PROSECUTING CYBERCRIMES: THE CASE FOR MAKING THE COMPUTER FRAUD AND ABUSE ACT A PREDICATE ACT UNDER THE RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS ACT

DIANA CHUNG*

INTRODUCTION

During the first six months of 2021, financial services firms throughout the United States raised alarms concerning nearly $600 million of transactions that were flagged as suspected payments to perpetrators of ransomware attacks.[1] Meanwhile, the U.S. Department of Treasury identified another $5.2 billion of potential ransomware payments that were funneled through bitcoin transactions.[2] In total, global ransomware attacks were expected to have accounted for about $20 billion of loss in 2021[3] and are predicted to result in $265 billion of loss by 2031.[4] Ransomware is just one of twenty-four different categories of internet crimes identified by the Federal Bureau of Investigation ("FBI") in its annual Internet Crime Report, and the figures cited in the report represent only a fraction of the total amount lost to cybercrime every year.[5] As the number of cybercriminals and the

* J.D. 2023, University of Southern California Gould School of Law.

1. Ian Talley, *Suspected Ransomware Payments Nearly Doubled This Year, Treasury Says*, WALL ST. J., http://www.wsj.com/articles/suspected-ransomware-payments-for-first-half-of-2021-total-590-million-11634308503 [http://perma.cc/KQC6-7DJH].

2. *Id.*

3. Steve Morgan, *Cybercrime to Cost the World $10.5 Trillion Annually by 2025*, CYBERCRIME MAG. (Nov. 13, 2020), http://www.cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021 [http://perma.cc/U266-HWZR].

4. David Braue, *Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031*, CYBERCRIME MAG. (June 2, 2022), http://www.cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031 [http://perma.cc/CMT4-MCER].

5. FED. BUREAU OF INVESTIGATION, INTERNET CRIME REPORT 2021, at 22 (2021) [hereinafter

sophistication of their methods continue to grow and evolve, the true cost of cybercrime worldwide is estimated to reach a disastrous $10.5 trillion by 2025.[6]

The scale and scope of cyberattacks have increased dramatically in recent years, spurred by a growing reliance on technology, increased connectivity among users, and the rise in popularity of virtual currency exchanges. Another contributing factor is that the very nature of cybercrime makes it difficult to block these attacks or punish those responsible. For example, cybercriminals frequently rely on a variety of techniques to hide their identities and evade detection by law enforcement, such as by operating out of the dark web or routing their activities through a virtual private network ("VPN"). The increasing use of virtual currencies also contributes to this problem by making it more difficult to trace monetary payments made by victims of cybercrime.

Prosecutions of cyberattacks have been constrained by decades-old statutes that are either inapplicable or insufficient to address rapidly changing social and technological environments that contribute to the proliferation of new cybercrimes. In addition to these challenges, many cybercriminals often reside in or flee to countries that are beyond the jurisdictional reach of the United States. In several widely publicized cases, cyberattacks were also believed to be sponsored by hostile foreign state actors. Unfortunately, many victims of these cybercrime attacks are reluctant to report them, usually due to the fact that while reporting an attack does little to address the harm caused, doing so may draw unwanted publicity or attention. Therefore, if the United States wishes to properly address the rise of cybercrime and its accompanying harm to the global economy, Congress must first pass legislation that would authorize the government to overcome these barriers and increase prosecutorial power over cybercrime.

One proposition that appeared before Congress was to expand the Racketeer Influenced and Corrupt Organizations ("RICO") Act, codified in 18 U.S.C. §§ 1961–1968. This proposition was included in Section II of the International Cybercrime Prevention Act, which was originally presented in 2018 and was later reintroduced by a bipartisan group in June 2021.[7] After it was referred to the U.S. Senate Committee on the Judiciary, the bill stalled

2021 INTERNET CRIME REPORT], http://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf [http://perma.cc/3HPR-MCQN].

6. Morgan, *supra* note 3 (noting that the estimated $10.5 trillion loss includes not just monetary payments made directly to ransomware criminals but also costs associated with data destruction and damage, lost productivity, intellectual property theft, fraud, investigations, restoring damaged systems, and harm to reputation).

7. International Cybercrime Prevention Act, S. 2139, 117th Cong. § 2 (2021).

and ultimately failed to pass.[8] The status of the bill reflects the general shortage of political capital when it comes to prioritizing cybercrime despite the FBI's characterization of "malicious cyber activity" as a threat to "the public's safety and our national and economic security."[9]

To raise awareness about the threats posed by cybercrimes, this Note will analyze the proposal to expand RICO and, in particular, examine the benefits of making a violation of the Computer Fraud and Abuse Act ("CFAA") a predicate act for RICO offenses. While a few successful prosecutions of organized cybercrime rings have already been brought under RICO, this Note will evaluate the limitations of those prosecutions when it comes to computer crimes. The Note will conclude that despite the many challenges associated with tackling cybercrime, the constructive application of RICO carries great potential in prosecuting cybercriminals.

Part I of this Note provides the historical context behind RICO and examines its role in the downfall of the American Mafia. It specifically looks at the provisions in RICO that uniquely positioned it for prosecuting organized crime groups as well as legitimate business enterprises that violated state and federal laws. Part II provides an analysis of how RICO applied to traditional organized crime groups and how cybercrime groups can fall under its broad definition of "enterprise." It also provides further context on the rise of cybercrime and introduces examples of RICO charges that were brought against two cybercrime enterprises. Part III introduces the CFAA and points to key provisions that could be used against cybercrime. It also seeks to address criticisms of the proposal to make violations of the CFAA a predicate act under RICO and evaluates key policy considerations involved in this discussion.

I. BACKGROUND

A. THE RISE OF THE MAFIA IN THE UNITED STATES

On October 15, 1970, Congress passed the RICO Act[10] as part of the Organized Crime Control Act of 1970.[11] Congress's actions were largely in response to the growing presence of a well-known criminal organization that wielded considerable influence and power: the American Mafia. Less than

8. *117 Legislative Outlook S. 2139*, LEXIS+, http://plus.lexis.com/api/permalink/c5af9789-ac9a-4b89-979f-a062c35d96e6 [http://perma.cc/9SEB-ZUV2] (showing the bill's failure to pass, even in the first committee).

9. *What We Investigate: Cyber Crime*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/investigate/cyber [http://perma.cc/EL3B-TV9B].

10. 18 U.S.C. §§ 1961–68.

11. Organized Crime Control Act of 1970, 91 Pub. L. No. 91-452, 84 Stat. 922, 923.

ten years after the Act was passed, prosecutors used RICO to successfully convict key members of the American Mafia and dismantle its operations. By 1985, the heads of each of the four New York City Mafia families had been convicted and jailed, each sentenced to heavy prison terms.[12] Over time, the prosecutorial power afforded by RICO led to the eventual downfall of these crime families, and to this today, they remain "shadows of their former selves."[13]

The American Mafia first rose to power during the 1920s and later became the preeminent organized crime syndicate in the United States.[14] By the 1960s, the Mafia had grown its operations from illicit liquor transactions during the Prohibition era to drug trafficking, illegal gambling, and infiltration of labor unions and legitimate businesses.[15] Prosecutions of mob-related crimes were difficult, hampered by laws that only allowed the prosecution of individual criminals. These particular criminals were frequently part of a criminal enterprise headed by a Mafia crime family, and while they acted at the direction of its leaders, they were usually low-level operatives, far removed from the top rungs of the organization.[16] The law treated their crimes as isolated incidents rather than as acts on behalf of a criminal enterprise and, by doing so, shielded the heads of these crime families from criminal prosecution.[17] As a result, the Mafia continued to expand their operations undeterred, secure in the fact that even if a low-level criminal was caught and convicted, another could simply take his or her place.

With the introduction of RICO, the government was finally able to break this cycle. RICO armed prosecutors with the ability to simultaneously prosecute multiple members of criminal organizations like the Mafia.[18] RICO also made membership itself a criminal offense.[19] The result was that the U.S. government finally had the prosecutorial power to pursue not only the lowest-ranking criminals but also the highest members of the crime

12. Nathan Koppel, *They Call It RICO, and It Is Sweeping*, WALL ST. J., http://www.wsj.com/articles/SB10001424052748704881304576094110829882704 [http://perma.cc/Z9HA-9SJT] (noting that the head of a fifth family, Paul Castellano, was assassinated before his case went to trial).

13. James B. Jacobs, *The Rise and Fall of Organized Crime in the United States*, 49 CRIME & JUST. 17, 17, 48–50 (2019).

14. *Origins of the Mafia*, HIST. (May 28, 2019), http://www.history.com/topics/crime/origins-of-the-mafia#section_3 [http://perma.cc/K8XW-932A].

15. *Mafia in the United States*, HIST. (June 7, 2019), http://www.history.com/topics/crime/mafia-in-the-united-states [http://perma.cc/9S5X-64LQ].

16. *Racketeer Influenced and Corrupt Organizations (RICO) Law*, JUSTIA, http://www.justia.com/criminal/docs/rico [http://perma.cc/N6PG-UURW].

17. *Id.*

18. Jacobs, *supra* note 13, at 20.

19. *Id.*

family. Over time, prosecutors were able to bring down major players within the Mafia, which in turn had a crippling effect on the rest of the enterprise.[20]

While RICO was initially passed to target the American Mafia, it was subsequently used to prosecute the crimes of other organized crime syndicates, ranging from gangs and cartels to even legitimate enterprises, like an antiabortion group that broke federal and state laws when attempting to bar access to reproductive healthcare.[21] For example, prosecutors invoked RICO when charging the Hells Angels motorcycle gang with numerous racketeering activities, which ranged from drug trafficking, arms trafficking, conspiracy, money laundering, attempted armed robbery, and more.[22] Its civil suit provision was also used to try and hold legitimate businesses like British Petroleum accountable for the 2010 Deepwater Horizon oil spill in the Gulf of Mexico that killed eleven people and injured seventeen others.[23] In the past few years, with the rise of cybercrime and a deeper understanding of the harm it causes, there has been renewed focus on the potential application of RICO to a new type of organized crime group: cyber gangs.

B. RELEVANT STATUTORY PROVISIONS UNDER RICO

The RICO Act makes it illegal for any person to acquire an interest in or control an enterprise through income produced from a pattern of racketeering activity.[24] It also prohibits participation in unlawful activities conducted by the enterprise that affect interstate or foreign commerce.[25] Under 18 U.S.C. § 1962(d), it is illegal to even conspire to violate any of the provisions in the section.[26] In the context of this criminal statute, a "person" refers to either an individual or an entity that has the capacity to hold a legal or beneficial interest in property.[27] This definition means that anyone from a corporate officer to the lowest-ranking individual in a criminal organization can fall under the scope of RICO. In addition, an "enterprise" consists of "any individual, partnership, corporation, association, or other legal entity,

20. *Id.* at 48–53.

21. Edward Hasen, Virginia Fergusson, Morgan Hensley, Jonghyun Lee & John Richardson, *Racketeer Influenced and Corrupt Organizations*, 58 AM. CRIM. L. REV. 1371, 1421 (2021).

22. *See* Press Release, U.S. Att'y's Off., Distr. of S. Carolina, Hells Angels Members Convicted of Racketeering Conspiracy for Their Dealings with Drugs, Guns, Armed Robbery, and Money Laundering (Mar. 20, 2013), http://archives.fbi.gov/archives/columbia/press-releases/2013/hells-angels-members-convicted-of-racketeering-conspiracy-for-their-dealings-with-drugs-guns-armed-robbery-and-money-laundering [http://perma.cc/6XSJ-68VT].

23. Dietrich Knauth, *BP Hit with RICO Action in Deepwater Horizon MDL*, LAW360 (Jan. 25, 2011, 3:26 PM), http://www.law360.com/articles/221825/bp-hit-with-rico-action-in-deepwater-horizon-mdl [http://perma.cc/K8X8-96JF].

24. 18 U.S.C. § 1962.

25. *Id.* § 1962(a).

26. *Id.* § 1962(d).

27. *Id.* § 1961(3).

and any union or group of individuals associated in fact although not a legal entity."[28] This broad definition of enterprise was meant to address the wide range of acts conducted by the Mafia and other organized crime groups.

A "pattern of racketeering activity" can be established if there are at least two acts of racketeering within ten years of each other that are related.[29] Racketeering acts are considered "related" if they demonstrate that they were conducted for the same or similar purpose or result or if they involved the same or similar participants, victims, or methods.[30] The acts must also be continuous or related to a threat that the criminal activity will continue.[31] Lastly, acts are "continuous" if they occur over a long-term closed period or if the very nature of the unlawful act establishes a threat that the act will be repeated in the future.[32]

RICO provides an enumerated list of thirty-five acts that can be construed as "racketeering activities."[33] At the time RICO was passed, some common racketeering activities included money laundering, murder, sexual exploitation of children, bribery, extortion, and obstruction of justice.[34] Since then, the utilization of new technology by sophisticated criminals has contributed to the creation of "acts" that are still conducted by organized crime groups but no longer fall squarely within the enumerated activities. These "cyber" crimes, ranging from illegal activity on the dark web to costly ransomware attacks against companies, have eclipsed the types of traditional crimes considered by Congress when it first drafted and passed RICO.

To bring a RICO charge, the government must prove beyond a reasonable doubt that (1) an enterprise existed; (2) the enterprise affected interstate or foreign commerce; (3) a person, whether an individual or an entity, was associated with, participated in, or was employed by the enterprise; (4) the person engaged in a racketeering activity; and (5) the person engaged in acts that showed a pattern of racketeering activity.[35] The requisite mens rea is simply the commission of a predicate act.[36]

When bringing a conspiracy charge under RICO, the government is not required to show that the defendant agreed with all the other conspirators,

28. *Id.* § 1961(4).
29. *Id.* § 1961(5); Hasen et al., *supra* note 21, at 1377–81.
30. Hasen et al., *supra* note 21, at 1377–81.
31. *Id.* at 1378.
32. *Id.* at 1380–82.
33. 18 U.S.C. § 1961(1).
34. *Id.*
35. *Criminal Resource Manual: 109. RICO Charges*, U.S. DEP'T OF JUST. ARCHIVES, http://www.justice.gov/archives/jm/criminal-resource-manual-109-rico-charges [http://perma.cc/ZJ2V-7XEN].
36. Hasen et al., *supra* note 21, at 1373.

was aware of and knew the other conspirators, or had full and complete knowledge of the conspiracy and its details.[37] Rather, the government need only show that the defendant agreed to engage in two or more racketeering activities, that the defendant was generally aware of a conspiracy, and that the defendant knew that the conspiracy went beyond the individual racketeering act.[38] These components of a RICO charge were intentionally crafted to be applicable to a wide variety of crimes, and today, they can be further utilized to investigate and prosecute cybercrime.

C. RISE OF CYBERCRIME

Today is an era of unprecedented digital connectivity, spurred by rapid advancements in technology and cultural shifts in how people live, work, and interact. Technology is now a part of our daily lives, and as our reliance on it has grown, so too has our vulnerability to attacks by cybercriminals. Before cybercrime grew into its own "industry," computer crimes were typically limited to small-scale blackmail operations, such as financial exfiltration, and usually involved financial institutions, petty theft, and reputational damage.[39] In a matter of years, they have evolved from a distant threat to an immense national security concern. Cybercrimes now affect millions of people and have led to increased vulnerabilities in both the private and public sectors.[40]

Events in 2020 and 2021 alone have demonstrated the increased frequency and sophistication of cybercrimes. For example, when the COVID-19 pandemic started around February 2020, businesses were forced to accelerate their digitization plans, which compromised the security of their systems and created new access points that became vulnerable to hackers. Employees were encouraged or required to work from home to prevent the spread of COVID-19, and while the remote working environment was key to public health, it was detrimental to cybersecurity. Many companies lacked remote-capable corporate devices, such as laptops or phones, that they could readily distribute to employees, so they often allowed the use of personal devices to access company files and records.[41] Personal devices rarely have adequate antivirus or antimalware programs, if at all, and the isolation of employees from their peers made them particularly susceptible to

37. *Criminal Resource Manual*, *supra* note 35.

38. *Id.*

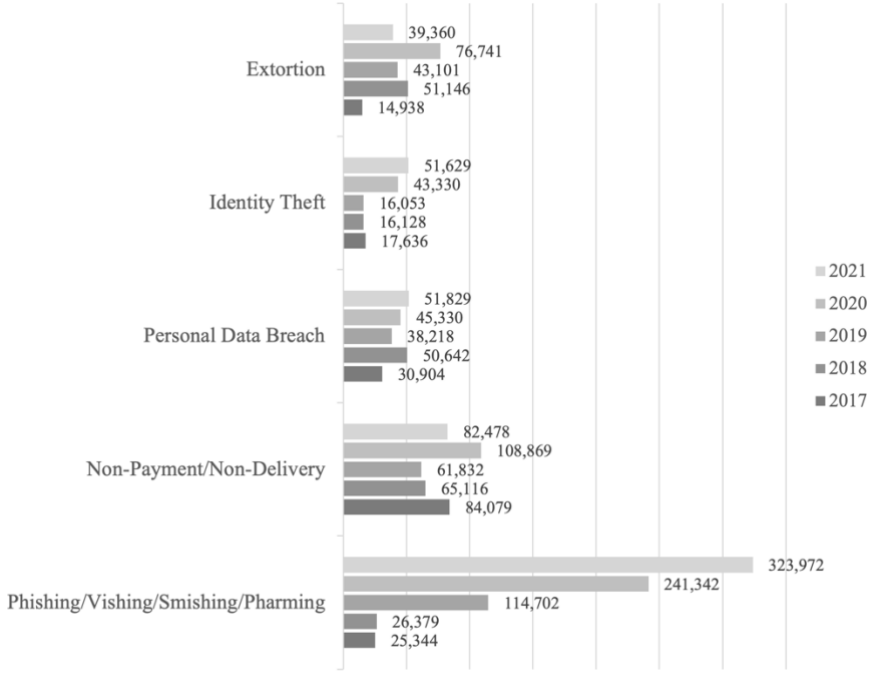
39. Dominic Rushe & Julian Borger, *Age of the Cyber-Attack: US Struggles to Curb Rise of Digital Destabilization*, GUARDIAN (June 14, 2021, 2:00 PM), http://www.theguardian.com/technology/2021/jun/14/age-of-the-cyber-attack-us-digital-destabilization [http://perma.cc/5L2W-ZYEH].

40. *Id.*

41. Cedric Nabe, *Impact of COVID-19 on Cybersecurity*, DELOITTE, http://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html [http://perma.cc/UL5V-QZQG].

cyberattacks like phishing, pharming, and vishing.[42] Those attacks significantly increased in volume during the pandemic and were commonly used to gain access to devices, as shown in Figure 1.[43]

FIGURE 1. Top Five Crime Types Compared with the Previous Five Years



Source: 2021 INTERNET CRIME REPORT, *supra* note 5, at 8.

In addition, personal wireless networks lack the security protections that companies use for their internal networks, which make them easier to infiltrate.[44] Once inside the network, hackers could easily install malware or key-logging software to steal account credentials and other sensitive

42. *Id.*

43. 2021 INTERNET CRIME REPORT, *supra* note 5, at 8. For other cybercrimes analyzed by the FBI in its 2021 report, see *id.* at 22–23.

44. Nabe, *supra* note 41.

information.

In 2020, the Internet Crime Complaint Center ("IC3") received a record 791,790 complaints from the public regarding suspected or proven cases of cybercrime, a 69% increase from 2019;[45] in 2021, the IC3 received 847,376 complaints, a 7% increase from 2020.[46] The IC3 is a platform operated by the FBI that allows people in the public to submit reports about suspected computer crimes, which range from economic espionage and theft of trade secrets to online extortion, identity theft, and money laundering.[47] In 2021, the costs associated with those complaints exceeded $6.9 billion.[48] Given that there is no strong incentive to report cybercrimes to the IC3 other than for data-collection purposes, these figures are widely known to be underreported.

TABLE 1. Cybercrime Costs for Victims by Age Range

Victims		
Age Range	*Total Count*	*Total Loss*
Under 20	14,919	$101,435,178
20 - 29	69,390	$431,191,702
30 - 39	88,448	$937,386,500
40 - 49	89,184	$1,192,890,255
50 - 59	74,460	$1,261,591,978
60+	92,371	$1,685,017,829

Source: 2021 INTERNET CRIME REPORT, supra note 5, at 19.

To maximize profits, cybercriminals often targeted specific demographic groups, such as the elderly. In 2021, cybercriminals exploited the elderly population out of nearly $1.7 billion, as shown in Figure 2.[49] In addition, while the number of elderly victims rose from 2019 to 2020 and

45. FED. BUREAU OF INVESTIGATION, INTERNET CRIME REPORT 2020, at 3 (2020) [hereinafter 2020 INTERNET CRIME REPORT], http://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf [http://perma.cc/8EDD-TD5M]. The sharp 69% increase from 2019 to 2020 reflects the unprecedented wave of cyberattacks brought on by the COVID-19 pandemic.

46. 2021 INTERNET CRIME REPORT, *supra* note 5, at 3.

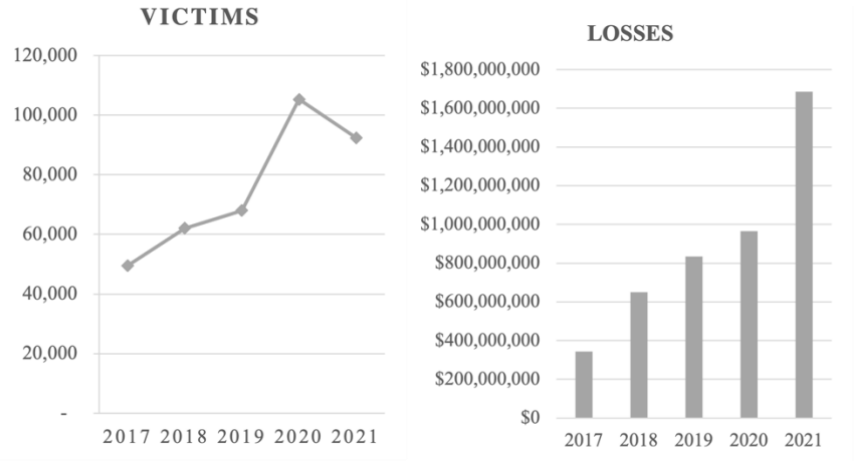
47. *Id.* at 4–5.

48. *Id.* at 3.

49. FED. BUREAU OF INVESTIGATION, ELDER FRAUD REPORT 2021, at 3, 5 (2021), http://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3ElderFraudReport.pdf [http://perma.cc/U7C2-BBCH].

slightly decreased in 2021, this change was accompanied by a sharp increase in the total losses, as shown in Figure 2 below.[50] This demonstrates that the total loss per victim rose significantly in 2021. Again, it is important to remember that this number only accounts for the losses that were actually reported to the FBI.

FIGURE 2. Reporting for Past Five Years for Victims Over 60



Source: FED. BUREAU OF INVESTIGATION, ELDER FRAUD REPORT 2021, *supra* note 49, at 5.

Since the COVID-19 pandemic started in early 2020, many elderly victims suddenly found themselves forced to shop online rather than in-person, which increased the risk of purchasing counterfeit goods and being deceived by fraudulent advertisements.[51] They were also more likely to be isolated from friends and family members, which made them particularly susceptible to romance scams, extortion, government impersonators, and investment scams.[52] Cybercriminals also targeted them through technology support fraud by offering to provide the elderly with unsolicited technical support that tricked them into providing access to their devices and bank accounts.[53]

50. *Id.* at 5.
51. *Id.* at 9.
52. *Id.* at 13–16.
53. *Id.* at 13.

D. TYPES OF CYBERCRIME

Cybercrime can present itself in a variety of forms but generally can be categorized into two groups: when a computer is used as a tool and when a computer is the target.[54] Commonly, cybercriminals behind malwares, ransomware attacks, and distributed denial-of-service ("DDoS") attacks target computers belonging to other people for the purpose of gaining unauthorized access and stealing information.[55] Other cybercriminals, usually less sophisticated, opt to use computers as a tool for cyberstalking, marketing scams, and identity theft.[56]

As can be seen in Table 2, crimes involving the use of a computer as a tool are more common than crimes where specific computer users or companies are targeted.[57] For example, there were only about 3,729 reported victims of a ransomware attack, which targets specific computers to access the information that they contain.[58] On the other hand, there were more than 323,972 victims of phishing, vishing, smishing, and pharming, which all utilize a computer as a tool to carry out scam campaigns.[59] This makes up almost half of the total 847,376 complaints reported to the FBI in 2021.[60]

TABLE 2. Types of Cybercrime by Number of Victims

By Victim Count

Crime Type	*Victims*	*Crime Type*	*Victims*
Phishing/Vishing/Smishing/ Pharming	323,972	Government Impersonation	11,335
Non-Payment/Non-Delivery	82,478	Advanced Fee	11,034
Personal Data Breach	51,829	Overpayment	6,108
Identity Theft	51,629	Lottery/Sweepstakes/ Inheritance	5,991
Extortion	39,360	IPR/Copyright and Counterfeit	4,270
Confidence Fraud/Romance	24,299	Ransomware	3,729

54. Guillermo Berasategui, *Cybercrime: Which Ones Are the Most Common Threats Today?*, RED POINTS, http://www.redpoint.com/blog/cybercrime [http://perma.cc/WZ6Z-QCXD].
55. *Id.*
56. *Id.*
57. 2021 INTERNET CRIME REPORT, *supra* note 5, at 22.
58. *See infra* Table 2.
59. *Infra* Table 2.
60. 2021 INTERNET CRIME REPORT, *supra* note 5, at 3.

Tech Support	23,903	Crimes Against Children	2,167
Investment	20,561	Corporate Data Breach	1,287
BEC/EAC	19,954	Civil Matter	1,118
Spoofing	18,522	Denial of Service/TDoS	1,104
Credit Card Fraud	16,750	Computer Intrusion	979
Employment	15,253	Malware/Scareware/Virus	810
Other	12,346	Health Care Related	578
Terrorism/Threats of Violence	12,346	Re-shipping	516
Real Estate/Rental	11,578	Gambling	395

Source: 2021 INTERNET CRIME REPORT, *supra* note 5, at 22.

Phishing involves using authentic-looking emails to trick people into providing their personal or financial information, and it is frequently accompanied by pharming, which involves the creation of a fake website that seems legitimate and prompts people to enter information like bank account usernames and passwords.[61] Vishing is similar to phishing except that it utilizes fraudulent phone calls or voice messages that appear to be coming from financial institutions or government agencies like the Internal Revenue Service ("IRS").[62] Smishing involves fraudulent text messages that induce people into clicking links that may prompt the disclosure of private information or secretly install malware.[63] Cybercriminals that utilize these methods usually do so as part of massive spam campaigns; the sheer volume of attacks contributes to their success and profitability, as can be seen in Table 3, which shows over $44.2 million in losses from phishing, vishing, smishing, and pharming in just 2021 alone.[64]

61. Anna Efimenko, *Phishing, Vishing, Smishing, Pharming – What Is the Difference*, PROTECTIMUS (Apr. 12, 2018), http://www.protectimus.com/blog/phishing-vishing-smishing-pharming [http://perma.cc/76DT-PWGN].

62. *Id.*

63. *Id.*

64. *2021 INTERNET CRIME REPORT*, *supra* note 5, at 23.

TABLE 3. Types of Cybercrime by Cost

By Victim Loss

Crime Type	*Loss*	*Crime Type*	*Loss*
BEC/EAC	$2,395,953,296	Lottery/Sweepstakes/ Inheritance	$71,289,089
Investment	$1,455,943,193	Extortion	$60,577,741
Confidence Fraud/ Romance	$956,039,740	Ransomware	$49,207,908
Personal Data Breach	$517,021,289	Employment	$47,231,023
Real Estate/ Rental	$350,328,166	Phishing/Vishing/Smishing/Pharming	$44,213,707
Tech Support	$347,657,432	Overpayment	$33,407,671
Non-Payment/ Non-Delivery	$337,493,071	Computer Intrusion	$19,603,037
Identity Theft	$278,267,918	IPR/Copyright and Counterfeit	$16,365,011
Credit Card Fraud	$172,998,385	Health Care Related	$7,042,942
Corporate Data Breach	$151,568,225	Malware/Scareware/Virus	$5,596,889
Government Impersonation	$142,643,253	Terrorism/Threats of Violence	$4,390,720
Advanced Fee	$98,694,137	Gambling	$1,940,237
Civil Matter	$85,049,939	Re-shipping	$631,466
Spoofing	$82,169,806	Denial of Service/TDoS	$217,981
Other	$75,837,524	Crimes Against Children	$198,950

Source: 2021 INTERNET CRIME REPORT, *supra* note 5, at 23

In other cyberattacks, criminals specifically target the computers and accounts of certain individuals within a company. In 2021, there were nearly 20,000 of these Business Email Compromise ("BEC") complaints, which constituted nearly $2.4 billion in losses.[65] Relying on social engineering tactics, criminals using BEC methods convince individuals responsible for transferring funds within a company to submit wire transfers to a fraudulent account or location.[66] They often pose as the company's chief executive officer or chief financial officer and "spoof" the business emails of their targets to make the transactions appear legitimate.[67] These types of cases have expanded over the years to include criminals that pose as vendors, attorneys, and the IRS.

However, crimes that involve targeting specific computers also generate massive profits for criminals and cause significant damage in their wake. In May 2017, a malicious malware quickly spread around the world and infected more than 230,000 computers across 150 countries within just a few hours.[68] The malware, called WannaCry, is estimated to have resulted in billions of dollars of losses, not only from the immediate ransom payments but also from the subsequent fallout.[69] The National Health Service in the United Kingdom was hit hard, with thirty-four hospital trusts infected and forty-six others affected as a result.[70] The malware took down computer systems, disabled medical devices like MRIs, rerouted emergency ambulances, and led to disruptions in medical care all over the country.[71] One of the reasons it spread so quickly and caused so much damage was because a large number of users and companies were still using outdated Microsoft Windows software.[72] An earlier patch update had identified and fixed this security vulnerability nearly two months before the attack, but it was overlooked by many.[73] The malware was later traced to the North Korean government, which has denied allegations that it was behind the attack.[74]

65. *Id.* at 9.
66. *Id.*
67. *Id.*
68. *What Is WannaCry Ransomware?*, KASPERSKY, http://usa.kaspersky.com/resource-center/threats/ransomware-wannacry [http://perma.cc/X68R-GWFC].
69. *Id.*
70. S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi & P. Aylin, *A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS*, NPJ DIGIT. MED., Oct. 2, 2019, at 1, http://www.nature.com/articles/s41746-019-0161-6.pdf [https://perma.cc/6RMK-BTGC].
71. *Id.*
72. *What Is WannaCry Ransomware?*, *supra* note 68.
73. *Id.*
74. *Id.*

II. ANALYSIS

Part II of this Note takes a deeper dive into how RICO, a statute primarily used against traditional crime groups, can be used to prosecute cybercriminal rings, which usually have a different membership structure. To start, Section A analyzes three different models that are typically associated with traditional organized criminal groups and examines the reasons why RICO applies to them.[75] It then compares and contrasts those models against a cybercriminal group to establish that RICO's broad definition of the word "enterprise" extends to organized cybercrime groups.[76] Sections B and C examine two cases that successfully invoked RICO to prosecute members of a cybercriminal ring as well as a business that facilitated cybercrime. Both Sections, however, point to the limitations of RICO in those cases as well as other situations involving computer crime.[77]

A. RICO'S APPLICATION TO CYBERCRIME ENTERPRISES

When RICO was passed in 1970, Congress intended that it be used to prosecute traditional organized crime groups, such as the American Mafia. Given the broad swath of activities and operations conducted by the Mafia and similar organized crime groups, Congress did not strictly limit the type of enterprises that could be reached by the Act. Under RICO, the broad definition of "enterprise" includes not only illegal entities comprised of loosely connected associations but also legitimate business enterprises. In assessing whether RICO can be used to reach organized cybercriminal groups, we must first analyze how cybercriminal groups compare with traditional organized crime groups and legitimate business enterprises. It is also important to understand the characteristics of "cyber gangs" that support their designation as an enterprise under RICO.

There are three common models of traditional organized criminal groups, each of which fall under RICO's definition of enterprise: (1) the hierarchical model; (2) the local, cultural model; and (3) the enterprise or business model.[78] The hierarchical model is composed of interdependent individuals within a structure that clearly separates "leaders" from "members."[79] Leaders within this model make decisions about management,

75. *See infra* Section II.A.

76. *See infra* Section II.A.

77. *See infra* Sections II.B–C.

78. *Summary*, UNITED NATIONS OFF. ON DRUGS & CRIME (May 2018), http://www.unodc.org/e4j/en/organized-crime/module-7/key-issues/summary.html [http://perma.cc/Y9E4-9R7F].

79. *Hierarchical Model of Organized Criminal Groups*, UNITED NATIONS OFF. ON DRUGS & CRIME (May 2018), http://www.unodc.org/e4j/en/organized-crime/module-7/key-issues/hierarchical-

such as where to operate, which illegal activities to engage in, and how the business is run.[80] Members, on the other hand, are responsible for carrying out the unlawful activities of the group, such as kidnapping, drug trafficking, extortion, and bribery.[81]

The structure of the Mafia closely follows a strict, hierarchical model. At the top of each Mafia family is the "don" who is clearly and indisputably the head of the criminal group.[82] The don is counseled by a "consigliere" who serves as his confidant and trusted advisor on all matters and thus wields significant influence.[83] The second-in-command is the "underboss," who is usually the son of the don and expected to succeed him.[84] A group of "capos" report to the second-in-command, and they serve to provide liability protection for the highest-ranked Mafia members.[85] The capos also supervise "soldiers," who are the lowest-ranked members of the group but responsible for directly carrying out the crimes of the Mafia; they are often required to complete "initiation" acts to officially enter the organization.[86] Because of this structure, at each level of the Mafia, there are established roles and responsibilities that clearly delineate the leaders of the crime family from the low-level operatives. Insubordination by one of the lower-ranked members in such a model would not be acceptable and would likely result in the member's death or incapacitation.

In the local, cultural model, ties within the organization are usually based on either cultural or ethnic affiliations.[87] These shared characteristics tend to reinforce relationships between its members and allow them to operate within an environment of trust. Accordingly, the organization's structure is generally flat, and each member is given more power and responsibility with less supervision.[88]

The local, cultural model may serve as the basis for local terrorist groups, which tend to share a common religious ideology or a set of cultural beliefs. While these groups have historically operated in smaller and more

model.html [http://perma.cc/JL2S-23QQ].

80. *Id.*

81. *Id.*

82. *Mafia Org Chart*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/file-repository/mafia-family-tree.pdf/view [http://perma.cc/TL65-C9KU].

83. *Id.*

84. *Id.*

85. *Mafia*, BRITANNICA (Apr. 17, 2013), http://www.britannica.com/topic/Mafia [http://perma.cc/HR3Y-SZL8].

86. *Id.*

87. *Local, Cultural Model of Organized Crime*, UNITED NATIONS OFF. ON DRUGS & CRIME (May 2018), http://www.unodc.org/e4j/en/organized-crime/module-7/key-issues/local-cultural-model.html [http://perma.cc/6HE4-XZWZ].

88. *Id.*

localized areas and have not been affiliated with bigger national groups, there has been an emergence in the last decade of larger groups, like the Islamic State terrorist group. While terrorist groups are not the focus of this Note, their activities are often financed by cybercrimes involving illicit cryptocurrency fundraising, money laundering using bitcoin, and fraudulent sale of goods online.[89] This serves as an important reminder that fighting cybercrime is not only isolated to the context of cyberattacks themselves but also necessary to undercut other dangerous criminal activities that threaten national security.

The enterprise model of organized crime is based on the notion that criminals structure their unlawful activities around the need to make a profit, which lends them the appearance of entrepreneurs and small businesses.[90] Rather than relying on "massive, centralized bureaucracies," members independently collaborate with each other and take on roles typically found in businesses, such as finance, operations, security, and strategy.[91] In doing so, members must identify customer demand, detect market shifts, and counter competition, just as a legitimate small business would do; the difference is that criminal organizations focus on selling or buying illegal goods or brokering illegal transactions.[92]

Cybercriminal groups frequently display behavioral traits of legitimate companies, as embodied in the above enterprise model. For example, researchers at IBM and Google studied the way these groups operate and found that at the top of some of these groups is an individual that serves as the equivalent of a CEO.[93] This "CEO" oversees the activities of "project managers" who specialize in and take responsibility for various components of a crime. For example, a hacker may be responsible for developing the malware used to later infect targeted companies or individual devices. Following the creation of the malware, another hacker may be in charge of distributing it through phishing campaigns. Once a computer or network is infected, a separate hacker can step in to search for information that could be sold or held for ransom. Others may be simultaneously launching DDoS attacks to compromise certain accounts and networks. Throughout the

89. *Global Disruption of 3 Terror Finance Cyber-Enabled Campaigns*, U.S. IMMIGR. & CUSTOMS ENF'T, (Aug. 13, 2020), http://www.ice.gov/news/releases/global-disruption-3-terror-finance-cyber-enabled-campaigns [http://perma.cc/Y335-KQLM].

90. *Enterprise or Business Model of Organized Crime*, UNITED NATIONS OFF. ON DRUGS & CRIME (May 2018), http://www.unodc.org/e4j/en/organized-crime/module-7/key-issues/enterprise-or-business-model.html [http://perma.cc/UF75-2K55].

91. *Id.*

92. *Id.*

93. Kate Fazzini, *Cybercrime Organizations Work Just Like Any Other Business: Here's What They Do Each Day*, CNBC (May 5, 2019, 12:49 PM), http://www.cnbc.com/2019/05/05/heres-what-cybercriminals-do-during-the-workday.html [http://perma.cc/5A5P-Q7A3].

process, these "project managers" continually collaborate and coordinate with each other to avoid detection.[94] Cybercriminal groups also compete with each other to increase their share of the market and aggressively market their services for hire.

One such notorious cybercriminal group is the ransomware group Conti, who was responsible for hundreds of ransomware attacks over the past two years alone.[95] By January 2022, over one thousand victims of the Conti malware had been forced to make ransomware payments that in total exceeded $150 million.[96] In February 2022, Conti itself was subject to a massive data breach that showed insights into the group's structure.[97] It displayed remarkable similarities to a corporation, with salaried teams of developers, specialists, HR leads, and other experts.[98] It allocated funds for salaries and services, made strategic business decisions on ways to increase revenue, such as through research and best practices, and addressed threats to their business—usually law enforcement and competition.[99]

While there are a large number of cybercriminal groups that still resemble traditional organized crime groups and thus clearly fall under RICO's definition of enterprise, there are certain groups that have changed into a new, more amorphous form.[100] Colloquially called "cyber gangs," these organized cybercriminal groups consist of loosely affiliated individuals that operate under "networks of convenience" that are "more fluid, less formal, and [involve] temporary associations."[101] The structure is widely

94. *Id.*

95. *Reward for Information: Owners/Operators/Affiliates of the Conti Ransomware as a Service (RaaS): Transnational Organized Crime Rewards Program*, U.S. DEP'T OF STATE (May 6, 2022), http://www.state.gov/reward-for-information-owners-operators-affiliates-of-the-conti-ransomware-as-a-service-raas [http://perma.cc/54UA-PXHK].

96. *Id.*

97. Phil Muncaster, *Conti Group Compromised 40 Firms in Just One Month*, INFOSECURITY (June 24, 2022), http://www.infosecurity-magazine.com/news/conti-group-compromised-40-firms [http://perma.cc/RX8K-6MDC]; Matt Burgess, *The Workaday Life of the World's Most Dangerous Ransomware Gang*, WIRED (Mar. 16, 2022, 11:00 AM), http://www.wired.co.uk/article/conti-leaks-ransomware-work-life [http://perma.cc/3WTP-VX6J].

98. Burgess, *supra* note 97; Phil Muncaster, *Conti Group Suffers Massive Data Breach*, INFOSECURITY (Feb. 28, 2022), http://www.infosecurity-magazine.com/news/conti-group-data-breach [http://perma.cc/ZEP7-XRVG].

99. Burgess, *supra* note 97; Muncaster, *supra* note 98.

100. Diana Labori, *As US Pursues Tougher Cybercrime Enforcement, RICO Returns to Disarm Cyber-Mafias*, ASS'N OF CERTIFIED FIN. CRIME SPECIALISTS (July 24, 2014), http://www.acfcs.org/as-us-pursues-tougher-cybercrime-enforcement-rico-returns-to-disarm-cyber-mafias [http://perma.cc/53TA-X6SL].

101. *New Forms of Organized Crime: Networked Structure*, UNITED NATIONS OFF. ON DRUGS & CRIME (May 2018), http://www.unodc.org/e4j/en/organized-crime/module-7/key-issues/networked-structure.html [http://perma.cc/E9LN-DJYD].

decentralized, and members are spread all over the world.[102] Even when cybercriminals do associate, their interactions are usually conducted over online forums or sites on the dark web, and their criminal activities are performed purely through the computer.[103] While this "model" of organized crime is relatively new and unlike the traditional organized crime groups that RICO was originally passed to prosecute, it can still fall under RICO's broad definition of enterprise that includes "*any* union or group of individuals associated in fact."[104] In 2013, the government relied on this interpretation of enterprise to prosecute the first cybercriminal ring under RICO.

B. RICO CHARGES AGAINST A CYBERCRIME ENTERPRISE–*UNITED STATES V. CAMEZ*

One of the first computer crime cases prosecuted under RICO took place in 2013 and involved twenty-two-year-old David Ray Camez. Camez was convicted and sentenced to twenty years in prison for facilitating crimes over an Internet site called "Carder.su" that consisted of a loosely connected ring of users and served as a marketplace for stolen financial information, drug trafficking, and money laundering.[105] As part of a four-year joint investigation by the U.S. Secret Service and Homeland Security Investigations, an undercover special agent gained access to Carder.su and started selling counterfeit driver's licenses.[106] Some of the sales were made to Camez, and after searching his home and computer, agents also found counterfeit credit cards and gift cards as well as counterfeit U.S. currency. This information led to the indictment of thirty-nine members of the criminal ring, which was estimated to have over 5,500 members in total.[107]

The prosecution charged Camez on two RICO counts, one under 18 U.S.C. § 1962(c) for Camez's substantive participation in illegal acts perpetrated through Carder.su and the other under 18 U.S.C. § 1962(d) for conspiring to participate in the criminal enterprise.[108] These RICO charges were brought against Camez on the grounds that Carder.su and its users were comparable to a sophisticated organized crime group, or an enterprise. Similar to how the Mafia screened and initiated its low-ranking "soldiers,"

102. Labori, *supra* note 100.

103. *Id.*

104. 18 U.S.C. § 1961(4) (emphasis added).

105. Kevin Poulsen, *Guilty Verdict in First Ever Cybercrime RICO Trial*, WIRED (Dec. 9, 2013, 4:39 PM), http://www.wired.com/2013/12/rico [http://perma.cc/3K4Z-9BAZ].

106. Press Release, U.S. Dep't of Just., Member of Organization That Operated Online Marketplace for Stolen Personal Information Sentenced to 20 Years in Prison (May 15, 2014), http://www.justice.gov/opa/pr/member-organization-operated-online-marketplace-stolen-personal-information-sentenced-20 [http://perma.cc/5AA2-JETP].

107. *Id.*

108. United States v. Camez, 839 F.3d 871, 873 (9th Cir. 2016).

each potential Carder.su user had to go through rigorous security procedures designed to prevent detection by law enforcement or infiltration by rival criminal organizations.[109] In addition, Carder.su operated under a hierarchical structure that included an "administrator, moderators, reviewers, vendors, and members."[110] The Acting Assistant Attorney General who announced Camez's sentencing results—twenty years in prison—stated that the organization was "the new face of organized crime – a highly structured cyber network [that] operated like a business to commit fraud on a global scale."[111]

On the other hand, while this case demonstrated that RICO's broad definition of enterprise could apply to organized cybercrime groups, it only succeeded because the committed crime was an enumerated predicate act under RICO. For example, if this crime had involved hacking into a secure government database rather than fraudulent activity regarding identification documents, RICO would not have been effective here. Therefore, it is vital that violations of the CFAA be added as an additional predicate act under RICO.

C. RICO CHARGES AGAINST A BUSINESS ENTERPRISE THAT FACILITATES CYBERCRIME

While the case against Camez included a conspiracy charge, it was primarily built upon his direct participation in the criminal ring and its illegal activities. A more recent case brought in the Eastern District of Michigan established the possibility of using the existing conspiracy provision under RICO to convict owners and employees of a seemingly legitimate business enterprise that knowingly helped facilitate the crimes of cybercriminals.[112] The relevant RICO provision in this case was 18 U.S.C. § 1962(d), which makes it "unlawful for any person to conspire to violate" any of the other prohibited activities in the section.[113]

As part of this case, two Eastern European nationals were convicted and sentenced in 2021 for conspiring to engage in a racketeer-influenced and

109. U.S. Dep't of Just., *supra* note 106.

110. *Camez*, 839 F.3d at 873.

111. U.S. Dep't of Just., *supra* note 106.

112. Gov't's Sent'g Memorandum at 1, United States v. Grichishkin, No. 19-cr-20478 (E.D. Mich. 2021) [hereinafter Government's Sentencing Memorandum], http://www.courtlistener.com/docket /16927827/94/united-states-v-grichishkin [http://perma.cc/5ALZ-6Q8Z] (providing reasons for the government's sentencing request prior to the sentencing hearing); Judgment in a Criminal Case at 1, United States v. Grichishkin, No. 19-20478 (E.D. Mich. 2021) [hereinafter Judgment in a Criminal Case], http://storage.courtlistener.com/recap/gov.uscourts.mied.340252/gov.uscourts.mied.340252.116.0.pdf [http://perma.cc/43YF-58X4] (containing the court's final judgment).

113. 18 U.S.C. § 1962(d).

corrupt organization.[114] The two individuals—Pavel Stassi and Aleksandr Skorodumov—worked for a company that rented out IP addresses, servers, and domains to clients.[115] Skorodumov was a lead system administrator and helped manage the domains and IP addresses provided to clients, providing technical assistance and responding to requests for support from clients. Stassi was involved in administrative tasks that ranged from online marketing to setting up webhosting and financial accounts for the organization. At first glance, their roles were very similar to those that would be found in legally operated information technology service providers.

However, from 2008 to 2015, both Skorodumov and Stassi performed their duties with the knowledge that their company was providing bulletproof hosting services, which are frequently used by cybercriminals to launch malware and cyberattacks on companies, agencies, and individuals throughout the United States. They were also aware that their clients were cybercriminals who utilized the technical infrastructure provided by the company to gain unauthorized access to people's systems, create botnets, steal financial information, and hide from law enforcement. The defendants, along with their co-defendants—Aleksandr Grichishkin and Andrei Skvortsov—actively monitored law enforcement or security sites that exposed technical infrastructure linked to criminal activity and moved any flagged content to new infrastructure, usually registered to other false or stolen identities. The malware that was hosted by the company included Zeus, SpyEye, Citadel, and Blackhole Exploit Kit. The SpyEye and Zeus malwares alone led to millions of dollars in damages to financial institutions and their corporate clients.[116]

Skorodumov and Stassi were both convicted of one count of conspiracy under RICO even though they were only considered "employees" of the company.[117] Grichishikin, who was the founder and leader of the business, was later convicted of one count of conspiracy under RICO and sentenced to sixty months in prison.[118] Grichishkin argued that he was not engaging in illegal acts because the business itself was not directly propagating malware

114. Press Release, U.S. Dep't of Just., Four Individuals Plead Guilty to RICO Conspiracy Involving "Bulletproof Hosting" for Cybercriminals (May 7, 2021), http://www.justice.gov/opa/pr/four-individuals-plead-guilty-rico-conspiracy-involving-bulletproof-hosting-cybercriminals [http://perma.cc/3XCE-RCSH].

115. *Id.*

116. *Id.*

117. *Id.*

118. Press Release, U.S. Dep't of Just., Russian Man Sentenced for Providing 'Bulletproof Hosting' for Cybercriminals (Dec. 1, 2021), http://www.justice.gov/opa/pr/russian-man-sentenced-providing-bulletproof-hosting-cybercriminals [http://perma.cc/57UY-NSQP]; Judgment in a Criminal Case, *supra* note 112, at 2–7 (ordering a 60-month sentence but reducing it by the 109 days that Grichishkin already served in an Estonian prison and also ordering restitution damages of nearly $800 thousand).

related to "child pornography, terrorism, and fake charities."[119] However, as one of the prosecutors in the case pointed out, businesses that provide bulletproof hosting "share the criminal responsibility of their clients."[120]

This case shows that RICO may be used to charge even businesses that directly or indirectly facilitate and aid the activities of cybercriminals, including virtual cryptocurrency exchanges, VPN service providers, and certain e-commerce platforms like the Silk Road market. Cybercriminals utilize many of these services to host their malware, funnel ransomware payments, evade law enforcement, and sell illegal products like hacking software and services, drugs, weapons, and stolen data. Many of the companies that generate profit from these illegal activities turn a blind eye to them and, in several cases, like the one above, choose to help facilitate the activities of their criminal clients. As part of a whole-of-government approach against cybercrime, the Department of Treasury has already taken action against several virtual currency exchanges complicit in these sorts of schemes.[121] At the same time, just like in *Camez*, the charges here were brought based on enumerated racketeering activities that are currently within the scope of RICO. Had their acts been purely based on computer crimes alone, the charges could not have been brought against them, which underscores the need to pass effective legislation that captures violations of the CFAA under RICO.

III. ARGUMENT

Part III of this Note highlights the limitations of RICO when it comes to computer crimes and introduces the CFAA as well as the context in which it was passed.[122] Section A outlines key provisions in the CFAA that enable it to be used against a variety of cybercrimes, including ransomware attacks,[123] and demonstrates how the CFAA could be used to prosecute the cybercriminal group behind the Colonial Pipeline ransomware attack.[124] Section A also examines the benefits of making violations of the CFAA a predicate act under RICO, such as the ability to impose heftier penalties and prison terms on those convicted and thus further deter cybercrimes.[125]

119. Government's Sentencing Memorandum, *supra* note 112, at 11.
120. *Id.*
121. Press Release, U.S. Dep't. of Treasury, Treasury Continues to Counter Ransomware as Part of Whole-Of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange (Nov. 8, 2021), http://home.treasury.gov/news/press-releases/jy0471 [http://perma.cc/46LF-YF8Q].
122. *See infra* Sections III.A.1, III.A.2.
123. *See infra* Sections III.A.2, III.A.3.
124. *See infra* Section III.A.4.
125. *See infra* Section III.A.5.

Sections A and B also address common criticisms of this proposal[126] and raise important policy considerations that support the expansion of RICO.[127] Section C then examines other challenges associated with cybercrime, such as safe havens, foreign state actors, and multilateral cooperation.[128] Lastly, Section D draws attention to the overall lack of cybersecurity infrastructure in the United States in order to emphasize that while the expansion of RICO is a key element in the fight against cybercrime, it must be accompanied by other major initiatives that strengthen cybersecurity in both public and private sectors.[129]

A. EXPANDING RICO TO INCLUDE VIOLATIONS OF THE CFAA AS PREDICATE ACTS

1. Limitations to RICO's Enumerated Racketeering Acts

While there are existing provisions in RICO that may apply to cybercrime, further changes must be made to expand and strengthen its reach. Currently, the thirty-five enumerated racketeering activities cover traditional crimes that range from murder, robbery, and bribery to sexual exploitation of children and human trafficking.[130] These activities were intended to comprise an extensive list of crimes committed by criminal organizations when RICO was passed, and while they have been updated over the years, only a few can be stretched to address the types of cybercrimes we see today.

For example, within the context of cybercrimes, criminals can commit cyber extortion, sexual exploitation of children through social media, and financial crimes through the use of ransomware. They may also perpetuate identity theft by hacking into databases of credit bureaus and stealing social security numbers or commit wire fraud by making online money transfers with stolen credit card accounts. However, much of the language is outdated and insufficient to address Internet crimes. If violations of the CFAA could be used as predicate acts for a RICO charge, prosecutors would be able to bring racketeering charges against Internet crimes that range from trespassing on government computers and credit bureau hacks to double extortion schemes commonly associated with ransomware attacks.

126. *See infra* Section III.A.5.
127. *See infra* Section III.B.
128. *See infra* Section III.C.
129. *See infra* Section III.D.
130. 18 U.S.C. § 1961(4).

2. Relevant Statutory Provisions in the Computer Fraud and Abuse Act

In the early 1980s, Congress faced a similar problem concerning outdated statutory language when the public began using personal computers, which was accompanied by a steady rise in computer fraud. In an effort to address gaps in the federal criminal code for prosecuting computer crimes, Congress adopted 18 U.S.C. § 1030, which was later amended by the CFAA in 1986.[131] For nearly two decades, Congress continued to make amendments to 18 U.S.C. § 1030, slowly broadening its scope and reach while attempting to balance "the Federal Government's interest in computer crime and the interests and abilities of the States to proscribe and punish such offenses."[132] As a result of these periodic updates, provisions of the CFAA contain language that apply directly to Internet crimes.

Under the CFAA, a person that intentionally accesses a computer without authorization or exceeds authorized access is liable if (1) the person obtains information from a protected computer or from a financial record of a financial institution or (2) the act was done "knowingly and with intent to defraud" for the purpose of obtaining something of value over $5 thousand in a one-year period.[133] In addition, the CFAA extends to "knowingly" transmitting a program, code, or command with the intent of damaging a computer, as seen with malware attacks; accessing a computer without authorization for the purpose of causing damage or loss; and trafficking passwords or other information that could be used to facilitate another's authorized access of a computer.[134]

The 2008 amendment to the CFAA also expanded 18 U.S.C. § 1030(a)(7), which criminalizes acts associated with cyber extortion, such as a threat to damage a computer, steal or corrupt data, or disclose sensitive, confidential information to the public.[135] This amendment also included a clause that punished those who were part of a conspiracy to violate provisions of the CFAA.[136] With the various cyberattack methods available to criminals today, these provisions of the CFAA are more relevant than ever. The broad language employed by Congress when drafting these provisions has made it possible to prosecute a variety of cyberattacks, including those that utilize newer methods and technologies.

131. COMPUT. CRIME & INTEL. PROP. SECTION, U.S. DEP'T OF JUST., PROSECUTING COMPUTER CRIMES 1 (Scott Eltringham ed., 2d ed. 2017).
132. *Id.* at 1–2.
133. 18 U.S.C. § 1030(a)(3).
134. *Id.* § 1030(a)(5)–(6).
135. *Id.* § 1030(a)(7).
136. COMPUT. CRIME & INTEL. PROP. SECTION, U.S. DEP'T OF JUST., *supra* note 131, at 2.

3. The CFAA's Application to Various Cybercrimes

The provisions of the CFAA, codified in 18 U.S.C § 1030, are well-suited for prosecuting the most prominent and damaging cyberattacks seen today. The 2021 IC3 report indicated that common methods used to initiate cyberattacks were phishing, vishing, smishing, and pharming.[137] Each of these attacks violates 18 U.S.C. § 1030(a)(5), which makes it illegal to "knowingly" transmit "a program, information, code, or command" that damages a computer without authorization, as is the case with malware infections.[138]

Botnets are another common form of cyberattack that can be prosecuted under the CFAA. To create a botnet, the cybercriminal first infects computer devices with malware, which can be done by exploiting security loopholes in software or by using one of the above phishing, pharming, vishing, or smishing schemes;[139] this again is a violation of 18 U.S.C § 1030(a)(5). The cybercriminal then organizes all the infected computers into a network of "bots" that the criminal can control remotely. These botnets can be used to launch massive spam campaigns, engage in DDoS attacks, and gather sensitive or confidential data from infected computers. The use of botnets to commit these criminal activities is clearly a violation of 18 U.S.C. §§ 1030(a)(2), (4), (5)(B), and (5)(C). If criminals later steal information gathered from these computers, it would also be a violation of 18 U.S.C. § 1030(a)(6).

Ransomware attacks have also been growing significantly in recent years. Hackers often start these attacks by utilizing social engineering or computer intrusion techniques to install malware on a computer.[140] From there, hackers can encrypt data on that computer or on its network and hold it for ransom, threaten to release sensitive data like social security numbers to the public, or threaten to destroy the data. Ransomware attacks, one of the major categories of cybercrime, disrupted hospitals, schools, food manufacturing, emergency services, and energy production across the world in 2020 and 2021.[141]

While the FBI discourages ransom payments, primarily because payment of the ransom does not guarantee that the cybercriminals will not carry out their threats, companies often feel that they have no choice but to

137. 2021 INTERNET CRIME REPORT, *supra* note 5, at 8.

138. 18 U.S.C. § 1030(a)(5).

139. *What Is a Botnet?*, KASPERSKY, http://usa.kaspersky.com/resource-center/threats/botnet-attacks [http://perma.cc/NK7V-37E4].

140. *Id.*

141. Rushe & Borger, *supra* note 39.

pay. When the meatpacker JBS USA was hit with a ransomware attack in June 2021, it paid $11 million to the cybercriminals—even after the majority of its plants were back in operation—in the hopes that it would prevent further disruption and harm.[142] The City of Baltimore was also hit with a ransomware attack in May 2019, and while it refused to pay the $760 thousand ransom, the cost of rebuilding its system has steadily ticked up, hitting $18.2 million by the middle of 2021.[143] Cybercriminals have also started offering ransomware-as-a-service ("RaaS"), which has contributed to the proliferation of ransomware attacks.

4. CFAA's Application to the Colonial Pipelines Ransomware Attack

On April 29, 2021, hackers gained access to the VPN account of an employee working at Colonial Pipeline ("Colonial"), which owns the largest fuel pipeline in the United States and controls forty-five percent of gasoline, diesel fuel, and jet fuel on the East Coast.[144] The cybercriminal group, called DarkSide, posted a ransom note to the company's control room that was promptly brought to the attention of an operations supervisor. Within an hour, Colonial shut down its entire gasoline pipeline, fearing the infection would spread to its operational technology network, which contained a system of computers that controlled the physical flow of gasoline.

In the end, Colonial ended up paying roughly $4.4 million in bitcoin to DarkSide to prevent the leak of over one hundred gigabytes of data that the hackers had taken from the information technology network.[145] The shutdown wreaked havoc on gas prices on the East Coast and created a shortage scare that led to long lines at gas stations up and down the coast.[146] A report prepared by the Department of Homeland Security during that period found that the country could withstand only an additional three-to-five days of the shutdown before a lack of diesel fuel would start interfering with mass transit as well as with the distribution of products from chemical factories and refineries.[147]

DarkSide's unauthorized access into Colonial's information technology

142. *Id.*
143. *Id.*
144. William Turton & Kartikay Mehrotra, *Hackers Breached Colonial Pipeline Using Compromised Password*, BLOOMBERG (June 4, 2021, 12:58 PM), http://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password [http://perma.cc/3DN7-T2UE].
145. *Id.*
146. David E. Sanger & Nicole Perlroth, *Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity*, N.Y. TIMES (June 8, 2021), http://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html [http://perma.cc/C99N-37KV].
147. *Id.*

network constituted multiple violations of the CFAA. It committed double extortion by holding the data it had stolen hostage and by threatening to release or destroy it if a ransom was not paid, in violation of 18 U.S.C. § 1030(a)(7). It was also involved in the trafficking of the password that was used to break into the employee's VPN account, which violates 18 U.S.C. § 1030(a)(6). It then violated 18 U.S.C. §§ 1030(a)(2)(C) and (5)(C) by intentionally accessing a computer without authorization and obtaining valuable information as well as causing damage and loss to Colonial. In sum, while the CFAA is well positioned to address these violations, none of the statutory language in RICO is sufficient to address them. There is no provision in RICO that expressly refers to "unauthorized access" of a computer or network, and while extortion is an enumerated activity, RICO does not extend to the types of extortion seen in computer crime cases.

5. The Benefit of Making CFAA Violations a Predicate Act Under RICO

The CFAA allows prosecutors to charge cybercriminals who violate its provisions or conspire to violate them. It levies jail terms ranging from one-to-ten years depending on the crime, with heftier terms for felony convictions.[148] These penalties would increase significantly if a violation of the CFAA is made a predicate act under RICO. The jail term would have a new maximum of twenty years, and each individual case could be assessed against the backdrop of the entire criminal enterprise, rather than the isolated act of the criminal.[149] Facing the prospect of much longer prison terms, potential cybercriminals may be deterred from engaging in the crime to begin with.

In addition, those who have already committed crimes may be more willing to cut plea deals and cooperate with the government. This could lead to valuable intel on their criminal counterparts within a cyber gang, including higher-ranked leaders that either operate or play a large role in the cyber gang's unlawful activities. In addition to lengthier prison terms, RICO can also be used for the seizure and forfeiture of the criminals' assets, including their online platforms and real property, such as computers and other electronic devices.[150] RICO would also prevent cybercriminals from using the proceeds of their crimes to fund their defenses.

Critics of this proposal argue that adding CFAA violations as a predicate act could subject regular individuals to RICO charges for minor crimes, such as lying on a social media platform or dating application.[151]

148. COMPUT. CRIME & INTELL. PROP. SECTION, U.S. DEP'T OF JUST., *supra* note 131, at 2.
149. 18 U.S.C. § 1963.
150. *Id.*
151. W. Joseph Salvador, *Dismantling the Internet Mafia: RICO's Applicability to Cyber Crime*,

However, this can be rebutted on the basis that the criminal provisions of RICO were intended to prosecute members of organized crime groups like the Mafia and drug cartels, not ordinary citizens. RICO specifically requires the establishment of a "pattern of racketeering activity" and the participation in or employment by an enterprise.

Back when Congress passed RICO in 1970, the concept of cybercrime as we know it today did not exist. As such, it is imperative that decades-old statutes like RICO be updated so that they can be used to prosecute cybercrimes that currently "pose a significant threat to the privacy and economic security of American consumers and businesses."[152]

B. POLICY REASONS FOR SUPPORTING THE USE AND EXPANSION OF RICO

As cybercrimes have grown in volume and intensity, legislation to prevent, deter, or prosecute cybercrime has lagged behind. A spate of high-profile incidents across the country in 2021 has shaken the public's confidence in the government's ability to fend off cyberattacks and revealed alarming gaps in the cybersecurity infrastructure of both the public and private sectors. The SolarWinds hack in 2019 alone compromised over one hundred companies in the private sector as well as nine federal agencies,[153] including the Department of Homeland Security.[154] Accordingly, there has been increased scrutiny of the impact of cybercrime on national security and the lives of individuals who fall victim to it.

When hackers from a group called Babuk penetrated the District of Columbia Police Department's network and stole thousands of sensitive documents containing the personal information of officers, the chairman of the police union expressed his disappointment in "how careless D.C. government officials can be when it comes to protecting such sensitive information" and how they are "unable to . . . be trusted with protecting our data."[155] When Colonial was attacked, "television images of gas lines and

41 RUTGERS COMPUT. TECH. L.J. 268, 295–96 (2015).

152. *The Cybersecurity Program*, U.S. ATT'Y'S OFF. CENT. DIST. CAL., http://www.justice.gov/usao-cdca/cybersecurity-program [http://perma.cc/73U9-ZVZC].

153. Jon Porter, *White House Now Says 100 Companies Hit by SolarWinds Hack, but More May Be Impacted: Plus Nine Federal Agencies*, VERGE (Feb. 18, 2021, 1:40 AM), http://www.theverge.com/2021/2/18/22288961/solarwinds-hack-100-companies-9-federal-agencies [http://perma.cc/YS8Q-EM2A]; *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (Infographic)*, U.S. GOV. ACCOUNTABILITY OFF. (Apr. 22, 2021), http://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic [http://perma.cc/P7RB-H875].

154. Alan Suderman, *AP Sources: SolarWinds Hack Got Emails of Top DHS Officials*, ASSOCIATED PRESS, (Mar. 29, 2021), http://apnews.com/article/solarwinds-hack-email-top-dhs-officials-8bcd4a4eb3be1f8f98244766bae70395 [http://perma.cc/4THU-V9F9].

155. Peter Hermann & Dalton Bennett, *Hackers Post Hundreds of Pages of Purported Internal D.C. Police Documents*, WASH. POST (May 13, 2021, 1:26 PM), http://www.washingtonpost.com/local/public-

rising prices" caused political damage to the Biden administration and demonstrated that even a single compromised password could wreak havoc on people's day-to-day lives.[156] Effective legislation must therefore be passed to instill trust in the government and protect the American people, the majority of whom are not equipped with the technical skills and knowledge to fend off cyberattacks.

C. INNATE CHALLENGES OF CYBERCRIME

While evaluating the application of criminal statutes to prosecuting or deterring cybercrime, it is also important to assess the challenges posed by cybercrime as it stands today. In many cases, cyberattacks are committed by loosely associated groups of people who make up a criminal enterprise and thus may fall under RICO but not under the prosecutorial reach of the United States. In particular, many cybercriminals operate from "safe haven" countries that either tolerate their illegal activities, like Russia and China, or have laws that are inadequate to convict them.[157]

The United States, therefore, must rely not just on legislation, but also on the international cooperation of countries around the world. Unfortunately, this is easier said than done, especially given the nature of authoritarian regimes like that of North Korea, which frequently conduct their own state-sponsored cyberattacks against the United States.[158] Accordingly, the United States must rely on a multilateral approach to this problem, utilizing sanctions, diplomacy, and the power of multilateral institutions to facilitate the indictment, extradition, and conviction of cybercriminals, wherever they are hiding.[159]

In addition, there is a lack of cybersecurity infrastructure in both the public and private sectors of the United States. For example, the attack on Colonial demonstrated the vulnerability of critical infrastructure in the United States to cyberattacks.[160] It drew attention to the fact that a hack that had no effect on operational control systems still managed to "mess[] with a society's ability to operate."[161] The majority of critical infrastructure, approximately eighty percent, is owned by the private sector, and there is no

safety/dc-police-hackers-ransomware-babuk/2021/05/13/d0280fb4-b3f7-11eb-a980-a60af976ed44_story.html [http://perma.cc/T4H3-7N6N].

156. Sanger & Perlroth, *supra* note 146.

157. Graham Kennis, Laura Bate & Mark Montgomery, *Agile Multilateralism Is Needed to Address Cybercrime Safe Havens*, LAWFARE (Nov. 16, 2021, 9:01 AM), http://www.lawfareblog.com/agile-multilateralism-needed-address-cybercrime-safe-havens [http://perma.cc/7Y5P-NW3A].

158. *Id.*

159. *Id.*

160. Sanger & Perlroth, *supra* note 146.

161. *Id.*

national standard or guideline on how to maintain robust cybersecurity measures to defend against cyberattacks.[162]

In response, President Biden issued an executive order designed to support and reinforce a partnership between the public and private sectors, including requiring disclosure in the event of a ransomware attack, consulting private-sector cybersecurity experts, and including representatives from the private sector in the new Cyber Safety Review Board, which is tasked with reviewing significant cyber incidents.[163] However, these measures must be implemented in conjunction with new legislation that bolsters the United States' prosecutorial power against cybercrimes.

D. BUILDING CYBERSECURITY INFRASTRUCTURE

While legislative changes can go a long way toward putting cybercriminals in prison, they must be accompanied by efforts to build and strengthen cybersecurity infrastructure, not just in the United States but also across the world. In October 2021, representatives from thirty-one different countries around the world released a statement acknowledging that "ransomware poses a significant risk to critical infrastructure, essential services, public safety, consumer protection and privacy, and economic prosperity."[164] It acknowledged the importance of fighting cybercrime on a global level in partnership with the private sector and the general public.[165] Four key efforts were outlined: (1) build network resilience to prevent and deter cybercrime, (2) block the methods that cybercriminals use to get paid, (3) work together to investigate and prosecute the crimes, and (4) address the way that safe havens are used to hide illegal activity and prevent legal action.[166]

In addition, many cybersecurity experts agree that one of the best ways to build and reinforce cybersecurity in both the public and private space is to follow a few basic steps.[167] For example, a large number of cyberattacks could have been deterred simply by updating software and using strong

162. *Id.*

163. Exec. Order No. 14028, 3 C.F.R. 14028 §§ 4–5 (2022), https://www.govinfo.gov/content/pkg/CFR-2022-title3-vol1/pdf/CFR-2022-title3-vol1-eo14028.pdf [http://perma.cc/89U2-D3LT].

164. Press Release, The White House, Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting (Oct. 14, 2021), http://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021 [http://perma.cc/6TNB-BGVE].

165. *Id.*

166. *Id.*

167. *Cybersecurity*, READY.GOV, http://www.ready.gov/cybersecurity [http://perma.cc/HEB4-7ZBR].

passwords that contain special characters and numbers.[168] Companies are increasingly also turning to multifactor authentication, which sends a message or code to another device to confirm the authenticity and identity of the user.[169] To bolster impact, these essential "cyber hygiene" methods can be paired with education that teaches users how to handle suspicious phone calls, text messages, links, or documents.[170]

Moreover, by blocking payments to cybercriminals, governments can effectively disrupt the business model that fuels highly lucrative attacks like WannaCry.[171] Many cybercrimes, especially those that involve extortion, receive payments through virtual assets like Bitcoin.[172] These payment methods are, by their very nature, more difficult to track.[173] Regulation of virtual asset companies is inconsistent across various jurisdictions, and this contributes to the formation of money laundering networks. Even legitimate businesses can unknowingly play a role in transferring criminal proceeds, and many may also choose to turn a blind eye to it.

Accordingly, international cooperation is critical to addressing cybercrime as a whole. No one individual country can take down an entire ring of cybercriminals, especially if they are scattered in countries that serve as safe havens or where the prosecutorial power of the government is limited.[174] Countries must make a concerted effort to share information in a timely manner, beginning at the time an attack is first reported. To do this, governments must establish robust public-private partnerships with companies that are the targets of such attacks and consult leaders in cybersecurity.[175] They must also establish reporting channels and create requirements that allow for more disclosure and transparency on the specific scale and volume of these attacks.[176] While this Note has sought to highlight the value of expanding existing law to help investigate and prosecute cybercrime, it also acknowledges that without simultaneous implementation of these above measures, the cybersecurity vulnerabilities and their resulting damage to society will only grow in the years to come.

168. *Id.*

169. Mathieu Chevalier, *Five Ways You Can Help Protect Your Organization from Cyber Attacks*, GENETEC, http://www.genetec.com/blog/cybersecurity/five-ways-you-can-help-protect-your-organization-from-cyber-attacks [http://perma.cc/43Z7-PHPQ].

170. *Id.*

171. Jamie Tarabay, *How Cryptocurrency Turbocharged the Cybercrime Racket*, BLOOMBERG (July 7, 2021, 6:22 AM), http://www.bloomberg.com/news/articles/2021-07-03/how-cryptocurrency-turbocharged-the-cybercrime-racket-quicktake [http://perma.cc/4H6D-2D45].

172. *Id.*

173. *See id.* (noting description of cryptocurrency mixers).

174. Kennis et al., *supra* note 157.

175. Exec. Order No. 14028, *supra* note 163.

176. *Id.*

CONCLUSION

While there are many challenges associated with combating cybercrimes, such as the transnational nature of many attacks and the roles played by hostile nation states, Congress must take action to address gaps in legislation caused by its reliance on decades-old laws. An expansion of RICO to include violations of the CFAA as a predicate act will increase the government's prosecutorial power over even loosely associated cybercriminals, and its harsher penalties and sanctions will serve to deter future criminal conduct. In addition, existing provisions of RICO should be reassessed for their potential in prosecuting cybercrime, either against members of cybercriminal groups or businesses that knowingly facilitate their unlawful acts. By doing so, the government will have an opportunity to rebuild the public's trust concerning matters of cybersecurity and will clearly demonstrate the government's commitment to preventing and stopping cybercrimes, which is indisputably "an escalating global security threat with serious economic and security consequences."[177]

177. Kennis et al., *supra* note 157.