9] or someone with access to another person's account information logging in to that person's account and sending e-mails as them.[10] While these are easily-recognized examples, they are crude and — ironically — often more difficult to execute than more sophisticated forgeries.[11]

A more serious threat is the fact that e-mail itself is a generally insecure medium that lacks authentication.[12] For example, the involvement of multiple service providers that are used to gain access to the Internet and send e-mail, such as the local cable company or e-mail providers like Yahoo or Google, complicates authentication due to the different layers of security or lack thereof.[13] "[U]nlike former days when a user's posts were easily traceable through [an] online access provider [like AOL]'s billing records, today, the World Wide Web host of an e-mail…service obtains only as much information about an individual as it requires for registration, and even then, there are few checks to ensure the validity and accuracy of that information."[14] As a result, in many cases a person can send an e-mail under any name or e-mail address that they like, fooling credulous users who assume that the simple header data displayed by their e-mail client is reliable. Next, this section explains the basics of how e-mail protocols work, followed by a discussion of how they can be exploited. This section then discusses why these exploits are so effective and gives examples of common ways they are used.

Simple Mail Transfer Protocol: How E-mail Works

E-mail messages are generally relayed according to a technological protocol named the Simple Mail Transfer Protocol, or SMTP.[15] SMTP was originally written in 1982 and is still the most commonly-used e-mail protocol today.[16] SMTP was designed as a system based on trust; as a result, it is less secure than most end-users assume.[17]

As its name implies, SMTP works in a fairly uncomplicated fashion. First, the sender's computer establishes a connection to the e-mail server and greets it with a "hello" command — "HELO" or "EHLO," depending on how complex the sender wants their e-mail message to be[18] — followed by the domain where the sender's e-mail address is registered.[19] This lets the SMTP server know that the sender's computer is attempting to send an e-mail through the server, and assuming the request is formatted properly, the SMTP server responds by recognizing the greeting and readying itself for the e-mail message.[20] Next, the sender's computer transmits the sender's e-mail address to the SMTP server, followed by the recipient's address.[21] Finally, the sender's computer sends the actual e-mail message itself, along with any data it wants to include in the header (for example, displaying that the message is from "John Doe" instead of johndoe@emailaddress.com), and then ends the connection.[22] The SMTP server interprets all of this data and delivers or relays the message to the appropriate e-mail address.[23]

This all seems simple and secure enough, and it happens countless times a day behind the scenes of a computer- or Web-based e-mail program.[24] But notice what is missing: a check by the SMTP server that any of the data it is receiving is authentic.[25] All the SMTP server does is make sure the information is in a form that it can use, not that the data is actually coming from where it is purporting to originate.[26] When this information is intentionally forged, it is called spoofing.[27]

E-mail Spoofing: How it Works

E-mail spoofing is accomplished by telling the SMTP server fraudulent information. When a SMTP server requires the spoofer to specify the domain where the spoofer's e-mail address is registered, it does not check if the domain is the actual domain the spoofer is using.[28] Thus, when a spoofer begins the SMTP connection, they can specify any random domain after the "hello" command, whether it is the correct one or not — and in many cases, whether it is even an existing domain at all — so long as it is formatted properly.[29] SMTP servers also do not check the veracity of the sender's e-mail address or the content of the message itself, which allows a spoofer to easily pose as someone else by putting in false information.[30] The only way to detect the fraud is to review the e-mail's full header data[31] to view the sender's IP address[32] and the servers the e-mail passed through; hidden by default in almost every e-mail program, this information can be obtained through a request for production of metadata related to the e-mail[33] or by a subpoena to the e-mail service provider.[34] However, even an e-mail's full header data can be forged or obscured.[35]

Even worse, the same e-mail programs that most people use to send and receive e-mails make spoofing user-friendly.[36] A spoofer can simply change the display name and return address in their e-mail program.[37] Since most e-mail programs only display simple header data, this is an effective method of spoofing unsophisticated users.[38] And for individuals who do not even wish to take that step, companies such as hoaxMail and Sharpmail provide automated spoofing services for a fee.[39] Finally, because all of these methods allow the spoofer to forge the sender's e-mail address and/or put a different address in the "reply-to" header field, pressing the "reply" button will do nothing to determine the true sender; the e-mail address that appears in the "to" field of the recipient's e-mail client can be whatever the spoofer wants it to be.[40] In some instances, forging this field is the spoofer's main goal.[41]

More advanced e-mail protocols have been developed to attempt to provide some method of authentication that can be used to end spoofing, and their implementation can be an effective, [42] if burdensome,[43] tool in the fight against spoofed e-mails. While these authentication schemes can frustrate spammers and large-scale phishing schemes, they still can be circumvented by dedicated spoofers.[44]

Spoofing has been around almost as long as SMTP, and it will continue to be around for the foreseeable future.[45] Even if the information security community succeeds in implementing a new protocol that is effective in preventing large-scale spoofing by spammers and phishing scammers, this will not stop individual, targeted spoofing. After all, spoofing is popular for one simple reason: it works. We now turn to the question of why this is the case, and discuss forms of common spoofing attacks.

E-mail Spoofing: Why it Works and Examples

A spoofing attack will only succeed if the targeted user believes that the e-mail came from its purported source. This kind of attack relies on a tactic known as "social engineering," which relies on the power of persuasion and human psychology over technological expertise.[46] A person who has gained the trust of an unwitting user can cause an incredible amount of damage. Kevin Mitnick, a famous hacker and the most-wanted computer criminal in United States history at the time of his arrest,[47] exclusively used social engineering tactics throughout his hacking career.[48]

Spoofing tends to work because most people are trusting, not particularly technologically savvy, and desire to be helpful.[49] Thus, even if a victim is otherwise sophisticated and educated, they will tend to trust the stated source, even when it goes against what they know of the sender.[50] This is not only true in individual cases, but in the population as a whole: people generally trust that e-mail headers provide them with reliable information, and scammers routinely try to take advantage of that fact for their own benefit. To illustrate how prevalent this trust is, and how effective a scam that exploits it can be, we now examine three popular methods of exploitation: worms, phishing scams, and Joe Jobs.

Worms

A worm is a self-replicating computer program that spreads by causing an infected computer to send out more versions of itself across a network.[51] Typically, a user receives a worm from someone they know, either embedded in an e-mail or sent as an attachment.[52] When the user opens the e-mail or attachment, the script or program runs, automatically scanning the user's e-mail address book and sending itself to all of those addresses.[53] Since the worm is sending itself out from the infected user's e-mail program, the recipients believe that the worm was sent by someone they know, open the e-mail or attachment, and the process starts again.[54]

Worms are not true spoofing attacks in the sense that the e-mails used to spread the worm actually are being sent from the source they claim to be, albeit unintentionally so.[55] But they are effective because they rely on the same method of deception used by typical spoofing attacks; users tend to blindly accept things that they believe to be sent by parties they trust. When this fact is exploited by a worm, the results can be devastating; in 2004, the "MyDoom" worm caused an estimated $250 million in damage,[56] and infection became so widespread that e-mails sent by the worm at the peak of its activity accounted for 20 to 30 percent of all e-mail traffic.[57]

Phishing Scams

A "phishing" scam uses spoofed e-mails and fraudulent Web sites to trick users into divulging sensitive information to the scammer.[58] Phishing scams are a common — and effective — way for identity theft to occur.[59] In a typical phishing scam, the scammer identifies a financially consequential group of potential victims — for example, the online customers of a bank.[60] Then, the scammer sends out spoofed e-mails that purport to be from the bank.[61] Diligent scammers will supplement this basic forgery with other elements of brand authenticity — for example, they may include an image from the bank's Web site or a trailer used by the bank.[62] The e-mail will request that the user take some sort of urgent action by logging in to the bank's Web site to update or verify information, and will provide a link in the e-mail itself.[63]

Users who click on the link will be directed to an official-looking but fraudulent Web site; the scammers create a copy of the log-in page from the targeted institution and create an alternate page at their own Web site.[64] If the user does not check the actual Web address, relying only on the appearance of the site itself, they will be sending any information they enter into the site directly to the phishing scammers.[65] The scammers will then take that opportunity to log into the user's account and clean it out — and if the information that they have phished lets them do so, engage in further identity theft and proceed to establish new accounts and lines of credit using the victim's information.[66] Phishing scams are very popular and have targeted entities such as Citibank,[67] Wells Fargo,[68] Gmail,[69] and Myspace.com.[70] Once again, these scams work because users play along; here, the user's trust in simple header data causes them to not just open an e-mail or attachment, but take action and divulge sensitive personal information as well.

Joe Jobs

Finally, a "Joe Job" is a method of using spoofed e-mails to malign the reputation of another person or organization.[71] This attack was named after Joe Doll, its first victim.[72] Doll runs Joe's Cyberpost, a Web site that historically offered free Web hosting services to individuals.[73] In 1997, a spammer started using Doll's service to plague other users with spam.[74] After Doll warned the spammer and the conduct continued unabated, Doll deleted the spammer's account.[75] The spammer retaliated by sending millions of spam messages with forged headers stating that the messages originated from Doll.[76] Doll was buried under the responses from furious recipients, and subsequent attacks of this type now bear his name.[77]

Thus, in this method, the attacker will put offensive content into the body of the e-mail and then spoof the e-mail's header data to make the e-mails appear to be coming from the victim.[78] The outraged recipients then retaliate against the victim, who only becomes aware of the attack when e-mails begin pouring in from angry recipients.[79]

Despite its simplicity — reviewing the full header data would demonstrate the forgery — the Joe Job is a highly effective method of attack, even against sophisticated parties. Francis Boyle, a law professor at the University of Illinois and pro-Palestinian activist, came back from a vacation in 2002 to find 55,000 messages in his e-mail inbox.[80] Boyle had fallen victim to a Joe Job that had him purportedly writing "when I see in the newspapers that civilians in Afghanistan or the West Bank were killed by American or Israeli troops, I don't really care."[81] Even though Boyle was a well-known pro-Palestinian activist, he had to spend days issuing apologies to colleagues and friends who believed that the wildly anti-Palestinian remark had actually originated from him.[82]

Boyle's case illustrates how much users tend to rely on simple header data as inherently reliable. Even though the content of the Joe Job was the exact opposite of what people knew to be true about him, many believed that the e-mail was genuine because they relied on the forged header data. This problem is not limited to casual Internet users or credulous individuals, but impacts highly sophisticated and educated people.

This translates into a significant problem in court. When e-mail printouts are offered into evidence, they will only contain the e-mail's easily-forged simple header data in nearly every case. And since, as explained above, even sophisticated individuals tend to trust this information, a forged e-mail that makes its way into evidence has the potential to be massively prejudicial. As a result, the court's work in authenticating a proffered e-mail for evidentiary purposes is incredibly important. In the next section, the cases that have sought to undertake this analysis to date are examined.

CURRENT STANDARDS FOR THE EVIDENTIARY AUTHENTICATION OF E-MAILS

Evidence may only be admitted if it is shown to be authentic, and electronic evidence is no exception to this rule.[83] This requirement is met when a party offers evidence sufficient to support a finding that the piece of evidence in question is what the party claims it to be.[84] For example, the proponent "need only adduce evidence that the document is an e-mail" between certain persons, "not that the contents of the e-mail are the actual thoughts of the author."[85] Thus, the court does not need to actually find that the evidence is what the party claims it is, only that a jury could make that finding based on the information that the party has offered — information that, for e-mail evidence, must itself constitute admissible evidence.[86] In the context of computer-based evidence, this finding of reliability includes an analysis of factors unique to this type of evidence, such as the security of the system that generated the evidence.[87] Ultimately, authentication ensures that evidence is trustworthy, which is of particular importance if the evidence involves hearsay — as in the case of almost every e-mail.[88]

In this section, we discuss the current standards applicable to efforts to authenticate e-mails for evidentiary purposes. First, the basic standards for authenticating unchallenged e-mails is addressed. The few cases where specific claims of forgery have been raised will also be discussed.

Authentication: The Basic Standards

Although courts are increasingly faced with the issue of admitting e-mails into evidence, few reported decisions examine the issue in depth. Indeed, in the absence of a challenge to the authenticity of a specific e-mail, courts have generally followed the analysis of the three cases that dominate this area of law.

U.S. v. Siddiqui

The rules on the initial showing required for authenticity were first outlined by the Eleventh Circuit in its *U.S. v. Siddiqui* opinion.[89] Mohamed Siddiqui was an Indian citizen who was a visiting professor at the University of South Alabama in 1996.[90] Siddiqui was nominated for the Waterman Award that year, a $500,000 research grant issued by the National Science Foundation (“NSF”) to an outstanding scientist or engineer.[91] The form nominating Siddiqui listed references and included a form recommending Siddiqui that was signed by a Dr. von Gunten, one of the references listed on the form.[92] The nominating form was filled out by a Dr. Hamuri Yamada.[93]

Unfortunately, neither von Gunten nor Yamada had any knowledge of this; Siddiqui had fabricated the whole thing.[94] After Siddiqui fraudulently submitted the package on Yamada’s behalf, Siddiqui e-mailed Yamada and asked her to “please tell good words about me” if the NSF called.[95] Siddiqui also sent an e-mail to von Gunten, asking von Gunten to tell the

NSF that von Gunten had given Siddiqui permission to use von Gunten's name.[96] Both e-mails were admitted into evidence, and Siddiqui was convicted of fraud, providing false statements to a federal agency, and obstruction in connection with a federal investigation.[97] He appealed on several grounds, including that the district court erred by entering the e-mails into evidence without proper authentication.[98]

The Eleventh Circuit held that the district court did not abuse its discretion in admitting the e-mails.[99] In doing so, the court referenced a "number of factors" that supported the e-mails' authenticity under Federal Rule of Evidence 901(b)(4), including the fact that the content of the e-mails showed that the sender had knowledge of Siddiqui's conduct, that the sender referred to himself by Siddiqui's nickname, and that Siddiqui himself later repeated the requests contained in the e-mails in phone calls to von Gunten and Yamada.[100] The court also referenced two factors unique to e-mail messages: that the e-mails sent to von Gunten and Yamada "bore Siddiqui's e-mail address" and that von Gunten had testified "that when he replied to the e-mail apparently sent by Siddiqui, the 'reply-function' on von Gunten's e-mail system automatically dialed Siddiqui's e-mail address as the sender."[101]

U.S. v. Safavian

The next major opinion came six years later, from the District Court for the District of Columbia in its 2006 *U.S. v. Safavian* opinion.[102] *Safavian* concerned the Jack Abramoff scandal, and the e-mails at issue were thousands of e-mails produced from Greenberg Traurig, LLP, Abramoff's former employer.[103] The government attempted to enter the e-mails into evidence *en masse*; after holding that the e-mails could not be admitted as self-authenticating, the court turned to authentication under Rule 901.[104] Citing to *Siddiqui*, the court held that "most of the proffered exhibits" could be authenticated under Rule 901(b)(4), using the evidence's "distinctive characteristics and the like," including "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances."[105]

Specifically, the court found that the "distinctive characteristics" present in the proffered e-mails included the "actual e-mail addresses containing the '@' symbol, widely known to be part of an e-mail address," the fact that most of the e-mail addresses contained the name of the person attached to the address, and that the e-mails frequently contained the names of the sender or recipient in the body and header.[106] Those facts, combined with the content of the e-mails that concerned the matters at issue, sufficiently authenticated the e-mails to permit their admissibility.[107] Moreover, once one e-mail from a given e-mail address was found sufficiently authentic, all other e-mails from that address were automatically found authentic by comparison to the first e-mail under Federal Rule of Evidence 901(b)(3).[108]

After authenticating the e-mails at issue, the court turned to the defendant's contention that e-mails were untrustworthy in general, particularly those that had been embedded within other e-mails as a result of the e-mails being forwarded, or that had been embedded as the originating e-mail in a reply.[109] The court acknowledged that the embedded e-mails could have been altered, but refused to allow the mere possibility of alteration as a basis for excluding the e-mails as unidentified or unauthenticated as a matter of course.[110] Because the defendant had not raised any specific evidence showing alteration — instead attempting to generally exclude the e-mails as being inherently untrustworthy because they were e-mails — the court admitted the e-mails and instructed the defendant that its arguments were more appropriately directed to the weight the jury should give the evidence.[111]

Lorraine v. Markel Am. Ins. Co.

Finally, the District of Maryland's 2007 opinion in *Lorraine v. Markel Am. Ins. Co.* provides a much-heralded discussion of authentication standards applicable to electronic evidence.[112] *Lorraine* gives an exhaustive view of evidentiary issues in electronic discovery overall, and it has been hailed as a watershed moment in the field.[113] But *Lorraine* also reflects the limited analysis available on e-mail authentication, basing its analysis almost exclusively on Weinstein's Federal Evidence treatise.[114]

Lorraine concerned a suit brought to enforce an arbitrator's award.[115] After discovery, both sides moved for summary judgment, which the court dismissed without prejudice because neither party had produced any admissible evidence; although e-mails constituting parol evidence were at the heart of the dispute, neither party authenticated any of their proffered e-mails, instead attaching them as exhibits to their motions.[116] After dismissing the motions, the court informed the parties that it intended to file a more comprehensive opinion that explained its ruling; this opinion is *Lorraine*.[117]

After providing that background, the court undertook an effort to provide the parties and the bar at large with a comprehensive analysis of the issues associated with electronic evidence.[118] The court then discussed general authentication issues at length before turning to specific types of electronic evidence, beginning with e-mails.[119]

Lorraine's examination of the existing authorities on e-mail authentication is short, as the available analysis is limited.[120] The court focuses exclusively on the analysis in § 900.07[3][c] of Weinstein's treatise, which provides for two methods of authenticating e-mails: by the distinctive characteristics standard of Federal Rule of Evidence 901(b)(4) and as a self-authenticating business record under Federal Rule of Evidence 902(7).[121] As to the former, Weinstein offers several distinctive characteristics that can be used to authenticate an e-mail.[122] First, a print-out of an e-mail typically bears the sender's e-mail address, which provides circumstantial evidence that the message was transmitted by that person.[123] Second, the reply function in an e-mail program "automatically routes the message to the address from which the original message came," so using this function can demonstrate that the reply message would be sent to the sender's listed e-mail address.[124] Weinstein notes that a sender's address is, by itself, insufficient, as someone could have gained access to the sender's account; because of this, authentication requires testimony from a person with personal knowledge of the e-mail's transmission or receipt.[125]

This is the extent of *Lorraine*'s discussion of authenticating e-mails specifically; the court cites to a total of four cases to demonstrate that courts have approved Weinstein's methods: *Siddiqui* and *Safavian* for the "distinctive characteristics" analysis,[126] one case for the general proposition that e-mails can be authenticated by direct or circumstantial evidence,[127] and one case to support authentication of qualified e-mails as business records.[128]

Prima Facie Authentication Generally: Methods and Problems

In sum, these cases and their progeny demonstrate that e-mails may be initially authenticated by many means.[129] E-mails can be authenticated by a lay or expert witness with personal knowledge through live testimony,[130] affidavit,[131] or deposition.[132] E-mails may be authenticated by the author's own actions.[133] E-mails are deemed authentic when produced under oath in discovery[134] or when produced by the party that is challenging the e-mail's authenticity when offered by the other party.[135] E-mails may be authenticated as business records,[136] by trade inscriptions,[137] or by reference to a previously-authenticated exemplar.[138] And e-mails may be authenticated by their "distinctive characteristics"[139] or surrounding circumstances.[140] In a few instances, courts have considered whether e-mails possessed "significant indicia of trustworthiness."[141]

These standards only address the initial showing. They are insufficient when authenticity is at issue. Because the very purpose of a spoofed e-mail is to appear authentic, these standards — which generally rely on the appearance of the proffered e-mail in some way — do nothing to prevent a spoofed e-mail from finding its way into evidence.

When a party attempts to authenticate an e-mail using its distinctive characteristics, authorities have focused on the data contained in an e-mail's "to," "from," "subject" or "re," and "date" fields as the source of this information.[142] All of this information is contained in the "header" of an e-mail, the portion of an e-mail that contains the information about who sent the e-mail, who it was sent to, when it was sent, and how it was transmitted.[143] In most e-mail programs and print-outs of e-mails, this data appears in a limited form as the "from," "to," "date," and "subject" or "re:" fields; [144] we refer to this as the "simple header," and it is the information that authorities have referred to as an e-mail's distinctive characteristics.[145]

The problem with using an e-mail's simple header data as the source of its distinctive characteristics is that simple header data can be very easily forged, both in appearance and function.[146] Although these issues do not mean that e-mails are generally unreliable,[147] they do mean that the simple header standard is unhelpful for authentication in cases when there are specific allegations of forgery; the standard will do nothing to determine whether the e-mail is genuine or not. If all a party has to do to authenticate an e-mail is attest that they received it, that the simple header contains the sender's e-mail address or name, and that the sender's e-mail address automatically appeared in the "to" field when the party pressed "reply," then they can truthfully offer that testimony even when they have altered the contents of the message[148] or fabricated an entire e-mail that they sent themselves.[149]

Of course, the fact that e-mails can be forged will not exclude an otherwise authenticated e-mail.[150] Nor will a bald assertion of forgery that is unsupported by evidence.[151] But where specific, evidence-backed allegations of forgery of evidence are present, the previous cases[152] are simply not instructive. Thus, we now turn to a discussion of the cases that have been faced with the more difficult situation involving allegations of forgery.

Determining Authenticity in the Face of Specific, Evidence-Backed Forgery Allegations

Specific, evidence-backed allegations of e-mail forgery are rare — often the question of forgery turns out to be unnecessary because the proponent has failed to make any showing of authenticity in the first place.[153] When the issue has arisen, the factual complexity of the allegations and testimony has yielded a confusing — or arguably incorrect — decision by the court faced with the evidence. None of the decisions reference each other, and their discussion of applicable precedent on e-mail authentication is scant — where it exists at all. Accordingly, we now address each of the cases that have considered this issue.

The dueling affidavits: *Chiu v. Plano ISD*

Chiu v. Plano Independent School District is the earliest and most straightforward of the decisions involving allegations of e-mail forgery.[154] In *Chiu*, a group of parents clashed with the superintendent of their school district over a new math curriculum.[155] The parents, who opposed the new curriculum, claimed that the superintendent had sent an e-mail to all principals that targeted the parents' views in an effort to exercise in viewpoint discrimination.[156] The superintendent executed an affidavit unequivocally denying authoring the e-mail; a parent executed an affidavit stating that she had received the e-mail from a school employee, who in turn had received it from one of the principals, and that she had "no reason to believe" that the e-mail had been altered or had not been received by the principal.[157] There was no additional testimony or evidence supporting or attacking the e-mail; and, in upholding the district court's denial of the school district's motion for summary judgment, the Fifth Circuit held that a genuine issue of material fact existed as to the authenticity of the e-mail,[158] which the district court had correctly recognized "would be a question for the jury."[159]

Chiu is an easy case; in the absence of any forensic evidence, the court simply had to weigh the appearance of the e-mail against the testimonial evidence. With the purported author disavowing authorship, and the proponent disavowing forgery, the court was faced with admissible evidence that could have supported either conclusion. Thus, the decision to admit the evidence and allow the jury to determine its ultimate authenticity was undoubtedly correct.

Dueling affidavits redux: *Munshani v. Signal Lake Venture Fund II*

The second decision, *Munshani v. Signal Lake Venture Fund II, LP*, is factually similar to *Chiu*, but the court handled the allegations of fraud in a different manner.[160] In *Munshani*, the plaintiff claimed that he had raised funds for the defendant venture capitalists on the basis of oral promises they had made to him.[161] In response, the defendants raised the affirmative defense of the Statute of Frauds.[162] The plaintiff then produced an e-mail that he claimed he had received from the president of the largest company in the defendants' venture capital portfolio that supported his allegations.[163] Both the plaintiff and the alleged sender offered affidavits, respectively affirming and attacking the authenticity of the e-mail.[164] The plaintiff suggested that the court appoint a neutral expert to investigate each party's allegations, which the court did.[165]

After seven months of investigation, the court-appointed expert concluded that the e-mail was "clearly not authentic."[166] The judge allowed the parties an opportunity to comment on the expert's conclusions; the plaintiff offered no objections, but filed a written response on the last day of the comment period invoking his privilege against self-incrimination.[167] The judge inferred that the e-mail was wholly false and a "deliberate and intentional fraud on the court."[168] The plaintiff's complaint was dismissed with prejudice, and he was ordered to pay the costs and fees of the expert, as well as the fees and costs related to the defense attorneys' discovery of the fraud.[169] The Massachusetts Appeals Court upheld these remedies on appeal, noting that, "in brief, the judge, in the exercise of inherent powers, acted within his discretion in ordering dismissal."[170]

Introducing forensic testimony: People v. Downin

In *People v. Downin*, the earliest decision involving forensic evidence (here, in the form of testimony), the Illinois Appellate Court considered a convicted sex offender's claims that the trial court should have excluded e-mails that he allegedly sent to his victim that contained admissions of guilt.[171] The appellant, Nicholas Downin, pointed to testimony from the victim's friends, who had testified that the victim had access to the defendant's e-mail account and had said that "if she was having problems with a man she could create trouble for him by falsifying e-mails."[172] Downin also pointed to testimony from an e-mail and computer expert, who stated that the e-mail at issue appeared to have been sent from Downin's e-mail address, which was registered at the galesburg.net domain, "through the website 'hotmail,' run by Microsoft."[173] The expert further testified that the only way to truly authenticate the e-mail would be by examining the IP addresses, which were not present in the exhibit.[174]

In support of the e-mail's authenticity, the victim testified that she had sent an e-mail to Downin at the same e-mail address she had used for him previously, and that she had received a reply from that address.[175] That, combined with the fact that the e-mail in question was responsive to the victim's e-mail and contained information known exclusively to the victim and Downin, was sufficient for the court to hold that the prosecution had satisfied its burden.[176] The appellate court found that the trial court had properly admitted the e-mail and considered Downin's arguments about its authenticity as a matter of the weight it should assign to the e-mail.[177]

On those grounds, the appellate court's decision is confusing. Downin pointed to specific evidence that supported his contention that the e-mail had been fabricated, and the prosecution's showing of authenticity was lacking. Because the victim had access to the defendant's e-mail account and had stated that she could fabricate e-mails from him, it seems inappropriate to find that a response to her e-mail from his e-mail address sufficiently established authenticity — the victim could have responded to the e-mail herself, and by definition, she would have known information "known exclusively to her and Downin."[178] Likewise, the victim's testimony that she "received a reply from Downin's e-mail address at her e-mail address" does not establish authentication — could have been truthfully made even if the victim had logged into Downin's account and sent the e-mail herself.[179]

In fact, the reason that best justifies the court's conclusion rests on what is missing from the opinion: any evidence that Downin affirmatively disavowed the e-mail's authenticity prior to its admission.[180] Although Downin raised several reasons why the e-mail's authenticity should be questioned, the opinion is silent as to whether he elected to undertake the most fundamental attack on its authenticity — testifying that he did not send the e-mail before the e-mail was admitted into evidence.[181] If he did not — and otherwise did testify (thus making concerns of Fifth Amendment waiver moot) — the appellate court's decision is likely correct; Downin's other allegations of forgery mean very little if he declined to testify that he actually did not send the e-mail.[182] Conversely, if he had so testified or had declined to testify at all, then the Appellate Court's decision becomes more muddled; if Downin had unequivocally denied sending the e-mail, and the victim's testimony only described the e-mail without stating that the e-mail had not been forged or altered, then the e-mail perhaps should have been excluded — particularly given that the victim had access to Donwin's e-mail account and claimed that she would forge e-mails to get men into trouble.[183] The opposite conclusion may have been appropriate if Downin had generally refused to testify — in which case the court's finding of authenticity draws uncomfortable questions of whether his silence was used against him as an implicit admission of the e-mails' authenticity.[184] None of this information was discussed by the court, however, and in its absence the opinion sheds little light on the situation.

Using forensic data: Brown v. Great-West Healthcare

In the fourth case, *Brown v. Great-West Healthcare*, several plaintiffs brought employment actions alleging discrimination under Title VII.[185]

The plaintiffs offered paper copies of 11 e-mails into evidence which contained racially offensive statements about African Americans, both in general and specifically targeted at some of the plaintiffs.[186] None of the plaintiffs were recipients of the e-mails; they had been exchanged among three other Great-West employees, all of whom denied sending or receiving them.[187] One of the plaintiffs came into possession of the e-mails when they were left on her desk chair one day.[188] A former computer administrator for Great-West testified that they had seen a racially offensive e-mail about one of the plaintiffs on the computer screen of one of the three employees implicated in the e-mails, but the testimony was considered to be "vague" and constituted the only evidence that any racially offensive e-mails had ever been seen on a computer screen.[189]

Both parties retained computer experts, neither of whom were able to determine if the e-mails in question were authentic.[190] Neither expert found the e-mails on Great-West's computer system; Great-West's expert, however, found copies of other e-mails that were identical to the e-mails at issue but lacked the racially offensive statements.[191] Great-West's expert testified that he believed that the racially offensive e-mails were the forged versions, and that they could have been fabricated by someone who had access to one of the three employees' passwords, which would have allowed that person to alter the originals and then print them out without saving the changes to the authentic versions; other testimony established that one of the plaintiffs did have such access.[192]

Great-West moved for summary judgment, filing a separate motion to exclude the e-mails from consideration.[193] Great-West argued that the testimony of the involved employees denying ever having sent or received the e-mails, the lack of evidence demonstrating that they had ever existed on Great-West's servers, the inability of forensic experts to authenticate them, the presence of identical e-mails that lacked the offensive content on Great-West's servers, and the fact that one of the plaintiffs had access to the purported sender's e-mail account meant that the e-mails were inauthentic.[194] The plaintiffs responded that they had established the requisite *prima facie* case because the e-mails stylistically matched properly authenticated e-mails from their alleged sender, the e-mails appeared to be from their purported senders, and the purported sender had made other racially insensitive remarks to the plaintiffs.[195] In its reply, Great-West argued that, because it had challenged the authenticity of the e-mails, the plaintiffs now had to carry a more demanding burden than a *prima facie* showing, and that, in the face of Great-West's proffered evidence of forgery, they had failed to do so.[196]

The Northern District of Georgia excluded the e-mails, holding that the evidence that the plaintiffs had offered in support of authenticity did not overcome the evidence offered by Great-West.[197] Specifically, the evidence of other "racially-tinged" remarks or actions by the purported authors of the e-mails and similarities in style between the e-mails in question and those that were known to be authentic was not enough to overcome the fact that "(1) Brown found the questioned e-mails on her chair; (2) Brown had access to [one employee's] private e-mail account; (3) neither party's expert could find the questioned e-mails on Great-West's computer system; and (4) the purported authors and recipients den[ied] that they [were] authentic."[198]

Left unsaid by the court is the fact that, although they had been on notice for months that Great-West challenged the authenticity of the e-mails — and that the obvious implication was that the plaintiffs had forged them — none of the plaintiffs testified that, to their knowledge, the e-mails had not been altered or forged. Instead, the plaintiffs' briefing goes to great lengths to avoid making this claim, instead focusing on the way the e-mails appeared even after they had been on notice of the specific challenges that Great-West made to their authenticity.[199]

Searching back-up tapes: *Bell v. Rochester Gas & Electric Corp.*

Finally, *Bell v. Rochester Gas & Electric Corp.*, a decision recently affirmed by the United States Court of Appeals for the Second Circuit, was another employment discrimination case strikingly similar to *Brown*.[200] Bell was an African-American contract employee of Energetix, Inc. ("Energetix") who had been suspended and then terminated in late May 2002, for allegedly attempting to alter his wife's gas contract in order to obtain a lower billing rate.[201] Bell brought suit, claiming that this reason for his termination was pretextual.[202] In support of this allegation, Bell offered a document that appeared to be a print-out of an e-mail sent from his supervisor to two other supervisors.[203] This e-mail had been sent around the time of the meeting when the supervisor suspended Bell on May 21, 2002, and consisted of a single sentence: "The jig has been lynched."[204] The e-mail print-out was sent to Bell's attorney by another Energetix employee, who found it commingled with papers she had printed off and removed from a shared printer "weeks or months" after Bell had been terminated;[205] she testified that she had not created or altered the e-mail, and she only vaguely knew Bell and his supervisors.[206] Bell argued that this e-mail, which contained obvious slurs against African-Americans, referred to him and his suspension, and was evidence that his termination was based on racial animus.[207]

Energetix moved to exclude the e-mail as unauthenticated and offered several reasons why the e-mail was inauthentic.[208] First, the supervisors all denied any involvement with the e-mail.[209] Energetix conducted an internal investigation and determined that there was no evidence on any of the supervisor's hard drives that they had ever received, sent, stored, or deleted the e-mail.[210] Energetix then retained an outside vendor to restore backup tapes and search for electronic copies of the e-mail; it was not found on any of the tapes, although it was possible that the e-mail could have still been sent and deleted without being captured on a tape.[211] Energetix retained a different outside vendor to examine the supervisors' hard drives again; nothing was found on two of the hard drives, but the third had been corrupted and could not be examined.[212] Finally, Energetix maintained that the e-mail did not resemble other e-mails that had been printed out, and it appeared to have been created in a word processor or other program.[213]

Bell argued that the e-mail could have been sent and overwritten between its noted sent date of May 21, 2002, and June 2, 2002, the date that Energetix ran the next back-up tape, but did not offer any expert opinion or other evidence to suggest that this was the case.[214] Bell also admitted that no electronic evidence of the e-mail had been located that could have been used to confirm its origin,[215] and that he personally did not know whether the e-mail had been forged.[216]

The Western District of New York excluded the e-mail from evidence, holding that Bell had failed to show that the e-mail had not been fabricated.

The court reasoned that Energetix had offered evidence that showed that the e-mail had been fabricated in its testimony about the work of its outside vendors,[217] and that it would have been impossible for the supervisor to have printed out the e-mail from his computer "weeks or months" after May 21, 2002, when the other employee discovered it on the printer, and still escape capture on the June 2, 2002 back-up tape.[218] On appeal, the Second Circuit found no abuse of discretion and affirmed the district court's exclusion of the e-mail "[g]iven, for example, the lack of evidence that the email was ever sent or received through Energetix's email system."[219]

Thus, unlike in *Brown*, there was no evidence that anything close to that e-mail had ever existed on Energetix's servers that would have indicated that the e-mail at issue was a forgery. And although the evidence in the record trends towards a finding that the e-mail was inauthentic, there was no hard evidence that would clearly exclude it as a forgery. Ironically, Energetix's argument that the court did not address — that the e-mail's format did not match any other known e-mail from Energetix's system, using a different font, spacing, and format than any other authenticated message — is easily the most persuasive argument in favor of a finding that the e-mail should have been excluded from evidence, as it negates Bell's sole authenticity argument, which was premised upon the distinctive characteristics of the e-mail.[220]

Authenticating Allegedly Forged E-mails: Making Sense of it All

The relevant cases present two distinct situations. On the one hand, e-mails with authenticity not in dispute can be authenticated by a myriad of methods, and the ways that this can be done are relatively well-settled and uncontroversial.[221] On the other hand, when an adversary has raised a specific, evidence-backed allegation of forgery, no consensus exists for how to proceed. Although the simple situations presented by *Chiu* and *Munshani* — where forensic evidence is not at play, and the court is faced with dueling affidavits or other testimony — make for a fairly straightforward analysis,[222] the fact patterns faced by the courts in *Downin*, *Bell*, and *Brown* created highly fact-specific opinions that are ultimately unhelpful for proscriptive purposes.[223] None of the courts attempted to undertake any systematic analysis of the various evidence presented in front of them, instead preferring to look generally at the factual gestalt before them.[224] But with parties increasingly engaging forensic experts in cases involving e-mail evidence, the lack of any coherent, systematic framework for analyzing proffered e-mails in light of that forensic data is troublesome, particularly given that the decisions that are available rely on divergent grounds.[225] Thus, in the next section of this article we suggest such a framework.

A SUGGESTED FRAMEWORK FOR ANALYZING EVIDENCE-BACKED ALLEGATIONS THAT A PROFFERED E-MAIL HAS BEEN FORGED

To date, no authority has provided a framework to assist a court in determining whether it has been presented with sufficient evidence to support a finding that an e-mail is authentic in the face of a specific, evidence-backed allegation that it has been forged. We now suggest a framework that provides for a systematic, efficient analysis of such evidence.

Step One: Has the proponent made a showing that the e-mail is reliable, such that it would be admissible in the absence of a challenge to its authenticity?

a. If yes, move on. The proponent can ultimately make this showing in any way the court deems acceptable, but previous courts have allowed e-mails to be authenticated by testimony, production by the opposing party, a showing that it is a business record, the presence of a trade inscription, reference to other previously-authenticated exemplars, and distinctive characteristics.[226]

b. If no, the e-mail should be *excluded*. The proponent has failed to carry his burden.[227]

Step Two: Has the objecting party raised a specific allegation of forgery?

a. If yes, move on.

b. If no, the e-mail should be *admitted*. Generalized challenges to the reliability of e-mail as a medium are insufficient.[228]

Step Three: Has the objecting party pointed to admissible evidence that supports his specific allegations of forgery?[229]

a. If yes, move on.

b. If no, the e-mail should be *admitted*. Specific challenges that are raised without evidentiary support or that rely on inadmissible evidence are insufficient.[230]

Step Four: If the objecting party was a party to the e-mail, has he testified that he did not send/receive the e-mail (as appropriate)? *If the objecting party was not a party to the e-mail, go to Step Five.*

a. If yes, move on.

b. If no, then the e-mail should be *admitted*.[231] If the objecting party was a party to the e-mail and declines to disavow the e-mail's authenticity, any other basis for challenging the e-mail is one that should be made to the jury.[232]

Step Five: If the proponent was a party to the e-mail, has he testified that he did send/receive the e-mail (as appropriate), and that he did not alter the e-mail in any way? *If the proponent was not a party, go to Step Six.*

a. If yes, move on. But ensure that the proponent's testimony sufficiently binds him to the e-mail; testimony that simply describes the e-mail's characteristics or simple header data could be truthfully made even if the proponent has personally spoofed the e-mail.[233]

b. If no, then the e-mail should be *excluded*. If allegations of forgery are present and the proponent declines to attest to the veracity of an e-mail of which he has personal knowledge after being given an opportunity to do so, the e-mail should be excluded.

Step Six: If the proponent was not a party to the e-mail, has he testified that he did not fabricate or alter the e-mail, and that he believes it to be a true and correct copy of what he purports it to be?

a. If yes, move on.

b. If no, the e-mail should be *excluded*. If allegations of forgery are present and the proponent declines to testify that he did not fabricate the e-mail after being given an opportunity to do so, the e-mail should be excluded.

Step Seven: If the e-mail was produced with full header data, does the full header data either match known e-mails or otherwise show a lack of tampering?

a. If yes, move on.

b. If no, the e-mail should be *excluded*. The e-mail has been spoofed.[234]

Step Eight: If an electronic copy of the e-mail exists on a server or personal computer, does the full header data match known e-mails or otherwise show a lack of tampering? *If no electronic copy exists, go to Step Nine.*

a. If yes, the e-mail should be *admitted*. Additionally, if neither party has custody of the original e-mail and the original cannot be obtained from the third party who does have it, the e-mail should be admitted.[235]

b. If no, the e-mail should be *excluded*. The e-mail has been fabricated.

Step Nine: If the e-mail does not exist on any server or computer, is it possible for the e-mail to have existed without being captured by a back-up tape or becoming otherwise viewable upon forensic review?

a. If yes, the e-mail should be *admitted*. There is no technical method to prove that the e-mail is forged, and the fact-finder should weigh the testimony of the parties to determine its authorship.[236]

b. If no, the e-mail should be *excluded*. The e-mail has been fabricated.[237]

This framework should suffice for the vast majority of cases. It prioritizes testimonial evidence as the first method of determining authenticity as a matter of efficiency. If a party is unwilling to testify that a proffered e-mail is authentic to the best of their knowledge, then their opponent should be able to exclude the e-mail on that basis without having to go to the expense of obtaining forensic review of the message and soliciting expert testimony. Likewise, if a party is unwilling to testify that they believe an e-mail that they are attacking is not authentic, any forensic evidence they procure will be offered in an attempt to disguise an attack on the general reliability of e-mails as a specific attack on the e-mail at issue. By prioritizing testimonial evidence, the parties can avoid retaining forensic experts to investigate spurious claims, and the courts can avoid the ridiculous — but likely — circumstance of reviewing forensic evidence that attacks the credibility of an e-mail when the proponent refuses to testify that they did not forge the very e-mail that they have offered into evidence. Of course, courts should be careful to ensure that testimonial evidence actually binds the witness to the e-mail; a clever affiant can avoid actually testifying to the genuineness of the e-mail by merely describing the characteristics of the e-mail.

In cases where both parties offer testimonial evidence, or where testimonial evidence is not available or practicable, forensic evidence is appropriate. But even then, it should be viewed logically; if the proponent can produce an electronic copy of the e-mail with the original header data, then that can allow the court to eliminate the vast majority of cases of e-mail forgery without requiring the objecting party to do a forensic review of its servers. It is only when the full header data is unavailable or shows no fraud that the forensic review of server data becomes relevant, thus placing the most expensive and time-consuming step at the end of the process.

Of course, the parties could also elect to circumvent this procedure by following the neutral expert protocol outlined in *Munshani*; in such cases, it is best for this to occur after both parties have sworn to the authenticity (or lack thereof) of the e-mail, as it ensures that the expert's time will be worthwhile. At any rate, this framework provides parties with a rational, cost-effective way to deal with allegations that an e-mail has been forged and provides courts with a way to sift through the evidence that they have been presented in a logical, systematic way. By using this framework, courts can exclude e-mails that are clearly fabricated while reserving any e-mail that is potentially legitimate for the fact-finder's review.

CONCLUSION

E-mails will continue to be the centerpiece of discovery for the foreseeable future. While attorneys and judges do not need to be able to write code, they should have a working knowledge of the security issues that impact the reliability of evidence that they routinely use. In this article, we addressed one such issue — the problem of forged e-mails — and explained why the basic standards used to authenticate unchallenged e-mails fail to provide courts with any guidance in situations where forgery. Existing decisions provide no systematic analysis of forgery claims. This article also presented a framework for the analysis of such a claim, prioritizing testimonial evidence as the first line of inquiry in an effort to save both litigants and courts the cost of forensic review in cases where it is ultimately unnecessary. By using this framework, courts and litigants can maximize efficiency while obtaining predictable, logical conclusions as to the authenticity of a given e-mail.

NOTES

[1] Email Statistics Report, 2010-2014, 2-3 (Sara Radacati ed., The Radicati Group, Inc. 2010), http://www.radicati.com/wp/wp-content/uploads/2010/04/Email-Statistics-Report-2010-2014-Executive-Summary2.pdf.
[2] *Id.* at 3.
[3] Adam I. Cohen and David J. Lender, Electronic Discovery: Law and Practice §6.02[D] (2000).
[4] *See id.*
[5] *See, e.g., U.S. v. Safavian*, 435 F. Supp. 2d 36, 40 (D. D.C. 2006); Fed. R. Evid. 901(b)(4).
[6] *See, e.g., Safavian*, 435 F. Supp. 2d at 41.
[7] *See infra*.
[8] *See generally Safavian*, 435 F. Supp. 2d at 41 (potential of forgery does not cut against the reliability of e-mail evidence in general).
[9] *See, e.g.*, *Brown v. Great-W. Healthcare*, No. 1:05-CV-2676 RWS-GGB,

2007 WL 4730651 (N.D. Ga. June 8, 2007) (considering allegations that proponent who had access to purported sender's e-mail account had forged proffered e-mail).

[10] *See, e.g.*, *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 554 (D. Md. 2007) (quoting Jack B. Weinstein & Margaret A. Berger, Weinstein's Federal Evidence § 900.07[3][c] (Joseph M. McLaughlin ed., Matthew Bender 2d ed. 1997)); *Commonwealth v. Amaral*, 78 Mass. App. Ct. 671, 676 (2011) ("It appears patently clear that in the computer age, one may set up a totally fictitious e-mail account, falsely using the names and photographs of "others.").

[11] As explained below, because e-mail is a generally insecure form of communication, obtaining a user's password in order to forge an e-mail from that user can actually be one of the more difficult methods of accomplishing that goal.

[12] *See* CERT, *Spoofed/Forged Email*, Sept. 4, 2002, http://www.cert.org/tech_tips/email_spoofing.html ("It is easy to spoof because STMP (Simple Mail Transfer Protocol) lacks authentication.").

[13] *See Griffin v. Md.*, 995 A.2d 791, 802 (Md. Ct. Spec. App. 2010) (citing *Indep. Newspapers, Inc. v. Brodie*, 966 A.2d 432 (Md. 2009) (anonymous communications on the Internet)).

[14] *Id.* at 803 (emphasis omitted).

[15] *See* Jonathan B. Postel, *RFC 821: Simple Mail Transfer Protocol*, Aug. 1982, http://www.faqs.org/rfcs/rfc821.html (original Request For Comments memorandum detailing SMTP).

[16] *Id.*

[17] *See* Dave Anderson, *E-mail Authentication. Then what?*, Cnet.com, March 22, 2005, http://news.cnet.com/E-mail-authentication.-Then-what/2010-1071_3-5629318.html.

[18] *See* Heinz Tschabitscher, *SMTP Inside Out — How Internet Email Works*, About.com, http://email.about.com/cs/standards/a/smtp.htm (last visited August 11, 2009) (the "EHLO" command requests that the SMTP server report back all additional features it supports, such as delivery status notification; the "HELO" command is the basic command accepted by all SMTP servers).

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] *See* Heinz Tschabitscher, *SMTP Inside Out — How Internet Email Works*

(cont.), About.com, http://email.about.com/cs/standards/a/smtp_2.htm (last visited August 11, 2009).

[23] *See id.*

[24] For example, popular e-mail clients such as Microsoft Outlook or Gmail hide these steps; the user simply has to type out the e-mail and press the "send" key in the client's graphical interface.

[25] *See* CERT, *supra* note 12.

[26] *See generally* CERT, *supra* note 12.

[27] *See* CERT, *supra* note 12. *See also Premiere Digital Access, Inc. v. Cent. Tel. Co.*, 360 F. Supp. 2d. 1161, 1163 (D. Nev. 2005) (defining "spoofing" as "the practice of forging e-mail header information to hide the source of the e-mail.").

[28] *See* Frank Dzedzy, *Email Address Spoofing*, Dec. 13, 2005, http://frankdzedzy.com/2005/12/13/email-address-spoofing/ (explaining how domain requirements can be spoofed.).

[29] *See id.*; *see* CERT, *supra* note 12.

[30] *See* Dzedzy, *supra* note 28; *see* CERT, *supra* note 12.

[31] In this article, we use "full header data" to describe the full set of information, contained in every e-mail, that provides information about the sending, transmission, and receipt of the e-mail. This information includes the e-mail addresses of the sender and recipient, IP addresses, and the names and addresses of the servers that the e-mail passed through. Most e-mail programs display a truncated form of this information, which we define *infra* as "simple header data," by default, and users have to actively seek out the full header data in most cases.

[32] "An IP address is a set of numbers…assigned to a computer in order for it to communicate on a network, which also includes communicating to the outside world; internet, web pages, e-mail as an example. An IP log is a log that many companies use to capture the source IP address of the network or computer that's connecting to the service…." *Passlogix, Inc. v. 2FA Tech., LLC*, 708 F. Supp. 2d 378, 386-387 (S.D.N.Y. 2010) (internal quotations and citations omitted). In layman's terms, the IP address can tell you the actual physical location of where the e-mail was sent from, and sometimes the exact computer it was sent from.

[33] *Lorentz v. Sunshine Health Prods., Inc.*, No. 09-61529-CIV, 2010 WL 1856265, at *1 (S.D. Fla. May 10, 2010) ("[I]f authenticity of particular emails is at issue, a request for production of metadata related to a particular

email is certainly possible. That is less intrusive than a full-fledged general rummaging through another party's computer systems." The court granted defendant's motion for a protective order to prevent plaintiff from obtaining access to its computers where plaintiff claimed she was "entitled to obtain discovery to verify the authenticity of certain emails and obtain access to emails on Defendants' computers that are believed to exist.").

[34] *Passlogix*, 708 F. Supp. 2d at 386 (party subpoenaed "Hushmail" e-mail service provider); *see also Beluga Shipping GMBH & Co. KS "Beluga Fantastic" v. Suzlon Energy Ltd. (In re Beluga Shipping)*, No. C 10-80034 JW (PVT), 2010 WL 3749279, at *1 (N.D. Cal. Sept. 23, 2010) [hereinafter *Beluga*] (party subpoenaed Google).

[35] *See, e.g.,* Heinz Tschabitscher, *How to View All Message Headers in Outlook*, About.com, http://email.about.com/cs/outlooktips/qt/et011302.htm (last visited August 11, 2009) (describing procedure for viewing full headers in several versions of Microsoft Outlook, which are normally hidden by default); *see* CERT, *supra* note 12 (describing forging IP addresses or connecting directly to the recipient's SMTP port as a method of evading detection).

[36] *See* CERT, *supra* note 12 ("In addition to connecting to the SMTP port of a site, a user can send spoofed email via other protocols (for instance, by modifying their web browser interface).").

[37] Deb Shinder, *Understanding E-mail Spoofing*, WindowSecurity.com, April 6, 2005, http://www.windowsecurity.com/articles/Email-Spoofing.html (explaining how crude spoofing works using e-mail clients to change account information).

[38] *Id.*

[39] *See* hoaxMail — Anonymous Spoof Email and SMS, http://www.hoaxmail.co.uk/ (last visited August 11, 2009); *see* Sharpmail.co.uk — Anonymous Email — Anonymous SMS, http://www.sharpmail.co.uk/ (last visited August 11, 2009).

[40] *See e.g.,* Shinder, *supra* note 37 (users can forge a replyto field in Microsoft Outlook by typing "anything you like in the field…that asks for your e-mail address.").

[41] For example, some spoofers send millions of e-mails to non-existent e-mail addresses with the targeted victim's e-mail address as the "reply-to" address. This results in the victim receiving millions of automated replies to their e-mail address, each notifying them that the e-mail address that the spoofer wrote to does not exist. *See* Brian McWilliams, *Time-Travel Spammer Fights*

Back, Wired, Nov. 1, 2003, http://www.wired.com/science/discoveries/news/2003/11/61026.

[42] *See, e.g.,* CERT, *supra* note 12 (recommending use of Pretty Good Privacy ("PGP") to thwart spoofing).

[43] *See* Steve Sheng et. al, *Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software* (2006), http://www.chariotsfire.com/pub/sheng-poster_abstract.pdf (research into use of PGP found that as of PGP 9, none of the novice users that participated in the research could figure out how to use PGP).

[44] For example, PGP is a method of e-mail encryption that relies on certificates and digital keys to ensure that other users are who they claim to be. *See generally* Network Associates, An Introduction to Cryptography (1999), http://www.pgpi.org/doc/pgpintro/ (developers' description of how PGP works). While this can be an effective way of preventing spammers and phishing scammers from reaching users' inboxes, methods like this can still be circumvented, particularly when users do not put in the effort to check each PGP key they receive. *See, e.g.,* Christopher Budd, *Microsoft Security E-mail Spoofs with Malware*, Oct. 13, 2008, http://blogs.technet.com/msrc/archive/2008/10/13/microsoft-security-e-mail-spoofs-with-malware.aspx (malicious hacker circulated spoofed e-mails with virus attached claiming to be latest Microsoft update; the e-mails circumvented PGP safeguards by spoofing the PGP key of a Microsoft employee).

[45] Although spoofed spam messages were banned by the CAN-SPAM Act of 2003, this technique is still being extensively used. *See*, *e.g.,* McAfee, Inc., June 2009 Spam Report: McAfee Avert Labs Discovers and Discusses Key Spam Trends 7-8 (2009), http://newsroom.mcafee.com/images/10039/rpt_spam_0509_002.pdf. Indeed, the FTC's 2005 report to Congress on the effectiveness of the CAN-SPAM Act noted that the FTC did not "believe that CAN-SPAM's effectiveness can be determined by measuring changes in the amount of types of spam since the Act's passage because numerous variables, such as changes in anti-spam technologies and spammers' tactics, are predominantly responsible for such changes." Federal Trade Commission, Effectiveness and Enforcement of the CAN-SPAM Act: A Report to Congress A-7 (2005), http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf. Put simply, spoofers and spammers can innovate faster than Congress can act.

[46] *See* Stuart McClure et. al., Hacking Exposed: Network Security

Secrets and Solutions 623 (5th ed. 2005).

[47] U.S. Department of Justice, *Kevin Mitnick Sentenced to Nearly Four Years in Prison; Computer Hacker Ordered to Pay Restitution to Victim Companies Whose Systems Were Compromised*, Aug. 9, 1999, http://www.usdoj.gov/criminal/cybercrime/mitnick.htm.

[48] *See* Kevin Mitnick and William Simon, The Art of Deception: Controlling the Human Element of Security (2002) (Mitnick's account of hacking career and description of how social engineering works).

[49] *See, e.g., id.* at 199 (social engineers pose as important people when obtaining information from low-level employees because "the natural instinct of wanting to be helpful is multiplied when you think that the person you're helping is important or influential."); *see also* Rachna Dhamija, J.D. Tygar, and Marti Hearst, *Why Phishing Works*, Experimental Social Science Laboratory Paper XL06-013, Aug. 14, 2006, http://repositories.cdlib.org/iber/xlab/XL06-013/ (describing phishing attacks and reasons why victims fall for them, including victims being trusting and lacking computer knowledge).

[50] As an example, see the discussion of the Francis Boyle Joe Job, *infra*.

[51] *See* McClure, *supra* note 46, at 634.

[52] *See id*. at 589-90.

[53] *Id.*

[54] *See id.*

[55] *See generally id*. at 589-90, 634.

[56] Andrew Stein, *Microsoft offers MyDoom reward*, CNNMoney.com, Jan. 30, 2004, http://money.cnn.com/2004/01/28/technology/mydoom_costs/index.htm.

[57] David Becker, *MyDoom virus declared worst ever*, ZDNet.com, Jan. 29, 2004, http://news.zdnet.com/2100-1009_22-134051.html.

[58] *See* McClure, *supra* note 46, at 623.

[59] *See id.* at 626.

[60] *Id.* at 624.

[61] *Id.*

[62] *Id.* at 624-625.

[63] McClure, *supra* note 46, at 625-626.

[64] *Id.* at 625.

[65] *See id.* at 624-626.

[66] *See id.* at 626.

[67] *38 arrested in international phishing scam*, N.Y. Times, May 19, 2008,

http://www.nytimes.com/2008/05/19/technology/19iht-webphish.13021360.html; Stephen J. Dubner, *Phun Phatcs About Phishing (and Spam)*, N.Y. Times Freakonomics Blog, July 7, 2006, http://freakonomics.blogs.nytimes.com/2006/07/07/phun-phacts-about-phishing-and-spam/; Citibank, *E-mail Fraud & Security — Learn About Spoofs*, http://www.citi.com/domain/spoof/learn.htm (last accessed August 11, 2009).

[68] Dubner, *supra* note 67; Wells Fargo, *Privacy and Security — Report Fraudulent Emails and Websites*, https://www.wellsfargo.com/privacy_security/fraud/report/fraud (last accessed August 11, 2009).

[69] Jenna Wortham, *Fast-Spreading Phishing Scam Hits Gmail Users*, N.Y. Times Bits Blog, Feb. 24, 2009, http://bits.blogs.nytimes.com/2009/02/24/viddyho-phishing-scam-hits-gmail/?hp&apage=2.

[70] Tom Anderson, *protect yourself from phishing!*, Tom Anderson's MySpace Blog, Feb. 6, 2008, http://blogs.myspace.com/index.cfm?fuseaction=blog.view&friendID=6221&blogID=355522809 (MySpace's founder discussing phishing attacks against the site).

[71] *See* Dillian Thomas, *Sabotage! Coping with the Joe Job*, Feb. 4, 2004, http://www.sitepoint.com/article/sabotage-coping-joe-job; *see also* Brian McWilliams, *Time-Travel Spammer Fights Back*, Wired, Nov. 1, 2003, http://www.wired.com/science/discoveries/news/2003/11/61026; *see also* Chris Gaither, *Can Spam Be Canned?*, L.A. Times, May 23, 2004, http://articles.latimes.com/2004/may/23/business/fi-spam23?pg=4.

[72] *Id.*

[73] Thomas, *supra* note 71; Joe Doll, *Spam Attack!*, Jan. 3, 1997, http://www.joes.com/spammed.html.

[74] Doll, *supra* note 73.

[75] *Id.*

[76] *Id.*

[77] *Id.*; Thomas, *supra* note 71.

[78] Thomas, *supra* note 71.

[79] *Id.*

[80] Noah Shachtman, *Return to Sender — 55,000 Times*, Wired, Aug. 23, 2002, http://www.wired.com/culture/lifestyle/news/2002/08/54708.

[81] *Id.*

[82] *Id.*

[83] *See Lorraine,* 241 F.R.D. at 541-542; Cohen and Lender, *supra* note 3, at §6.01.

[84] *See Lorraine*, 214 F.R.D. at 538; Fed. R. Evid. 901(a).

[85] *U.S. E.E.O.C. v. Olsten Staffing Servs. Corp.*, 657 F. Supp. 2d 1029, 1034 (W.D. Wis. 2009).

[86] *See Lorraine*, 214 F.R.D. at 542; *Safavian*, 435 F. Supp. 2d at 41; Paul Grimm et al., *Back to the Future: Lorraine v. Markel American Insurance Co. and New Findings on the Admissibility of Electronically Stored Information*, 42 Akron L. Rev. 357, 365-366 (2009).

[87] *See Lorraine*, 214 F.R.D. at 544.

[88] *See id*. at 542.

[89] 235 F.3d 1318 (11th Cir. 2000).

[90] *Id.* at 1320.

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] *Siddiqui*, 235 F.3d at 1320, 1325.

[95] *Id.* at 1321.

[96] *Id.*

[97] *Id.* at 1320-1322.

[98] *Id.* at 1322.

[99] *Siddiqui*, 235 F.3d at 1322-1323.

[100] *Id.*

[101] *Id.* at 1322.

[102] 435 F. Supp. 2d 36.

[103] *See id.* at 39.

[104] *Id.*

[105] *Id.* at 40.

[106] *Id.*

[107] *Safavian*, 435 F.Supp.2d at 40.

[108] *Id.*

[109] *See id.* at 41.

[110] *Id.*

[111] *Id.*

[112] 241 F.R.D. 534.

[113] *See id.*; *see* Lindsay J. Kemp, Recent Development, *Lorraine v. Markel: An Authoritative Opinion Sets the Bar for Admissibility of Electronic Evidence (Except for Computer Animations and Simulations),* 9 NC JOLT Online Ed. 16 (2007), http://cite.ncjolt.org/9NCJOLTOnlineEd16.

[114] *See* 241 F.R.D. at 554-555.
[115] *Id.* at 534-535.
[116] *Id.* at 537.
[117] *See id.* at 534.
[118] *Id.* at 537.
[119] *See Lorraine*, 241 F.R.D. at 554.
[120] *See generally id.* at 554-555.
[121] *Id.* at 554.
[122] *See id.*
[123] *Id.*
[124] *Lorraine*, 241 F.R.D. at 554. As discussed, this statement — also made by the court in *Siddiqui* — is factually incorrect.
[125] *Id.*
[126] *Id.*
[127] *Id.* at 555 (citing *In re F.P.*, 878 A.2d 91, 94 (Pa. Super. Ct. 2005).
[128] *Id.* at 554-55 (citing *Rambus, Inc. v. Infineon Techs. AG*, 348 F. Supp. 2d 698 (E.D. Va. 2004)).
[129] *See, e.g., Lorraine*, 241 F.R.D. at 554-555; *In re Second Chance Body Armour, Inc.*, 434 B.R. 502, 505 n.1 (Bankr. W.D. Mich. 2010) (citing Mark D. Robins, *Evidence at the Electronic Frontier: Introducing E-mail at Trial in Commercial Litigation*, 29 Rutgers Computer & Tech. L.J. 219, 226, 227-28 (2003)).
[130] *See Lorraine*, 241 F.R.D. at 545; *U.S. v. Gagliardi*, 506 F.3d 140, 151 (2d Cir. 2007) (e-mails and instant-message chats were authenticated by the testimony of conversation participants); *In re Second Chance Body Armour*, 434 B.R. at 505 (court rescinded provisional admission of e-mail exhibit because the e-mail was "a purely internal communication" between non-parties, witness was not listed as e-mail recipient; witness testified that he had never seen the document before; and witness was not in attendance at the meeting described in the communication); *Olsten Staffing Servs. Corp.*, 657 F. Supp. 2d at 1034 ("Testimony from someone who personally retrieved the e-mail from the computer to which the e-mail was allegedly sent is sufficient.") (citing *U.S. v. Hampton*, 464 F.3d 687, 690 (7th Cir. 2006) (custodian of record may authenticate)); *Commonwealth v. Purdy*, 923 N.E. 2d 122 (Mass. App. Ct. 2010) (unpublished) (computer forensics expert testified at trial that he seized computer from defendant's business, defendant "admitted control over the computer and provided all necessary passwords from memory," e-mails

"originated from or were addressed to the defendant's e-mail address," and "all e-mails contained either the defendant's name or business address"); *but see Ashley v. Commonwealth*, Nos. 2008-CA-000089-MR, 2008-CA-000327-MR, 2009 WL 3785848, *2-3 (Ky. Ct. App. Nov. 13, 2009) (unpublished) (no abuse of discretion where court refused to allow a minor victim to testify that she received *anonymous* e-mails from criminal defendant and that he acknowledged to her that he sent them because of the "unique opportunities that emails present for fabrication" (emphasis added)); *cf. U.S. v. Barlow*, 568 F.3d 215, 220 (5th Cir. 2009) (chat log authenticated by a chat participant's testimony since she had direct knowledge of the chats); *cf. Irish v. Burghuis*, No. 1:08-CV-142, 2010 WL 2757119, at *5 (W.D. Mich. June 8, 2010) (e-mail not authenticated because petitioner failed to prove that e-mail was authored by victim and that victim ever used or maintained the e-mail account from which the correspondence was sent); *U.S. v. Lane*, No. 07-CR-00835-H, 2009 WL 2366431, at *4 (S.D. Cal. July 27, 2009) (computer forensic examiner who examined co-conspirator's computer and testified at co-conspirator's trial will testify at defendant's trial).

[131] *Brunskill v. Kansas City S. Ry. Co.*, No. 06-00205-CV-W-REL, 2008 WL 413281, at *17 (W.D. Mo. Feb. 12, 2008); *see also McIntosh v. Partridge*, 540 F.3d 315, 322 (5th Cir. 2008) (e-mails properly authenticated because the proponent attached affidavits authenticating the e-mails in its reply brief in support of summary judgment); *Madison One Holdings, LLC v. Punch Int'l, NV*, No. 4:06-cv-3560, 2009 WL 911984, at *11 (S.D. Tex. Mar. 31, 2009) (e-mails were authenticated by declaration of the e-mail's recipient and attachments to the e-mail were similarly authenticated); *Pfeffer v. Hilton Grand Vacations Co., LLC*, No. CV. 07-00492 DAE-BAK, 2009 WL 37519, at *7 (D. Hawaii Jan. 7, 2009) (e-mails can be properly authenticated by plaintiff's declaration); *Whatley v. S.C. Dep't of Pub. Safety*, No. 3:05-0042-JFA-JRM, 2007 WL 120848, at *13-15 (D.S.C. Jan. 10, 2007) (e-mails were not authenticated because neither plaintiff nor any of the communicants had authenticated the e-mails by affidavit, nor had the plaintiff provided any other authentication); *Malone v. Becher*, No. NA 01-101-C, 2003 WL 22080737, at *2 (S.D. Ind. Aug. 29, 2003) (defendant's objection to e-mail exhibits sustained because plaintiff did not provide an affidavit or other document authenticating the e-mail exhibits); *Cantu v. Vitol, Inc.*, No. H-09-0576, 2011 WL 486289, at *5-6 (S.D. Tex. Feb. 7, 2011) (e-mails authenticated where party's human resources director testified in sworn affidavit that he collected

e-mails from its system); *In re Ockerlund*, No. 10 C 5738, 2011 WL 249456, at *3 (N.D. Ill. Jan. 25, 2011) (citing Fed. R. Evid. 901(b)(1)) ("The [appellant's] *affidavit authenticated the…e-mails*, which otherwise would not have been admissible as evidence because [the appellee] did not submit [the e-mails] with an affidavit.").

[132] *Brunskill*, 2008 WL 413281, at *17; *Read v. Teton Springs Golf & Casting Club, LLC*, No. 08-CV-00099, 2010 WL 5158882 (D. Idaho Dec. 14, 2010) (numerous e-mail exhibits authenticated by deposition).

[133] *Amaral*, 78 Mass. App. Ct. at 674-75 (defendant appeared at certain place and time that he indicated in his e-mails, answered the telephone number that he provided in e-mails; and was same person as photograph he e-mailed); *Lane*, 2009 WL 2366431, at *5 (e-mails authenticated where, *inter alia*, defendant "admitted to agents during the interviews that he had emailed [co-conspirator], including emails containing photographs of [the victim] and hotel information," "[h]otel information and photographs were found in emails from [co-conspirator to government informant]on [co-conspirator]'s computer," and co-conspirator "states in a telephone call with [informant] that he had emailed a picture" of victim to informant").

[134] *Hernandez v. Wal-Mart P.R., Inc.*, No. 09-1379 (GAG), 2010 WL 4273927, at *3 (D.P.R. Oct. 29, 2010) (e-mail authenticated by answers to interrogatories).

[135] *See Sklar v. Clough*, No. 1:06-CV-0627-JOF, 2007 WL 2049698, at *4-5 (N.D. Ga. July 6, 2007); *see also Phillip M. Adams & Assocs., L.L.C. v. Dell, Inc.*, 621 F. Supp. 2d 1173, 1183 (D. Utah 2009) (e-mails authenticated against all defendants when one co-defendant authenticated them by producing them); *see also Kasten v. Saint-Gobain Performance Plastics Corp.*, 556 F. Supp. 2d 941, 948 (W.D. Wisc. 2008) (defendant's challenge to the authenticity of e-mails that defendant produced was somewhat disingenuous); *Dominion Nutrition, Inc. v. Cesca*, No. 04 C 4902, 2006 WL 560580, at *5 (N.D. Ill. Mar. 2, 2006) ("documents produced by an opponent may be treated as authentic"); *contra Complete Conference Coordinators, Inc. v. Kumon N. Am., Inc.*, 915 N.E. 2d 88, 108-109 (Ill. App. Ct. 2009) (Illinois Court of Appeals refused to create rule validating authentication by production absent any Illinois authority but recognized that other jurisdictions (Tex. R. Civ. 193.7) and the federal courts allow authentication of emails when the documents were produced in discovery.); *see Clark v. Cnty. of Tulare*, --- F. Supp. 2d ---, 2010 WL 4791683, at *3-5 (E.D. Cal. Nov. 17, 2010) (An attorney's declaration

that the e-mails were produced in discovery was insufficient to establish the authenticity of the e-mails for summary judgment purposes.).

[136] *See, e.g., Lorraine*, 241 F.R.D. at 554-555 (citing *Rambus*, 349 F. Supp. 2d 698); *Amaral*, 78 Mass. App. Ct. at 673-674 (Commonwealth introduced an account management tool provided by Yahoo indicating that the login name was registered to defendant and an affidavit from Yahoo's custodian of records to authenticate e-mail as a business record).

[137] *See, e.g., Lorraine*, 241 F.R.D. at 555; *cf. Purdy*, 923 N.E.2d 122 (e-mails authenticated where, *inter alia*, "all e-mails contained either the defendant's name or business address" and were retrieved from computer seized from defendant's business); *cf. Amerisource Corp. v. Rx USA Int'l Inc.*, No. 02-CV-2514 (JMA), 2010 WL 2730748, at *2-3 (E.D.N.Y. July 6, 2010) (court sanctioned defendant and its nonparty principal for fabricating e-mails where, *inter alia*, e-mails contained defendant's fax header, insignia which indicated that the e-mails were printed from a computer on defendant's network, and a stamp from computer scanning software used by defendant).

[138] *See, e.g., Safavian*, 435 F. Supp. 2d 36 at 40.

[139] *See* Fed. R. Evid. 901(b)(4); *See, e.g., Siddiqui,* 235 F.3d at 1322-1323; *Cantu*, 2011 WL 486289, at *5-6 (cursory application of *Siddiqqi*; "The emails have the distinctive characteristics of emails."); *Gary v. Combined Grp. Ins. Servs., Inc.*, No. 3:08-CV-228-L, 2009 WL 2868485, at *6 (N.D. Tex. Sept. 4, 2009) (because e-mails have distinctive email characteristics coupled with affidavit by plaintiff that she wrote and sent the emails; exhibits met threshold for authentication for summary judgment purposes); *Hardin v. Belmont Textile Mach. Co.*, No. 3:05-CV-492-M, 2010 WL 2293406, at *5-6 (W.D.N.C. June 7, 2010) (citing *Safavian*, 435 F. Supp. 2d at 40) (court denies plaintiff's motion to strike e-mail exhibits finding that e-mails were authenticated because of distinctive characteristics such as familiar Microsoft Outlook format, name of the person connected to the address, a signature at bottom from "Bill," and "Hardin, Bill" appears in the "From" row); *Ashley*, 2009 WL 3785848, *2-4 (unauthenticated *anonymous* e-mails allegedly sent by criminal defendant were properly excluded because they lacked "distinctive indicia of authorship, such as the use of [defendant's] nickname or information known solely by [defendant]," and sender of the e-mails was "not apparent from the face of the emails"); *Lane*, 2009 WL 2366431, at *5 (citing Fed. R. Evid. 901(b)(4)) (e-mails authenticated where, *inter alia*, co-conspirator's e-mail address was listed as "having subscriber information identifying [co-conspirator] with an

address and telephone number that match the address and telephone number listed on [co-conspirator's] business website," "business website contains an 'Email' button allowing visitors to email [co-conspirator]," and Web site lists "the email address which matches the email address found on the emails obtained by the Government"); *Sánchez-Medina v. Unicco Serv. Co.*, No. 07-1880 (DRD), 2010 WL 3955780, at *5 (D.P.R. Sept. 30, 2010) (citation omitted) (E-mails can be authenticated by their "authorship," "additional data such as the address of the original sender," "the content of the information included in the e-mail," that they were sent and received from the relevant e-mail system; however, the court did not consider the e-mails on summary judgment because they lacked a "complete history of the conversations," "four pages of electronic messages," a mention that "the documents attached were sent to or received by" certain persons, and the origin of the attachments was undetermined.); *see generally Shah v. Eclipsys Corp.*, No. 08-CV-2528 (JFB) (WDW), 2010 WL 2710618, *14 (E.D.N.Y. July 7, 2010) (authenticity of e-mail questioned where, *inter alia,* e-mail lacked a colon after "To" and differed in appearance from other e-mails).

[140] *Reynolds v. Family Dollar Servs., Inc.*, No. 09-56-DLB, 2011 WL 618966, at *4-5 (E.D. Ky. Feb. 10, 2011) (court excluded anonymous e-mail because, *inter alia*, the "timing of the e-mail makes its authentication somewhat suspicious" and the exact duplication of two sentences "leads the Court to conclude that it may not be authentic"); *cf. Amerisource Corp.*, 2010 WL 2730748, at *3 (court sanctioned defendant and its nonparty principal for fabricating emails where, *inter alia*, principal verified both fake and real emails as authentic but agreed that it was "impossible for the same email account to send two different emails to the same address at the same time").

[141] *Fisher v. Vizioncore, Inc.*, No. 09 C 6853, 2010 WL 4932612, at *1 (N.D. Ill. Nov. 30, 2010) (although pro se litigant's email exhibits attached to motion for summary judgment response were not properly authenticated, court held that they have "*sufficient indicia of reliability*" "for consideration to the extent they are relevant" because of the proponent's pro se status. (emphasis added)); *Green Ventures Int'l, LLC v. Guttridge*, No. 2:10-CV-01709-MBS, 2010 WL 5019363, at *4, n.4, *11 (D.S.C. Dec. 1, 2010) (Defendants contested the authenticity of e-mail exhibits attached to plaintiff's amended complaint because plaintiffs stated that "[t]he content of the various Exhibits represents a limited selection of relevant e-mails and other material, and is not intended to represent or constitute all or necessarily an exact duplication of the form

of the material as originally communicated; " however, the court reviewed the e-mail exhibits in their entirety and concluded that they have "*significant indicia of trustworthiness*" although it ultimately granted defendants' motion to dismiss plaintiff's amended complaint. (emphasis added)); *Reynolds*, 2011 WL 618966, at *5 (court excluded anonymous e-mail because, *inter alia*, it lacked "sufficient indicia of trustworthiness to allow its admission at trial").

[142] *See, e.g., Safavian*, 435 F. Supp. 2d at 40; *see also Olsten Staffing Servs. Corp.*, 657 F. Supp. 2d at 1034 ("even without a custodian, e-mails may be authenticated through the e-mail addresses in the headers and other circumstantial evidence, such as the location where the e-mail was found.") (citing *U.S. v. Vaghari*, No. 08-693-01-02, 2009 WL 2245097, *8-9 (E.D. Pa. July 27, 2009); *Safavian*, 435 F. Supp. 2d at 39-42)); *cf. Purdy*, 923 N.E.2d 122 (e-mails authenticated where, *inter alia*, they "originated from or were addressed to the defendant's e-mail address"); *see generally Shah*, 2010 WL 2710618, at *13 (authenticity of e-mail questioned where e-mail lacked a colon after "To"); *see generally In re White*, Nos. 09-BG-1012 & 10-BG-795, 2011 WL 166079, at *44 (D.C. Jan. 20, 2011) (unpublished) (attorney disbarred where court found, *inter alia*, that attorney falsified e-mails noting that transmittal time on e-mail was inconsistent with facts, there were commas instead of semicolons between addresses on the "cc" line, and incorrect addresses on "to" line would have generated a notice of returned e-mail "within milliseconds of the transmission").

[143] *See* Heinz Tschabitscher, *What Email Headers Can Tell You About the Origin of Spam*, About.com, http://email.about.com/cs/spamgeneral/a/spam_headers.htm (last visited August 12, 2009).

[144] *See id.*

[145] *See, e.g., Lorraine*, 241 F.R.D. at 554-555.

[146] *See generally* Bozidar Spirovski, *Tools for Detecting Spoofed Email Headers*, July 20, 2009, http://information-security-resources.com/2009/07/20/tools-for-detecting-spoofed-email-headers/ (describing "from" information as "very easily forged" and advising to "NEVER trust that information"). Simple headers can be forged so that they both appear to be from a different source and so that a party that attempts to respond to the e-mail will be directed to a different source than the forger's true e-mail address.

[147] *See generally* Spirovski. *Id.*

[148] *See, e.g.*, *Amerisource Corp.*, 2010 WL 2730748, at *2.

[149] This was the required showing in *Siddiqui*. *See* 235 F.3d at 1322.

[150] *See, e.g., Safavian*, 435 F. Supp. 2d at 41.

[151] Many cases involving specific assertions of forgery fail to rise to more than bare assertion. *See, e.g., Monte v. Ernst & Young LLP*, 330 F. Supp. 2d 350, 358 n.2 (S.D.N.Y. 2004) (plaintiff's allegations of forgery failed where plaintiff offered no evidence to support a finding that the defendant had fabricated or altered the e-mails in question), *aff'd*, 148 F. App'x 43 (2d Cir. 2005); *see also Massimo v. State*, 144 S.W.3d 210, 216-217 (Tex. App.–Fort Worth 2004, no pet.) (although defendant argued that someone was impersonating her and sending threatening e-mails on her behalf, she could not point to any evidence to support that assertion, and the e-mails were thus admissible).

[152] *See supra*.

[153] *See Telewizja Polska USA, Inc. v. Echostar Satellite Corp*, No. 02 C 3293, 2004 WL 2367740, at *7 (N.D. Ill. Oct. 15, 2004) (redacted e-mail excluded when only evidence in support was testimony from president of plaintiff company that the e-mail address on the proffered e-mail was his; president testified that he did not remember sending nor recognize the e-mail, and the recipient was unknown); *see also Hollie v. State*, 679 S.E.2d 47, 50 (Ga. Ct. App. 2009) (e-mail excluded for failure to make *prima facie* showing when only evidence offered in support was testimony from alleged sender that her e-mail address was the one on the proffered e-mail; sender claimed to have never seen nor sent proffered e-mail before, and recipient was not asked about e-mail when she testified), *aff'd*, 696 S.E.2d 642 (Ga. 2010). The proponents in *Telewizja Polska USA, Inc.* and *Hollie* failed to make any showing beyond the sender's e-mail address; despite the low standard of the "distinctive characteristics" test, this single fact is insufficient to make a showing of authenticity even if the e-mails' authenticity had not been challenged. *See also Hood-O'Hara v. Wills*, 873 A.2d 757 (Pa. 2005) (likely also under this description, but the opinion is silent as to what showing the proponent initially made).

[154] 260 F.3d 330 (5th Cir. 2001).

[155] *See id.* at 336-338.

[156] *Id.*

[157] *Id.* at 338, n.2.

[158] *Id.* at 351, 353.

[159] *Id.* at 338, n.2.

[160] 805 N.E.2d 998 (Mass. App. Ct. 2004).

[161] *Id.* at 1000.

[162] *Id.*
[163] *Id*. at 1000-1001.
[164] *Id.* at 1001.
[165] *Id.*
[166] *Id.*
[167] *Munshani*, 805 N.E.2d at 1001.
[168] *Id.*
[169] *Id.*; *see also Amerisource Corp.*, 2010 WL 2730748, at *1, *3, *7-8 (court sanctioned defendant and its nonparty principal jointly and severally in the amount of $50,000 payable to plaintiff and $50,000 payable to court clerk where court found that nonparty principal created and defendants intentionally repeatedly relied on fabricated e-mails in bad faith; defendants falsely testified to the authenticity of the altered e-mails numerous times).
[170] *Munshani*, 805 N.E.2d at 1002.
[171] 828 N.E.2d 341 (Ill. App. Ct. 2005).
[172] *Id.* at 346.
[173] *Id.* at 346-347.
[174] *Id.* at 347.
[175] *Id.* at 351.
[176] *Downin*, 828 N.E.2d at 351.
[177] *Id.*
[178] *See id.* at 346, 351.
[179] Additionally, there was no showing that the original, electronic copy of the e-mail was unavailable (and thus the IP addresses could not have been authenticated), nor was there any further analysis of the expert's testimony that the e-mail was sent from Downin's e-mail account "through" a different domain. It is unclear from the opinion whether this means that the victim's e-mail account was registered at the hotmail.com domain, or if this was evidence that the victim had forged the e-mail by changing the header information. At any rate, it appears that this was simply not explored.
[180] *See generally Downin*, 828 N.E.2d 341.
[181] *See generally id.* Although the opinion states that Downin "challenged the genuineness of the documents" after they were admitted, it is silent as to whether he did so before they were authenticated. *See id.* at 351.
[182] In practice, a purported author of an e-mail who fails to offer testimony disavowing authorship of the e-mail is not truly making a claim that the e-mail was forged. Instead, they are attempting to present evidence of the fact that

e-mails *can* be forged as evidence that a particular e-mail *has* been forged. If the purported author of an e-mail attempts to enter forensic evidence attacking the e-mail, but will not actually testify that they did not send the e-mail, the forensic evidence is really only attacking e-mails in general, not that specific e-mail.

[183] *Downin*, 828 N.E.2d at 346.

[184] The opinion is silent as to whether Downin testified, but given the court's recital of the others witnesses' testimony, it seems very unlikely that Downin testified and the court found it unnecessary to note that fact. *See generally id.*

[185] 2007 WL 4730651, at *1.

[186] *Id.*

[187] *Id.*

[188] *Id.*

[189] *Id.*

[190] *Brown*, 2007 WL 4730651, at *2.

[191] *Id.*

[192] *Id.*

[193] *Id.* at *1.

[194] Defendants' Memorandum of Law in Support of Their Motion to Exclude Purported E-mails From Consideration on Summary Judgment at 8-15, *Brown*, 2007 WL 4730651.

[195] Memorandum in Response to Defendant Great-West's Motion to Exclude Purported E-mails from Consideration on Summary Judgment at 5-8, *Brown*, 2007 WL 4730651.

[196] Defendants' Reply Brief in Support of Their Motion to Exclude Purported E-mails from Consideration on Summary Judgment at 4-5, *Brown*, 2007 WL 4730651.

[197] *Brown*, 2007 WL 4730651, at *4.

[198] *Id.*

[199] *See generally* Memorandum in Response to Defendant Great-West's Motion to Exclude Purported E-mails from Consideration on Summary Judgment at 5-8, *Brown*, 2007 WL 4730651.

[200] *See* 540 F. Supp. 2d 421 (W.D.N.Y. 2008), *aff'd in part and rev'd in part*, 329 F. App'x 304 (2d Cir. 2009) ("*Bell Appeal*").

[201] *Bell*, 540 F. Supp. 2d at 423-425.

[202] *See id.* at 428-430.

[203] *Id.* at 428-431.

[204] *Id.* at 429.
[205] *Bell*, 540 F. Supp. 2d at 428-429.
[206] *See* DeJesus Dep. 10:12-14:12, 34:5-35:6, 68:7-20, Oct. 10, 2006, *Bell*, 540 F. Supp 421; *see also* Plaintiff's Memorandum of Law in Opposition to Motion for Summary Judgment at 5, 7, *Bell*, 540 F. Supp. 2d 421 (citing Thomas Aff., Ex. C (DeJesus Dep. excerpts)).
[207] *See Bell*, 540 F. Supp. 2d at 429-430.
[208] *See* Defendants' Memorandum of Law at 13-15, *Bell*, 540 F. Supp. 2d 421.
[209] *Id.; Bell*, 540 F. Supp. 2d at 429.
[210] Defendants' Memorandum of Law at 14, *Bell*, 540 F. Supp. 2d at 429.
[211] Defendants' Memorandum of Law at 14, *Bell*, 540 F. Supp. 2d at 421, 429-430.
[212] Defendants' Memorandum of Law at 14-15, *Bell*, 540 F. Supp. 2d at 421, 429-430.
[213] Reply Memorandum of Law in Support of Motion for Summary Judgment at 11-12, *Bell*, 540 F. Supp. 2d 421.
[214] *Bell*, 540 F. Supp. 2d at 430.
[215] *Id.*
[216] *See* Statement of Facts Not In Dispute at 17, *Bell*, 540 F. Supp. 2d 421 ("Mr. Bell does not know if the alleged May 21, 2002 e-mail was a forgery.").
[217] *Bell*, 540 F. Supp. 2d at 430.
[218] *Id.*
[219] *Bell Appeal*, 329 F. App'x at 306.
[220] *See* Reply Memorandum of Law in Support of Motion for Summary Judgment at 11-12, *Bell*, 540 F. Supp. 2d 421.
[221] *See supra*.
[222] *See supra*.
[223] *See supra*.
[224] *See supra*.
[225] *See supra*.
[226] *See supra*.
[227] *See generally* note 139, *supra*. Note that this is where *Bell* should have ended; the fact that Bell's proffered e-mail did not even contain the same font or format as the truly authentic, uncontested e-mails should have precluded any further analysis. *See* Reply Memorandum of Law in Support of Motion for Summary Judgment at 11-12, *Bell*, 540 F. Supp. 2d 421.
[228] *See*, *e.g.*, *Safavian*, 435 F. Supp. 2d at 41.

[229] *See* note 138, *supra*.

[230] *See* note 128, *supra*; *see also* Grimm et al., *supra* note 86, at 365-366 (because authenticity in this context is ultimately a matter of conditional relevance, evidence offered to show an e-mail's authenticity — or lack thereof — must itself be admissible) .

[231] This should be the general rule in cases where Fifth Amendment waiver concerns are not an issue. Where this framework would require a criminal defendant to testify — and the defendant has not otherwise elected to testify so as to make the issue moot — we suggest that the court skip this step and proceed as if the defendant *had* so testified. As the prosecutor already shoulders the burden of avoiding the use of perjured testimony, allowing a criminal defendant's objection to be raised without the necessity of testimony should not result in any significant changes in procedure or trial efficiency. For a discussion of the prosecutor's duties here, *see, e.g., U.S. v. Creek Nation*, 295 U.S. 103 (1935) and *Giglio v. U.S.*, 405 U.S. 150 (1972).

[232] Note that this is where *Downin*'s analysis should have ended if it were a civil case, or if Downin had already testified so as to make Fifth Amendment waiver issues irrelevant. *See supra*.

[233] Failing to require such binding testimony could give rise to a situation similar to that in *Munshani* — except that the spoofer would have the benefit of being able to point to a truthfully-executed affidavit. This could allow a clever litigant to delay matters for months as a matter of litigation strategy while simultaneously avoiding the sanctions that were leveled against Munshani in that case.

[234] This allows the court to exclude the vast majority of forgeries. Comparing the full header data to that of known e-mails will let the court see if the e-mail addresses in the full header match those in the simple header, and determine if the server names that the e-mail passed through match the server names used in known exemplars. This can be done by the court, or by anyone with basic computer knowledge; extensive work by a forensic expert is unnecessary at this stage.

[235] A party may subpoena an e-mail service provider for information regarding the identity of specific e-mails; and if the e-mail account holder consents, as required by the ECPA, to allow the e-mail service provider, like Yahoo or Google, to release the content of an e-mail account, then this data can be examined and compared to the proffered e-mail for evidence of tampering. *See Beluga*, 2010 WL 3749279, at *3.

[236] As stated *supra*, *Bell*'s analysis should have ended after a simple comparison of the proffered e-mail and the known exemplars, which demonstrated that the proffered e-mail was forged. Were that not the case, *Bell* was arguably decided incorrectly and the e-mail should have been admitted into evidence; although it may have been unlikely that the e-mail was genuine, there was no way to preclude a finding that it was, and it should have been left to the jury to decide. *See supra*.

[237] This step represents where the court in *Brown* eventually ended up, demonstrating that the framework we have offered here can substantially cut down on the amount of work parties and courts need to do in order to address forgery allegations. *See supra*.