UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

DRAFTKINGS INC.	)	
	)	
Plaintiff,	)	
	)	Civil Action Case No. _____
v.	)	
	)	
JOHN DOES #1-10	)	**JURY DEMANDED**
	)	
Defendants.	)	
	)	

COMPLAINT

Plaintiff DraftKings Inc., ("Plaintiff"), by and through its attorneys Boies Schiller Flexner LLP, bring this action seeking injunctive relief and monetary damages against Defendants Doe 1 through Doe 10 (collectively referred to as "Defendants") for Defendants' unlawful conduct, as set forth below.

NATURE OF THE ACTION

1. On August 8, 2018, Defendants launched a malicious Distributed Denial of Service ("DDoS") attack against Plaintiff's website, www.draftkings.com ("draftkings.com" and/or the "Website") (the "Attack"). The Attack interrupted, blocked, harassed, and burdened Plaintiff's operations for a period of approximately twenty-six minutes. During this time, the Attack prevented legitimate DraftKings users from actively engaging with the DraftKings Website. As a result of the Attack, Plaintiff's personnel spent several days containing the Attack and mitigating further potential damage from the malicious Attack.

2. Plaintiff brings this John Doe matter under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA") to unmask the perpetrators responsible for the Attack, to prevent

future attacks, and to hold the Defendants accountable by seeking compensation for the economic damages Plaintiff suffered as a result of Defendants' unlawful and malicious conduct.

3. Plaintiff does not presently know the identities of Defendants John Does 1-10. Accordingly, Plaintiff, by separate motion, will seek the Court's authorization to conduct discovery from the third parties who have registered the identified IP addresses in order to obtain Defendants' identifying information. With this information, Plaintiff will be in a position to amend this Complaint to substitute the actual names of the Defendants.

THE PARTIES

4. Plaintiff is a Delaware corporation with its principle place of business in Boston, Massachusetts. Plaintiff provides the world's leading online platform for individuals to compete in daily fantasy sports ("DFS") contests, and other fantasy sports contests, with friends, family, and other competitors. It offers DFS contests for a variety of sports, such as football, baseball and basketball, among many others.

5. Defendants, whose identities are unknown, are individuals or entities that are responsible for the Attack.

6. Plaintiff is informed and believes and therefore alleges that each of the fictitious named Defendants is responsible in some manner for the occurrences herein alleged, and that Plaintiff's injuries as herein alleged were proximately caused by such Defendants.

7. Third party American Registry for Internet Numbers ("ARIN") is a Regional Internet Registry incorporated in the Commonwealth of Virginia. ARIN manages the distribution of Internet number resources such as Internet Protocol ("IP") Addresses for the United States, Canada, and many Caribbean and North American islands. ARIN's mailing address is PO Box 232290, Centreville, Virginia 20120.

8. Third party ColoCrossing is a co-location and cloud services provider. ColoCrossing is located at 325 Delaware Avenue, #302, Buffalo, New York 14202.

9. Third party Deluxe Corporation is a small-businesses and financial services company. It recently acquired ColoCrossing and is located at 3680 Victoria Street North, Shoreview, Minnesota 55126.

10. Third party Google LLC is a technology company located at 1600 Amphitheatre Parkway, Mountain View, California 94043.

11. Third party Verizon Wireless is a telecommunications company located at One Verizon Way, Basking Ridge, New Jersey 07920.

12. Third party T-Mobile is a telecommunications company located at 12920 SE 38th Street, Bellevue, Washington 98006.

13. Third party NetActuate is a cloud and network services company located at 7780 Brier Creek Parkway, Suite 415, Raleigh, North Carolina 27617.

JURISDICTION AND VENUE

14. The Court has subject matter jurisdiction over the CFAA claims, 18 U.S.C. § 1830 *et seq*., pleaded herein pursuant to 28 U.S.C. § 1331.

15. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) and (c), because a substantial part of the events or omissions giving rise to the claims occurred in this judicial district or will occur in this judicial district; and Plaintiff's headquarters are located in the judicial district.

16. Defendants' whereabouts are presently unknown. Upon information and belief, Defendants have directed the acts complained of herein toward and have utilized

instrumentalities located in the Commonwealth of Massachusetts and the District of Massachusetts to carry out the acts complained of herein.

17. Defendants have undertaken the intentional acts alleged herein with knowledge that such acts would negatively impact draftkings.com, thereby injuring Plaintiff located in the District of Massachusetts. Therefore, this Court has personal jurisdiction over the Defendants.

FACTUAL ALLEGATIONS

18. DraftKings provides an online platform on which individuals can compete in DFS contests. DFS—an outgrowth of season-long fantasy sports—is a skill-based form of competitive entertainment that millions of Americans enjoy. Customers primarily interact with Plaintiff through its Website and mobile applications.

19. DraftKings is the premier DFS platform in the world. DraftKings offers paid, prize-eligible DFS contests in forty-one U.S. states and the District of Columbia, across thirteen different sports. DraftKings offers more than 20,000 public contests per day, and has paid out $5 billion across all sports. In April 2018 alone, DraftKings' DFS contests had approximately 23 million entries and $150 million in entry fees.

Computer "Botnets"

20. A DDoS attack, or Distributed Denial of Service attack, is an attack in which multiple computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for legitimate users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.

21. A computer or networked device under the control of an intruder is known as a zombie, or bot. The attacker may create what is called a command-and-control server to

command the network of bots, also called a botnet. The person in control of a botnet is sometimes referred to as the botmaster.

22. A botnet infection spreads very easily. In a typical botnet infection, the assailant begins by using one computer system and linking it to the botnet master. The botnet master system identifies other systems and gains control over them.

23. Botnets can be comprised of almost any number of bots; botnets with tens or hundreds of thousands of nodes have become increasingly common. Once the botnet is assembled, the attacker (s) can use the traffic generated by the compromised devices to flood the target domain and knock it offline, or prevent legitimate users from accessing the target domain.

24. Botnets are often created and controlled by sophisticated criminal organizations and are used to carry out misconduct that harms others' rights. Malicious attacks using botnet infrastructure, such as a DDoS attack, wreak havoc on online businesses, applications, or services, such as those Plaintiff provides.

The Attack

25. DraftKings brings this action to stop Defendants from harming Plaintiff and its customers through the malicious use of IP addresses that are central to Defendants' botnet.

26. On August 7, 2018, at almost midnight eastern daylight saving time, the Website was targeted by a DDoS Attack perpetrated by Defendants. Plaintiff successfully neutralized the first attack.

27. The subject Attack, which overwhelmed DraftKings' resources and negatively impacted its business, occurred on August 8, 2018 at approximately Noon, around twelve hours after the first attack. The Attack occurred because Defendants intentionally sent thousands of packets of information or commands to Plaintiff's Website with the intent of damaging and

negatively impacting Plaintiff and its operations. For instance, Plaintiff's primary Website normally handles thousands of requests per second; during the Attack, Plaintiff's Website faced a three-fold increase of requests per second. The Attack prevented legitimate DraftKings users from actively engaging with the Website.

28. This Attack was a clear violation of draftkings.com's Terms of Use which prohibit using automated means to interact with Plaintiff's website, to tamper with the administration of a contest, or to abuse the website in any way. It specifically informs all users that "any attempt . . . to deliberately damage the website or undermine the legitimate operation of any contest is a violation of criminal and/or civil laws and should such an attempt be made, DraftKings reserves the right to seek damages and other remedies from any such person to the fullest extent permitted by law."

29. After the Attack began, Plaintiff's personnel immediately worked to identify the nature and source of the Attack.

30. Approximately twenty-six minutes after the Attack began on August 8, Plaintiff's personnel successfully stopped the Attack from overwhelming DraftKings' resources and negatively impacting its business. Plaintiff discovered the Defendants used dozens of IP addresses to perpetrate the Attack. Plaintiff stopped the Attack from continuing by internally identifying the subject IP addresses and then blocking said IP addresses. The following is a list of these IP addresses and their geographic locations:

Attacking IP Addresses	**Geographic Location**
ip_static_ban-172.245.73.229	ElkGrove IL USA
ip_static_ban-23.94.108.162	ElkGrove IL USA
ip_static_ban-104.168.115.90	NJ USA
ip_static_ban-192.3.250.111	Dallas USA

ip_static_ban-198.12.106.118	ElkGrove IL USA
ip_static_ban-172.245.73.201	Buffalo USA
ip_static_ban-23.95.49.196	LA USA
ip_static_ban-104.168.95.214	LA USA
ip_static_ban-104.168.114.8	NJ USA
ip_static_ban-23.95.49.242	LA USA
ip_static_ban-192.3.76.116	Romania
ip_static_ban-23.94.20.118	Romania
ip_static_ban-104.168.92.158	LA USA
ip_static_ban-192.227.150.48	Ontario Canada
ip_static_ban-192.227.150.22	Ontario Canada
ip_static_ban-104.168.113.152	NJ USA
ip_static_ban-104.168.92.244	LA USA
ip_static_ban-192.3.253.16	Seattle USA
ip_static_ban-198.12.106.50	ElkGrove IL USA
ip_static_ban-104.168.95.186	LA USA
ip_static_ban-192.3.76.2	Romania
ip_static_ban-41.102.189.132	Algeria
ip_static_ban-46.148.147.160	Poland
ip_static_ban-37.8.4.27	Palestine
ip_static_ban-41.37.77.175	Egypt
ip_static_ban-176.224.83.81	Saudi Arabia
ip_static_ban-192.99.242.86	Venezuela
ip_static_ban-199.38.183.35	Reston VA
ip_static_ban-190.204.84.195	Venezuela
ip_static_ban-102.158.13.208	Tunisia
ip_static_ban-196.65.149.200	Morocco
ip_static_ban-174.205.21.40	Washington DC USA
ip_static_ban-107.178.196.211	Indiana USA
ip_static_ban-107.178.193.169	Indiana USA
ip_static_ban-107.178.193.189	Indiana USA
ip_static_ban-172.56.14.116	Houston USA

31. Third party ARIN is responsible for managing and distributing Internet number resources such as IP addresses in the United States, Canada, and other areas of North America. Based on directories of the registrants of IP Addresses published by ARIN, Plaintiff determined that more than seventy-five percent of the U.S. IP addresses used in the Attack are registered to ColoCrossing, a co-location and cloud services provider based in Buffalo, New York. ColoCrossing is itself owned by Deluxe Corporation, a small businesses and financial services company based in Shoreview, Minnesota. The remaining handful of IP addresses located in the United States are registered to Google LLC, T-Mobile, Verizon Wireless, and NetActuate.

32. On August 9, 2018, Plaintiff sent ColoCrossing an abuse report via its published abuse reporting email address. Plaintiff notified ColoCrossing that the above-referenced IP addresses belonged to ColoCrossing and were used in the Attack against Plaintiff in violation of ColoCrossing's Acceptable Use Policy, which states that: customers must only use bandwidth services "for lawful purposes" and specifically prohibits "transmission[s] . . . in violation of any applicable law." It also prohibits "interference with a third-party's . . . ability to connect to the Internet or provide services to Internet users." Plaintiff also informed ColoCrossing that the Attack had a negative impact on Plaintiff's business operations and asked that ColoCrossing immediately stop activity originating from its networks. Plaintiff also requested that ColoCrossing identify the parties involved in this activity. ColoCrossing did not respond to this message.

33. On August 10, 2018, Plaintiff sent a second message to ColoCrossing, again requesting that ColoCrossing immediately cease the activity originating from its network and identify the attackers. Again, ColoCrossing did not immediately respond to the message.

34. After ColoCrossing failed to respond to Plaintiff's second message, Plaintiff's counsel called ColoCrossing in an attempt to speak with someone who could resolve the issue. Plaintiff's counsel spoke with Greg Clark, ColoCrossing's Director of Business Development ("Mr. Clark"). Mr. Clark informed Plaintiff's counsel that the individual responsible for responding to abuse reports was out of the office and requested that Plaintiff's counsel forward him the abuse reports. Plaintiff's counsel did so on the evening of August 10, 2018.

35. On August 13, 2018, Alex Vial, ColoCrossing's Director of Information Technology ("Mr. Vial"), responded to Plaintiff's abuse report messages. Mr. Vial informed Plaintiff that the IP addresses were leased or operated by a ColoCrossing client called HighProxies.com. Mr. Vial stated that he forwarded the abuse reports to HighProxies.com "for them to advise and deal with these issues." Mr. Vial did not provide any of the information Plaintiff requested in its abuse reports, nor did Mr. Vial indicate that ColoCrossing would take any action to prevent the malicious activity from originating from its network.

36. To date, DraftKings has not received any response from HighProxies.com.

37. On information and belief, HighProxies.com is a proxy service provider based in Romania. Generally speaking, proxy services are used, among other reasons, to hide a user's identity. On information and belief, HighProxies.com sells a variety of different private proxies, shared proxies, and virtual private network ("VPN") services. HighProxies.com advertises its services through a variety of channels, including on internet forums dedicated to hackers, such as www.blackhatworld.com. According to the company's website, HighProxies.com specifically targets customers who want to circumvent terms of use for companies such as Instagram and Ticketmaster. See https://www.highproxies.com/ticketing-proxies/.

38. On August 14, 2018, Plaintiff requested that Mr. Vial provide more information about HighProxies.com's networking information in order for Plaintiff to prevent further attacks. Plaintiff also requested all of ColoCrossing's contact information for HighProxies.com so that Plaintiff could contact them directly. Plaintiff further requested that ColoCrossing provide a complete list of all IP addresses and subnets it provides to HighProxies.com so that Plaintiff could block them and prevent further attacks.

39. Mr. Vial did not respond to Plaintiff's request in a timely manner. On August 18, 2018, Plaintiff's counsel again contacted Mr. Clark at ColoCrossing to request a response.

40. On August 20, 2018, Mr. Vial responded. He provided HighProxies.com's generic administrative email address along with a foreign phone number for HighProxies.com. He specifically refused to provide any additional information on the IP addresses or subnets ColoCrossing assigns to HighProxies.com, absent a subpoena.

41. On August 23 and 24, 2018, Plaintiff's counsel communicated with Mr. Vial. Plaintiff's counsel informed him once again that the information was critical to protecting Plaintiff from future attacks and requested that he provide the IP address and subnet information for HighProxies.com. Mr. Vial once again refused to provide the information without a subpoena.

42. On August 27, 2018, Plaintiff submitted an abuse report directly to HighProxies.com. Plaintiff has still not received a response from HighProxies.com, despite having filed an initial report to ColoCrossing approximately three weeks earlier on August 9 and a subsequent report on August 27.

43. On August 27, 2018, Plaintiff's counsel filed a report with in-house counsel for Deluxe Corp., ColoCrossing's parent company, regarding the Attack. The report again requested

the IP address and subnet information for HighProxies.com. On August 28, 2018, Deluxe Corp. responded, stating: "absent a properly served subpoena or law enforcement investigative request, ColoCrossing is unable to provide the information you have requested."

44. As the direct and proximate result of Plaintiff's operations being negatively impacted by the Attack which, among other things, prevented legitimate users from actively engaging with its Website, Plaintiff suffered monetary harm in the form of lost business and costs for recovery in an amount that has not yet been determined, but certainly in excess of $5,000.

45. Despite its efforts, Plaintiff is unable to identify the true source of the Attack because it has not received any helpful information from Deluxe, ColoCrossing or HighProxies.com. Plaintiff, therefore, brings this action to uncover the identities of the attackers and prosecute claims against them for the harm they caused Plaintiff and take actions to prevent the Defendants from causing DraftKings further harm.

46. Because ColoCrossing and other third parties are in possession of information concerning the identity of the Defendants, such as names, other IP addresses, and email addresses, Plaintiff, by separate motion, will seek the Court's authorization to conduct emergency discovery from the third parties who have registered the identified IP addresses in order to obtain Defendants' identifying information and thereafter amend this Complaint to substitute the actual names of the Defendants.

CAUSE OF ACTION
(VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030)

47. Plaintiff repeats and re-alleges the allegations contained in each and every preceding paragraph of this Complaint.

48. Plaintiff's computers are involved in interstate and foreign commerce and communication and are protected computers under 18 U.S.C. § 1030(e)(2).

49. By reason of the acts and omissions complained of herein, Defendants, and/or others acting in concert with Defendants, or with their knowledge, knowingly caused the transmission of a program, information, code or command without authorization and intentionally and/or knowingly caused damage to a computer protected by the CFAA.

50. Defendants DDoS Attack negatively impacted Plaintiff's business and prevented authorized users from actively engaging with the Website.

51. As a result of Defendants' conduct, Plaintiff suffered damages in excess of the $5,000 statutory minimum. Plaintiff has been damaged by Defendants' action, including experiencing decreased participation in its DFS contests and other fantasy sport contests, expending resources to respond to the Attack, paying for attorneys, and paying the cost of staff dealing with the Attack.

52. Plaintiff also suffered irreparable and incalculable harm and injuries resulting from Defendants' conduct in the form of damages to its customers' goodwill and trust.

53. Defendants violated the CFAA, and are likely to continue with their unlawful behavior unless enjoined from doing so. If not enjoined, Defendants actions create the risk of irreparable harm, in that their actions could permanently damage Plaintiff's relationships with its user base and/or cause additional disruptions in service and downtime of Plaintiff's operations. Plaintiff's legal remedies may be inadequate because, if and when its relationships with its user base are damaged, monetary damages may not restore those relationships.

PRAYER FOR RELIEF

54. Plaintiff repeats and re-alleges the allegations contained in each and every preceding paragraph of this Complaint.

55. WHEREFORE, Plaintiff requests that this Court order the following relief:

A. Enter judgment in favor of DraftKings and against the Defendants;

B. Enter an order requiring Defendants, and all persons in active concert or participation with them who receive actual notice or knowledge of an injunction by personal service or otherwise, be enjoined and restrained preliminarily and permanently, from accessing, using, or in any way interacting with, either directly, indirectly or by proxy, in any manner, any domain owned, operated or controlled by Plaintiff, including www.draftkings.com, or knowingly or recklessly causing others to do the same;

C. Enter judgment awarding money damages in an amount to be proven at trial, but in excess of $5,000;

D. Enter judgment ordering that, because of the willful and deliberate nature of Defendants' acts, and the willful disregard for Plaintiff's rights, Defendants be required to pay Plaintiff punitive/exemplary or trebled damages in an amount determined by law and at trial;

E. Enter judgment ordering Defendants to pay Plaintiff's reasonable attorney's fees and costs;

F. Enter judgment awarding Plaintiff all legally available pre-judgment and post-judgment interest on any award determined by the Court;

G. Order such further relief as the Court may deem just and reasonable.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of all of the claims asserted in this Complaint so triable.

Dated: August 30, 2018

Respectfully Submitted,

BY: /s/ William C. Jackson

William C. Jackson BBO #637636
Travis LeBlanc (*Pro Hac Vice* Pending)
Jon R. Knight (*Pro Hac Vice* Pending)
BOIES SCHILLER FLEXNER LLP
1401 New York Avenue, N.W.
Washington, D.C. 20005
Telephone: (202) 237-2727
Facsimile: (202) 237-6131
WJackson@BSFLLP.com
TLeBlanc@BSFLLP.com
JKnight@BSFLLP.com

Counsel for Plaintiff DraftKings Inc.