University of Michigan Journal of Law Reform

Volume 54

2021

Impostor Scams

David Adam Friedman
Willamette University

https://doi.org/10.36646/mjlr.54.3.imposter

IMPOSTOR SCAMS

David Adam Friedman*

ABSTRACT

Impostor scams have recently become the most common type of consumer scam in America, surpassing identity theft. It has never been easier and more profitable to be an impostor scammer. Though the core of these scams dates back centuries, these fraudsters consistently find novel ways to manipulate human motives and emotions. Nonetheless, the public should not give up hope. Policymakers and private actors can slow down this scourge if they focus on the key chokepoints that impostor scammers rely upon to achieve their ends. This Article provides a roadmap for a solution to impostor scams, offering specific suggestions for mitigating this fraud today, while advocating the adoption of a "least-cost avoider" approach to address the whole of the ongoing problem.

TABLE OF CONTENTS

* Professor of Law, Willamette University. B.A., Yale College, J.D., Yale Law School. I thank Justin Simard for helpful research suggestions and Jay Gatz for introducing me to the concept of the impostor. Historian Edward Balleisen's rich and thorough history of fraud in America inspired me to look harder for solutions to this puzzle of impostor fraud. I also thank Susan Alterman and Laura Appleman for their comments.

INTRODUCTION

Impostors are scoundrels who pretend to be someone they are not for their personal gain. They have been swindling Americans out of their money and property for centuries.[1] Today, however, impostors are operating on a much broader scale, using new technology and hiding in distant jurisdictions. Impostor scams are now public enemy number one—the most frequently reported category of consumer fraud, according to the Federal Trade Commission (FTC), even exceeding identify theft complaints.[2] They account for nearly $500 million in consumer losses, and that figure includes only *reported* consumer losses,[3] so total losses may be larger but impossible to measure.

In this Article, I explore how impostor scams are generally impossible to stop. Impostor tricks are diverse, clever, and innovative. Public education has limitations. Technological advances in communications, the ascent of social media, and new payment systems have supercharged the ability of scammers to commit fraud with minimal downside. Impostors have never been able to reach so many potential marks so inexpensively and with so little fear of consequences from prosecution and enforcement.

In the days before the Internet, global telecommunication, and advanced payment systems, impostor scams required perpetrators to operate on a smaller scale and assume more risk. Imposture in the flesh requires a deeper time investment and, quite often, direct physical exposure to those who might unmask and report the impostor. Today, impostors can spam millions with their fraud attempts from a safe distance.

---

1. *See* EDWARD BALLEISEN, FRAUD: AN AMERICAN HISTORY FROM BARNUM TO MADOFF 14–23 (2017) (describing the "shape-shifting, never-changing world of fraud").

2. *See* FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK 2018, at 84 (2019).

3. *See id.* at 8, 84.

Despite these complications, it is imperative for policymakers and regulators to throw considerably more sand into the gears of impostor scams. Although such efforts to eliminate them might prove futile, failure to pursue them aggressively will only enable their acceleration. Technological and educational interventions from the public and private sectors can reduce the effectiveness of impostor fraud efforts, thus raising the cost of implementing these scams. Without sustained interventional efforts, impostor scams will proliferate even faster. The goal should not be an unrealistic elimination of impostor ploys that have durable core effectiveness. Instead, the goal should be to reduce their incidence. The alternative, which would be to give up or let up, would enable the scammers to improve their methods and thrive.

The question turns to how to find the right levers and weapons to reduce impostor fraud in what likely will be a perpetual struggle. Certain common avenues or chokepoints can be throttled to raise the costs of committing impostor fraud. Scammers often rely on legitimate intermediaries in communications services and financial transactions to achieve their ends. Policymakers, regulators, and private actors themselves should ensure that intermediaries internalize some of the responsibility for slowing down impostor scammers. These intermediaries are the classic low-cost avoiders in this scenario and are often best positioned, at the very least, to make impostor scamming more expensive and difficult.[4]

In Part I, I discuss the power of the impostor and the history of the impostor scam. I describe the transformation of impostor scams, in their various forms, into "public enemy number one." Part II explains how the economics of launching impostor scams dramatically improved and why the scourge has become an epidemic. Part III discusses regulatory and enforcement efforts to address impostor fraud and why they have fallen short. In Part IV, I suggest that waging a concerted war against impostor fraud is possible, and I offer specific tactical suggestions that put more burden on telecommunications providers, social media platforms, and financial intermediaries to put their unique "chokepoint" positions to good use.

Today, most losses from impostor fraud fall on the victims. By shifting more responsibility on potentially preventative parties at the chokepoints for impostor fraud, a least-cost-avoider-like approach could be adopted. Though no "silver bullet" exists to re-

---

4. *See* GUIDO CALABRESI, THE COST OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 135–40 (1970) (famously contending that the cost of accidents could be minimized by assigning liability to the cheapest cost avoiders).

solve impostor fraud, as fraudsters will always innovate, I conclude that mitigation of the problem may be quite possible.

I. THE HISTORY AND GROWTH OF IMPOSTOR FRAUD

There is no doubt that impostor scams have become a top consumer fraud nuisance in the United States. Impostor scam reports are up twenty-five percent since 2016, surpassing identity theft reports and replacing debt-collection complaints as the most commonly-reported consumer complaint.[5] The Consumer Sentinel, which aggregates federal and state data, counted over three million total reports of fraud, identity theft,[6] and other types of complaints in 2018. Fraud accounted for forty-eight percent of these complaints by volume and identity theft for fifteen percent.[7] Within the fraud category, the total 2018 reported losses from impostor schemes towered over the rest at $488 million, nearly exceeding the total losses associated with the other top ten types of fraud combined.[8]

Though the scale of the problem is new, impostor scams are as old as the hills. As I discuss in Section I.A, impostor powers find deep roots in our social history and constructs. Section I.B shows how the underlying schemes from the nineteenth century still retain their same form today. In detailing the recent explosion of impostor fraud that vaulted it to the current epidemic, in Section I.C, I show that today's impostor fraud just employs modern technology and social structures to use the same basic means to achieve the same ends.

A. *The American Impostor*

Impostors have long captured the American imagination. In F. Scott Fitzgerald's *The Great Gatsby*, the protagonist, a con artist from the Midwest, constructs a false identity as an Oxford graduate, a hero of the Great War, and an all-around "old sport," wooing old money socialites to cover his status as an organized crime fig-

---

5. *See* FED. TRADE COMM'N, *supra* note 2, at 84.

6. The FTC distinguishes "identity theft" from impostor fraud. The Sentinel describes the identity theft scenario as when a scammer "appropriates . . . personal identifying information (like a Social Security number or credit card account number) to commit fraud or theft." *Id.* at 82. In effect, the difference, though subtle, is one of significance. The victim of the impostor scam has been ripped off by someone claiming to be who they are not. The victim of an identity theft scam has been ripped off by someone claiming to be that victim.

7. *Id.* at 4. Thirty-eight percent of complaints were tagged with "other." *Id.*

8. *Id.*

ure.[9] The 2002 Steven Spielberg movie *Catch Me if You Can,* based on the autobiography of Frank Abagnale, Jr., documented Abagnale's false impersonation of an airline pilot, an attorney, and a physician, among other personas.[10] More recently, an entire television series, *Imposters*, aired for two seasons on the Bravo network.[11] The protagonist of this show was a "persona-shifting con artist" romance scammer pursued by "a trio of her recent, heartbroken victims."[12]

Impostors have faked credentials to induce a major research university into hiring them as a senior administrator,[13] fooled the media into covering ridiculous fake stories[14] (long before the emergence of the "fake news" concept-meme), and impersonated government officials and new eyewitnesses to prank broadcasters into putting them on the air.[15] Whether for money, thrill-seeking, or purposes of performance art, determined impostors can use similar authority and confidence to achieve their ends. People want to believe their stories, or they choose to believe their stories because they seek heuristics to enable them to decide about whom to listen or assign credibility.[16] Though imposture and misuse of authority presents all sorts of problems, I focus here on the fraudulent portrayal of identity to scam consumers out of their money.

---

9. *See generally* F. SCOTT FITZGERALD, THE GREAT GATSBY (1925).

10. CATCH ME IF YOU CAN (Dreamworks Pictures 2002).

11. *Imposters*, IMDB, https://www.imdb.com/title/tt5212822/ [https://perma.cc/8339-6ACP].

12. *Imposters: Cast & Info*, BRAVO, https://www.bravotv.com/imposters/about [https://perma.cc/F9BD-AUA8].

13. Falsely claiming to hold advanced degrees from Tufts University and service as a Navy SEAL, a highly-paid senior vice president for administration served as top adviser to the president of Texas A&M University for over a year, until he was caught. Vimal Patel, *Texas A&M Administrator Resigns amid Questions over Resume*, THE EAGLE (June 18, 2010), https://www.theeagle.com/news/a_m/a-m-administrator-resigns-amid-questions-over-resume/article_b8fddfb5-95d9-58db-886d-1b1251b04a45.html [https://perma.cc/EX3R-8L9A]. Coincidentally, the author of this article briefly worked with this man in the private sector in the 1990s and completely believed that he held these degrees from Tufts and that he had served as a Navy SEAL.

14. *See generally* Margalit Fox, *Alan Abel, Hoaxer Extraordinaire, Is (on Good Authority) Dead at 94*, N.Y. TIMES (Sept. 17, 2018), https://www.nytimes.com/2018/09/17/obituaries/alan-abel-dies.html (describing Alan Abel's successful efforts to garner news coverage for his hoaxes, including creating "Yetta Bronstein," a fake candidate for the 1964 presidential election, a false claim that he won the New York state lottery, the creation of an advocacy group that in the name of decency would cover up the private parts of animals, and faking his own death and convincing the *New York Times* to run the obituary).

15. *See* Paul Farhi, *Prank-call Legend Captain Janks Is Still a Nemesis of News Outlets*, WASH. POST (July 30, 2014), https://www.washingtonpost.com/lifestyle/style/prank-call-legend-captain-janks-is-still-a-nemesis-of-news-outlets/2014/07/30/a9ad9134-175e-11e4-9e3b-7f2f110c6265_story.html [https://perma.cc/6JWA-36VS].

16. *See* Miriam J. Metzger, Andrew J. Flanagin & Ryan B. Medders, *Social and Heuristic Approaches to Credibility Evaluation Online*, 60 J. COMMC'N 413 (2010).

Historian Edward Balleisen observed that the consummation of commerce, including consumer commerce, "depend[s] on trust in far-flung counterparties across lengthening divides of space."[17] The "complexity" of transactions and this general need for social trust has always been ripe for exploitation by those who maintain asymmetric information, and consumers would expect a seller or authority figure, or one purporting to be such, to have that asymmetric information.[18] Impostor scams rely on the premise that consumers trust those who seem to know more about a problem than they do. Swindles "have been especially evident in sectors dominated by complex products or services and characterized by transactions among strangers."[19]

According to Balleisen, "the staying power of the dominant forms of deception reflects enduring dilemmas about whom and what to trust in a complex, integrated economy shot through with inequalities of access to information."[20] A scammer pretending to be affiliated with Microsoft, perhaps by spoofing Caller ID, or simply, for example, claiming to be from Microsoft, would appear to have asymmetric information; that is, the scammer counts on having more information than the target. The trust engendered can be exploited by scammers who are trying to gather personal information or sell a phony fix. These common and "enduring psychological [consumer] vulnerabilities" and "cognitive and emotional susceptibilities" have forced "industrialized and industrializing societies on every continent . . . [to] confront[] . . . commercial misrepresentation."[21]

Balleisen centers his analysis on the "modern problem of trust in the marketplace."[22] He points to more than century-old journalistic accounts observing that there was a "perennial crop of fools" always falling for "plausible cheats."[23] In 1859, one journalist wondered how "the man of to-day, with all the lights of the past to guide him, is just as much of a credulous idiot as at any time since the fall of Adam?"[24] In 1923, however, a reformed swindler observed that no amount of education could defeat these schemes.[25] William H. Crosby, in the book, *Confessions of a Confidence Man,* noted that "[e]very few months the newspapers and periodicals expose some

17. BALLEISEN, *supra* note 1, at 5.
18. *Id.* at 5.
19. *Id.* at 16.
20. *Id.* at 14.
21. *Id.* at 5.
22. *Id.* at 23–33.
23. *Id.* at 23.
24. *Id.*
25. *Id.*

sort of bunko game. . . . The people are much better educated than they used to be . . . . But the confidence game is greater than ever . . . ."[26] Perhaps people aren't "credulous idiot[s]"—they are rational actors who depend on a measure of trust to play in the commercial economy.[27] The schemes may change, but the psychology of scams does not.

In the nineteenth century, advancements in communication and transportation enabled the geographic scope of transactions to expand, thus putting an increased number of strangers into contact with other strangers.[28] More frequently, consumers were transacting with others whom they knew by reputation on financial and credit matters, investment opportunities, or consumer items.[29] Improvements in transportation likely fueled the advancement of being able to work speedily through the mail.[30]

In an ever-dispersed transactional environment still devoid of name brands, firms or scammers could take advantage of consumers more readily because "exacerbated inequalities in access to pertinent economic information"would make assessing quality more difficult for retailers.[31] The very development of brands, which was intended to instill consumer trust and confidence in their transactions with distant players, was also used as a tool by scammers. Balleisen notes that the rise of brands reacted to a need for assessment of quality in the developing national marketplace, where reputation could be harder to assess.[32] Like every conceptual innovation, the rise of brands "spawned new opportunities for misrepresentation and fraud. . . . so as to carry out fraud against economic neophytes and sophisticates alike."[33]

Even with modern market evolutions, as a whole, technological solutions cannot evade the fundamental structure of impostor fraud, evident since Herman Melville's time. Melville observed that information asymmetries in the market afforded a blueprint to swindlers who realized that in order to pull off a fraud, they "must

---

26. EDWARD H. SMITH, CONFESSIONS OF A CONFIDENCE MAN 9 (1923); BALLEISEN, *supra* note 1, at 23.

27. BALLEISEN, *supra* note 1, at 23.

28. *Id.* at 24.

29. *Id.* at 24.

30. Richard Sears of Sears, Roebuck & Co. tangled with fraud accusations from the Post Office in 1894. The Post Office refused to deliver return correspondence to Sears as a means to stop what they had considered to be fraudulent activity. *Id.* at 3–4. Though misguided in this instance, the Post Office took initiative as an intermediary chokepoint for fraud, and I later contend that the key to slowing down impostor fraud will be to shift responsibility to the stewards of similar chokepoints.

31. *Id.* at 24.

32. *See id.* at 26.

33. *Id.*

look the part, possess the right props, [and] know the right cues."[34] Melville may have operated in a time where "Spanish prisoner" scams, discussed below in Section I.B, dominated, but he might recognize the structure of the robocall operation that mimicked Microsoft or the IRS. The "Indonesian Hollywood" scam, discussed in Section I.B, might not have surprised him one bitThe means, the stories, and the instrumentalities of fraud change, but "social mimicry" efforts never cease and seemingly never fail to find success.[35]

The dramatic advancements and changes in communications over the past twenty years have been just as transformative as the nineteenth-century changes in consumer markets. The nineteenth century first brought the telegraph, and later the telephone,[36] and speedier and cheaper mail,[37] all of which facilitated imposture. Twenty-first-century advancements offer similar opportunities for the advancement of impostor schemes. The Internet allows people falsely to claim affiliation with government entities, including law enforcement and legitimate businesses, and to connect using false personas through dating and social media applications.[38] The now close-to-zero cost of long-distance telephone calling, a fairly new phenomenon,[39] as well as the ease of money transfer facilitated by the proliferation of new payment devices like gift cards[40] have also moved imposture forward by a leap.

---

34. *Id.* at 27.

35. *Id.* at 29.

36. For a comprehensive understanding of the development of communications technology during this period through the early internet, see JOHN BRAY, THE COMMUNICATIONS MIRACLE: THE TELECOMMUNICATION PIONEERS FROM MORSE TO THE INFORMATION SUPERHIGHWAY (1995).

37. *See* Fred J. Romanski, *The Fast Mail: A History of the U.S. Railway Mail Service*, PROLOGUE MAG., Fall 2005, https://www.archives.gov/publications/prologue/2005/fall/fast-mail-1.html [https://perma.cc/WU6V-JJTP] (describing the role of the railways in the development of postal services).

38. *See infra* Section I.C.

39. *See Freeing Up the Telephone*, THE ECONOMIST (Dec. 1, 2015), https://www.economist.com/science-and-technology/2015/12/01/freeing-up-the-telephone [https://perma.cc/SA9T-DYX6] (attributing the historic and recent drops in cost both to technological innovation and competition, particularly from VoIP).

40. Cyndie Martini, *Gift Cards: Everyone's Favorite Gift, Including Criminals*, CPO MAG. (Nov. 22, 2019), https://www.cpomagazine.com/cyber-security/gift-cards-everyones-favorite-gift-especially-criminals/ [https://perma.cc/P8NF-Z7PC] (discussing growth of gift cards and associated fraud).

B. *The Past and Present of Impostor Scams: New Dogs Learning Old Tricks*

Impostor scams have a rich heritage and, in many ways, have retained their original form.[41] They were so established by the late nineteenth century that contemporaneous news accounts referred to these scams as resurgences of an already old problem. An 1898 *New York Times* article described the *return* of an impostor scam, one that had acquired the name, "the Spanish [P]risoner."[42] At that point, the scheme had become regarded as one of the more successful artifices for swindling people out of their money. "As it . . . worked in two countries[,] the detection and punishment of the operators are practically impossible, especially as the victims rarely complain,"[43] and the *Times* expressed suspicion that local authorities overseas may have been in cahoots with the scammers.[44]

The crux of the Spanish prisoner scheme will sound similar to many that we see today, albeit using different communications mediums and methods of payment. In the Spanish prisoner scheme, a person in the United States would receive a letter purporting to be sent from a person of seeming prominence claiming to be a prisoner overseas and explaining that the writer was imprisoned for a "political offense."[45] The "prisoner" would contact the American mark, claiming that a trusted mutual acquaintance (who, of course, could not be named for secrecy purposes) had put the prisoner in contact with the mark in order to receive help in unlocking a hidden fortune.[46] (Today, a simple Google search might prevent this racket from getting too far, but even that is uncertain.)

The "prisoner" might write that he had a daughter being held for "board" by a boarding school overseas, but that the prisoner had a stash of money in the false bottom of a trunk being held in pawn.[47] If the American could send money to a trusted overseas associate to secure the trunk, the money inside the trunk could be

---

41. Edward Balleisen's comprehensive tome details the history of fraud in America and the constant dynamics that have driven—and continue to drive it. *See* BALLEISEN, *supra* note 1. However, Balleisen explicitly "steer[s] clear of [discussing] most of the classic swindles directed at individuals by con artists" to focus on business fraud. *Id.* at 10. He severs off "bunco steering" (inducing people to play "rigged game[s] of chance") and the "many types of advanced fee scams," for example. *Id.* Even though he steers clear of direct discussion, much of Balleisen's work applies to the impostor scams, too, as I discuss *infra*.

42. *An Old Swindle Revived*, N.Y. TIMES, Mar. 20, 1898, at 12, https://timesmachine.nytimes.com/timesmachine/1898/03/20/102108294.pdf [https://perma.cc/F2JA-2MJ9].

43. *Id.*

44. *See id.*

45. *Id.*

46. *Id.*

47. *Id.*

used to free the daughter, and of course, the American would get to keep a substantial portion of the money for their kind service.[48] A skilled scammer could find a number of ways to manipulate and extract more money from a mark, once hooked. Similar "advance fee" scams have emanated from places like Nigeria using email and social networks,[49] making it apparent that modern scammers may have updated the scheme, but they certainly did not invent it. Perhaps an old dog cannot be taught new tricks, but new dogs can be taught old tricks—and modernize and improve them.

Like some of today's schemes, as the *Times* reported, the Spanish prisoner impostor scheme typically operated in two countries, making enforcement difficult. Today's impostor fraud has accelerated due to the plunging costs of communication with potential victims and the continued ease of finding payment mechanisms to facilitate the scheme.[50] Apparently, devising a sympathetic story, mixed with an opportunity to make money, has a fundamental timeless appeal. Again, even before the turn of the twentieth century, the *Times* had reported that the Spanish Prisoner scheme was already decades old and difficult to address.

It may prove tempting to conceive of impostor fraud as a phenomenon that only preys on the naïve or vulnerable populations like the elderly,[51] but such conclusions are mistaken and serve to diminish appreciation for the absolute power of impostor fraud. Impostor schemes, when artfully designed, can hook an array of sophisticated people motivated by fear or by the same core desire to leap at opportunities for success.

---

48. *Id.*

49. *Nigerian Letter or 419 Fraud*, *Scams and Safety*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/scams-and-safety/common-fraud-schemes/nigerian-letter-or-419-fraud [https://perma.cc/7MVJ-QWTQ].

50. Old-fashioned letter writing outreach, however, apparently never completely goes out of style, despite the labor-intensiveness and postage expense. Professor Eric Goldman of Santa Clara Law School shared a handwritten letter that he recently received that originated in Uganda. *See* Letter from "a/k/a likely scammer" to Professor Eric Goldman (July 17, 2018) (on file with author). The letter purported to be from a young, female student who had been forced to drop out of tailoring school because after her father's death, she was unable to continue to afford tuition. The letter seeks Professor Eric Goldman's charity to help her complete school, promising nothing in return. My cursory research into her plea for help revealed that there was a website for the tailoring school and the church that appeared to verify elements of the story, but the contact information on the website did not mesh with what was in her letter. Although it is possible that this letter writer does exist and suffers from these circumstances, a recipient would have to take a leap of faith if he were to send money per the instructions.

51. *See* FED. TRADE COMM'N, *supra* note 2, at 13 (showing that fraud as a general category is reported at all age groups, and perhaps more likely to be reported by younger demographics).

Consider the recent case of the "Indonesia Showbiz" scam,"[52] also known as the case of the "Hollywood Con Queen."[53] In this impostor fraud iteration, entertainment industry participants had been targeted by a scammer conducting an elaborate impersonation of prominent female studio executives via telephone, text messages, or email. The scammer lured the victims to travel to Indonesia at their own expense to follow up on an attractive job offer. A "driver" would meet the target in Indonesia and then fleece the victims for cash for driving services and other services until the target realized they were a mark. The scam has taken another turn, perhaps toward what could also look like a setup of sexual blackmail.[54] The Hollywood Con Queen scam (or scammers) has launched impersonations of "nearly two dozen" people and lured "dozen[s]" of victims, enough to warrant the FBI creating a webpage for victims.[55]

New dogs have indeed learned the old tricks and have occasionally honed them into spectacular acts. As I detail below in my discussion of scams often delivered through robocalling, many of the common impostor scams reported to federal and state authorities involve similar elements. They frequently include an overseas component that shields scammers from law enforcement, and they cruelly manipulate human hopes for a financial or emotional windfall or to instill great fear in their targets, all to induce a cash transfer.

C. *Impostor Scams Today*

The Spanish prisoner and Indonesia Showbiz scams provide colorful examples of impostor fraud, but impostor fraud has become a routine today. What is modern impostor fraud and how does it differ from other categories of fraud? The FTC Consumer Sentinel describes impostor fraud as where "[s]omeone pretends

---

52. *See* Press Release, Fed. Bureau Investigation, Seeking Victims in Indonesia Showbiz Scam Investigation (July 15, 2019), https://www.fbi.gov/resources/victim-services/seeking-victim-information/seeking-victims-in-indonesia-showbiz-scam-investigation [https://perma.cc/22KF-3UU5].

53. *See* Rhodes Murphy, *Hollywood's Mysterious "Con Queen" Is Now Impersonating Marvel Executives*, SLATE (July 15, 2019, 6:06 PM), https://slate.com/culture/2019/07/a-mysterious-con-artist-is-impersonating-female-marvel-executives-for-elaborate-sham.html [https://perma.cc/K8K2-NS64].

54. *See id.*

55. Scott Johnson, *FBI Seeks More Victims of Hollywood Con Artist After Marvel Executive Targeted*, HOLLYWOOD REP. (July 15, 2019, 7:01 AM), https://www.hollywoodreporter.com/news/fbi-seeks-more-victims-hollywood-con-artist-marvel-executive-targeted-1137712 [https://perma.cc/TKE9-JXSD] .

to be a trusted person to get consumers to send money or give personal information."[56] The Sentinel provides examples of such schemes, where each scheme offers a unique twist on the scourge. There are schemes where the scammer falsely claims a government affiliation, like law enforcement and tax authorities, or charities and private companies.[57] Impersonations of the Internal Revenue Service or of a Microsoft-related entity appear to be common flavors of that variety.[58] Some schemes involve the scammer claiming to be a known friend or relation in an emergency cash crisis.[59] Other impostors pretend to be a "romantic interest" and extract cash by exploiting that dynamic.[60] Because impostor fraudsters manufacture authority to manipulate emotions like fear, greed, and loneliness to motivate people to "transact" with them or otherwise give them money, combating impostor fraud proves somewhat more complex.

Within the category of impostor fraud reports, the Consumer Sentinel breaks them down further.[61] Though dollar losses are a significant measure, each report reflects some degree of loss to an individual, which reflects the infliction of a nonpecuniary and emotional impact, as well. Government impostor scams are the most heavily reported, accounting for nearly half of all impostor scams.[62] "Tech support" impostor scam reports tripled between 2016 and 2018, becoming the second most commonly reported impostor scam.[63] Business imposture is also on the rise, as the third most common.[64] Though friends and family and romance scams account for only ten percent of impostor scam reports, friends and family scam reports have spiked nearly fifty percent since 2016, while reported incidents of romance scams have nearly doubled.[65]

1. Government Impostors

"Government impostors" will use counterfeit authority to fake their status to appeal, for instance, to the hope of those who think they may have had the good fortune of winning a lottery, or to the fear of those who think that they might be arrested, imprisoned, or

---

56. FED. TRADE COMM'N, *supra* note 2, at 81.
57. *Id.*
58. *Id.* at 82.
59. *Id.* at 81.
60. *Id.*
61. *See id.* at 86.
62. *See id.*
63. *See id.*
64. *See id.*
65. *See id.*

sued for leaving an unknown debt, tax liability, or fees unpaid.[66] Government imposture could involve using the telephone, email, texting, or other means to inform a victim that they have won a lottery, but in order to collect the big prize, they will have to pay a service charge.[67] The impostor poses as a lottery official, the Federal Trade Commission, or even fictional agencies such as "the national consumer protection agency," or the "National Sweepstakes Bureau" as the cover of authority to require the advance payment to receive the big winnings.[68]

Government impostors are also known to use the telephone to impersonate the Internal Revenue Service, local sheriff's offices, and even judges to try to "collect" non-existent debts, threatening the victim with severe consequences for not paying.[69] These schemes, as noted below, involve wire transfers and "rechargeable money card[s]," also known as gift cards, as mechanisms for the victim to transfer money to the impostor.[70] Another common variation involves the imposture of the Social Security Administration, also via telephone.[71] The scammer poses as an agent, claiming that the victim's social security number has been "blocked" due to suspicious and nefarious activity, like use in a crime or an illegal money transfer.[72] There might be a false reactivation fee involved or an instruction to remove money out of a bank account to prevent authorities from seizing it.[73] The scammer may also threaten the consequence of discontinuation of Social Security benefits, which for many are a complete financial lifeline.[74] Imposture of a government official in these contexts often exploits the low-cost mechanism of the telephone to reach a range of vulnerable people and a set of common mechanisms to facilitate an irreversible money transfer.

---

66. *Government Imposter Scams*, FED. TRADE COMM'N, https://www.consumer.ftc.gov/articles/0048-government-imposter-scams [https://perma.cc/S8TA-CE99].
67. *Id.*
68. *Id.*
69. *See id.*
70. *Id.*
71. Jennifer Leach, *Fake Calls About Your SSN*, FED. TRADE COMM'N (Dec. 12, 2018), https://www.consumer.ftc.gov/blog/2018/12/fake-calls-about-your-ssn [https://perma.cc/3Q5J-SDAM].
72. *Id.*
73. *Id.*
74. *Id.*

2. Tech-support Impostors

Tech support scams often lure victims through outbound telephone calls and fabricated pop-up warnings on websites, where victims are told that their computer has a virus or malware that they must fix with some urgency.[75] Tech support scammers also use search-word driven web advertisements (driven off keywords around tech support) and in search engine results.[76] Their goal is to convince people to pay for technical assistance that they do not need and to solve non-existent technical problems with their computers.[77] These scammers impersonate employees at tech companies, often identifying themselves as associated with Microsoft or related entities.[78] According to the FTC, the preferred payment methods for these scammers include "wiring money, putting money on a gift card, prepaid card or cash reload card, or using a money transfer app because they know those types of payments can be hard to reverse."[79]

3. Friends and Family Impostors

Though not the highest in volume, perhaps the cruelest and most calculating of scams involves the imposture of family or friends in distress or long cons where the impostor poses as a long-distance romantic partner to steal money from a victim seeking companionship. One example of this type of scam is known as the "grandparent scam." As the AARP warns members:

> This is how the grandparent scam typically plays out: You get a call from someone pretending to be your grandchild. The person explains that he is in trouble, with a story that goes something like this: "There's been an accident and I'm_____ (in jail, in the hospital, stuck in a foreign country), and I need your help." The caller adds enough details about how, what or where the emergency happened to make the story seem plausible. And the distraught caller,

---

75. *How to Spot, Avoid, and Report Tech Support Scams*, FED. TRADE COMM'N, https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams [https://perma.cc/CPZ6-92M5].
76. *Id.*
77. *Id.*
78. *See id.*
79. *Id.*

> you think to yourself, does sort of sound like your grandson or granddaughter.[80]

The social engineering escalates if the victim hooks into this story. Under some executions of this scam, the initial caller next directs the target to call another person who will impersonate an authority figure like a physician, an attorney, or a law enforcement official, who will offer more of a story.[81] The use of an inbound telephone number and authority enables the impostor to carry the deceit further because, as one FTC lawyer put it, "[t]his makes it seem more real when you call and talk to the *authority*."[82] Of course, the way out of the jam offered to the grandparent to rescue their grandchild is to send or wire money immediately—with a message relayed: "Don't tell Mom and Dad!"[83] Sometimes, the victims will even desperately send cash to the scammers.[84] The "grandparent" victim may be led to believe that their relative needs payment to a hospital for urgent treatment, or to an authority like a lawyer or law enforcement official to keep their impostored grandchild out of jail.[85]

Unlike the other scams, which seem to strike broadly, using massive low-cost telephone outreach operations, scams involving impersonation of family, friends, and romantic interests may require the scammer to invest more in cultivating and grooming individual targets. Some of the victims can indeed be hooked at random because "these scammers are experts at impersonating people they've never even met . . . . [T]hey may simply wait for their target to use a name–'Steve, is that you?' " and take the impersonation from there.[86] Some scammers buy lists of people who have been easy marks before or older people who might fall prey to this type of operation.[87] Others use information that may be available from social media sites, where people put their families on open display with information about names, relationships, and locations for scammers to exploit the dynamics with a high degree of credibility.[88] When scammers add urgency and safety of a loved one to this

---

80. Stacy Colino, *Beware of Grandparent Scam*, AARP, https://www.aarp.org/money/scams-fraud/info-2018/grandparent-scam-scenarios.html [https://perma.cc/VZL9-MBCV].
81. *Id.*
82. *Id.*
83. *Id.*
84. Emma Fletcher, *New Twist to Grandparent Scam: Mail Cash*, FED. TRADE COMM'N (Dec. 3, 2018), https://www.ftc.gov/news-events/blogs/data-spotlight/2018/12/new-twist-grandparent-scam-mail-cash [https://perma.cc/N2KK-D2SF].
85. Colino, *supra* note 80.
86. Fletcher, *supra* note 84.
87. Colino, *supra* note 80.
88. Fletcher, *supra* note 84.

dynamic, "critical thinking faculties are just not the way they are normally."[89] To the scammer who might be operating on a portfolio of marks, the only cost to losing control of such a scheme is the opportunity cost, but the emotional and financial costs to the mark are substantial.

The payment schemes for this scam are typical of the others, including wiring money and the use of gift cards. This particular scam, however, may be evolving toward cash payment, delivered through the mail or overnight services.[90] Perhaps cash has proven to be an easier mechanism for extracting money because the older segments of the population might not have access or as much familiarity with newer payments systems or might not have the ease of leaving home. Some victims have been instructed to do quite specific things with the cash, like "divid[ing] the bills into envelopes and plac[ing] them between the pages of a magazine" before sending out the payment,[91] perhaps, one speculates, for scammers to avoid detection if the cash was being shipped overseas. Scamming people out of cash currency may prove to be the most difficult system for policymakers and institutions to fix, so extra enforcement vigilance may be required here.

4. Romance Impostor Scams

Romance scams are yet another impostor scam, except that instead of using the cover of authority, the scammer assumes a false identity and cultivates a relationship with their mark, often online. This is a modern-day version of in-person scams where the scammer would invest heavily and at greater risk to swindle and deceive people *face-to-face*, in what Jill Hasday has extensively documented as "an abundance of intimate deception."[92] This recent version, largely executed through online dating, involves less in-person risk of detection and permits the scammers to access and work on more victims simultaneously. Of note, online dating has become a leading avenue for how couples meet in the United States, so, of course, enterprising impostors will follow along for the ride.[93]

---

89. Colino, *supra* note 80.

90. Fletcher, *supra* note 84.

91. *Id.*

92. JILL ELAINE HASDAY, INTIMATE LIES AND THE LAW 6 (2019). Hasday documents a number of contexts for financial fraud among intimates who know each other in person. *Id.* at 16.

93. *See generally* MICHAEL J. ROSENFELD, REUBEN J. THOMAS & SONIA HAUSEN, DISINTERMEDIATING YOUR FRIENDS: HOW ONLINE DATING IN THE UNITED STATES DISPLACES OTHER WAYS OF MEETING (2019), https://www.pnas.org/content/116/36/17753/tab-figures-data [https://perma.cc/56PR-SNWX].

The FTC recently warned the public about this scam on Valentine's Day, of course.[94] "What do we mean by romance scams? We're not talking about the person you thought was 'the one' but ended up being a dud. We're talking about people you meet online, who lavish you with attention . . . and then ask for money."[95] The scammers source their targets from social media and dating sites and go to work from there, using fake profiles or misappropriating the identity of a real person.[96] Again, the scammers seek their "gifts" by wire transfer or, appropriately enough, via gift cards.[97] The pretext for needing the money might be an emergency or for a trip to meet up, the former of which is contrived, the latter never to happen.[98] The ability to scale this scam is more challenging for the swindler than blast robocalling and the time investment in each target is larger. The potential return from this type of scam, however, is apparently higher than the other operations.[99] The median reported loss on all impostor scams is $500,[100] while the median loss from romance scams was $2,600, over five times as much.[101]

On the whole, two themes run throughout the recent rise of the common impostor scams. First, communication technologies and platforms have made the process of imposture less risky and less expensive than ever before. Second, payment system innovations, particularly the rise of pre-paid gift cards, which can function as cash, have also facilitated the ability of impostors to receive payment. The core structure of the scams, which use fear, greed, and in some cases, *loneliness*, remain the same as they did in the Spanish prisoner era, but the ability to seek potential targets and complete their victimization has become much easier, less costly, and less risky, which explains their rise.

II. IMPOSTOR SCAM ECONOMICS

Like any other economic activity, if the costs and risks of engaging in scams drop and the returns from scams grow or even hold steady, more scams will likely surface. Incentives will drive decision

---

94. Lisa Weintraub Schifferle, *Romance Scams Will Cost You*, FED. TRADE COMM'N (Feb. 12, 2019), https://www.consumer.ftc.gov/blog/2019/02/romance-scams-will-cost-you [https://perma.cc/B69Y-29TB].
95. *Id.*
96. *Id.*
97. *Id.*
98. *Id.*
99. *Id.*
100. FED. TRADE COMM'N, *supra* note 2, at 8.
101. Schifferle, *supra* note 94.

making. In the analog era, the "classic" impostor scam often required the scammer to have a physical presence, which created both risk of detection and punishment and required more time investment. In the modern era, the economics of scamming improved as developments in communications and payment systems enabled scammers to scale up their activities inexpensively. This lowers costs and expands the reach of scammers, while increasing their distance from their victims and, thus, lowering their risk of directly confronting enforcement. The economics explain why impostor scams have proliferated and prove critical to understanding how to slow them down. I discuss next how the economics and use of technology evolved over the past several decades.

A. *Economics of "Classic" Impostor Scams*

The economics of a pre-modern impostor scam emerges crisply and colorfully from the facts of a 1957 New Jersey agency law case that has become a favorite of a generation of Business Associations' instructors and students,[102] *Hoddeson v. Koos Bros.*[103] This case typifies the architecture of an impostor scam, and the common law provided a solution—pushing the cost onto the intermediary for negligently allowing the scammer to use their instrumentality and legitimacy to pull off the scam.[104] The impostor scam that befell the shopper, Mrs. Hoddeson, at a retail furniture store, Koos Bros., in Rahway, New Jersey serves as an ancestor, perhaps, to the tech-support scam, where the scammer purports to work for a company, but does not. The physical store serves as much as an instrumentality and venue for the transfer of payment as modern payment systems do in other scams.

Before presenting the facts, the judge observed that impostor scams were nothing new, but always evolving: "The occurrence which engages our present attention is a little more than conventionally unconventional in the common course of trade. . . . A digest of the story told by Mrs. Hoddeson will be informative and perhaps admonitory to the unwary shopper."[105]

On a previous visit to Koos Bros., Hoddeson had scouted out some pieces of bedroom furniture on display.[106] As the court observed, "it has been said that 'the sea hath bounds but deep desire

---

102. *See* WILLIAM A. KLEIN, ET AL., BUSINESS ASSOCIATIONS, CASES AND MATERIALS ON AGENCY, PARTNERSHIPS, LLCS, AND CORPORATIONS 29–32 (10th ed. 2018).
103. 135 A.2d 702 (N.J. Super. Ct. App. Div. 1957).
104. *Id.*
105. *Id.* at 703.
106. *Id.*

hath none' " and Hoddeson had received a $165 gift from her mother to indulge her desire to buy the furniture.[107] Hoddeson took this gift money, and one morning, brought her aunt and four children to the store to make the furniture purchase.[108] Instead of meeting with a salesperson, they encountered an ingenious impostor carrying all sorts of airs of authority and the aura of belonging to the store.[109]

The court recounted that "[u]pon entering, she was greeted by a tall man with dark hair frosted at the temples and clad in a light gray suit."[110] The tall man "inquired if he could be of assistance" and led Hoddeson and her "flock" to the display of the furniture that Hoddeson wanted.[111] Next, he wrote down a calculation of the purchase price, $168.50, after which Hoddeson gave him cash, for which she did not ask for a receipt.[112] This entire exchange took place over thirty to forty minutes.[113] The tall man informed her that the furniture she had selected and purchased was not in stock and would be delivered to her the following month.[114] Unfortunately for Hoddeson, the furniture would never arrive and the store claimed to have no record of the sale.[115]

In the aftermath, the store owners held fast to their assertion that the sale had been made by an impostor and not by one of their salesmen.[116] In fact, the store paraded the salesmen in that department past Hoddeson and her aunt, in something like a police lineup, offering the "opportunity to gaze intently" at them.[117] They were unable to definitively identify any of them as the aforementioned "tall man" who took the money—and the one who came closest to suspicion had supposedly been on vacation during Hoddeson's visit.[118] All in all, however, the jury found that Hoddeson "established by a preponderance of the credible evidence that the $168.50 was paid in fact to an *employee* of the defendant," and the trial judge concluded that the evidence warranted such a finding.[119]

---

107. *Id.* Though the court appears to set Hoddeson on a course where she could be made whole, the tone of the opinion could be characterized as disrespectful to the scam victim.
108. *Id.*
109. *Id.* at 703–04.
110. *Id.*
111. *Id.* at 704.
112. *Id.*
113. *Id.*
114. *Id.*
115. *Id.*
116. *Id.* at 704–05.
117. *Id.*
118. *Id.*
119. *Id.* (emphasis added).

On appeal, Koos Bros. argued that "there was a deficit of evidence to support the conclusion that a relationship of master and servant existed between the man who served and received the money from Mrs. Hoddeson and the defendant company."[120] The court agreed with Koos Bros., finding that the plaintiffs had failed to allege and prove the existence of an agency relationship between the "tall man" and the store.[121] Therefore, Hoddeson failed to allege that the "tall man" had express, implied, or actual authority to establish privity of contract. The appellate court reversed the trial court on this point.[122] "Assuredly, the law cannot permit apparent authority to be established by the mere proof that a mountebank [or 'humbugger'] in fact exercised it."[123]

For Hoddeson, however, all was not lost. Though the court reversed on the grounds prosecuted in *assumpsit* by the plaintiff, the court "recommended . . . the allowance of a new trial with the privilege accorded the plaintiff to reconstruct the architecture of [the] complaint"[124] in order to plead "agency by estoppel" or "tortious dereliction of duty owed to an invited customer."[125] The court hypothesized that if the facts were as alleged, "would the defendant be immune as a matter of law from liability for the plaintiffs' loss?"[126] The court answered with an approach that warrants some modern extension:

> The tincture of estoppel that gives color to instances of apparent authority might in the law operate likewise to preclude a defendant's denial of liability. . . . [W]e have in mind . . . the unique occurrences where solely through the lack of the proprietor's reasonable surveillance and supervision an impostor falsely impersonates in the place of business an agent or servant of his.[127]

The court noted that a proprietor's duties to customers "certainly . . . encompass more than the diligent observance and removal of banana peels from the aisles."[128] Further, the court articulated a rationale for shifting the costs of deception from the consumer to the department store. "The rule that those who bargain without

---

120. *Id.* at 705.
121. *Id.* at 705–06 .
122. *Id.* at 706.
123. *Id.*
124. *Id.* at 707.
125. *See id.* at 706–07.
126. *Id.* at 706.
127. *Id.* at 706–07.
128. *Id.*

inquiry with an apparent agent do so at the risk and peril of an absence of the agent's authority has a patently impracticable application to the customers who patronize our modern department stores."[129] The court confronted the new landscape of the modern department store, recognized the possibility of newfound impostor scams, and put the burden on the department stores to absorb losses—thus, putting the incentives for mitigating this fraud into the laps of these stores.

Just as we note that new technologies and new consumption and payment mechanisms enable impostors today, in 1957 this court noted that "modern department stores," presumably with their broad layouts, presented new challenges for consumers, who could be taken in by a "mountebank" roaming the floor in search of vulnerable customers.[130] Indeed, the *Hoddeson* court observed that "old questions appear in new styles."[131] This case noted that such impostor occurrences had not been commonly reported in decisions in the early half of the twentieth century, but had occurred nonetheless. Among them: impostors posing as hotel, railroad, and parking lot personnel, purporting to have the authority to hold guest, passenger, and automobile property for safekeeping.[132]

In these cases, the courts held accountable the entities whose personnel were impersonated for making the defrauded property owner whole. Given a choice between victims, the courts in essence lay the responsibility for exercising care at the feet of those who failed to exercise due care. The *Hoddeson* court left open the possibility that the plaintiff herself could have been at fault, though on the known facts, that result would seem unlikely.

A few things about this previous generation of impostor tactics repeat with the problems of impostors today. First, these particular impostors had to operate in close quarters to the victims, of which there were two: the victim losing the money and the entity suffering from being impersonated. Certainly both Hoddeson and Koos Bros. were displeased with how events unfolded that day. Hoddeson lost money and Koos Bros lost a sale to the same thief. So, who should bear the loss?

Data collected in the FTC Consumer Sentinel inform us that we may have turned the corner into a different landscape that requires more emphasis on shifting the prevention burdens onto

---

129. *Id.* at 707.
130. *Id.*
131. *Id.* at 703.
132. *See* Kanelles v. Locke, 12 Ohio App. 210 (Ohio Ct. App. 1919) (impersonating a hotel clerk); Miltenberger v. Hulett, 175 S.W. 111 (Mo. Ct. App. 1915) (impersonating railroad transfer agent); Luken v. Buckeye Parking Corp., 68 N.E.2d 217 (Ohio Ct. App. 1945) (impersonating parking lot attendant).

those who are in a better position to mitigate impostor damage. The technology and payment mechanisms that have enabled impostors to increase their scale, and lower the costs and risks of operation, are ultimately controlled by identifiable lower-cost avoiders. For example, telecommunications providers have benefitted from technology that has lowered the costs of international outbound calling, and this has unwittingly, perhaps, enabled fraud. Popular payment mechanisms like gift cards have yielded benefits to retailers but have also presented impostors and scammers with a clean mechanism for stealing money from consumers. The means and locations for risky transactions have shifted, thus measures to address impostor fraud must shift.

B. *The Economics of "Modern" Impostor Scams*

Classic impostor scams operated successfully in a world where reaching victims at scale was expensive and often riskier. Technology and the overall improved economics of imposture have recently driven an acceleration of the problem. But this "technology as accelerant" dynamic is nothing new.

It did not take long for the criminally enterprising to figure out that a new invention called the telephone provided an opportunity to defraud people. The Patent Office attributes the 1876 telephone invention to Alexander Graham Bell.[133] By 1878, the first telephone switching network had been deployed as a Bell franchise in Connecticut, with the publication of the first phone directory also following that year.[134] As a Chicago police inspector observed in 1888, after pondering the aftermath of an early telephone scam, "The educated criminal skims the cream from every new invention, if he can make use of it."[135] The telephone was apparently no exception, and reports of telephone impostor fraud arrived almost within a decade of the invention.

Though the means and methods involved physically commandeering a phone, the elements of a modern "grandparent"-type

---

133. *See Who Is Credited With Inventing the Telephone?*, LIBR. OF CONG. (Dec. 19, 2019), https://www.loc.gov/everyday-mysteries/item/who-is-credited-with-inventing-the-telephone/ [https://perma.cc/9MZ6-6BMP].

134. Kat Eschner, *The First Telephone Book Had Fifty Listings and No Numbers*, SMITHSONIAN (Feb. 21, 2017), https://www.smithsonianmag.com/smart-news/first-telephone-book-had-fifty-listings-and-no-numbers-180962173/ [https://perma.cc/Q9NW-4A79].

135. *See* Simon van Zuylen-Wood, *How Robo-call Moguls Outwitted the Government and Completely Wrecked the Do Not Call List*, WASH. POST (Jan. 11, 2018), https://www.washingtonpost.com/lifestyle/magazine/how-robo-call-moguls-outwitted-the-government-and-completely-wrecked-the-do-not-call-list/2018/01/09/52c769b6-df7a-11e7-bbd0-9dfb2e37492a_story.html [https://perma.cc/83YY-FNUY].

hostage scam are all present in an 1888 account offered in the *Electrical Review*.[136] One weekday, a "smartly dressed" charlatan, who perhaps could be regarded as the Alexander Graham Bell of telephone impostor fraud, knocked on the door of a prominent, well-to-do trader.[137] Introducing himself as "Thomas Jefferson Odell," he asked the butler if he could use "the house phone."[138] Somehow, "Thomas Jefferson Odell" managed to rouse the trader on the phone at his place of business to inform him falsely that he had bound and gagged the cook, the chambermaid, and his wife.[139] "Odell" demanded a ransom of $20,000 in cash, which the trader promptly sent to an accomplice in the scheme. Of course, the trader "rushed home to find his wife in fine shape and none the wiser."[140]

The telephone-based impostor scam had arrived. The telephone offered a means to rapidly deliver a high-pressure, time-sensitive scam—with much of the concealment of any Spanish prisoner letter scheme. Of course, the Thomas Jefferson Odell gambit demanded more risk and cost to the perpetrators, requiring at least two personal physical appearances to create the imposture. The target had to be carefully selected, and the execution had to be perfect, because the entire imposture, including the cash transfer, was happening right in Chicago, not originating from a distant country. As a scamming device for impostors, however, the exploitation of the telephone would take some time—and additional technology—to reach a greater scale. In the time of Thomas Jefferson Odell, not many people had phones, so accessing a phone by deceit would be accordingly difficult. As access to telephones increased, and as calling became less expensive, the form of imposture, as well as the method, changed. As payment transfer could be done from a distance, making the handoff less risky, imposture changed, too.

What happens when scammers take the power of the impostor and deploy wider-reaching, lower-cost technology that also enables them to remain at a distance? Robocalling has proven to be a prolific means for spreading impostor scams. By one account, robocalls "have been around since at least the 1980s, when someone first thought to attach a tape deck to a phone."[141] A classic scene in

---

136. *Id.*
137. *Id.*
138. *Id.*
139. *Id.*
140. *Id.*
141. Alex W. Palmer, *On the Trail of the Robocall King*, WIRED (Mar. 25, 2019, 6:00 AM), https://www.wired.com/story/on-the-trail-of-the-robocall-king/ [https://perma.cc/A96Z-EULK].

the 1983 movie WarGames revealed the way an enterprising teenage hacker could program his home computer to dial every phone number with a certain prefix until a modem answered.[142] But delivering a message to recipients was more complicated in that analog time because "the hardware was clunky, expensive, and difficult to operate."[143] Audio cassettes, which carried and delivered the outbound messages, required rewinding after use and suffered from wear and tear.[144] Of course, this all changed with the arrival of digital technology, which made robocalling substantially less expensive and easier to implement.[145]

The bombardment of preprogrammed unsolicited telephone calls, in an era before Caller Identification (Caller ID) and when people regularly answered their phones, led to a collective social outcry.[146] Congress answered these complaints with a flurry of legislation. Senator Ernest "Fritz" Hollings deemed robocalls "the scourge of modern civilization," and apparently Americans concurred with the sentiment, "despite the competing scourges of war . . . or the spread of AIDS."[147] Senator Hollings, who cosponsored the Telephone Consumer Protection Act (TCPA) of 1991,[148] lamented that these calls "wake us up in the morning, they interrupt our dinner at night, they force the sick and elderly out of bed, they hound us until we want to rip the telephone right out of the wall."[149] Bear in mind, Senator Hollings was ranting about robocalls long before scammers began to weaponize them by using the instrument of the robocall to defraud people out of their money and, in some cases, jeopardize public safety by overwhelming telecommunications systems.[150] As discussed later, much of the same sort of activity would eventually shift into email systems as that communications mechanism matured.

Scammers have uncovered the ability to mesh digital technology with automated telephone calling, enabling them to conduct scams on a massive scale at a low expense. Thus, impostor scams are cost-

---

142. *See* WARGAMES (United Artists 1983).
143. Palmer, *supra* note 141.
144. *Id.*
145. *Id.*
146. *See, e.g.*, Barry Meier, *Intruder on the Phone: Ending a Sales Talk Before It Begins*, N.Y. TIMES (Mar. 3, 1990), https://www.nytimes.com/1990/03/03/style/consumer-s-world-intruder-on-the-phone-ending-a-sales-talk-before-it-begins.html [https://perma.cc/5KZW-GJ3U] (as one telemarketing call recipient put it, telemarketing callers "are very considerate, . . . [t]hey only call during the dinner hour when I am there").
147. Palmer, *supra* note 141.
148. Pub. L. No. 102-243 (1991) (codified at 47 U.S.C. § 227).
149. 137 CONG. REC. 30821 (1991) (statement of Sen. Hollings).
150. The FCC first became aware of the Adrian Abramovich robocalling scheme, discussed *infra* Section III.B, when a hospital network reported major disruptions of its paging system from floods of inbound phone calls.

effective scams. Although policymakers and private entities cannot eliminate them, the ability to make impostor scams more expensive and less effective could reduce their incidence. And a significant portion of the ability to slow down and obstruct scammers must rest in the hands of private players, who ultimately control the means of communication and payment, either on their own accord to compete for customers or at the behest of lawmakers and regulators seeking to protect the public. Every solution and obstruction, of course, could be circumvented. But keeping private actors that often provide the tools that enable impostors, albeit unintentionally, at the forefront of prevention can help.

Telecommunications providers offer low-cost tools for impostors to reach an expansive field of targets, and with more reachable targets, more infliction of harm from fraud is inevitable. Perhaps regulators can require or encourage the providers of intermediary devices to take more responsibility for educating the public and their users about impostor fraud by offering more security and providing more disclosures.

III. FIGHTING IMPOSTOR SCAMS

Industry, lawmakers, and regulators have not sat on their hands while impostor fraud has grown. They have taken recent action to slow the roll of impostors, but the road ahead appears to be fairly bleak, even with measures and enforcement action already taken. Robocalling has been at the core of this scourge and addressing telephone scams has been a decades-long effort that continues to face new challenges. As noted, telephones are not the only mechanisms for scammers to communicate with their victims, so even solving this problem only solves part of the problem.

How difficult is the robocall problem to solve? According to the CEO of YouMail, Alex Quilici, the telephone scam has taken the miracle of low-cost long-distance calling to realize a nightmarish promise of AT&T's old advertising jingle that anyone can "reach out and touch someone."[151] YouMail provides robocaller blocking services.[152] Quilici observes that "a 16-person call center in India can make $75,000 per day" and these call centers span the globe—"from Florida to Guatemala to Nigeria to New Delhi to Philadelph-

151. *See* Linda Robertson, *Block those Robocalls from Scammers and Unwanted Companies. Here's How to Fight Back*, MIA. HERALD (June 15, 2019), https://www.miamiherald.com/news/local/community/miami-dade/article231323738.html; *see also* AT&T, *AT&T Reach Out and Touch Someone Commercial - 1987*, YOUTUBE (Mar. 13, 2014), https://www.youtube.com/watch?v=OapWdclVqEY [https://perma.cc/6JCN-TKRS].

152. Robertson, *supra* note 151.

ia."[153] All it takes to get a robocall operation rolling is to "get four friends together in your apartment with a laptop and make millions of calls for nothing. There's not a lot of overhead. Collect an average of $1 per robocall and your profit scales up pretty quickly."[154]

Robocallers will often use inexpensive and easily accessible telecommunications systems not just to reach people directly but also to exploit features like Caller ID to facilitate imposture. Scammers can operate from Guatemala, Nigeria, or Delhi and impersonate anyone. In other words, robocallers can make it appear that they are calling from a legitimate business, government agency, or a nearby location.[155]

In Section III.A, I discuss at length the efforts to promulgate a regulatory solution through the telecommunications sector and in Section III.B, I describe some of the more aggressive enforcement actions taken against these fraudsters. As I observe in Section III.C, many involved in these efforts share pessimism about ultimately stopping impostor fraud, which is unsurprising given the capability of scammers to innovate. The policy goal, however, should be oriented to make imposture less lucrative and as costly and risky as reasonably possible.

A. *Telecommunications Regulation*

The legislative and regulatory efforts to combat impostor fraud have focused on mitigation of the broader robocalling issue but have found limited success. These efforts have further focused on attempts to address the marriage of robocalling with manipulation of Caller ID information (also known as number "spoofing"). As scammers have moved on from using traditional telephone carriers, the technological focus has shifted to this problem. Ultimately, if these problems are to be addressed, regulators and industry must collaborate proactively to stay ahead of scammers.

The Federal Communications Commission (FCC) has recognized the trouble resulting from Caller ID spoofing which tricks call recipients into thinking scammers and other callers are someone who they are not.[156] The FCC warns that "spoofing is often used as part of an attempt to trick someone into giving away valua-

153. *Id.*
154. *Id.*
155. *Caller ID Spoofing*, FED. COMMC'NS COMM'N, https://www.fcc.gov/consumers/guides/spoofing-and-caller-id [https://perma.cc/9BVN-97EV].
156. *Id.*

ble personal information so it can be used in fraudulent activity . . . ."[157] The FTC has warned that "scammers are using fake caller ID information to trick you into thinking they are someone local, someone you trust – like a government agency or police department, or a company you do business with . . . . One scammer recently used the phone number of an FTC employee."[158]

FCC Chairman Ajit Pai "has made combatting unlawful robocalls and malicious caller ID spoofing his top consumer protection priority,"[159] labeling them a "scourge."[160] In February 2019, the FCC released a report on robocalls and caller ID spoofing.[161] The FCC noted that it has only recently begun to find effective means "to stem the tide" of robocalling by intervening with technology and changes in systems and promoting "aggressive enforcement action."[162]

Starting in 2017, the FCC focused directly on the problem, prioritizing putting a halt to "unwanted calls before they even reach consumers' phones."[163] To begin to achieve these ends, the FCC "enabled voice service providers to block certain obviously-spoofed calls, authorized the creation of a reassigned numbers database so consumers do not get calls intended for others, and pushed the industry to implement Caller ID authentication, a key to stopping spoofing."[164]

As the FCC notes, however, not all robocalls are illegal.[165] The task for policymakers is to prevent abuse of the telecommunications infrastructure, through illegal robocalls, to further curb impostor scams, while preserving avenues for legitimate automated calling. Several laws and rules prohibit the misuse of robocalling and Caller ID,[166] but the effectiveness of their enforcement stands

---

157. *Id.*

158. Andrew Johnson, *Scammers Can Fake Caller ID Info*, FED. TRADE COMM'N (May 4, 2016), https://www.consumer.ftc.gov/blog/2016/05/scammers-can-fake-caller-id-info [https://perma.cc/TUJ7-UXU6].

159. *The FCC's Push to Combat Robocalls & Spoofing*, FED. COMMC'NS COMM'N, https://www.fcc.gov/about-fcc/fcc-initiatives/fccs-push-combat-robocalls-spoofing [https://perma.cc/68Q5-HUDU].

160. FED. COMMC'NS COMM'N, CG DOCKET NO. 17-59, REPORT ON ROBOCALLS 15 (2019), https://docs.fcc.gov/public/attachments/DOC-356196A1.pdf [https://perma.cc/95RH-VGYR].

161. *Id.* at 1.

162. *Id.* at 2.

163. *See id.*

164. *Id.*

165. The FCC elaborates, "Consumers frequently associate "robocalls" with annoying calls and, indeed, unwanted calls are a perennial top consumer complaint. . . . And yet the term "robocall" covers a wide array of calls, many of which are legal, such as school closing announcements and prescription or medical appointment reminders." *Id.*

166. *See id.* at 2–3.

at odds with the recent growth of impostor scams that rely on robocalling, like tech scams.

The Telephone Consumer Protection Act (TCPA)[167] and associated Delivery Restrictions rules[168] serve to prohibit:

> [initiation of] any telephone call to any residential telephone line using an artificial or prerecorded voice to deliver a message without the prior express consent of the called party, unless the call is initiated for emergency purposes, is made solely pursuant to the collection of a debt owed to or guaranteed by the United States . . . .[169]

Many of the impostor scams use prerecorded voices to impersonate authorities in order either to generate a return call or to draw the recipient to enter a phone tree leading them to an impostor. The use of such mechanisms by impostors flagrantly violates this section of the TCPA and the accompanying FCC rules.[170]

Similarly, scammers, particularly overseas scammers, appear undeterred by laws and rules serving similar protective purposes, like the Do Not Call Implementation Act,[171] the Telemarketing Consumer Fraud and Abuse Prevention Act,[172] and the Telemarketing Sales Rule.[173] Those laws require telemarketers (although presumably it only affects the telemarketers that care about compliance) to check the National Do Not Call Registry before dialing numbers and generally prohibit deceptive practices through telemarketing.[174] Like the TCPA, these laws were intended to rein in the nuisance and deceptive marketing abuses of those who solicit business through the telephone, but they primarily serve to reach violators within the realm and reach of domestic enforcement.[175] Domestically, the fines and penalties for violating these laws and regulations can be severe when directed against those within reach of enforcement. For example, the FTC sought to collect $280 million from DISH Network and its agents for "committing more than 65 million violations of telemarketing statutes and regulations."[176]

---

167. 47 U.S.C. § 227.
168. 47 C.F.R. § 64.1200 (2020).
169. 47 U.S.C. § 227(b)(1)(B).
170. 47 C.F.R. § 64.1200(a)(1) (2020) (prohibiting the initiation of "an automatic telephone dialing system or an artificial or prerecorded voice" without consent).
171. 15 U.S.C. § 6101.
172. *Id.* §§ 6101–6108.
173. 16 C.F.R. § 310 (2020).
174. *See* FED. COMMC'NS COMM'N, *supra* note 160, at 3.
175. *See id.* at 2–3.
176. United States v. DISH Network, LLC, 954 F.3d 970, 973 (7th Cir. 2020), *cert. dismissed*, 141 S.Ct. 729 (2021) (mem.).

When directed against the overseas operation that operates an impostor scheme on a massive scale, however, these laws and regulations have no teeth.

The 2009 Truth in Caller ID Act[177] (TCIDA) offers a direct tool for combating telephone harassment and imposture scam tactics.[178] This tool only has teeth if policymakers direct resources toward enforcement, including overseas efforts to combat call spoofing. TCIDA "prohibits . . . provision of inaccurate caller identification information."[179] Specifically, it declares unlawful the practice of "causing any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value."[180]

Presumably, this broad language incorporates prohibition of the abuse of newer technologies that have proliferated, like IP-enabled voice service.[181] Many impostors use services like Skype to hide and spoof their identities.[182] But again, like the other federal statutes and rules, TCIDA only serves a purpose if enforced.

The FCC has since moved beyond the enforcement of these statutes to look for other solutions to prevent or slow down the use of telecommunications systems as tools for impostor scams. As the report summarized, "the same characteristics that make robocalls appealing to businesses also make them appealing to scammers."[183] Robocalling "efficiently and cost-effectively" enables scammers and impostors to pull off their fraud.[184] The FCC is well aware that impostor scammers "may not be deterred by the prospect of enforcement and may be especially difficult to locate."[185] As a result, the FCC "has focused on stopping illegal robocalls before they reach consumers' phones."[186]

The public may be fooled by impostor scammers because when called, they "may not have enough information to tell whether the call is wanted, unwanted, or illegal."[187] If they have Caller ID, the display may show a "spoofed" or a blocked number.[188] The recipi-

177. 47 U.S.C. § 227(e).
178. *See* FED. COMMC'NS COMM'N, *supra* note 160, at 3.
179. 47 U.S.C. § 227(e).
180. *Id.* § 227(e)(1).
181. *Id.*
182. Samantha Murphy Kelley, *The Frightening Future of Robocalls: Numbers and Voices You Know*, CNN BUS. (Apr. 6, 2019), https://www.cnn.com/2019/04/06/tech/robocalls-scam-voice/index.html [https://perma.cc/UA8M-MK7T].
183. *See* FED. COMMC'NS COMM'N, *supra* note 160, at 3.
184. *Id.* at 3–4.
185. *Id.* at 4.
186. *Id.*
187. *Id.* at 6.
188. *Id.*

ent of the call, if interested in figuring out who is trying to reach them, must answer the call or let the caller leave a voicemail.[189]

Mitigating abusive spoofing of Caller ID calls for more than a statutory solution, and the FCC has taken note of collaboration between government and industry to stop the problem.[190] The FCC has moved forward on several different fronts, which I will describe next, but still faces significant challenges in addressing impostor fraud, even with success on these fronts.[191]

The FCC has moved to expand the circumstances where voice service providers can engage in call blocking. The solution provided by this expansion, however, proves somewhat easy for the determined impostor scammer to evade. In November 2017, the FCC "authorized providers to block Do Not Originate (DNO) calls"[192] and calls originating from "invalid, unallocated, or unused" numbers.[193] Service providers were able to block the spoofing of actual IRS phone numbers, which led to a dramatic reduction in scam complaints to the IRS.[194] Ultimately, this provides an example of how impostor scammers can be slowed down by a move but not stopped. Impersonation of IRS personnel does not require a number associated with the IRS, though it certainly made the process easier for the scammers by lending credibility.

According to the FCC, voice service providers report "widespread implementation of DNO blocking, and several . . . have implemented or are implementing blocking of invalid, unallocated, and unused numbers."[195] The FCC, at long last in December 2018, adopted a rule to clarify that the wireless carriers could also take specific measures to block "robotexts" and other unwanted messaging.[196]

The FCC also took note of the wave of private innovation that enables users to employ apps and other means of call blocking,[197] observing that "[h]undreds of call-blocking apps have been developed for mobile telephones."[198] Some services block all calls that

---

189. *Id.*
190. *Id.* at 7.
191. *See id.* at 6–14.
192. *Id.* at 7 n.37 ("Do Not Originate calls are calls made from a number that the subscriber does not use to make outgoing calls and requests that calls purporting to originate from that number be blocked.").
193. *Id.* at 7.
194. *Id.* at 7 n.38. For a description of the immediate impact of this initiative, see FED. COMMC'NS COMM'N, ROBOCALL STRIKE FORCE REPORT 1 (2016), https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf [https://perma.cc/AX4J-NHQD].
195. FED. COMMC'NS COMM'N, *supra* note 160, at 7.
196. *Id.*
197. *Id.* at 8.
198. *Id.*

use Voice-over-Internet Protocol (VoIP) services,[199] a favorite of scammers.[200] For landline consumers, blocking services are offered by some carriers for a fee and by others for free. Consumers Union, the National Consumer Law Center, and the Consumer Federation of America have advocated that such services and tools should all be offered by providers for free.[201] If voluntarily adopted, however, these tools will most likely be adopted by those already wise to the impostor scams. The adopters may be looking to stamp out the nuisance of these calls, but, as noted, there are other means by which scammers can defeat these safeguards.

In addition to their engagement on call blocking, voice service providers, with a bit of a push from the FCC, have made advancements on Caller ID authentication.[202] This technology could put another technological obstacle in front of impostor scammers. As the FCC notes, "[t]he benefits of authentication are substantial: consumers and voice service providers will know that callers are who they say they are, thereby reducing the risk of fraud and ensuring that callers can be held accountable for their calls."[203] Authentication could obstruct such pernicious practices as "neighbor spoofing," which supposedly induces people to answer calls when a scammer spoofs a number that looks local, by using the same area code or prefix.[204]

A variety of private task forces and alliances have converged to develop a system that uses Caller ID authentication to stop impostor calls from reaching the caller by "confirming that a call actually comes from the number displayed in the Caller ID."[205] It turns out a technological solution that uses a "framework of interconnected standards" may exist that might put a speed bump into scamming operations[206] Appropriately, given the difficulty of weeding out these scammers, the framework has drawn upon the James Bond movie franchise for a name worthy of the role, "SHAKEN/STIR."[207]

---

199. *Id.*

200. Catey Hill, *Don't Pick Up! This Is the No. 1 Time Scammers Are Calling You*, MARKETWATCH (Dec. 18, 2018, 09:00 AM), https://www.marketwatch.com/story/dont-pick-up-this-is-the-no-1-time-scammers-are-calling-you-2017-11-22 [https://perma.cc/ZC3V-A4HF] (Spamming technology "is cheap and easy to make thanks to Voice over Internet Protocol (VoIP), which lets scammers make billions of automated calls").

201. FED. COMMC'NS COMM'N, *supra* note 160, at 8 n.43.

202. *See id.* at 8–10.

203. *Id.* at 8.

204. *Id.*

205. *Id.*

206. *Combating Spoofed Robocalls with Caller ID Authentication*, FED. COMMC'NS COMM'N, https://www.fcc.gov/call-authentication [https://perma.cc/E7F5-F2NW].

207. FED. COMMC'NS COMM'N, *supra* note 160, at 9. Fictional spy hero James Bond always orders his martinis shaken, not stirred. Karen Kaplan, *Docs Explain Why James Bond Prefers His Martinis 'Shaken, not Stirred,'* L.A. TIMES (Dec. 12, 2013), https://www.latimes.com

"SHAKEN" stands for Signature-based Handling of Asserted Information Using toKENs and "STIR" refers to the Secure Telephone Identity Revisited standards.[208]

The approach, though not as deadly as a James Bond device, strengthens security protocols to enhance the likelihood that only identified phone numbers reach recipients.[209] In essence, the protocol would only let calls through that meet the criteria for an electronic handshake. "Calls traveling through interconnected phone networks would have their Caller ID 'signed' as legitimate by originating carriers and validated by other carriers before reaching" recipients.[210] In other words, the SHAKEN/STIR framework "digitally validates the handoff of phone calls passing through the complex web of networks, allowing the phone company of the consumer receiving the call to verify that a call is in fact from the number displayed on Caller ID."[211]

According to the FCC, "SHAKEN/STIR does not authenticate the content of the call, only the identity of the caller."[212] By "identity of the caller," the FCC means the identity of the originating line. Presumably, a person could pick up a phone and make a call and pretend to be someone whom they are not and initiate a scam. Nonetheless, full implementation of SHAKEN/STIR would not only eliminate the nuisance of unlawful robocalls, but it would also create a significant hurdle for impostor scammers. The FCC set a goal to implement this system in 2019, relying on the cooperation of private industry groups and service providers.[213] But rulemaking advanced through 2020.[214] With the adoption of SHAKEN/STIR, the almost free and unfettered access to telephone call recipients would be removed as a device for scammers to use to reach large numbers of people. Or at least, until this system is defeated by other scammer methods, within telephony or without.

Indeed, Congress has recently made noise about robocalling, ultimately, moving forward with a display of bipartisanship. The 115th Congress conducted three hearings between 2017 and 2019 about

---

/science/sciencenow/la-sci-sn-james-bond-alcohol-shaken-not-stirred-20131212-story.html [https://perma.cc/RQF7-PHAW].

208. FED. COMMC'NS COMM'N, *supra* note 160, at 8.

209. *See id.* at 8–10.

210. FED. COMMC'NS COMM'N, *supra* note 206.

211. *Id.*

212. FED. COMMC'NS COMM'N, *supra* note 160, at 9.

213. *Id.* at 8–10.

214. *See* Press Release, Fed. Commc'ns Comm'n, FCC Mandates that Phone Companies Implement Caller ID Authentication to Combat Spoofed Robocalls (Mar. 31, 2020), https://docs.fcc.gov/public/attachments/DOC-363399A1.pdf [https://perma.cc/GYG8-S59L].

the robocall scourge and passed thirteen bills.[215] In 2019, Congress finally enacted into law the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (the TRACED Act),[216] which attracted over eighty co-sponsors.[217]

The TRACED Act does not add much to the existing enforcement frameworks, aside from enhanced penalties for robocalling.[218] But enhancing penalties will not likely deter those who perceive no possibility of being caught, like overseas operators, or those with no assets, however.[219] Apart from enhancing penalties, the Act merely promotes the establishment of interagency working groups to study and report to Congress on the problem and enables the FCC to promulgate appropriate rules to accommodate SHAKEN/STIR.[220]

Cynically, one might conclude that the TRACED Act merely enables authors, sponsors, and supporters to brag to constituents that they are working across the aisle to fight against a universally detested and common practice, without accomplishing much. The substance of the TRACED Act brings to mind the admonition of two-time presidential candidate and businessman, H. Ross Perot: "If you see a snake, just kill it—don't appoint a committee on snakes."[221]

Certainly, this legislation "appoint[s] a committee on snakes," while increasing the bounty on snakes. But can these snakes actually be killed? As the character Dr. Steven Price warned about snakes in the classic film *Snakes on a Plane*, "[m]ake it fast. Time is tissue."[222] Observers have pointed out that "early iterations" of the technology needed to implement a plan like SHAKEN/STIR have

---

215. Emily Birnbaum, *Senate Passes Bill Penalizing Illegal Robcalls*, THE HILL (May 23, 2019), https://thehill.com/policy/technology/445255-senate-passes-bill-penalizing-illegal-robocalls [https://perma.cc/Y46A-A43G].

216. Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105, 133 Stat. 3274 (2019).

217. Birnbaum, *supra* note 215.

218. *See* Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105, § 3, 133 Stat. 3274, 3274-76 (2019).

219. *See* Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169, 183 (1968) (The probability of prosecution for the overseas fraudsters might approach zero, so the "rational" fraudster would likely not be deterred much by any increase in penalty).

220. *S. 151 - Pallone-Thune TRACED Act, 116th Congress (2019-2020)*, CONGRESS.GOV, https://www.congress.gov/bill/116th-congress/senate-bill/151/ [https://perma.cc/DH7X-ABGU].

221. Jessica Kwong, *Ross Perot Quotes: Most Famous Lines from Former Third-party Presidential Candidate*, NEWSWEEK (July 9, 2019), https://www.newsweek.com/ross-perot-famous-quotes-1448287 [https://perma.cc/YJ3S-K6RY].

222. SNAKES ON A PLANE (NEW LINE CINEMA 2006).

been extant since 2006.[223] Regulatory movement and enforcement have been slow to arrive, even as the menace has developed in the years since.

As the public sector regulates and enforces, and the private sector collaborates on enforcement, development, and implementation of technological solutions, many predict the scammers will adapt and innovate, and robocalls and their associated scams will continue.[224] Any "committee on snakes" that produces a snake study would have to account for the evolutionary biology that will follow the first wave of diversion and killing of the snakes.

For example, some predict that scammers will defeat SHAKEN/STIR and other initiatives "by buying cheap, 'legitimate' United States-based numbers in the hundreds, maybe thousands," instead of spoofing them from abroad.[225] Will an industry-regulatory partnership be "nimble enough to catch spammers as they adapt"?[226]

Other observers believe that the FCC and other regulators must emerge as the leaders here, even though the telecom providers are closer to the technology and the fraud.[227] This is because private telecom players lack a financial incentive to defeat robocalling scammers. Certainly, voice communication, though at the historic core of their offerings, does not project into their priorities for innovation. Voice calls "are dirt cheap" and not lucrative, for one thing.[228] And no direct loss accrues to the telecom providers from these scams[229] unless and until regulators put certain compliance onuses on them. After all, "why invest a lot of resources [into blocking robocalls] when "developing 5G networks" appears to be the next field for competitive investment? The providers will be less likely to invest in old technology unless given a push.

The flag-waving of the ninety-seven senators who voted for the TRACED Act may enable them to return home to brag about passing a law, but the act provides no real push besides an added measure of accountability for agency focus on the problem. If the robocalling snakes had a lobby, and could breathe sighs of relief,

---

223. Editorial, *You're About to Get Fewer Robocalls. But Maybe Not for Long*, N.Y. TIMES (Apr. 23, 2019), https://www.nytimes.com/2019/04/23/opinion/robocalls-phone-scams.html [https://perma.cc/R38Z-JVU6].

224. *See id.*

225. *Id.*

226. Jake Swearingen, *Spam Robocalls Aren't Slowing Down. Here's the Tech that Could Stop Them*, N.Y. MAG. (May 16, 2018), https://nymag.com/intelligencer/2018/05/how-to-stop-spam-robocalls-with-stir-shaken.html [https://perma.cc/56CZ-9FPA].

227. Editoral, *supra* note 223.

228. *Id.*

229. *Id.*

their lobby would still breathe easily, even if the House of Representatives passed this legislation and it was signed into law.

B. *Enforcement Initiatives*

The FCC and the FTC have taken a host of enforcement actions against violators of the aforementioned laws and regulations, but that does not seem to have stemmed the growth of impostor scams. Perhaps the growth continues because enforcement does not effectively reach the overseas generators of impostor scams. It is worth noting the efforts because they are substantial, yet the incidence of these scams has continued to grow.

During the period between 2010 and 2018, the FCC "took enforcement actions involving proposed or imposed monetary forfeitures . . . against violators or apparent violators of either the Truth in Caller ID Act or the TCPA" that totaled nearly $250 million,[230] reflecting 140 enforcement actions.[231] Warning citations have also been issued to over three dozen violators.[232] The FCC highlighted seven enforcement examples in their Robocall Report that apparently typify the magnitude of the problem, but also highlight the limitations of their reach—they are all domestic examples.[233]

In one of the highlighted forfeiture cases, the one of the largest magnitude, a single person was held to account for launching a staggering "96 million illegal spoofed robocalls" over the course of three months, impostoring major hotel chains and online travel agencies, including Hilton, Marriott, Expedia, and TripAdvisor.[234] Adrian Abramovich allegedly used robocalling and neighbor Caller ID spoofing tactics to induce people to hear a message falsely purporting affiliation with legitimate travel companies.[235] Through his network of Florida companies, he was directing calls to travel agencies that directed calls to Mexican call centers selling Mexican timeshares and vacation packages.[236] For perspective, that amounts to twelve calls made per second,[237] and, by one description, would

---

230. FED. COMMC'NS COMM'N, *supra* note 160, at 10.

231. *Id.* at 11. A description of selected enforcement actions indicates that most of these actions pursued smaller fines. The Abramovich action described below accounts for $120 million. *Id.*

232. *Id.* at 10.

233. *See id.* at 10–11.

234. *Id.* at 10.

235. *In re* Adrian Abramovich, Mktg. Strategy Lenders, Inc., & Mktg. Leaders, Inc., Forfeiture Order, 33 FCC Rcd. 4663, 4665 (May 10, 2018).

236. *Id.* at 4664.

237. Ethan Wolffe-Mann, *How TripAdvisor Hunted a Robocaller that Made 100 Million Calls to Random People*, YAHOO FIN. (June 27, 2017), https://finance.yahoo.com/news/tripadvisor-

qualify the perpetrator for the "Guinness World Record," if there were such a thing, for robocalling.[238]

Note, however, that though part of the scheme took place outside the United States, the lead perpetrator, his entities, and assets, resided in Florida, which made enforcement easier. The FCC began investigating Abramovich due to complaints from a medical paging company about dangerous interference with their network from a massive onslaught of outbound calls.[239] Not only was enforcement able to reach Abramovich at his actual front door, but the United States Senate was also able to subpoena his appearance.[240] It is forgivable for the FCC to lead their reporting on enforcement with this massive and satisfying win, but this result may not typify the sort of enforcement actions that must be taken to shut down the robocalling and spoofing mechanisms.

Similar efforts have been made to bring enforcement actions against people and entities, all within jurisdictional reach. The FCC alleged that Philip Roesel, a resident of Wilmington, North Carolina,[241] generated over twenty-one million robocalls, including eighty-two thousand spoofed calls, through his insurance marketing businesses during the period between October 2016 and January 2017.[242]

Roesel flooded recipients with these unlawful phone calls "in order to drum up sales of the health insurance policies he and his associated agents were selling."[243] His businesses had been set up to "generate leads for himself and other affiliated agents" for the sale of "health insurance products."[244] Roesel used false CallerID information to "avoid detection" and "evade law enforcement" and thus "make it more likely that unwitting consumers would answer the phone."[245] The impostor here deployed these tactics to achieve the ultimate goal of generating business. Ultimately, this typical scheme led to the FCC imposing an eighty-two million dollar pen-

---

hunted-robocaller-made-100-million-calls-random-people-124348420.html [https://perma.cc/PL8Y-U8PZ].

238. Rob Wile, *Miami Man Made Nearly 100 Million Robocalls. Now He's Paying a Big Price*, MIA. HERALD (May 11, 2018), https://www.miamiherald.com/news/local/community/miami-dade/article210861109.html.

239. The FCC enjoyed extensive assistance from TripAdvisor, one of the companies impostored. *See* Palmer, *supra* note 141; *In re Adrian Abramovich*, 33 FCC Rcd. at 4664–65.

240. Palmer, *supra* note 141.

241. *See* Press Release, Fed. Commc'ns Comm'n, FCC Proposes $82 Million Fine for Spoofed Robocalls (Aug. 3, 2017), https://www.fcc.gov/document/fcc-proposes-82-million-fine-spoofed-telemarketing-robocalls [https://perma.cc/G5E2-9G4W].

242. *In re* Best Ins. Contracts, Inc., & Philip Roesel, dba Wilmington Ins. Quotes, Notice of Apparent Liability for Forfeiture, 33 FCC Rcd. 6403, 6403, 6414 (Sept. 26, 2018).

243. *Id.* at 6.

244. *Id.* at 6–7, 9.

245. *Id.* at 9.

alty on Roesel and his entities, an amount which he claimed he would have a great difficulty paying.[246] Again, in this highlighted instance, the robocalling spoofer impostor was within reach of the authorities.

The third highest penalty in the report, thirty-seven million dollars, was also levied against an alleged domestic offender, Affordable Enterprises of Arizona, LLC.[247] Affordable Enterprises generated over two million robocalls through a telemarketing platform, more than thirty thousand of which the FCC verified to be spoofed.[248] In this matter, a former employee of the entity, which marketed home remodeling and improvement services, blew the whistle on the operation to the FCC and revealed the inner workings of the scheme.[249]

Affordable Enterprises purchased a list of home and cell phone numbers of individuals and called them, using the numbers from prepaid cell phones purchased at Walmart as the spoofed identity.[250] A significant effort was made to conceal the identity of the calling entity in order to further the scheme. If call recipients called back to complain, the Affordable Enterprises employees had been instructed to pick up the phone to apologize and limit the conservations to minimize conflict.[251] In addition, if a burner phone number generated too many complaints, the company would discard it.[252] Consumers reported to the FCC that they had been ridiculed and harassed by some of the employees when returning the calls and failed to receive identifying information about to whom the number belonged.[253]

This enterprise yielded remarkable financial success. The whistleblowing employee reported that the center was generating $300,000 per month from these calls.[254] This operation continued for well over a year, right in Tucson, Arizona. As with the Roesel matter, no evidence surfaced that the actual services being marketed were illegitimate, but the imposture was a key vehicle in getting leads.

These three operations represent the largest fines in the robocall cases highlighted by the FCC in its report. The other four

---

246. *Id.* at 20–24.
247. *In re* Affordable Enters. of Ariz., LLC, Notice of Apparent Liability for Forfeiture, 33 FCC Rcd. 9233 (Sept. 26, 2018).
248. *Id.* at 2.
249. *Id.*
250. *Id.* at 3–4.
251. *Id.*
252. *Id.*
253. *Id.*
254. *Id.*

actions listed in the FCC report involve penalties under three million dollars, and a few well under that. They were all also domestic: a dialing technology and service platform, based in New Mexico;[255] a stalker and his co-worker, located in New York, making menacing and threatening phone calls to an ex-spouse;[256] another travel marketer located in Florida;[257] and an Alabama bank.[258] In total, the FCC reported only three enforcement actions in the robocalling report that involved imposture or spoofing, and all were domestic.

Not to be outdone, the FTC and approximately two dozen state and local enforcement agencies "announced a major crackdown on illegal robocalls, including 94 actions targeting operations around the country."[259] The June 2019 initiative was deemed "Operation Call it Quits."[260] The Operation Call it Quits complaints and actions were directed toward actors similar to the ones pursued by the FCC.

Among those in the net of Operation Call it Quits are alleged impostor scams, including a complaint against a "dialer"/"information technology guy" who supposedly used Caller ID spoofing as part of his services to other scammers.[261] Another FTC target used a pre-recorded message pretending to be "John from the shipping department," falsely informing call recipients "that a medical alert system had been purchased for them, and they could receive it 'at no cost whatsoever.' "[262] Although this operation skirt-

---

255. *In re* Dialing Servs., LLC, Forfeiture Order, 32 FCC Rcd. 6192 (July 26, 2017).

256. *In re* Steven Blumenstock & Gary Braver, Notice of Apparent Liability for Forfeiture, 31 FCC Rcd. 8648 (Aug. 2, 2016). These individuals used a third-party spoofing service to modulate their voices, and the number appears to be from locations such as prisons. Though this use of imposture is highly disturbing and worthy of serious attention, this article focuses on the use of imposture at higher volume for financial gain and to further swindles. *Id.*

257. *In re* Travel Club Mktg., Inc., Forfeiture Order, 30 FCC Rcd. 8861 (11) (Aug. 11, 2015). Note that imposture and caller identification spoofing did not appear to be involved in this scheme. At the time, this action held the record for the highest robocalling fine. Chris Morran, *Travel Club Telemarketer Fined $2.96M for Robocalling Consumers*, CONSUMERIST (Aug. 11, 2015), https://consumerist.com/2015/08/11/travel-club-telemarketer-fined-2-96m-for-robocalling-consumers/ [https://perma.cc/E9HQ-NMMU].

258. *In re* Sec. First of Ala., LLC, Forfeiture Order, 30 FCC Rcd. 2377 (Feb. 13, 2015) (also note that imposture was not part of this scheme).

259. Press Release, Fed. Trade Comm'n, Law Enforcement Partners Announce New Crackdown on Illegal Robocalls (June 25, 2019), https://www.ftc.gov/news-events/press-releases/2019/06/ftc-law-enforcement-partners-announce-new-crackdown-illegal [https://perma.cc/WSU7-YA49].

260. *Id.*

261. *See* Complaint, United States v. Derek James Bartoli, No. 19-1160 (M.D. Fla. June 21, 2019); Press Release, Fed. Trade Comm'n, Law Enforcement Partners Announce New Crackdown on Illegal Robocalls (June 25, 2019), https://www.ftc.gov/news-events/press-releases/2019/06/ftc-law-enforcement-partners-announce-new-crackdown-illegal [https://perma.cc/WSU7-YA49].

262. Press Release, *supra* note 259; *see also* Stipulated Order Permanent Injunction and Monetary Judgment, FTC v. Lifewatch, No. 1:15-cv-05781 (N.D. Ill. June 24, 2019).

ed the line of pure imposture, the operators falsely claimed product endorsement from credible authorities "like the American Heart Association, American Diabetes Association, National Institute on Aging, or the AARP."[263]

FTC declared that these entities were "responsible for more than one billion calls pitching a variety of products and services including credit card interest rate reduction services, money-making opportunities, and medical alert systems."[264] Just like the FCC actions, however, the targets, though significant, are all only within domestic reach.[265] Although the FTC and FCC appear to have overlapping missions and actions, both have enforcement authority. As one observer put it, though there are certain "legal distinctions," "the FTC is the sheriff here . . . prosecut[ing] shady business practices," but "other state and federal agencies, including the [FCC], also police nuisance calls."[266] But as the FTC told one reporter, "there are enough violators in this space to keep us both busy."[267]

C. *A Bleak Prognosis*

Jealousy of interagency authority does not appear to be the obstacle to stopping impostor scams. The FTC has established enforcement operations and the FCC likely has closer familiarity with the technology.[268] As the FTC staff attorney dedicated as the "point person on robocalls" explained, "the FTC is largely a civil law enforcement agency. We have a whole lot of attorneys, and a whole lot of economists, and a few technologists . . . we don't have the expertise."[269]

Although all of these FCC, FTC, state, and local enforcement actions appear worthy of pursuit and resources, the massive problem of using telephone voice calls to achieve impostor scams is unlikely to be addressed this way. This leaves solving the problem to the technologists. Massachusetts Attorney General Maura Healey recognized the challenge of using domestic rules and law enforcement. "There is a problem with a lot of these calls emanating from

---

263. Press Release, *supra* note 259; Stipulated Order Permanent Injunction and Monetary Judgment, FTC v. Lifewatch, No. 1:15-cv-05781 (N.D. Ill. June 24, 2019).
264. Press Release, *supra* note 259.
265. *Id.*
266. van Zuylen-Wood, *supra* note 135.
267. *Id.*
268. *Id.*
269. *Id.*

overseas, [thus] [t]he practicalities of enforcement become problematic."[270]

The FCC concedes Attorney General Healey's point at the end of its Report on Robocalls as one of its primary enforcement challenge. "Many illegal robocallers are operating in foreign countries. Although Congress recently gave the Commission express jurisdiction over foreign Caller ID spoofers, in practice the Commission may also need cooperation from foreign governments."[271]

Alex Quilici also offers some reasoned pessimism about regulatory and enforcement solutions to robocalls.[272] (YouMail also provides a variety of blocking services for phone users, so his pessimism may offer his business some grounds for optimism.)[273] Quilici notes that "phone spam," as he deems it, cannot be controlled as easily as "email spam."[274] Scammers have some fundamental advantages in telephony that they do not have in the email sphere, which can be better controlled through algorithms.[275]

For example, emails that are flagged as spam by email providers are still available if the recipient wants to safely inspect them, but they are separated from other messages and, therefore, suspicion is heightened.[276] There are no spam folders for storing phone calls, however.[277] "Once the robocall is bounced at the network level, the consumer never sees it."[278] Phone service providers do not want to inadvertently prevent a recipient from receiving a legitimate message. Quilici added, "No carrier wants to make national news because grandma tried to reach her grandson to go to the hospital but her call was blocked. Robocall blocking is complicated. You have to figure out if a number is misbehaving."[279]

With telephone scams, Quilici observes that "the bad guys keep finding new ways and new numbers to lure you into answering the phone and falling for the scam. For them, it's easy and cheap to operate, difficult to trace and extremely lucrative."[280] He notes that accessing the phone network, acquiring and disguising numbers,

---

270. Elaine S. Povich, *States Try to Silence Robocalls, but They're Worse Than Ever*, PEW STATELINE (July 25, 2018), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2018/07/25/states-try-to-silence-robocalls-but-theyre-worse-than-ever [https://perma.cc/C9N5-EXHU].
271. *See* FED. COMMC'NS COMM'N, *supra* note 160, at 14.
272. *See* Robertson, *supra* note 151.
273. *See* YOUMAIL, https://www.youmail.com [https://perma.cc/S5KS-ERAU].
274. *See* Robertson, *supra* note 151.
275. *See id.*
276. *See id.*
277. *See id.*
278. *Id.*
279. *Id.*
280. *Id.*

and switching phone service providers can be done with ease.[281] Although Quilici concedes that there will be some advancement in the blocking of illegal calls with new framework approaches like SHAKEN/STIR, "it won't be a panacea. We've never seen regulation solve technical problems."[282] Yet, he retains some measured optimism about robocalls: "Even though we're at an all-time high . . . [and] the numbers may be creeping up a little bit . . . the situations seems to be mostly stable at this point. We have not turned the corner, but maybe the corner is in sight."[283]

No miracles should be expected. The "[hope] that, 'poof,' robocalls will just be gone [is] the wrong mind-set," according to a senior consultant at one of the industry standards bodies, but the systems are in place to bring the calls "down to a manageable level."[284]

There have been *some* efforts to address the problem by attacking call centers overseas that are operating full-on impostor scams.[285] But the question will remain. The coordination of international law enforcement resources may be prioritized to focus on other areas of higher urgency and importance, like terrorism and human trafficking, rather than phone calls.

If the impracticalities of enforcement hold, the solution to curbing modern impostor scamming lies in finding strategic ways to raise the risks and costs of scamming. This is best accomplished through the pursuit of proactive technological solutions that disrupt the intermediary mechanisms for scamming on a large scale, through precisely targeted enforcement and education. Perhaps at some point, voice calling will not be trusted or might even be abandoned, as alternate means of popular communication take hold.[286] Fewer people will answer telephone calls. But would that not simply shift the scammers to communications mediums that

---

281. *Id.*

282. *Id.*

283. Lily Hay Newman, *The Robocall Crisis Will Never Be Fixed*, WIRED (Apr. 4, 2019), https://www.wired.com/story/robocalls-spam-fix-stir-shaken/ [https://perma.cc/52F4-3F3B].

284. *Id.*

285. Though the efforts do not appear to be full scale, some overseas scams have been investigated and prosecuted. *See, e.g.*, Press Release, U.S. Dep't of Just., Three Defendants and India-based Call Center Indicted in Phone Scam Targeting U.S. Victims (Mar. 12, 2019), https://www.justice.gov/usao-ndga/pr/three-defendants-and-india-based-call-center-indicted-phone-scam-targeting-us-victims [https://perma.cc/Q7PS-SYAG]; Press Release, U.S. Dep't of Just., Indian National Convicted of Role in Call Center Scam that Victimized Thousands in the U.S. (Jan. 9, 2020), https://www.justice.gov/usao-sdtx/pr/indian-national-convicted-role-call-center-scam-victimized-thousands-us [https://perma.cc/8CMY-Z348].

286. *See* Newman, *supra* note 283 ("Much like the firehose of spam that made email almost unusable in the late 1990s, robocalls have made people in the US wary of picking up their cell phones and landlines.").

remain more trustworthy, like texting, social media, and other applications?

The robocalling "cat and mouse" game has not ended, and the people playing the role of cat seem to know that the mouse shall adapt and return.[287] As noted, SHAKEN/STIR still allows the use of "legitimate phone numbers" for scams—it just will block spoofed ones from reaching their destination.[288] The industry and FCC have expressed awareness that these changes will "inevitably spur criminal innovation in robocalling to evade or manipulate the new cryptographic baseline."[289]

In fact, Quilici points out that the improved ability to flag suspicious calls by apps and providers has compelled an acceleration in the number of calls made.[290] The robocallers need to make more phone calls in order to overwhelm those systems. "If you don't answer the phone, the robocaller has to work harder, so they generate more calls. It's a death spiral."[291]

And although the death spiral can be slowed down, the meshing of technology with the ability to impostor always returns. Ultimately, the determined and bold impostor scammer can accomplish seemingly anything, manipulating trust, authority, and fear and deploying technology in all sorts of ways. What amount of education or technological advancement will stop modern-day Spanish prisoner scams, where the perpetrators are hiding overseas?

The approach that I propose suggests more concentrated ways to combat the impostor fraud problem. The efforts underway to address impostor scammers through telecommunications provide a starting point, but more than that, they provide an example of a pragmatic approach for slowing the roll of the basic scam. By forcing scammers to resort to less-preferred means of communications, or to engage in the search for new means, the logistical difficulty of pulling off scams and the cost of executing scams should increase.

This would mean that the impostor scam might be less prevalent if the economics could be shifted back to resemble that of the scams embodied in the Spanish prisoner mailings and the salesperson imposture in *Hoddeson*. One way to achieve this would be to take a "least-cost avoider" approach toward these scam busting efforts, putting to work those who operate and profit from offering the intermediary services that enable the fraudsters. They have the means, opportunity, and expertise to make impostor scamming

287. *Id.*
288. *Id.*
289. *Id.*
290. *Id.*
291. *Id.*

more difficult. Certain industries can take voluntary measures to choke impostor fraud, and regulators and lawmakers can formally incentivize certain players to take action.

IV. FINDING THE RIGHT WARRIORS TO FIGHT IMPOSTOR FRAUD

Ultimately, a policy approach should aim to make impostor fraud riskier and more expensive. The scammer's scheme in *Hoddeson v. Koos Brothers*, though effective against both the consumer and the store, would be difficult to execute on mass scale without detection. Impostors thrive on concealment of identity and eluding identification, and as noted, schemes like that one required more risk and could not operate at a scale like that of an operation that could leverage technologies like robocalling, ID spoofing, social media networks, or easily-accessible payment systems.

Regulators could require more vigilance from these chokepoint fraud intermediaries. Additional voluntary measures, if coordinated, might also help. Successful impostor fraud has always relied upon marrying emotions of fear and greed with the best and cheapest means for exploiting them. Those who straddle these "means" have the best knowledge of their mechanisms and the best opportunity to police their abuse. Many already have some incentives to do so—a social media platform for dating, for example, already wants to avoid reputational damage from misuse, but perhaps these sorts of entities can absorb more burden. They are classic examples of least-cost avoiders for preventing this social harm.

A. *Finding the Least-Cost Avoiders*

A least-cost avoider approach would focus on ensuring that those entities that engage in activities that yield a harm absorb the cost of that harm. This would compel entities to internalize the harm in a way that would motivate them to manage and contend with these costs.[292] A least-cost avoider mindset can help policymakers design the most efficient system and framework for combating impostors, making their scams more difficult to execute. A framework that assigns a duty to the intermediaries and owners of instrumentalities who benefit from providing these services to the

---

292. *See generally* Guido Calabresi, *Some Thoughts on Risk Distribution and the Law of Torts*, 70 YALE L.J. 499 (1961) (an embryonic discussion of the implications of least-cost avoidance principles).

public would be justifiable from a distributive standpoint and efficiency standpoint.[293] That is, those who profit from offering a service should internalize more costs and thus more burdens.

Summarizing the vast literature that explains and applies the least-cost avoider (LCA) concept proves challenging, but a revisit of the basics offers worthwhile context. As Guido Calabresi and Douglas Melamed summarized Justice Holmes, "[p]erhaps the simplest reason for a particular entitlement is to minimize the administrative costs of enforcement," unless shifting the burden improves welfare.[294] Allowing the costs of impostor fraud to fall where they lie would be certainly the most inexpensive system to administer. Calabresi and Melamed observed the social problem that follows from only applying this "simplest reason," concluding that minimizing administration "by itself . . . will never justify any result except that of letting the stronger win."[295]

Aside from the scattered enforcement measures discussed above, letting the costs of impostor fraud fall where they lie seems to be the dominant system in place, and that approach has apparently enabled impostor fraud to flourish. In our current system, victims of impostor fraud appear to bear most costs. Scammers, by and large, seem to be beyond the reach of the system, and intermediaries bear little burden.

Famously, Calabresi and Melamed laid out the premise of the least-cost avoider (LCA), which has been much discussed over the past half-century. An LCA-themed framework could lead to the most efficient solution to minimize the impact of impostor fraud and other associated problems. As they wrote, "economic efficiency standing alone would dictate that set of entitlements which favors knowledgeable choices between social benefits and the social costs of obtaining them, and between social costs and the social costs of avoiding them."[296] They suggest "the cost should be put on the party or activity best located to make such a cost-benefit analysis."[297]

Are consumers the LCAs here or are the intermediaries the LCAs? The operators of intermediaries have technological capabilities and a centralized knowledge base that the potential targets do not have. Scammers are able to study and exploit these systems and

---

293. *See generally* Benjamin Edelman, *Least-Cost Avoiders in Online Fraud and Abuse*, 8 SEC. & PRIV. ECON. 78 (2010) (discussing the roles that the Communications Decency Act and the Digital Millennium Copyright Act play in involving intermediaries in policing defamation and copyright violations, respectively).

294. *See* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1093 (1972).

295. *Id.*

296. *Id.* at 1096.

297. *Id.*

experiment with using them to their ends. These intermediaries are better positioned, as repeat players, to create and mine their own knowledge base about how scammers use their platform and to develop and implement approaches to fight impostors. Scammers have asymmetric information relative to consumers about how to exploit these systems and the intermediaries have the best means for leveling out these advantages. Consumers do not work full time to detect scams and even if they are able to avoid some of them with common sense, this Article has documented that some impostors are sophisticated enough to deceive anyone. Therefore, attempting to induce stronger consumer detection efforts through liability assignment is unlikely to alter the frequency of impostor fraud significantly.

Unsurprisingly, and perhaps reflecting these observations, proposals have been made to apply these LCA principles to address the slightly different scourge of identity theft, which can play a role in impostor fraud. Again, impostor fraud focuses on the impact on those who have been deceived by false identity, whereas identity theft focuses on the impact on those who have had their identities stolen. In 2004, Jeff Sovern suggested that the burden should be shifted from consumers to creditors, and the credit bureaus should absorb losses.[298] He identified the "credit industry" as the LCA of identity theft and suggested that if they bore the costs, they would have more of an incentive to combat this social problem.[299] Over a decade later, Mark Geistfeld recognized that private tort law alone would be insufficient to address the identity theft problem, even with the application of strict liability principles.[300] Geistfeld concluded that such an approach to identity theft could "only complement other regulatory efforts."[301] Because the operators of intermediaries may not be sufficiently internalizing the costs of fraud, market forces will not solve this growing impostor scam problem unless some burdens are shifted. Ordinarily, one might ask what the optimal level of impostor fraud might be—that is, what level of fraud might be tolerable in the aggregate? For now, the concern can be leveled at the mere growth of impostor fraud over time, both in terms of incidence and magnitude of losses.

With impostor fraud, the problem may be broader and require more of a coordinated regulatory attack than identity fraud. Impostor fraud has many more chokepoints. In essence, the credit

---

298. Jeff Sovern, *Stopping Identity Theft*, 38 J. CONSUMER AFFS. 233 (2004).
299. *See id.*
300. *See* Mark A. Geistfeld, *Protecting Confidential Information Entrusted to Others in Business Transactions: Data Breaches, Identity Theft, and Tort Liability*, 66 DEPAUL L. REV. 385 (2017).
301. *Id.* at 412.

industry is the "chokepoint" for much of identity fraud, maintaining the ability to manage and verify credit and identity information, while financially benefiting from lending and maintaining this data. The chokepoints for impostor fraud are broader and cross multiple sectors of the economy, as well as emerging technologies.

Impostor fraud should be treated as a byproduct of the profitable activity of providing telecommunications services, social media services, or stored-value money cards. All of those create social value, but can also produce a destructive social byproduct akin to "accidents or pollution."[302] "The costs should be put on the party or activity which can, with the lowest transaction costs act in the market to correct an error in entitlements by inducing the party who can avoid social costs most cheaply to do so."[303] There are measures that intermediaries and instrumentalities can take to avoid social costs, and given their knowledge of technology and repeat-player wisdom, they may be in the LCA position.

Of course, macro decisions need to be made about how much to economically burden these intermediaries, much in the same manner that decisions were made about how much to burden (or unburden) information and content distribution intermediaries. The model does not mesh perfectly with the classic Calabresi-Melamed application to accidents, in that we are not addressing a problem of legitimate operators engaging in risky activities. But this impostor problem may call for an approach "in which the permitted level and manner of accident-causing activities is determined collectively,"[304] if one can define an incident of impostor fraud as an "accident" that can spill over from the activity of providing an infrastructure for communication or money transfer. Although only one "avoider" can truly qualify as the "least" of the LCAs, a few contenders emerge.

B. *Shifting Burdens to Communications Intermediaries and Payment Systems*

To address impostor fraud, policymakers and regulators can allocate more responsibility to providers of telecommunications services, social media services, and stored-value card offerors for absorbing the costs of impostor fraud.[305] Regulators and lawmakers

---

302. *See* Calabresi & Melamed, *supra* note 294, at 1096–97.
303. *Id.* at 1097.
304. *Id.* at 1097 n.19.
305. Such measures do not preclude self-regulation.

can mandate adoption of certain technologies, mandate disclosure of warnings (akin to safety warnings), or otherwise place restrictions on their business practices to decrease the incidence of impostor fraud. Of course, many instrumentalities and intermediaries can be used to perpetrate impostor fraud, but these services appear to be among those strategically positioned to intervene if required, or otherwise incentivized, to do so. Fraudulent innovation can never be squelched, given the opportunities and potential payoffs to scammers, but an LCA approach demonstrates that more care can be taken by the entities that economically benefit from these systems. As controllers of key chokepoints, however, these sectors are in a superior position to block or intervene in fraud than the intended victims. Having perhaps greater knowledge about these scams, their fraud reporting obligations should also be stronger, as they can better alert both regulators and citizens.[306]

1. Telecommunications Carriers

The push from lawmakers, regulators, and enforcement to pressure telecommunications-carrier intermediaries to solve this problem has been a focus for those who have studied the evolving robocall problem for several years.[307] Mass impostor scams rely on a " 'chokepoint' in which illegal conduct may be cut-off and deterred."[308] Applying pressure at this chokepoint will raise the costs of enacting such prolific impostor scams but will require both government intervention and incentives for industry innovation and cooperation.

In 2014, the Institute for Consumer Antitrust Studies (ICAS) published an extensive and thorough report assessing the state of TCPA effectiveness, suggesting "certain modifications and improvements" to the 1991 statute in the wake of technological and other developments in the years since passage.[309] Spencer Weber Waller and the co-authors of this report recognized the difficult challenges of enforcement in the wake of evolving technology.[310]

---

306. *See generally* David Adam Friedman, *Reinventing Consumer Protection*, 57 DEPAUL L. REV. 45 (2007) (proposing leveraging fraud reporting in a way that adapts to new scams).

307. Spencer Weber Waller, Daniel Heidtke & Jessica Stewart, Loyola U. Chi. Sch. L., Inst. for Consumer Antitrust Stud., *The Telephone Consumer Protection Act of 1991: Adapting Consumer Protection to Changing Technology* 61 (Loyola U. Chi. Sch. L., Pub. L. & Legal Theory Rsch. Paper No. 2013-016, 2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2327266 [https://perma.cc/JB54-RT54].

308. *Id.* at 60.

309. *Id.* at 4–6.

310. *See id.* at 36.

Prior to the current impostor scam proliferation, they observed the futility of stopping "calls . . . routed through a 'web of automatic dialers, caller ID spoofing, and [voIP] protocols.' "[311] They recognized that the TCPA's effectiveness depended on the robust use of the "private right of action"[312]—not public enforcement.[313]

The ICAS report observed that the private right of action would provide little incentive for private actors to pursue and deter "intentional violators" like the impostor-scam perpetrators of concern here, as they were designed to deter "otherwise legitimate companies."[314] Further, "when TCPA violators are located overseas or are judgment proof, there is little incentive for an individual or class of private plaintiffs to bring a lawsuit. *The effort becomes futile when the violator cannot even be located.*"[315] As noted, "companies that are increasingly responsible for the majority of TCPA violations are located overseas,"[316] where many of the impostor scams originate, true to their Spanish prisoner heritage.

Though the ICAS report makes many recommendations, for example, to redouble efforts to stop unlawful Caller ID manipulation,[317] ultimately, the report recognizes that these recommendations cannot effectively address overseas-operated impostor fraud that already violates the law. "Government enforcement is necessary. Private parties do not possess the resources or the incentive to track and locate entities located outside the United States."[318]

Given the weakness of laws on the books, including the toothless recently-enacted TRACED Act and the chokepoint position of telecommunications providers, carriers should carry more of a burden as a potential LCA of impostor fraud. The available technology to verify caller identity has evolved to a point where carriers are able to make massive calling more difficult and expensive—and more innovative. The more expensive the generation of impostor scam calls is to impostors, the fewer calls there will be. These calls are an externality absorbed by consumer subscribers that result from consumers using the services, and consumer use benefits the carriers. Although some consumers can and do avoid the scourge, the owner and controller of the chokepoint and its technology can more easily perform the choking.

---

311. *Id.*
312. *Id.* The TPCA enables private plaintiffs to sue for $500 for each separate violation and $1,500 if the violation is willful. 47 U.S.C. § 227 (b)(3), (f)(1).
313. See Waller et al., *supra* note 307, at 36.
314. *Id.* at 37.
315. *Id.* at 37 (emphasis added).
316. *Id.* at 45.
317. *Id.* at 60.
318. *Id.* at 45.

Even if only *some* impostor scams can be choked, the technological mass production of outbound calls could be slowed down. If policymakers design and enforce legislation and regulation to incentivize carriers, and carriers innovate and demonstrate proactivity, impostor phone calls should diminish. Of course, if robocalls start to stop, more people might regain trust in inbound phone calls, more calls might be answered because recipients could let their guard down, and a new, different wave of imposture could begin via the same telecommunications systems. As previously noted, if the industry follows through on SHAKEN/STIR in some version, there are already means for scammers to defeat this system by buying identifiable phone numbers that enable scammers to continue to robocall. Lawmakers, regulators, and the private sector must always try to maintain tabs on how scammers abuse technology. If the gatekeepers stand still, the costs of imposture will drop again, and it will reemerge. In fact, they must make all efforts to *stay ahead* of the scammers and not rest on the recent regulatory innovations and technological gains.. Once again, the telecom sector, having access to how their technology is abused, are in an LCA position and responsibility should be shifted accordingly.

Right now, it is worth asking whether executing something like a "grandparent scam" by telephone would still be possible, even after SHAKEN/STIR. Certainly, as the way things are, scammers could use burner phones, and possibly even spoof them to present numbers that pretend to be a hospital or law enforcement. Tightening regulation on the sale of burner phones, particularly when purchased in bulk, might solve this problem, but, certainly, scammers can find other, perhaps less easy, means. Email spoofing could still be used if the scammer skims information from social media. But such measures by scammers require more skill and expense to execute, so one would expect fewer grandparent scams. The IRS and Social Security scams in their current forms, however, could be significantly slowed down, as could the widespread scourge of imposture of hospitality providers through blast systems.

Given that impostor scam reports now exceed identity theft scams on the FTC Sentinel report, pushing the LCAs to mitigate high-volume generation of impostor calls would have an outsized impact, at least in the near term. Unfortunately, this approach alone would not be enough to put a permanent dent in the problem. For example, another medium used to exploit people through imposture, email and social media, will be explored in the next subsection, and none of the above telecommunications efforts address that potential chokepoint.

2. Social Media and Email Systems

Social media platforms and email systems provide ample opportunities for scammers to pretend that they are someone they are not. Social media impostor scams are distinct from basic email impostor scams. For contrast, in a pure email "phishing" scam, a scammer can scour organizational websites for organizational hierarchies, scan or scrape email addresses, and discern supervisor and colleague relationships.[319] They can easily create an email account that spoofs a supervisor, for example, to impersonate and scam subordinates and colleagues with an urgent plea to help them out of a temporary cash fix.[320] (After all, a "boss" needs to be accommodated and can always be trusted to pay the money back.) A few primary ways to address these scams right now are to educate people in organizations about phishing and apply pressure on the "payment" chokepoint.

Straight-up email scams present a problem, but social media platforms afford certain scammers with even more high-powered tools for imposture, including the ability to create a false persona or impersonate a real person, establish a long-distance relationship (often with the promise of romance), and manipulate targets into handing them their money. The elements of the basic Spanish prisoner routine are present. There is an emotional appeal, perhaps a deeper one here that takes longer to cultivate.[321] The scammers can launch their entire scam from overseas, in countries where enforcement and tracking would be almost impossible.[322] The payment systems involved are easy to manipulate[323] and, under the right circumstances, a scammer can score a significant amount of money from victims.[324]

---

319. *See, e.g.*, U.C. BERKELEY INFO. SEC. OFF., PHISHING EXAMPLES ARCHIVE, https://security.berkeley.edu/education-awareness/phishing/phishing-examples-archive [https://perma.cc/U3HA-TAY5].

320. *See id.*

321. *See generally Romance Scams: Online Impostors Break Hearts and Bank Accounts*, FED. BUREAU INVESTIGATION (Feb. 13, 2017), https://www.fbi.gov/news/stories/romance-scams [https://perma.cc/Q264-JVJ6].

322. *See generally id.* (for example, two Nigerian nationals pleaded guilty in U.S. federal court to participating in an elaborate romance scam scheme, but at least one of the perpetrators remains at large).

323. *See generally Online Dating Scams Infographic*, FED. TRADE COMM'N: CONSUMER INFO. (Feb. 2020), https://www.consumer.ftc.gov/articles/0560-online-dating-scams-infographic [https://perma.cc/Z77M-4M4V] (warning against wiring money, using or sending gift or reloadable cash cards, or sending cash to previously-unknown people who "profess love quickly" online).

324. *See generally* FED. BUREAU INVESTIGATION, *supra* note 321 (scammers in this case extracted at least $2 million from one victim).

If the scammers are beyond the reach of recovery, who should bear the cost of the scam? The victims bear some personal responsibility, but they are often the targets of masterful schemes of manipulation, facilitated by the vehicles of social media that enable scammers to gather personal information from targets and create realistic-looking impostor profiles. The *New York Times* profiled a common version of the romance scam, where the scammer used the unique tools provided by Facebook as the means for generating a false romantic connection.[325] This scam drew upon the imposture of real military personnel through the misappropriation of their likeness and creation of their own narrative.[326]

Congressman Adam Kinzinger, himself a repeated victim of identity spoofing, followed up after the *Times* story with a letter to Facebook Chief Executive Officer Mark Zuckerberg, asking him to provide extensive information about Facebook's identity security problems and the magnitude of efforts to prevent scammers from using their tools.[327] Although Kinzinger has yet to craft legislation to address this problem, he suggests that Facebook consider means of user identity authentication, such as using facial recognition technology or other proof of identification to establish or retain an account.[328]

As Facebook starts to explore developing its own cryptocurrency and confronts accompanying regulatory concerns on that front, they may need to take more measures to mitigate damage from scams perpetrated through their platform.[329] The marriage of a platform that manages both identities and currency transactions could prove to be an even more potent tool for scammers if appropriate measures are not taken to mitigate risk.

Facebook may be an example of an LCA in that they control the gate to those who use their platforms. They already exercise the power to ban real people from using their services, and they have more information and resources to verify accounts than their us-

---

325. *See* Jack Nicas, *Facebook Connected Her to a Tattooed Soldier in Iraq. Or So She Thought*, N.Y. TIMES (July 28, 2019), https://www.nytimes.com/2019/07/28/technology/facebook-military-scam.html [https://perma.cc/WL7J-W8NJ].

326. *See id.*

327. *See* Jack Nicas, *Another Victim in Facebook Romance Scams: A U.S. Congressman*, N.Y. TIMES (Aug. 1, 2019), https://www.nytimes.com/2019/08/01/technology/facebook-military-romance-scam.html [https://perma.cc/XH3F-FFZF] (describing Rep. Kinzinger's frustrations in dealing with impostor scams over several years and stories about the victims who were deceived by the imposture of his identity); Letter from Adam Kinzinger, Member of Cong., to Mark Zuckerberg, Chairman, CEO, Facebook, Inc. (July 31, 2019), https://int.nyt.com/data/documenthelper/1544-kinzinger-letter-to-zuckerberg/553570d65fe47a065b04/optimized/full.pdf#page=1 [https://perma.cc/KH6S-4NFR].

328. *See* Nicas, *supra* note 327.

329. *Id.*

ers.[330] Perhaps more verification could be required, even if it slows down platform entry and causes users to balk due to extra privacy concerns. These capabilites leave Facebook in the best position to internalize the costs of mitigating the risks of imposture on their platform. Of course, if Facebook becomes safer, the scammers will flee elsewhere. It is more expensive, however, for scammers to move away from safer, popular platforms to darker corners of the Internet where achieving scale is more difficult. Given this increased cost, the marginal impostor will no longer find it profitable to conduct scams, and thus the total number of impostor scams will decrease, at least temporarily. Additionally, if Facebook truly becomes safer, the public may place less trust in platforms that cannot verify user identity, incentivizing all of these platforms to be safer from fraud.

Naturally, dating-service sites and apps have become attractive hosts for impostor scammers. By 2015, Pew reported that nearly 15 percent of American adults reported using dating sites or apps.[331] Just in the prior two years, usage had been increasing substantially across age demographics.[332] At the very least, platforms should bear the costs of enhanced verification, additional education, and warnings for users to prevent impostors from using a false identity to create the appearance of a romantic interest[333] that will convince the target to send money to them.[334] Dating sites, like the proliferation of automated telephone technology, have enabled scammers to operate inexpensively, at scale, and at a safe distance. Before the advent of internet technology and social media, romance scammers would have to try to pull off these schemes in person.[335]

---

330. Todd Haselton, *Facebook Content that Gets You Banned According to Community Standards*, CNBC (Apr. 24, 2018), https://www.cnbc.com/2018/04/24/facebook-content-that-gets-you-banned-according-to-community-standards.html [https://perma.cc/9MPS-FBXG].

331. Aaron Smith, *15% of American Adults Have Used Online Dating Sites or Mobile Dating Apps*, PEW RSCH. CTR. (Feb. 11, 2016), https://www.pewinternet.org/2016/02/11/15-percent-of-american-adults-have-used-online-dating-sites-or-mobile-dating-apps/ [https://perma.cc/E96U-6KA4].

332. *Id.*

333. In this context, this is known as "catfishing." *See Catfishing*, URB. DICTIONARY, https://www.urbandictionary.com/define.php?term=Catfishing [https://perma.cc/E6FV-K73B].

334. For an example of warnings about these scams and safety recommendations, see Lisa Copeland, *9 Tips to Keep You Safe from the Scammers on Online Dating Sites*, HUFFINGTON POST (Dec. 6, 2017), https://www.huffpost.com/entry/online-dating-scammers-tips_b_6594250 [https://perma.cc/2LEE-G8SJ] (tips from a dating coach for identifying such scams and taking precautions to avoid them).

335. Apparently, they still do. The elderly appear to provide targets for cruel, in-person, versions of these scams, though not all of them conceal identity, just true motive. *See* Pam Zekman, *2 Investigators: Sham Marriage Drains Elderly Man's Savings*, CBS CHI. (Nov. 18, 2016), https://chicago.cbslocal.com/2016/11/18/2-investigators-sham-marriage-drains-elderly-mans-savings/ [https://perma.cc/3FW2-SGBD].

Again, scammers have always seemed to find avenues to exploit all forms of technology, as it lowers the cost of imposture. This puts more pressure on private and public actors to raise scam execution costs. Social media and dating site providers are custodians of identity and connection, and thus maintain an LCA status, carrying some means of putting on the brakes and raising the costs of imposture. Placing direct financial liability on these sites may prove impractical. But incentivizing platforms to make changes that protect users, either through required safety warnings and verification procedures when using the service, or through altruistically-inspired enhancement of voluntary measures already taken, could prove socially fruitful and enhance welfare.

Further, all of these scams can be defanged somewhat if fund transfer becomes more challenging for the scammers to realize. If scammers cannot get paid, or if it becomes more difficult to get paid, they will have to look for other, less convenient, means of acquiring cash. For example, after fraudulently creating a romantic attachment through a fake identity on a dating site, the scammer can fake a need for quick cash and can motivate those who trust him to resort to unconventional means of transferring money to him. With romance scams, as with all other impostor scams, money can flow through devices like gift cards, reloadable stored value cards, mobile payment services, or classic wire-transfer services. Next, I discuss how pressure has begun to be applied, and could be further placed, on these types of financial intermediaries to raise the cost of perpetrating impostor fraud.

3. Payment Mechanisms

Of course, if scammers cannot get paid, or paid easily, their motivation will evaporate. Ultimately, nothing can stop scammers from inducing victims from sending dollar bills through the mail except the inconvenience and suspicion that may be raised from doing so. Thus, wire service providers, including banks and entities like Western Union, should enhance their warnings about impostors. For example, banks can warn customers about impostor fraud during the mortgage lending escrow process, telling them to be vigilant about directing wire transfers.[336]

---

336. *See* Aly J. Yale, *Real Estate Wire Fraud Is Real—And It Almost Happened to Me*, FORBES (May 7, 2019), https://www.forbes.com/sites/alyyale/2019/05/07/real-estate-wire-fraud-is-real-and-it-almost-happened-to-me/#dabb2781c47a [https://perma.cc/FK2X-6PQR] (describing how this type of scheme works).

With respect to identity theft through credit and debit cards, federal law shifts the weight of heavy losses to the financial institutions with a cap on consumer exposure.[337] By pushing more of the responsibility onto the financial institutions, both the consumer and the financial institution bear some incentive to take measures to avoid fraud. Credit card charges can be canceled if the mark becomes aware of the fraud, depriving the scammer of the payment making this payment system less ideal than other alternatives.

In recent years, impostor scammers have increasingly asked victims to use stored-value cards (gift cards) to enable easy and untraceable methods of transferring money.[338] The FTC reports that the number of victims reporting use of these gift cards rose 270 percent between 2015 and 2018.[339] Gift and reloadable cards became the most common method of money transfer between victim and scammer, a match with the dynamic of impostor fraud becoming the most frequently reported scam. As with many steps in the impostor scamming chain, there are chokepoints for financial transfers that regulators and merchants can use to slow fraud.

The FTC reports that "scammers are telling people to buy gift cards at Walmart, Target, CVS, Walgreens, and other retail shops."[340] Forty-two percent of victims have used Google Play and iTunes cards for their payment.[341] Retailers have the opportunity at purchase to warn their customers about these scams. They can stop shoppers who buy cards, or a certain dollar amount of these cards, and warn them to be vigilant about scams. Customers can be required to sign electronic disclosures at the point of sale that can warn of the traditional and most recent flavors of scams. Further, providers of stored-value cards, like Google Play and iTunes, can take a role in warning users about how they can be vehicles for theft and deceit. Perhaps a twenty-four- to forty-eight-hour cooling off period before stored-value card usage would enable some time for consumers to figure out what may be happening. Although no degree of warnings may dissuade an overly stressed consumer from transferring money to a scammer, education, forced caution, and

---

337. The Fair Credit Billing Act caps consumer exposure to unauthorized credit card use and charges to $50 if reported in a timely way. 41 U.S.C. § 1643. The Electronic Fund Transfer Act provides a similar structure of caps for ATM and debit card consumer liability for unauthorized use with some burden on the user for disclosure. *Id.* § 1693.

338. *See* Cristina Miranda, *Scammers Demand Gift Cards*, FED. TRADE COMM'N: CONSUMER INFO. (Oct. 16, 2018), https://www.consumer.ftc.gov/blog/2018/10/scammers-demand-gift-cards [https://perma.cc/5C4W-97Y5].

339. *Id.*

340. *Id.*

341. *Id.*

deliberation may diminish the utility of these instruments to impostors.

The cutting edge of payment systems also warrants monitoring. The Fintech sector has enabled banks and credit card companies to enable person-to-person money transfers, which may also present novel technical challenges for consumers.[342] Finance entities using these applications, as well as their regulators, should promote consumer vigilance about transferring payments to people they might not know, and offer verification services that will make imposture difficult through these emergent technologies. As with other chokepoints, consumer education, mandatory warnings, and user verification can play a constructive role. Though these tools may be new, as explained here at length, imposture is an established phenomenon hungry for new tools.

As with other tools exploited by fraudsters, the financial transfer chokepoint presents an opportunity to slow down impostors—to prevent them from achieving their payday at the very last step. Similarly, citizens, policymakers, and the financial sector must be vigilant about how impostors can abuse technical advances in this innovative arena. Those who commercially benefit from this technology and these systems are closest to the potential solutions to impostor fraud at this crucial juncture.

CONCLUSION

Fraud is an old problem, and impostor fraud is not only persistent but also prevalent as a social and economic scourge. The justification for fighting this type of fraud has never been higher, given that the systems that impostors can appropriate and exploit have never been more efficient and effective for them. Policymakers should constantly scan the horizon to see how these scammers are succeeding, identify the least-cost avoider chokepoints for this fraud, and apply pressure. Given the tremendous power that impostor fraud has, the only prescriptions for slowing it down are vigilance and being as innovative as the fraudsters. To do any less will only encourage the problem to expand.

---

342. *See* Erin Fonte, *2017 U.S. Regulatory Overview of Mobile Wallets and Mobile Payments*, 17 WAKE FOREST J. BUS. & INTELL. PROP. L. 549 (2017) (describing the landscape of the challenges presented by mobile payments systems and associated risks).