NEW YORK LAW SCHOOL

NYLS Law Review

Volume 61 | Issue 3 Article 8

January 2017

Opening a Can of Worms and Viruses: The Impact of E-Service on E-Mail Users Everywhere

JEFFREY WOLBER
New York Law School, 2016

VOLUME 61 | 2016/17

JEFFREY WOLBER

Opening a Can of Worms and Viruses: The Impact of E-Service on E-Mail Users Everywhere

61 N.Y.L. Sch. L. Rev. 449 (2016–2017)

ABOUT THE AUTHOR: Jeffrey Wolber was a Staff Editor of the 2015–2016 *New York Law School Law Review*. He received his J.D. from New York Law School in 2016.

I. INTRODUCTION

For the weary plaintiff burdened with the difficult task of serving an elusive defendant, Internet platforms[1] provide an ideal solution: compose a brief message, attach a PDF document, and press send. Although the practice is still in its infancy, a growing body of case law supports using e-mail and social media to effect service of process.[2] This manner of service is sometimes referred to as "e-service,"[3] and legal commentators have been forecasting its emergence for nearly two decades.[4]

Unfortunately, e-service may have unintended consequences on e-mail users. Spam e-mail attacks pose a significant threat to users' sensitive information, and messages that carry a legal obligation to open an e-mail attachment serve as an ideal template for such attacks.[5] Without safeguards, such as an independent way to determine authenticity, individuals who receive such messages will be unable to tell if an attachment is fraudulent until it is too late.[6] Many individuals will be at risk of

1. Here, the phrase "Internet platforms" refers to e-mail and social media. However, this note focuses primarily on the former, since e-mail poses a greater risk of spam attacks. Although social media is not immune to spam attacks, such attacks are more easily contained on social media because users can often view a sender's profile before opening a message and can set their privacy settings to allow messages only from individuals they have already added as "friends." *See, e.g.*, *Managing Messages: Which Messages Will I Receive on Facebook?*, Facebook Help Ctr., https://www.facebook.com/help/336759363070078 (last visited Apr. 6, 2017) (indicating that messages from individuals who are friends with the user on Facebook will be sent directly to the user's inbox, whereas messages from other individuals will be displayed as "message requests"). *But see Phishing: What Can I Do About Phishing?*, Facebook Help Ctr., https://www.facebook.com/help/217910864998172 (last visited Apr. 6, 2017) (indicating that accounts can be "hacked" if users provide their login credentials to a fake Facebook login page).

2. *See infra* text accompanying notes 34–51.

3. As used herein, the phrase "e-service" is limited to the method of serving process—serving originating documents such as summons and complaint—via e-mail or social media message without the recipient's consent. *See* Snyder v. Alternate Energy Inc., 857 N.Y.S.2d 442, 443 (Civ. Ct. 2008); Jeremy A. Colby, *You've Got Mail: The Modern Trend Towards Universal Electronic Service of Process*, 51 Buff. L. Rev. 337 (2003) (using the phrase "electronic service" throughout); Kevin W. Lewis, Comment, *E-Service: Ensuring the Integrity of International E-Mail Service of Process*, 13 Roger Williams U. L. Rev. 285 (2008) (using the phrase "e-service" in the title, but "e-mail service" throughout); Andriana L. Shultz, Comment, *Superpoked and Served: Service of Process Via Social Networking Sites*, 43 U. Rich. L. Rev. 1497, 1512 (2009) (using the phrase "e-service of process"). However, this phrase is also generally used to refer to the consensual exchange of documents and notices, including pleadings, between parties of a lawsuit. *See, e.g.*, Colo. R. Civ. P. 121, § 1-26(1)(d).

4. *See* Colby, *supra* note 3, at 337, 381–82 (noting a trend toward e-service and predicting that it will eventually become standard practice, as opposed to an exception); Yvonne A. Tamayo, *Are You Being Served?: E-mail and (Due) Service of Process*, 51 S.C. L. Rev. 227, 246–54 (2000) (discussing the use of electronic technology by the courts and advocating for courts to allow e-service); Frank Conley, Comment, *:-) Service with a Smiley: The Effect of E-mail and Other Electronic Communications on Service of Process*, 11 Temp. Int'l & Comp. L.J. 407, 412, 414, 427–28 (1997) (noting that nothing in the Federal Rules of Civil Procedure bars e-service, that e-mail has been widely accepted in society, and advocating for e-service).

5. *See infra* text accompanying notes 54–61.

6. Although some e-mail platforms allow a user to preview an attachment before opening it, all a spammer would have to do to successfully mislead a user is create a document that appears legitimate at first glance. Also, although many e-mail platforms automatically scan attachments for malware, they do not always identify malware ahead of time. *See infra* text accompanying notes 62–66.

identity theft as they must choose between opening a (perhaps dangerous) attachment and ignoring a message, which may be perfectly legitimate, altogether.[7] If they do the former, they can be exposed to malware and spyware, but if they do the latter, they can face unknown legal consequences.[8] Further, as e-service becomes more common, fraudulent e-service messages will appear more legitimate and will have a higher chance of deceiving recipients.[9]

This note consists of five Parts, and ultimately proposes three solutions to the problems that e-service presents. Following this Introduction, Part II surveys the jurisprudence of e-service, including the constitutional limitations on alternate service of process. Part III discusses technology, focusing on the current state of malware (software that can have a harmful impact on a user's computer) and spyware (software that monitors user activity and can secretly transmit personal information). Part IV examines the legal implications of failing to respond to personal service under New York and federal law, and submits that all e-mail and social media users currently have, at least as a practical matter, a duty to open any message that appears to contain pleadings, even if they have no reason to suspect they are being sued.

Part V proposes three possible solutions to the problems that e-service creates, and acknowledges the inherent limitations of each. First, jurisdictional rules should mandate that an index number, or other document identifier,[10] be included in the body of an e-service message. This would enable all recipients to safeguard their hard drives by ensuring the message is legitimate before opening its attachments.[11] Second, a policy should be imposed whereby defendants are freely allowed to vacate default judgments obtained through e-service and defend on the merits if they can establish that they either did not check their messages or that they saw the message, but had no reason to believe it was legitimate.[12] This would help prevent the emergence of a legal obligation to routinely check one's e-mail and social media accounts, and encourage plaintiffs to compose e-service messages so that they appear as authentic as possible to the recipient.[13] Third, either courts or the legislature should establish a uniform list of elements that must be present for e-service to be utilized.[14] By creating a clear and

7. This dilemma is discussed *infra* Part IV.

8. *See infra* text accompanying notes 71–94.

9. *See infra* Part III.

10. This note uses the phrase "document identifier" to refer to a piece of information that allows a user to verify that the document has been filed with the appropriate court. The importance of placing such an identifier in the body of an e-mail cannot be understated, since it would allow the recipient to verify the document without opening the attachment, which would substantially decrease the threat of downloading spyware. *See* discussion *infra* pp. 467–68. A document identifier could be an index or docket number, which recipients could use to obtain a copy of the initiatory documents through the court system.

11. *See* discussion *infra* pp. 467–68.

12. *See* discussion *infra* p. 469.

13. *See* discussion *infra* p. 469.

14. *See* discussion *infra* pp. 469–70.

definitive rule, individuals (and their attorneys) could precisely evaluate whether they have a legal obligation to open e-service attachments.

II. THE JURISPRUDENCE OF E-SERVICE

Due process of law requires that individuals be given a fair opportunity to defend themselves in an adjudicatory dispute.[15] Among other things, this necessitates that a defendant be afforded a reasonable opportunity to receive notice of an impending lawsuit.[16] Therefore, at a minimum, an individual seeking judicial action must reasonably attempt to notify the opposing party.[17] The Constitution does not require actual notice; all that is required is an attempt that is reasonably calculated to give actual notice and not substantially less effective than available traditional methods.[18] Such an attempt is a formality known as "service of process," or "service."[19] Once

15. *See* Henderson v. United States, 517 U.S. 654, 672 (1996) ("[T]he core function of service is to supply notice of the pendency of a legal action, in a manner and at a time that affords the defendant a fair opportunity to answer the complaint and present defenses and objections."); Grannis v. Ordean, 234 U.S. 385, 394 (1914) ("The fundamental requisite of due process of law is the opportunity to be heard.").

16. *See* Mullane v. Cent. Hanover Bank & Tr. Co., 339 U.S. 306, 314 (1950) ("Th[e] right to be heard has little reality or worth unless one is informed that the matter is pending and can choose for himself whether to appear or default, acquiesce or contest."); Shultz, *supra* note 3, at 1499 (stating that notice has been a prerequisite to legal action for over 4,000 years (citing Reuven Yaron, The Laws of Eshnunna, 118–19 (2d rev. ed. 1988))).

17. *Mullane*, 339 U.S. at 314–15 ("An elementary and fundamental requirement of due process in any proceeding which is to be accorded finality is notice reasonably calculated, under all the circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections. The notice must be of such nature as reasonably to convey the required information, and it must afford a reasonable time for those interested to make their appearance. . . . The means employed must be such as one desirous of actually informing the absentee might reasonably adopt to accomplish it." (citations omitted)).

18. *Id.* at 315 ("The reasonableness and hence the constitutional validity of any chosen method may be defended on the ground that it is in itself reasonably certain to inform those affected, or, where conditions do not reasonably permit such notice, that the form chosen is not substantially less likely to bring home notice than other of the feasible and customary substitutes." (citations omitted)); *id.* at 317–20 (contrasting the propriety of notice by publication for defendants whose addresses are unknown with the impropriety of such service for defendants whose addresses are known, in light of the ability of ordinary mail to reach those of the latter type); *see also* Dusenbery v. United States, 534 U.S. 161, 170–73 (2002) (applying *Mullane* and rejecting the assertion that due process required, as a "feasible substitute," *id.* at 171, to ordinary prison-mail delivery, the FBI to send notice of forfeiture to a prisoner in such a manner that the prison staff would ensure the prisoner opened it, since doing so would not "substantially improve[]," *id.* at 172, the likelihood of actual notice over the delivery system used at the time of service).

19. *See* 1 Robert C. Casad et al., Jurisdiction in Civil Actions § 1.01, at 8–9 (4th ed. 2014); *see also Process*, Black's Law Dictionary (10th ed. 2014) (defining "process" as "[a] summons or writ, esp[ecially] to appear or respond in court"); *id.* ("*Process* is so denominated because it *proceeds* or issues forth in order to bring the defendant into court, to answer the charge preferred against him, and signifies the writs or judicial means by which he is brought to answer." (citation omitted)).

service is complete, a court may exercise its adjudicatory authority over the dispute, provided jurisdiction is established.[20]

The extent of action required to complete service correlates with the nature of the suit and the amount in controversy.[21] Ideally, a defendant will be handed notice in person, which is often referred to as "personal service," but when this is not possible, a plaintiff must resort to "alternate service."[22] At a minimum, when a defendant's address is known, a plaintiff must attempt to give notice through U.S. mail.[23] However, when a defendant's address and whereabouts are unknown or inaccessible, plaintiffs may resort to other forms of alternate service.[24] These include service by affixture,[25]

20. Casad et al., *supra* note 19, § 1.01, at 2. In addition to the notice requirements, to adjudicate a dispute, a court must have the jurisdiction to do so. *Id.* There are two general components to jurisdiction: subject matter jurisdiction, which pertains to a court's ability to decide the legal issue before it, and personal or territorial jurisdiction, which pertains to the court's ability to bind the parties. *See generally id.* § 1.01[1]–[2]. There are three types of personal jurisdiction: *in personem* jurisdiction, or jurisdiction over a named defendant that provides the authority to adjudicate that defendant's personal obligations arising from the alleged conduct, *id.* § 1.01[2]; *in rem* jurisdiction, or jurisdiction over property within a state's territory that provides the authority to adjudicate title disputes over that property, *id.* § 1.01[3]; and *quasi in rem* jurisdiction, which confers the authority to adjudicate title of a defendant's property lying within a state's territory as partial compensation for the alleged conduct. *Id.*

At one point, *in personem* jurisdiction could only be obtained if a defendant was personally served within the forum state. *See* Pennoyer v. Neff, 95 U.S. 714, 720, 733 (1877). However, the Court repudiated this doctrine in *International Shoe Co. v. Washington*, when it allowed for "long-arm" jurisdiction by which defendants can be held liable within a forum state, to the extent that their actions affect individuals within that state in a legally cognizable manner, if they have sufficient "minimum contacts" within that state. 326 U.S. 310, 316 (1945).

21. *See* Walker v. City of Hutchinson, 352 U.S. 112, 115 (1956).

22. *See id.* at 116; *Mullane*, 339 U.S. at 315, 317; Casad et al., *supra* note 19, § 1.01[2][b]; *Personal Service*, Black's Law Dictionary (10th ed. 2014) (defining "personal service" as "[a]ctual delivery of the notice or process to the person to whom it is directed" and stating that it is "[a]lso termed *actual service*"); *Service*, Black's Law Dictionary (10th ed. 2014) (defining "constructive service" as "[s]ervice accomplished by a method or circumstance that does not give actual notice"). The phrase "constructive service" is sometimes used interchangeably with the phrase "substituted service," however the latter is also used to refer to delivery upon an individual other than the named defendant, such as an individual of suitable age at the defendant's residence. Casad et al., *supra* note 19, § 1.01[2][b]; *see also* David D. Siegel, New York Practice § 71, at 119 (5th ed. 2011) (noting the phrase "substituted service" can "confuse[] matters" because it "is sometimes used to refer to any method of summons service other than personal delivery"). To avoid confusion, this note uses the phrase "alternate service" to refer to all methods of service other than those involving personal delivery to an individual.

23. *See* Mennonite Bd. of Missions v. Adams, 462 U.S. 791, 800 (1983); *Walker*, 352 U.S. at 116; *Mullane*, 339 U.S. at 318–19.

24. *See, e.g.*, *Mullane*, 339 U.S. at 315, 317.

25. *See, e.g.*, N.Y. C.P.L.R. 308(4) (McKinney 2017) (allowing alternate service "by affixing the summons to the door of either the [defendant's] actual place of business, dwelling place or usual place of abode . . . and by . . . mailing the summons to [the defendant] at his or her last known residence . . . within twenty days").

publication,[26] telex,[27] facsimile,[28] and recently, e-mail[29] and social media.[30]

---

26. *See Mullane*, 339 U.S. at 316–17. In fact, at least one court has allowed online publication. *Compare* Microsoft Corp. v. Does, No. 12-CV-1335 (SJ)(RLM), 2012 WL 5497946, at *3 (E.D.N.Y. Nov. 13, 2012) (permitting service by e-mail and Internet publication where the defendants' whereabouts and identities were unknown, in an action for injunctive relief and damages for the alleged use of malware), *with* MLO v. "Younglawyer," No. 506175/2014, 2015 WL 1597530, at *2 (N.Y. Sup. Ct. Apr. 2, 2015) (rejecting service by online publication on a message board in response to anonymous defendants' allegedly tortious comments, even though service through e-mail was unavailable, because there was no indication that the defendants would become aware of such posts and also because no monetary relief could be accorded with the defendants' identities unknown, and injunctive relief to prevent further harm unlikely). *See generally* Lauren A. Rieders, Note, *Old Principles, New Technology, and the Future of Notice in Newspapers*, 38 Hofstra L. Rev. 1009 (2010) (arguing that courts should permit notice by publication in online newspapers).

27. *See* New Eng. Merchs. Nat'l Bank v. Iran Power Generation & Transmission Co., 495 F. Supp. 73, 81 (S.D.N.Y. 1980); Shultz, *supra* note 3, at 1504–05. The court in *New England Merchants Nat'l Bank* stated:

> Courts . . . cannot be blind to changes and advances in technology. No longer do we live in a world where communications are conducted solely by mail carried by fast sailing clipper or steam ships. Electronic communication via satellite can and does provide instantaneous transmission of notice and information. No longer must process be mailed to a defendant's door when he can receive complete notice at an electronic terminal inside his very office, even when the door is steel and bolted shut.

495 F. Supp. at 81. Merriam-Webster defines "telex" as "a system of communication in which messages are sent over long distances by using a telephone system and are printed by using a special machine (called a teletypewriter)." *Telex*, Merriam-Webster, http://www.merriam-webster.com/dictionary/telex (last visited Apr. 6, 2017).

28. *See* Broadfoot v. Diaz (*In re* Int'l Telemedia Assocs., Inc.), 245 B.R. 713, 722 (N.D. Ga. Bankr. 2000) (allowing service by e-mail); Aaron R. Chacker, Note, *E-ffectuating Notice:* Rio Properties v. Rio International Interlink, 48 Vill. L. Rev. 597, 607–10 (2003).

29. Fisher v. Petr Konchalovsky Found., No. 15-cv-9831(AJN), 2016 WL 1047394 (S.D.N.Y. Mar. 10, 2016) (allowing service by e-mail to a Russian defendant upon a showing that e-mail was likely to reach the defendant since he had responded to an e-mail concerning the subject matter of the dispute within the past two months at the e-mail address, and also that service by other means would not suffice since Russia had suspended judicial cooperation with the United States and objected to service by international mail); Dama S.P.A. v. Does, No. 15-cv-4528 (VM), 2015 WL 10846737 (S.D.N.Y. June 12, 2015) (permitting service by e-mail upon a defendant allegedly selling counterfeited goods through websites based in China); AMTO, LLC v. Bedford Asset Mgmt., LLC, No. 14-CV-9913, 2015 WL 3457452, at *7–10 (S.D.N.Y. May 29, 2015) (similar); Sulzer Mixpac AG v. Medenstar Indus. Co., 312 F.R.D. 329 (S.D.N.Y. 2015) (finding that service by e-mail at a "contact" address listed on the defendant's website was reasonably calculated to provide actual notice and thus comported with due process and international treaty); Phoenix-Dolezal v. Ni, No. 11 Civ. 3722(LAK)(JLC), 2012 WL 121105, at *5 (S.D.N.Y. Jan. 17, 2012) (finding that service through e-mail and certified mail was proper); D.R.I., Inc. v. Dennis, No. 03 Civ. 10026(PKL), 2004 WL 1237511 (S.D.N.Y. June 3, 2004) (allowing service by e-mail in addition to publication and certified mail sent to the defendant's last known address); *see In re* J.T., 37 N.Y.S.3d 846 (Fam. Ct. Sept. 2, 2016) (allowing service by e-mail in an action to terminate the recipient-father's parental rights where he had been deported to Jordan and had previously communicated with the social worker via e-mail but failed to provide a physical address).

30. *See* Ferrarese v. Shaw, 164 F. Supp. 3d 361, 368 (E.D.N.Y. 2016) (permitting service via Facebook, e-mail, and certified mail to the defendant's last known address in an action for, inter alia, parental custody); FTC v. PCCare247 Inc., No. 12 Civ. 7189(PAE), 2013 WL 841037, at *4 (S.D.N.Y. Mar. 7, 2013) (permitting service by e-mail and Facebook upon international defendants allegedly engaged in an Internet scheme to defraud American citizens); Baidoo v. Blood-Dzraku, 5 N.Y.S.3d 709 (Sup. Ct.

Beyond the minimum required by due process, each jurisdiction within the United States imposes its own statutory requirements that govern service of process.[31] With respect to alternate service, some of these statutes contain catchall-type provisions that allow courts to determine an effective manner of service when they find that another will be futile.[32] Through these catchall provisions, some courts have allowed e-service.[33]

The first published opinion in which a court allowed e-service was *In re International Telemedia Associates, Inc. v. Diaz*, where an international defendant-debtor had refused to provide a permanent address, but did provide a permanent facsimile number and e-mail address.[34] The court ordered service to be effected by facsimile, e-mail, and regular mail to the defendant's last known address.[35]

Subsequently, the court in *Rio Properties v. Rio International Interlink* allowed service to be effected by e-mail upon an international defendant entity that could not be served by conventional methods because its actual address was unascertainable.[36] Noting that the defendant had structured its business so that it could only be reached by e-mail, the court found that service by e-mail comported with both the Constitution and rule 4(f)(3) of the Federal Rules of Civil Procedure ("Federal Rules").[37] Nevertheless, the court noted that e-mail service has three shortcomings: (1) there is usually no way to confirm receipt, (2) system compatibility issues could lead to disputes over whether an attachment was actually received, and (3) attaching certain documents may be

2015) (discussing e-service generally, addressing the potential problems with service via social media, and permitting service to be made *solely* by Facebook after noting the futility of service by publication).

31. Alyssa L. Eisenberg, Comment, *Keep Your Facebook Friends Close and Your Process Server Closer: The Expansion of Social Media Service of Process to Cases Involving Domestic Defendants*, 51 San Diego L. Rev. 779 app. a (2014). Statutory approval of the particular method of alternate service is a prerequisite to obtaining *in personam* jurisdiction over a defendant thereby. *See* 62B Am. Jur. 2d *Process* § 134 (2017).

32. Typical of these provisions is rule 308(5) of the CPLR, which states that "service upon a natural person" may be made "in such manner as the court, upon motion without notice, directs, if service is impracticable under paragraphs one, two and four of this section." N.Y. C.P.L.R. 308(5) (McKinney 2017).

33. *See supra* notes 30–31; *infra* notes 48–51; *cf., e.g.*, Am. Heritage Int'l, Inc. v. Sarabi, No. 2:15-cv-00101-GMN-CWH, 2015 WL 6501129, at *2 (Nev. Dist. Ct. Oct. 27, 2015) (finding that rule 4 of the Nevada Rules of Civil Procedure, which contains no catchall provision, does not allow service by electronic means).

34. 245 B.R. 713, 715–18 (N.D. Ga. Bankr. 2000); *see* Colby, *supra* note 3, at 356–60.

35. *Int'l Telemedia Assocs., Inc.*, 245 B.R. at 718–19. As statutory authority, the *International Telemedia Associates* court relied on rule 4(f)(3) of the Federal Rules of Civil Procedure, *id.* at 719–21, which provides that service may be made on a foreign individual "by other means not prohibited by international agreement[, as the court orders]." *Id.* at 719 (quoting Fed. R. Civ. P. 4(f)(3)).

36. 284 F.3d 1007, 1013, 1016 (9th Cir. 2002). In *Rio Properties*, the plaintiff was unable to serve the defendant at the address listed on its trademark application because that address housed only its international courier, which was not authorized to accept service, and the plaintiff could not determine the defendant's Costa Rican address after searching international directory databases, but was able to uncover the defendant's e-mail address. *Id.* at 1012–13. The plaintiff attempted service through the defendant's international courier and Los Angeles attorney. *Id.* at 1013. See Chacker, *supra* note 28, for a detailed discussion of *Rio Properties*.

37. *Rio Props.*, 284 F.3d at 1017–18.

impossible because of imprecise imaging technology.[38] Despite these shortcomings, the court affirmed the use of e-mail to effect service and acknowledged that district courts will need to balance benefits and drawbacks of e-mail use on a case-by-case basis.[39]

In New York, the court in *Hollow v. Hollow* became the first court to authorize e-service under rule 308(5) of the New York Civil Practice Law and Rules (CPLR).[40] There, a defendant in a divorce action had been living in a secure complex in Saudi Arabia for over two years, and he had only been communicating with the plaintiff through e-mail.[41] The defendant's employer, who controlled the complex, refused to accept service on his behalf, and an international process server could have faced criminal charges for attempting to leave notice with the security personnel.[42] After concluding that other methods of service would be impracticable, the court allowed e-service, in combination with service through international registered and standard mail.[43]

The court in *Snyder v. Alternate Energy Inc.* followed suit, allowing e-service after the plaintiff demonstrated that obtaining the defendant's physical addresses was impracticable and that he previously communicated with the defendant by e-mail.[44] Once the plaintiff saw that the defendant was online regularly[45] and received notification that the defendant read the e-mails requesting his current address,[46] the court ordered the plaintiff to (1) send notice by e-mail on two consecutive dates bearing the subject line, "LEGAL PAPERS OPEN ATTACHMENT IMMEDIATELY"; (2) mail notice to the defendant's last known addresses; and (3) call the defendant's mobile number to advise him of the attempts being made.[47]

From these cases, a pattern emerges: E-service is generally permitted if (1) the court has the statutory authority to allow it;[48] (2) the plaintiff shows that personal

38. *Id.* at 1018. The court also noted that there could be issues about whether electronic signatures would comport with rules 4(a) and 11 of the Federal Rules. *Id.*

39. *Id.* at 1018–19, 1023. Following *Rio Properties*, courts have both allowed and declined e-mail service on an ad hoc basis. *See* Eisenberg, *supra* note 31, at 789 n.64.

40. 747 N.Y.S.2d 704 (Sup. Ct. 2002); Colby, *supra* note 3, at 366–67.

41. *Hollow*, 747 N.Y.S.2d at 705.

42. *Id.*

43. *Id.* at 706–08.

44. 857 N.Y.S.2d 442, 443–44 (Civ. Ct. 2008). There, the plaintiff had found the defendant's address vacant, and was unable to obtain a current address after employing the marshal, subpoenaing the defendant's cellular provider, checking with the local post office, and searching court records. *Id.* at 445; *see also* D.R.I., Inc. v. Dennis, No. 03 Civ. 10026(PKL), 2004 WL 1237511 (S.D.N.Y. June 3, 2004) (allowing service by e-mail, in addition to mailing notice to the defendant's last-known addresses with return receipt requested and publishing notice in newspapers local to those addresses for four weeks, after plaintiff's attempts to effect service at the last-known addresses were unsuccessful).

45. The defendant's screen name appeared on the plaintiff's AOL Messenger "buddy list" whenever the two were simultaneously online. *Snyder*, 857 N.Y.S.2d at 444–45.

46. The plaintiff requested a "return receipt" for the e-mails sent to the defendant. *Id.* at 445.

47. *Id.* at 449.

48. *See* 62B Am. Jur. 2d, *supra* note 31, § 134.

service by other methods would be impracticable;[49] (3) the plaintiff shows that the e-mail address is reasonably reliable;[50] and (4) e-service is used in conjunction with

49. Fed. R. Civ. P. 4(f)(3); N.Y. C.P.L.R. 308(5), 311(b) (McKinney 2017); *see also* Ferrarese v. Shaw, 164 F. Supp. 3d 361 (E.D.N.Y. 2016) (finding that the plaintiff established the requisite impracticability to justify e-service where the defendant had changed her name multiple times, personal delivery attempts at her last known address failed, and multiple skip trace searches yielded no current address); AMTO, LLC v. Bedford Asset Mgmt., LLC, No. 14-CV-9913, 2015 WL 3457452 (S.D.N.Y. May 29, 2015) (permitting service by e-mail upon a Russian defendant where the suspension of judicial cooperation with the United States made other methods of service unavailable); Transclick, Inc. v. Rantnetwork, Inc., No. 11 Civ. 8171(LTS), 2013 WL 4015768, at *7 (S.D.N.Y. Aug. 7, 2013) (vacating an order permitting service by e-mail where the defendant demonstrated that his address was readily attainable by a basic Internet search and where e-mail messages sent bore no indication that they pertained to legal matters); *D.R.I., Inc.*, 2004 WL 1237511 (finding impracticability established where personal service attempts at addresses found by, inter alia, searching DMV records failed); Hollow v. Hollow, 747 N.Y.S.2d 704, 706 (Sup. Ct. 2002) (stating that "[a]lthough a showing of impracticability does not require proof of due diligence or actual attempts to serve a party under each and every method prescribed in CPLR 308, the movant will be required to make a competent showing as to the actual prior efforts that were made to effect service" (citations omitted)); *Snyder*, 857 N.Y.S.2d at 446 (citing *Franklin v. Winard*, 592 N.Y.S.2d 726 (App. Div. 1993), for the proposition that a plaintiff can make a showing of impracticability through "diligent, albeit unsuccessful, efforts to obtain information regarding a defendant's current residence, business address or place of abode").

50. Fisher v. Petr Konchalovsky Found., No. 15-cv-9831(AJN), 2016 WL 1047394 (S.D.N.Y. Mar. 10, 2016) (allowing service by e-mail to a Russian defendant upon a showing that e-mail was likely to reach the defendant since within the past two months he had responded to an e-mail concerning the subject matter of the dispute that was sent to the same e-mail address, and discussing cases where service by e-mail was denied because the plaintiff failed to demonstrate that the e-mail address given was accurate or used by the defendant); Philip Morris USA Inc. v. Veles Ltd., No. 06 CV 2988(GBD), 2007 WL 725412, at *3 (S.D.N.Y. Mar. 12, 2007) (permitting service by e-mail upon corporations that routinely communicated with customers via that e-mail address); Safadjou v. Mohammadi, 964 N.Y.S.2d 801, 803–04 (App. Div. 2013) (affirming a judgment awarding divorce and parental custody where service by e-mail was effected upon the defendant at the e-mail addresses through which the defendant had previously communicated with the plaintiff); *In re* J.T., 37 N.Y.S.3d 846, 849–50 (Fam. Ct. 2016) (allowing service by e-mail where the defendant had been deported to Jordan and had previously communicated via e-mail but failed to provide a physical address); *see* Nykcool A.B. v. Pac. Int'l Servs., Inc., 66 F. Supp. 3d 385, 391 (S.D.N.Y. 2014) (finding that service by e-mail to an e-mail address that was listed as a "Contact Us" e-mail address on a website hyperlinked to the defendant's personal website was not reasonably calculated to provide actual notice, and directing service to be made upon the defendant's attorney by e-mail); SEC v. China Ne. Petrol. Holdings Ltd., 27 F. Supp. 3d 379, 399 (S.D.N.Y. 2014) (denying service by, inter alia, e-mail sent to the defendant's son where there was no indication that such an e-mail would reach the defendant); Silverman v. Blackman, No. CV 13-1349 (JS)(ARL), 2013 U.S. Dist. LEXIS 155779, at *5–6 (E.D.N.Y. Oct. 30, 2013) (denying service by e-mail in an action for, inter alia, trespass damages upon a finding that the plaintiffs failed to demonstrate that the defendant sought to be served was actually the named defendant); Fortunato v. Chase Bank USA, N.A., No. 11 Civ. 6608(JFK), 2012 WL 2086950, at *2 (S.D.N.Y. June 7, 2012) (denying service by Facebook message and e-mail address listed on a Facebook account where the plaintiff provided no evidence that the defendant accesses the Facebook account or even that the account was indeed the defendant's actual account); Ehrenfeld v. Salim a Bin Mahfouz, No. 04 Civ. 9641(RCC), 2005 WL 696769, at *3 (S.D.N.Y. Mar. 23, 2005) (denying service by e-mail where there was no showing that the defendant used the proffered e-mail address to exchange important business information or for any purpose other than receiving miscellaneous requests for information); *In re* Citigroup Glob. Mkts. Inc. v. Cid, No. 654211/12, 2013 WL 3724941 (N.Y. Sup. Ct. July 16, 2013) (denying service via e-mail to e-mail addresses provided on bank account applications that the defendants filled out in 2006 and 2009 because the plaintiffs failed to provide any information showing that the e-mail addresses were still valid or active). *But see* SEC v. Lines, No. 07 Civ. 11387(DLC), 2009 WL

other methods of alternate service, such as U.S. mail and publication, if available.[51]

III. THE TECHNOLOGY BEHIND E-SERVICE

E-mail and social media have become ubiquitous aspects of virtually every American's daily routine.[52] However, because of the relatively low cost associated with sending messages over the Internet, as well as the ability to send attachments that run programs on a user's computer when opened, these platforms are ideal mediums through which criminals can engage in fraud, such as identity theft.[53]

"Spam" is the term given to unsolicited e-mails, which are often sent to thousands of recipients at a time.[54] It can pose threats to recipients in three forms: (1) solicitations for fraudulent commercial products; (2) inducements to click on links to fraudulent websites, known as "phishing"; and (3) attachments that contain malware.[55] "Malware,"

3179503, at *4 (S.D.N.Y. Oct. 2, 2009) (citing *Mullane* and finding that it was not necessary to demonstrate that the defendant was known to use the e-mail address when his whereabouts were unknown).

51. *See Ferrarese*, 164 F. Supp. 3d at 386 (permitting service via Facebook, e-mail, and certified mail to the defendant's last known address in an action for, inter alia, parental custody); FTC v. PCCare247 Inc., No. 12 Civ. 7189(PAE), 2013 WL 841037, at *4 (S.D.N.Y. Mar. 7, 2013) (permitting service by e-mail and Facebook); Microsoft Corp. v. Does, No. 12-CV-1335 (SJ)(RLM), 2012 WL 5497946, at *3 (E.D.N.Y. Nov. 13, 2012) (permitting service upon defendants by e-mail and Internet publication); Phoenix-Dolezal v. Ni, No. 11 Civ. 3722(LAK)(JLC), 2012 WL 121105, at *5 (S.D.N.Y. Jan. 17, 2012) (finding that service through e-mail and certified mail was proper); Gurung v. Malhotra, 279 F.R.D. 215, 219–21 (S.D.N.Y. 2011) (granting default judgment where service had been effected through newspaper publication, certified mail, and e-mail to the defendant's publicly available government e-mail address despite the Indian government's intervention in an attempt to challenge the sufficiency of such service); *D.R.I., Inc.*, 2004 WL 1237511, at *2 (allowing service by e-mail in addition to publication and certified mail sent to the defendant's last known address). *But see* Baidoo v. Blood-Dzraku, 5 N.Y.S.3d 709, 715–16 (Sup. Ct. 2015) (allowing service by Facebook as the only method of service after noting the futility of service by publication).

52. *See* Andrew Perrin, *Social Media Usage: 2005-2015*, Pew Res. Ctr. (Oct. 8, 2015), http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015 (indicating that, as of 2015, seventy-six per cent of adult Internet users use social media); Aaron Smith, *U.S. Smartphone Use in 2015*, Pew Res. Ctr. (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015 (indicating that eighty-eight per cent of smartphone owners surveyed used e-mail at least once a week).

53. Harry Henderson, Encyclopedia of Computer Science and Technology 238 (rev. ed. 2009); *id.* at 451 ("The fundamental driving force of spam is the fact that, given one has Internet access, sending e-mail costs essentially nothing, no matter how many messages are sent. Thus even if only a tiny number of people respond . . . the result is almost pure profit for the spammer.").

54. *See id.* at 450–51 (noting that the term "spam" was likely coined in reference to a popular Monty Python sketch in which a group of Vikings use the word "spam" in an absurdly repetitious manner); *Spam: What Is Spam?*, Spam Laws, http://www.spamlaws.com/what-is-spam.html (last visited Apr. 6, 2017). Estimates suggest that spam e-mails comprise anywhere from 45%–73% of all e-mails sent, while only 2.5% of spam e-mails consist of scams and fraud, with 73% of those being attempts at identity theft. *Spam Statistics and Facts*, Spam Laws, http://www.spamlaws.com/spam-stats.html (last visited Apr. 6, 2017).

55. Henderson, *supra* note 53, at 451. This note is concerned with the lattermost threat, although the fraudulent e-service messages may also take the form of phishing attacks, for example where the recipient is directed to a fraudulent court website that will ask for personal information. *See infra* text accompanying notes 69–70.

short for "malicious software," includes computer viruses and worms.[56] Often these arrive in the form of a "Trojan Horse" ("Trojan"), a seemingly legitimate file that, when opened, installs malware on a user's computer.[57] Spammers will compose messages that trick recipients into opening the Trojan either by threatening or inciting them, usually suggesting that the recipient must act immediately to secure a financial gain or to prevent imminent harm.[58]

Once installed, the malware can perform a variety of functions. For example, a form of malware known as "spyware" can covertly scan a computer's hard drive in search of personal information and send the information back to the source after creating a "backdoor."[59] Some spyware can also record keystrokes in an attempt to retrieve a user's passwords and other information.[60] Further, malware can secretly hijack a user's computer to access other computers on the same network, or use that computer as a platform from which further spam attacks can be carried out.[61]

To counteract these threats, there are three common methods of scanning e-mails and their attachments for malware: (1) heuristics-based detection, which looks for words and phrases typically used in spam and phishing attacks; (2) signature-based detection and blacklisting, which searches for known malware code or untrustworthy IP addresses; and (3) behavioral detection, which observes how a program will operate before it is opened.[62]

---

56. Erin F. MacLean & Deborah M. Micu, *Internal Office Practices Can Make or Break a Law Firm's Cybersecurity*, Mont. Law., Dec./Jan. 2015, at 16, 25. A "virus" is a program that automatically reproduces itself throughout a user's hard drive, whereas a "worm" will exploit existing flaws in a computer's network without reproducing itself. Henderson, *supra* note 53, at 110–11; *see also Types of Malware*, Spam Laws, http://www.spamlaws.com/malware-types.html (last visited Apr. 6, 2017).

57. *See Types of Malware*, supra note 56.

58. *How Do I Know if It Is Spam?*, Spam Laws, http://www.spamlaws.com/learn-how-to-identify-spam.html (last visited Apr. 6, 2017). For discussions about phishing and other forms of identity theft in the digital age, see Jennifer Lynch, Note, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 Berkeley Tech. L.J. 259 (2005), and J. Anthony Vittal, *Phishing, Pharming, and Other Scams*, GPSolo, Dec. 2005, at 26.

59. *See Spyware and Trojan Horses*, Spam Laws, http://www.spamlaws.com/trojan-horse.html (last visited Apr. 6, 2017). This could be especially disastrous for law firms, considering the amount of confidential and sensitive information that would become exposed.

60. *See Avoiding Keystroke Loggers*, Spam Laws, http://www.spamlaws.com/keystroke-loggers.html (last visited Apr. 6, 2017).

61. John Markoff, *Attack of the Zombie Computers Is Growing Threat*, N.Y. Times (Jan. 7, 2007), http://www.nytimes.com/2007/01/07/technology/07net.html.

62. *See* Ted Green, Greenview Data, Inc., How URL Spam Filtering Beats Bayesian/Heuristics Hands Down 4–5 (2005), https://www.greenviewdata.com/library/white-papers/spam-url-filtering-vs-bayesian-heuristics.pdf; Lenny Zeltser, *How Antivirus Software Works: Virus Detection Techniques*, SearchSecurity (Oct. 11, 2011), http://searchsecurity.techtarget.com/tip/How-antivirus-software-works-Virus-detection-techniques.

However, none of these methods would be foolproof against fraudulent e-service messages.[63] Heuristic-based detection would likely be ineffective because the body of the message will usually be indistinguishable from a legitimate e-service message.[64] Signature-based detection and blacklisting would fail to identify attacks from unknown sources using previously unwritten code.[65] Finally, behavioral detection is limited in that certain behaviors, such as identifying keystrokes, would not be enough, on their own, to trigger filtration.[66]

E-service messages thus provide an ideal template for phishing attacks. A legitimate e-service message could come from an unknown e-mail address and contain an attachment that urges the recipient to act immediately.[67] A savvy spammer could easily send thousands of e-mails purporting to be e-service messages, address each one individually, and make them appear to have come from a legitimate sender.[68] If the malware goes undetected, there would be no way to differentiate between a legitimate e-service message and a spam attack.

Indeed, this practice has already begun. Today, spam attacks take the form of a "court notice" e-mail, whereby recipients are told that they must appear in a particular court on a given day, and that they should either open an explanatory attachment or call a listed telephone number.[69] In New York, for instance, this problem became so pervasive that the official website for the New York State Unified Court System now contains an advisory warning about the illegitimacy of such e-mails.[70] Unfortunately,

63. *See* Henderson, *supra* note 53, at 451 (stating that, because of the relentless battle between spammers and spam-fighters, perhaps the only way to prevent spam altogether is through an Internet-wide authentication of e-mail users).

64. Green, *supra* note 62, at 5–6; *see id.* at 6 (noting that "[h]euristic systems are unsuitable for some industries like medicine and law").

65. *See id.* at 4; Zeltser, *supra* note 62.

66. *See* Zeltser, *supra* note 62.

67. *See* sources cited *supra* note 58.

68. *See* Henderson, *supra* note 53, at 370; *How Spam Works*, Spam Laws, http://www.spamlaws.com/how-spam-works.html (last visited Apr. 6, 2017).

69. *See Court Summons Scam Emails Carry Malware*, Better Bus. Bureau (Sept. 9, 2014), http://www.bbb.org/upstatesc/news-events/bbb-scam-alerts/2014/09/court-summons-scam-emails-carry-malware.

70. *Important Notice About "Scam" Emails Involving Notices to Appear*, NYCourts.gov, https://www.nycourts.gov/contactus/scamemails.shtml (last visited Apr. 6, 2017). The notice reads:

> It has come to our attention that scam emails, purporting to be coming from the New York State Court System, directing recipients to report to court and to open an attachment for more information, are infecting recipients' computers with a virus.
>
> These scam emails typically instruct recipients to report to court on a specific day and time, and they often direct the recipient to bring documents and witnesses with them. They also typically warn that the court may proceed in their absence and that they will be sanctioned if they do not appear. The emails also instruct recipients to read a court notice that is attached. The attachment contains a computer virus. Do not open the attachment. Delete the email.
>
> Be on the alert, if you are not involved in a court proceeding and have not supplied the [New York] courts with an email address for receiving court notifications, the

this advisory warning only addresses e-mails purporting to come from the court itself, and not those purporting to come from parties or their attorneys, as a fraudulent e-service message would.

IV. THE LEGAL RAMIFICATIONS OF FAILING TO DOWNLOAD AN E-SERVICE ATTACHMENT

Consider the following scenario: A worried client pays her attorney a visit after receiving an e-mail with the subject line "Important: Legal Notice ***DO NOT IGNORE***." The message appears to have come from "Smith Law Firm," and it tells her to open an attached document labeled "Summons and Complaint." It provides no court information, let alone any indication of what state or county the supposed action was brought in. Should she be advised to open the attachment? If the e-mail is legitimate, has she properly been brought under the jurisdiction of the court? If she ignores the e-mail, might she face a default judgment that cannot be vacated? Finally, after considering all risks, what would the "reasonably prudent person" do under these circumstances?

A. Default Judgments in General

If the e-mail is legitimate and the client ignores it, the primary legal threat facing her would be a default judgment in favor of the plaintiff. A plaintiff who claims a legally cognizable cause of action will be entitled to a default judgment against a defendant who does not appear after being served with process.[71] A defendant seeking to vacate a default judgment must move to do so before the court that entered the judgment.[72] Otherwise, a plaintiff may enforce the judgment for up to twenty years after the date of entry.[73]

To assess the client's situation, the attorney must consider whether a court would vacate a default judgment resulting from the purported e-service message. After all, if the judgment could be vacated easily, there is little reason for her to risk identity theft by opening the e-mail attachment, since she would be able to safely await a default judgment as proof of its legitimacy and defend herself thereafter. Conversely,

---

> courts do not communicate with you by email. The court system does not send unsolicited emails or requests for personal information. The court system does not send emails threatening sanctions if you do not appear in court. Nor does the court system send emails that ask you to open attachments in order to obtain additional information.

Id. (emphasis omitted). The Better Business Bureau issued a similar advisory. *Scam Alert—You're On Trial? Watch Out for This Email Scam*, Better Bus. Bureau (Mar. 21, 2014), http://www.bbb.org/council/news-events/bbb-scam-alerts/2014/03/scam-alert-youre-on-trial-watch-out-for-this-email-scam.

71. Fed. R. Civ. P. 55; N.Y. C.P.L.R. 3215 (McKinney 2017).

72. *See* Fed. R. Civ. P. 60(b); C.P.L.R. 5015(a).

73. Fed. R. Civ. P. 69(a)(1) (providing that the forum state's procedure will govern execution of a money judgment); C.P.L.R. 211(b).

if a swift vacatur[74] cannot be assured, then perhaps it would behoove her to open the attachment and hope that her computer's security can ward off the virus.

B. Relief Due to Lack of Jurisdiction

Under both the Federal Rules and the New York CPLR, a defendant may seek relief from a judgment at any time for lack of jurisdiction.[75] Jurisdiction does not exist where a plaintiff did not serve the defendant as required by law or where a court does not have subject matter jurisdiction over the dispute.[76] Further, a defendant seeking relief for lack of jurisdiction need not assert a meritorious defense to the underlying claim because, as a constitutional imperative, a judgment entered without jurisdiction is a nullity.[77]

Unfortunately, this argument would likely not help the client if the e-service message were legitimate. Pending an unlikely determination that e-service does not comport with due process[78] or that the court did not have the authority to order it,[79] the e-service message would be sufficient to subject her to the court's personal jurisdiction.[80] Indeed, this would be true even if she could ultimately prove that she never saw the e-mail, because the Constitution does not require actual notice of the action.[81]

C. Relief Due to Fraud

A defendant may also move to vacate a judgment by showing that the plaintiff engaged in fraud.[82] Under the Federal Rules, defendants must assert these grounds within one year of the judgment's entry.[83] However, the CPLR allows defendants to

74. *Vacatur*, Black's Law Dictionary (10th ed. 2014) (defining "vacatur" as "[t]he act of annulling or setting aside" or "[a] rule or order by which a proceeding is vacated").

75. Fed. R. Civ. P. 60(b)(4); C.P.L.R. 5015(a)(4).

76. *See* 1 David L. Ferstendig, Weinstein, Korn & Miller CPLR Manual § 3.01, at 3-3 (3d ed. 2015). *See generally id.* § 3.02 (explaining subject matter jurisdiction). For "subject matter jurisdiction" defined, see *supra* note 20.

77. *See* Peralta v. Heights Med. Ctr., Inc., 485 U.S. 80 (1988); Gager v. White, 425 N.E.2d 851 (N.Y. 1981). In practice, it is best to move for relief in the alternative—by asserting either that no personal jurisdiction was obtained in the first place, or that if personal jurisdiction was obtained, the defendant has an excuse for the delay and a meritorious defense. *See* Siegel, *supra* note 22, § 108, at 202–03.

78. *See supra* notes 13–30 and accompanying text.

79. *See supra* text accompanying notes 30–33.

80. *See supra* notes 29–30, 52, and accompanying text. Of course, this assumes that the hypothetical plaintiff asserted an appropriate jurisdictional basis over the client. *See supra* note 20.

81. All that is required is a step "reasonably calculated" to provide actual notice. Mullane v. Cent. Hanover Bank & Tr. Co., 339 U.S. 306, 314 (1950).

82. Fed. R. Civ. P. 60(b)(3); N.Y. C.P.L.R. 5015(a)(3) (McKinney 2017).

83. Fed. R. Civ. P. 60(c)(1).

assert these grounds at any time,[84] and the defendant need not assert a meritorious defense to the underlying action.[85] In both jurisdictions, when a plaintiff lies to the court when requesting permission to resort to alternate service, such as by mischaracterizing or fabricating the attempts taken to effect in-person service, the fraud provides grounds for vacatur.[86]

Thus, if the plaintiff lied to the court about the steps taken to attempt service by other methods, and those lies are uncovered on a motion to vacate the judgment, the client would likely succeed under both the Federal Rules and the CPLR. However, there is an obvious practical difficulty: she might have to disprove the plaintiff's assertions long after the fact. Fortunately, estimating the degree of difficulty is fairly straightforward. If she has been residing in the same location for a long time, a court is less likely to believe that the plaintiff actually made the attempts alleged (and she should be expecting further notice to arrive in the mail).[87] However, if she has recently moved without leaving a forwarding address,[88] or is otherwise transient, there is a reasonable possibility that a court will believe a plaintiff's assertions about the difficulty of effecting in-person service and service by mail. Thus, the safest course of action for a client in this scenario might be to open the attachment.

D. Excusable Default

If the court were to believe the allegations supporting the plaintiff's original motion for e-service—that other methods of service were attempted but unsuccessful—then the client would need to assert "excusable default" as a ground for the vacatur.

Owing to the potential severity of default judgments, both the Federal Rules and the CPLR provide a statutory period allowing defendants to seek vacatur on the basis of "excusable default" by asserting both a justification for the delay in appearing

84. Rule 5015(a)(3) of the CPLR does not contain a time limit. *See* C.P.L.R. 5015(a)(3); Wells Fargo Bank N.A. v. Podeswik, 981 N.Y.S.2d 230 (App. Div. 2014).

85. *See* Tonawanda Sch. Emps. Fed. Credit Union v. Zack, 662 N.Y.S.2d 885 (App. Div. 1997).

86. *See, e.g.*, Shaw v. Shaw, 467 N.Y.S.2d 231, 233–35 (App. Div. 1983) (holding that a motion to vacate under rule 5015(c) of the CPLR based on "extrinsic fraud"—which prevents parties from fully and fairly representing themselves—need not be supported by a meritorious defense, analogizing it to a motion based on lack of jurisdiction owing to improper service, and differentiating extrinsic fraud from "sewer service"—where the fraud is made upon the court to conceal that no proper service has been made—although characterizing both as "fraud" and not "jurisdictional" per se).

87. *See* Transclick, Inc. v. Rantnetwork, Inc., No. 11 Civ. 8171(LTS), 2013 WL 4015768, at *7 (S.D.N.Y. Aug. 7, 2013) (vacating an order permitting e-mail service, where the defendant demonstrated that his address was readily attainable by a basic Internet search and where e-mail messages sent bore no indication that they pertained to legal matters).

88. *See* D.R.I., Inc. v. Dennis, No. 03 Civ. 10026(PKL), 2004 WL 1237511 (S.D.N.Y. June 3, 2004) (finding impracticability established where personal service attempts at addresses found by, inter alia, searching DMV records failed); Baidoo v. Blood-Dzraku, 5 N.Y.S.3d 709, 711–12, 716 (Sup. Ct. 2015) (finding that the defendant's failure to provide a forwarding address to the post office supported a finding of impracticability and justified resorting to service by Facebook).

and a meritorious defense to the underlying action.[89] Courts analyze the justification given for the delay on an ad hoc basis, often considering the length of delay, the reason for the default, and the prejudice that would result to the plaintiff if the motion were granted.[90] The Federal Rules require that this motion be made within one year of entry of the judgment,[91] and the CPLR requires that it be made within one year after notice of the judgment was served.[92]

Unlike the Federal Rules, the CPLR has a special provision for defendants who are served by a method other than personal delivery: Rule 317 states that if the court finds that the defendant did not receive actual notice, relief may be sought within one year of learning of the judgment, but not more than five years after its entry.[93] When this basis is relied on, the defendant need not assert any justification for the delay, but must still assert a meritorious defense.[94]

When considering the possibility of obtaining a vacatur for "excusable delay," there are time limits to consider. Under the Federal Rules, if the client fails to notice the default judgment for over a year after it is entered, she will be barred from asserting this defense. Under the CPLR, she could await notice of the judgment, but she would need to act within one year.[95] In both jurisdictions, she would have to assert a meritorious defense to the underlying cause of action. However, even if she responds on time and offers a meritorious defense, she would still be at a judge's mercy on the issue of whether her delay was justified, and so determining her likelihood of success would be difficult.

The alternate grounds for relief under rule 317 of the CPLR seem inapplicable to the client's situation. No court has addressed the issue of whether receipt of an e-mail, without opening the attached summons, would qualify as "actual notice" for the purposes of this rule. However, given the obvious analogy to receiving a letter but never opening the envelope, it seems unlikely—although certainly debatable—that she would succeed in maintaining that she did not receive "actual notice" of the action

89. Fed. R. Civ. P. 60(b)(1); C.P.L.R. 5015(a)(1); *see* 2 Ferstendig, *supra* note 76, § 24.05[b][1], at 24-24 to -25.

90. *See* 2 Ferstendig, *supra* note 76, § 24.05[b][1], at 24-24 n.5.

91. Fed. R. Civ. P. 60(c)(1).

92. C.P.L.R. 5015(a)(1).

93. *Id.* at 317. This provision is distinct from, and imposes no limitation on, the various grounds for relief available under rule 5015 of the CPLR. *See* Ariowitsch v. Johnson, 498 N.Y.S.2d 891, 893 (App. Div. 1986). Therefore, a defendant may assert lack of jurisdiction as a ground for relief at any time regardless of whether rule 317 would be available. *Id.*

94. *Ariowitsch*, 498 N.Y.S.2d at 893. However, this provision is unavailable in actions for divorce, annulment, or partition. C.P.L.R. 317.

95. Under New York law, she will still be able to resort to the court's discretionary authority to vacate judgment. *See infra* Part IV.E.

simply because she did not open the e-mail.[96] Therefore, there is an appreciable risk that she would not be given the ability to defend on the merits that rule 317 provides.

E. Discretionary Relief

Under rule 60(b)(6) of the Federal Rules, a federal court may grant relief from a judgment for "any other reason that justifies relief,"[97] as long as it is requested within a "reasonable time" after entry.[98] However, a defendant may not use this provision to circumvent the time limits of the other grounds for relief, since this provision is exclusive of those grounds.[99] Therefore, where a defendant is asserting excusable default or fraud, this provision is unavailable.[100]

New York courts have broader discretion, since they retain the inherent authority to vacate their own judgments at any time if doing so is in the interest of substantial justice.[101] Unlike the Federal Rules, the New York courts' discretion is in addition to their statutory authority; thus, defendants have a safety net if they must rely on grounds for which the statutory time period has elapsed or if they are unable to excuse a delay in seeking relief.[102]

Therefore, in federal court, rule 60(b)(6) would be of little use to the client. Since the Federal Rules consider this authority to be exclusive of the other statutory grounds for relief, her only available argument under this provision is that relief would be justified simply because of the unusual form of notice.[103] The likelihood of succeeding on this argument will vary depending, for example, on whether the details offered in the e-mail body supported an assumption of spam or legitimacy, the particular judge's philosophy on e-service and the Internet generally, and how common e-service had become by the time she received the message. Again, this provides no clear solution for the client.

96. *Cf.* Bennett v. Patel Catskills, LLC, 990 N.Y.S.2d 594, 595 (App. Div. 2014) (determining that the fact that the summons sent via certified mail was returned as "unclaimed" raised a triable issue of fact as to whether the defendant received notice). The negative ramifications of allowing a recipient to succeed on this argument are palpable. One could easily negate an otherwise valid e-service attempt by simply refusing to open the e-mail. Nevertheless, valid reasons for nonreceipt of e-mail might include that the message was routed into a "junk" mail folder or that it was sent to an outdated e-mail address. In those instances, a defendant might be able to prove that notice was never received, although obtaining evidence years later might be difficult.

97. Fed. R. Civ. P. 60(b)(6).

98. *Id.* at 60(c)(1).

99. Wesco Prods. Co. v. Alloy Auto. Co., 880 F.2d 981, 983 (7th Cir. 1989).

100. *Id.*

101. *See* Woodson v. Mendon Leasing Corp., 790 N.E.2d 1156, 1160 (N.Y. 2003); 1 Ferstendig, *supra* note 76, § 24.05[a].

102. *See* Piatt v. Horsley, 970 N.Y.S.2d 155 (App. Div. 2013); McMahon v. City of New York, 483 N.Y.S.2d 228 (App. Div. 1984).

103. Other available arguments, such as lack of jurisdiction, fraud, and excusable delay, would have to be considered under the other provisions of rule 60 of the Federal Rules, and thus be subject to the applicable time limits.

However, under New York law, the client would be able to seek relief from any judgment obtained, since New York courts retain inherent authority to do so. Even so, there is no guarantee that a court would agree to vacate the judgment, and so the best attorneys can do is predict the most likely outcome. Unfortunately, without opening the attachment to evaluate the underlying facts, the attorney would have no way to even speculate about the potential prejudice that might be in store for the plaintiff if the client ignores the e-mail. Thus, while the mere existence of this discretionary authority might provide some comfort for the client if she decides to ignore the e-mail altogether, it still fails to resolve the dilemma completely; there remains a risk that the judgment will not be vacated.

F. Resulting Policy Implications

Again, what would the "reasonably prudent person" do in this circumstance? Even if the client has maintained the same permanent residence for many years, there is a small possibility that the e-mail is legitimate and that the plaintiff has lied about attempting traditional methods of service, hoping to obtain a default judgment without her knowledge.[104] Further, if the client has recently moved, the possibility that the e-mail is legitimate increases, especially if she did not provide a forwarding address to the post office.[105] It would be helpful, especially in the latter case, to know more about the purported cause of action before deciding whether to open the attachment. For instance, she might be able to identify the plaintiff as someone she associated with prior to switching residences or find other useful information in the complaint. Unfortunately, without opening the attachment, there would be no way to conduct this investigation. In either scenario, there is no guarantee that the client would be able to vacate a resulting judgment, and, at the very least, attempting to do so would likely impose certain expenses that she would not otherwise incur, such as hiring an attorney.

The situation is made worse by two additional factors. First, given the relative infrequency with which e-service is used, it is more likely for the message to be fraudulent than legitimate. However, a default judgment might be even more

104. *See* Siegel, *supra* note 22, § 71, at 117; *supra* note 86 (discussing "sewer service," where the process server swears to service having been completed when none was ever attempted). For example, a debt-collector could have a legitimate cause of action against the client, but be reluctant to hire a reputable process server. *See Service*, Black's Law Dictionary (10th ed. 2014) (defining "sewer service" as "[t]he fraudulent service of process on a debtor by a creditor seeking to obtain a default judgment"); *Default Judgments, Gutter Service and the Statute of Limitations*, Hub Pages (Feb. 10, 2011), http://hubpages.com/money/Default-Judgments-Gutter-Service-and-the-Statute-of-Limitations; *see also* Pandiscia v. Pandiscia, No. 321/2012, 9 N.Y.S.3d 594, 2014 WL 7530334, at *2 (Sup. Ct. Dec. 22, 2014) (unpublished table decision) ("'[S]ewer service' . . . occurs 'when a process server discards court papers and claims they were duly served, recording a fictitious date and time of service in the log and in the court affidavits of service.'" (quoting First Commercial Bank of Memphis, N.A. v. Ndiaye, 733 N.Y.S.2d 562, 564 (Sup. Ct. 2001))).

105. *See* Snyder v. Alternate Energy Inc., 857 N.Y.S.2d 442, 448–49 (Civ. Ct. 2008) (finding that the plaintiffs established impracticability of serving the defendant because, inter alia, they were not able to locate a forwarding address at the local post office).

problematic than malware for the average recipient, especially if it cannot be vacated. Second, those recipients who are less technologically inclined, and thus less likely to have effective malware detection software, are more susceptible to such scams.

Therefore, the existence of e-service alone creates both legal and practical obligations for e-mail users to open an attachment from an unknown source. While the chance that a given message is legitimate will vary depending on the recipient's circumstances, there is no way for any individual to know for sure. This exposes individuals' sensitive information, and can punish e-mail users for being cautious about their legal rights.

V. POSSIBLE SOLUTIONS

From the above discussion, three points should be evident. First, there is no uniform way that e-service must be accomplished.[106] While it would be possible for a court to require the body of the e-service message to include helpful information about the court and claims alleged, it is not currently required. As a result, a legitimate e-service message might contain no information explaining the attachment, and so the recipient of a generic e-service message cannot safely disregard it.

Second, while e-mail and social media are ideal methods for reaching an elusive defendant who nevertheless maintains an online presence, those same platforms also serve as ideal mediums for fraud and identity theft.[107] Further, as e-service becomes more widely accepted, recipients of e-service messages will be more likely to believe they are legitimate and open the potentially harmful attachments.

Third, a recipient of a legitimate e-service message may be unable to vacate a resulting judgment, especially if the plaintiff was honest about her attempts to effect service by traditional means.[108] Even if they are not barred from obtaining a vacatur, recipients pursuing this relief may face practical difficulties that become greater with time. For instance, to prove that one did not receive notice is to prove a negative, and it could be difficult to demonstrate that the efforts outlined by a plaintiff to initially justify e-service were not actually attempted.[109]

Thus, in its current state, e-service creates a fertile environment for spam attacks purporting to contain service of process. If left unattended, this environment will only get worse as e-service becomes more routine.[110] However, there are ways to mitigate the risks while leaving intact the availability of e-service to plaintiffs who are frustrated by an elusive defendant, although each of the possibilities suffers from its own set of limitations.

One solution is to create a standard format for e-service messages to follow that would allow recipients to remotely verify that they are indeed named in a pending

106. *See supra* text accompanying notes 34–51.

107. *See supra* Part III.

108. *See supra* Part IV.E.

109. *See supra* Part IV.C–D.

110. *See supra* pp. 460–61.

action, not just targets of a spam attack. This requirement would provide certainty to recipients, since they could safely disregard any message without the requisite information. Perhaps the simplest, and most effective, method would be to require all e-service messages to contain, in the message body or subject line, a document identifier that will allow the recipient to search for the court filings independently.[111] The most readily available identifier would be an index number, which would be given to plaintiffs when they file the complaint.[112] By providing the index number, in addition to any other information required to search for the filings,[113] all the recipient would have to do is look up the index number and read the corresponding documents.

One shortcoming of this approach, however, is that spammers might attempt to create their own fraudulent means of "verifying" the message. A spammer might compose a message that follows the same general format as a legitimate e-service message, and directs recipients to a fraudulent website.[114] However, so long as a plaintiff is required to provide a specific type of document identifier, a recipient would, at the least, be able to confer with counsel before visiting the website and thereby be advised against doing so. This approach, of course, is of little help to those who are not computer savvy, or have no means of retaining counsel or verifying court documents.

Another possibility is to have courts send the messages via a central server.[115] At first glance, this would seem to reduce the threat of spam by allowing individuals to simply check the sender's information to confirm legitimacy. However, there are several problems with this proposal. First, courts do not typically take responsibility for effecting service on behalf of a plaintiff.[116] Second, this would require courts to devote their limited resources to creating an e-mail server and assigning personnel to compose and send such e-mails. Finally, spammers routinely "mask" their true e-mail

111. Individuals can search for a case by entering their name into the search field and checking if they are named as defendants in a pending action. *See WebCivil Supreme—Case Search*, N.Y. St. Unified Ct. Sys., https://iapps.courts.state.ny.us/webcivil/FCASSearch (last visited Apr. 6, 2017). However, this still does not alert individuals to whether the e-mail is legitimate, and the task could be arduous for individuals with fairly common last names. Further, this option is unavailable for some local courts. *See WebCivil Local—Available Courts*, N.Y. St. Unified Ct. Sys., https://iapps.courts.state.ny.us/webcivilLocal/LCAvailableCourts (last visited Apr. 6, 2017). Thus, providing court information and an index number, which would enable direct inquiry, is a better solution.

112. *See* N.Y. C.P.L.R. 306-a (McKinney 2017).

113. In New York, for example, one would also need the name of the court and county to conduct the necessary search by index number. *See, e.g.*, *WebCivil Supreme—Case Search*, *supra* note 111.

114. *See* Henderson, *supra* note 53, at 369–70.

115. The Colorado court system accepts filings through an integrated court filing system; however, it specifically excludes personal service of process and applies only to service of pleadings and other documents subsequent to the originating documents upon parties who have already registered for the system. Colo. R. Civ. P. 5(b)(2)(D); *ICCES User Agreement—Terms and Conditions of Use*, Integrated Colo. Cts. E-Filing Sys. 6, https://www.courts.state.co.us/userfiles/file/terms.pdf (last updated May 11, 2015).

116. *See* Fed. R. Civ. P. 4(c)(2) ("Any person who is at least 18 years old and not a party may serve a summons and complaint.").

address to make it appear that the message is coming from someone else.[117] Thus, this solution might be counterproductive by providing a "mask" that spammers know will be effective.[118]

Yet another solution is to allow e-service recipients to freely open judgments obtained against them if they (1) do so within a reasonable time after learning of the judgment, and (2) can establish ignorance of the underlying cause of action at the time of receipt. The first requirement could be modeled after rule 317 of the CPLR, which automatically allows defendants to open a judgment to defend on the merits if they move to do so within the time requirements. This would prevent a legal obligation to open an e-service attachment from being imposed on individuals who are not truly evading service—the vast majority of Internet users—provided they have no reason to suspect they are being sued. The second requirement would encourage plaintiffs to include detailed information in the body of an e-service message, thus facilitating a defendant's inquiry into its legitimacy, since any information provided will operate against the defendant's claim of ignorance.

However, this option may create uncertainty for a plaintiff, since it threatens the finality of a judgment obtained by e-service. Further, it would do nothing to address the *apparent* legitimacy of fraudulent e-service messages, and would not provide a way to determine, with certainty, whether an e-service message is legitimate. Thus, for the unsuspecting recipient who does not seek the advice of counsel before opening an attachment, this solution will provide no benefit.[119]

Finally, it may be helpful to establish uniformity among the circumstances for which e-service is allowed. For instance, jurisdictions could statutorily limit e-service to certain causes of action or require certain objective criteria to be met before e-service may be used.[120] Similar to the solution of requiring document identifiers to be placed in e-service messages, this would allow a recipient to independently determine whether there *could* be any legal consequences from not opening the attachment. However, unlike an index number, this would not allow an individual to guarantee, before opening the attachment, that an e-service message is legitimate; it only provides them with the enhanced ability to calculate the probability that they will face legal consequences if it actually is. Also, there is always the chance that an

117. *See* Henderson, *supra* note 53, at 370.

118. The same argument can be used against requiring a standard template for e-service messages that does not include an independently verifiable document identifier. For example, the court in *Snyder v. Alternate Energy Inc.* directed the e-service message to bear the subject line, "LEGAL PAPERS OPEN ATTACHMENT IMMEDIATELY." 857 N.Y.S.2d 442, 444 (Civ. Ct. 2008).

119. In contrast, if an e-mail contains an index number, recipients could consult the court's website to determine authenticity, which will spare them the expense of consulting an attorney.

120. For example, jurisdictions might limit e-service to defendants who are actively evading service or who moved without leaving a forwarding address. To challenge jurisdiction after the fact, defendants could simply offer evidence that they were not actively evading service or that they did leave a forwarding address with a post office.

individual recipient might meet the statutory criteria, but nevertheless open what turns out to be a fraudulent attachment.[121]

Overall, any solution, even a limited one, would be better established by statute than by case law. If courts continue to have unbridled discretion to allow e-service, limited only by "due process," there exists a possibility that a given judge will allow e-service for different criteria than those routinely required by other judges. Further, to establish binding precedent, it will be necessary for some individuals to bear the expense of appeal to establish a standard for others. If not addressed by statute, until a willing litigant steps forward, e-mail users everywhere will continue to be faced with a dilemma when confronted with an apparent e-service message.

VI. CONCLUSION

While e-service is beneficial for those plaintiffs seeking to serve an elusive defendant, it also enhances the apparent legitimacy of spam attacks that purport to contain e-service. These attacks pose a unique risk to recipients because, under current practice, e-service messages do nothing to distinguish themselves from spam. Also, because the authority to allow e-service is largely discretionary, there are few uniform rules to help someone determine, in advance of opening an attachment, whether the e-mail is legitimate, and, if so, what the legal ramifications of ignoring the message would be.

Among the solutions available, the simplest and most effective is to require all e-service messages to provide an index number and jurisdictional information within the body of the e-mail. This would allow recipients to conduct their own search to confirm whether the e-mail is legitimate before they open any attachment. Another useful solution would be to allow defendants to freely open a judgment obtained by e-service as long as they do so within a certain amount of time after receiving notice of the judgment and can establish ignorance of the underlying cause of action. This will encourage plaintiffs to provide enough information in the body of an e-mail to demonstrate to the recipient that the message is legitimate.

Fortunately, these options are not mutually exclusive. Though they are imperfect, implementing them will enhance the benefits of e-service, and reduce the risks.

121. Since spammers routinely send e-mails to thousands of recipients, there is always a chance that at least one recipient could satisfy the statutory criteria. *See* Henderson, *supra* note 53, at 370; *How Spam Works*, *supra* note 68.

NEW YORK LAW SCHOOL LAW REVIEW

www.nylslawreview.com