UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

NATIONAL NETWORK OF ABORTION FUNDS, EASTERN MASSACHUSETTS ABORTION FUND, GATEWAY WOMEN'S ACCESS FUND, KENTUCKY HEALTH JUSTICE NETWORK, NORTHWEST ABORTION ACCESS FUND, and PRETERM ACCESS FUND, Plaintiffs, v. JOHN DOES #1-15, Defendants.	Case No.: 1:18-cv-10596 **COMPLAINT** **with JURY DEMAND**

PLAINTIFFS, by their attorneys, file this Complaint as follows:

PRELIMINARY STATEMENT

1. This is a case about a malicious attack on access to abortion and the people who work to raise funds and build power for reproductive justice. Plaintiff National Network of Abortion Funds ("NNAF") and its co-Plaintiffs are nonprofit organizations with the mission of removing financial and logistical barriers to abortion access. They provide advocacy, outreach, and financial assistance to people in need of abortions. Plaintiffs hold an annual online fundraiser, the National Abortion Access Bowl-a-Thon ("Bowl-a-Thon"), to raise funds for their organizations and the individuals benefitting from their services. In 2016, the fundraiser was attacked by a malicious actor or actors who hacked into the fundraising site to deliberately interrupt, block, harass, and burden the Funds' work in providing access to abortions. During a crucial fundraising period, the Defendant(s) disabled the fundraising site through a distributed denial of service (DDoS) attack, impersonated Plaintiffs and sent donors deeply disturbing racist, anti-Semitic, and misogynistic emails. This attack sabotaged Plaintiffs' ability to collect

money for their critical mission and undermined access to abortion for an unknown number of persons. Defendant(s) further undermined donors' trust in Plaintiffs by stealing donors' financial and personally identifying information. By ransacking the single-most important abortion fundraiser of the year, Defendant(s) took away the ability to access abortions from the persons most in need of help.

2. The attack shut down the Bowl-A-Thon fundraiser, costing NNAF and its member funds hundreds of thousands of dollars in lost donations, substantial fees, time, and resources to address the attack and the loss of goodwill from its donors and member organizations.

3. Defendant(s) are liable to Plaintiffs under the Freedom to Access Clinical Entrances Act and the Computer Fraud and Abuse Act.

PARTIES

4. Plaintiff NNAF is a national 501(c)(3) not-for-profit corporation with 30 staff members in 13 states. NNAF's legal domicile is Massachusetts. NNAF operates the websites "abortionfunds.org" and "bowlathon.nnaf.org".

5. Co-Plaintiff Eastern Massachusetts Abortion Fund ("EMAF") is a Cambridge, Massachusetts based 501(c)(3) not-for-profit corporation, and a participant in the 2016 Bowl-A-Thon.

6. Co-Plaintiff Gateway Women's Access Fund ("GWAF") is a St. Louis, Missouri based 501(c)(3) not-for-profit corporation, and a participant in the 2016 Bowl-A-Thon.

7. Co-Plaintiff Kentucky Health Justice Network ("KHJN") is a Louisville, KY based 501(c)(3) not-for-profit corporation, and a participant in the 2016 Bowl-A-Thon.

8. Co-Plaintiff Northwest Abortion Access Fund ("NWAAF") is a Eugene, Oregon based 501(c)(3) not-for-profit corporation, and a participant in the 2016 Bowl-A-Thon.

9. Co-Plaintiff Preterm is a Cleveland, Ohio based 501(c)(3) not-for-profit corporation. It operates the Preterm Access Fund, a participant in the 2016 Bowl-A-Thon.

10. The exact identity and location of Defendant(s) is unconfirmed at this time.

11. Defendant John Doe #1 is the person believed to be primarily responsible for the actions complained of herein. Upon information and belief, John Doe #1 controls the twitter account "@matthewjames" referenced in paragraphs 26 through 28 below. Plaintiff believes and thereupon alleges that John Doe #1 may go by the name "Matthew James Davis" and may also be contacted through phone number (850) 329-5553, website http://davismj.me/contact/, and https://twitter.com/matthewjames?lang=en". Matthew James Davis is also listed as President and Lead Developer for Foursails Technology Group, located at 1 Chome-3-3 Kita 2 Jōhigashi, Chūō-ku, Sapporo-shi, Hokkaidō 060-0032, Japan (*see* www.forsails.co/company). Upon information and belief, John Doe #1 resides in either Florida or Japan.

12. Defendants John Doe Nos. 2-15 are persons who, on information and belief, participated in or assisted John Doe #1 in carrying out the actions complained of herein.

JURISDICTION AND VENUE

13. This Court has jurisdiction pursuant to 28 U.S.C. §§ 1331 because Plaintiffs' claims raise questions of Federal law.

14. Venue lies in this district pursuant to 28 U.S.C. § 1391(b) because the events giving rise to the claims set forth herein have occurred and will occur in this district; two of the Plaintiffs have offices in Massachusetts; and a substantial part of property that is the subject of the action is situated within the jurisdiction of the court.

15. Defendant's whereabouts are unknown.

FACTUAL BACKGROUND

THE NATIONAL NETWORK OF ABORTION FUNDS ("NNAF") & THE BOWL-A-THON FUNDRAISER

16. In early 2016 Plaintiffs launched their annual Bowl-a-Thon event. The National Abortion Access Bowl-a-Thon is a months-long grassroots fundraising campaign led by NNAF

along with approximately 40 of its member organizations located around the United States.

17. The money raised through the Bowl-a-Thon, collected via credit card payments, is used by Plaintiffs to cover costs so that individuals of any race and socioeconomic class can access abortion. Some of the local funds work with abortion clinics to help pay for abortions and offer other support such as transportation, childcare, translation, doula services, and lodging for people who must travel for abortions.

18. Not surprisingly, the Bowl-a-Thon is a controversial event for Anti-abortion extremists who seek to exercise reproductive coercion by preventing people from accessing their constitutional right to abortion.

19. Blue Sky Collaborative, LLC ("Blue Sky"), a company whose product, Blue Sky Business Application ("Business Application"), customizes online fundraising applications for charities, was hired by NNAF to manage its April 2016 Bowl-A-Thon online fundraiser.

20. Any individual was able to register as a Bowl-a-Thon participant to help fundraise. Such registrants did not have authorized access to NNAF's donor database or donor credit card information.

21. On April 7, 2016, Plaintiffs would later learn from forensics reports that Defendant(s) began their hack of the Bowl-a-Thon. On that date, Defendant(s) began searching for vulnerabilities on the Business Application using the TOR network to mask the origin of the HTTP requests. Defendant(s) placed malicious code within the Business Application which five days later they would unleash.

22. On April 8, 2016, NNAF employees began noticing suspicious actions in connection with the Bowl-a-Thon: an anonymous account began to post strange comments on Bowl-A-Thon registrant pages. NNAF flagged these comments for Blue Sky to check out.

23. On April 11, 2016, Defendant(s) registered several Bowl-a-Thon fundraising accounts under the names "qwerty", "qwerty2", "qwerty3", "adolph hitler", "Adolph",

"hitler", and "holifuk".

24. The next day the Bowl-a-Thon website began to display the receipt of absurdly large offline donations from registered participant accounts. For instance, one of these donations, from user qwerty, was for $999,999,999.00.

25. NNAF urgently reached out to Blue Sky to investigate the platform.

26. Minutes later, NNAF's Twitter.com account "@abortionfunds" received three consecutive tweets from a Twitter account called "@matthewjames". The tweets congratulated NNAF on "passing the $830 trillion mark" and added, "you're gunna [sic] make little boys and girls a complete thing of the past!"

27. The @matthewjames Twitter account, states it belongs to "Matthew James Davis." Upon information and belief, Davis is a religious anti-abortion activist with a background in technology and coding. Davis was believed to live in Florida, although the Twitter account states "Sapporo, Japan" in its user profile. A website, www.davismj.me, states that Matthew James Davis is a "core team member" at Aurelia. The website www.Aurelia.io states that Aurelia is "a JavaScript client framework for web, mobile and desktop that leverages simple conventions to empower creativity."

28. Upon information and belief, the individual in control of the @matthewjames Twitter account was involved in the overall Bowl-a-Thon attack given the suspicious timing of the tweets – and the fact that the tweets were deleted by the accountholder moments later. Fortunately, NNAF employees managed to screenshot the tweets before they were deleted.

29. Over the next couple of hours, the Bowl-A-Thon website appeared to receive $66 billion in fraudulent donations during a distributed denial of service attack (DDoS) which then caused the Bowl-A-Thon website to crash altogether.

30. Many of the fraudulent donations were made in the name of "Adolph [sic] Hitler".

31. These donations were visible to all other registrants for several hours. One of

NNAF's employees noted, "donors and registrants 'felt very scared when they logged in and saw donations from Adolph Hitler.'"

32. Later that night, NNAF's staff escalated their response to the attacks. They reached out to outside associates seeking additional technological expertise.

33. Bowl-a-Thon registrants began receiving emails alerting them to donations made by user "Adolph Hitler." The email sent by "Adolph Hitler" contained the following message ""I believe that the Aryan race is the Master Race; the purest human genetic strain currently available. Consequently, it tickles me to fund abortions for the lower races, such as the Negroes and the Jews. There is no longer any need to send these parasites to my concentration camps – they willingly slaughter their own young if given enough money to afford the ope [sic] I am indebted to feminism and this new opportunity it has provided to cleanse our future generations. Keep it up, NNAF!"

34. NNAF's employees were distraught when they learned that this anti-abortion, white supremacist, and anti-Semitic email had been sent to NNAF's donors – not to mention the sender had obviously hijacked their system to send it.

35. Forensics reports would show that starting on April 12th Defendant(s)' stored cross site scripting ("XSS") exploit was executed in the browsers of visitors to the NNAF fundraising website, infecting their profiles, and presenting users with a fraudulent donation form. Reports showed Defendant(s) used JavaScript in this endeavor.

36. The next morning, on April 13, 2016, a Blue Sky employee falsely assured NNAF that the attack had not obtained personally identifying donor information, including email and physical addresses.

37. After a lull in activity, at 4:53 AM on April 14, 2016, Defendant(s) escalated their assault on NNAF. From an account named info@nnaf.org Defendant(s) sent a spoofed email to hundreds of Bowl-a-Thon registrants. The email consisted of a picture of a fetus with the

message: "I hope I grow up big enough to go bowling someday".

38. A few hours later, around 7 am on April 14th, one of NNAF's employees received an electronic receipt from Mailchimp.com. The employee was notified that her subscription "order had been processed". The notification from Mailchimp contained the last four digits of that employee's American Express credit card. In addition to the employee's email address the receipt had been sent to the suspicious account "zpkxtrxv@sharklasers.com". Sharklasers.com creates disposable email addresses and is frequently used for anonymous communications. Upon information and belief, Defendant(s) were controlling this particular sharklasers.com account.

39. Early on April 14, 2016, NNAF's cyber-security consultant raised the possibility that Defendant(s) may have created sham donation pages as a means of harvesting credit card and other personally identifying information about Plaintiffs' donors. As noted above, Defendant(s) had actually been rerouting donors to the sham page since April 12, 2016.

40. By April 14, 2016, Defendant(s) had gained administrative access to Blue Sky using a malicious JavaScript attack.

41. On April 14, 2016, Defendant(s) used their access to Blue Sky to steal the personal identifying information – including names, mailing addresses, email accounts, and phone numbers of 2,705 participants and 14,333 donors to NNAF. Defendant(s) stole 435 credit card numbers, and infected 1,054 profile pages.[1]

42. Separate investigations commissioned by Blue Sky and NNAF into the crime concluded that Defendant(s) had patiently and precisely planned out the attack using a fair amount of technical sophistication to do it. All for the singular purpose of interrupting the Bowl-a-Thon.

[1] Defendant stole this information by exporting the data from Blue Sky's Business Application.

43. Responding to the multi-pronged attack against Bowl-a-Thon required a significant expenditure of resources and time by NNAF. In addition to addressing the live issue of their donation platform being disrupted, NNAF had to coordinate with its numerous participating local funds which were all confused and distressed by the attack.

44. These funds, as detailed below, which are the primary beneficiaries of the Bowl-A-Thon, experienced a major fundraising disruption during the crucial final ten-day stretch of fundraising for the event.

45. Efforts and resources were redirected from fundraising to crisis management. Plaintiffs scrambled to find alternate means of accepting donations, acted to protect their donor's private information, took preventive measures, and triaged their own reputational fallout from being victimized by an attack of this nature.

46. NNAF staff members spent the majority of April and May 2016 responding to the attack, supporting donors, and supporting funds in order to cope with, document, resolve, send out crisis communications, respond to media inquiries, provide status updates, communicate with consultants, and continue to run the Bowl-a-Thon fundraiser. NNAF staff were obligated to work overtime on nights and weekends to address the attack.

47. NNAF staff also had to endure the difficult task of contacting supporters and donors to inform them about the loss of their private information and to address security concerns.

48. The attack had profound and harmful effects on the relationship between NNAF and its member funds. NNAF risked losing the trust and confidence of member funds in the network due to the attack on the fundraising platform where the funds had been engaging existing and new supporters. Inviting abortion funds to participate in Bowl-a-Thon again the following year was very difficult for NNAF knowing that they were being targeted or that they might risk another attack.

49. NNAF incurred significant financial costs as a result of the attack.

50. Because of the attack, NNAF changed fundraising platforms, built a new front-end website, and set up secure hosting and a security audit for the website. All of this involved staff time as well as up-front and ongoing expenses which ultimately totaled more than $50,000.

51. As a result of the attack NNAF hired a crisis security firm to perform forensics and legal counsel at considerable expense. These costs totaled more than $200,000. NNAF spent the subsequent year revamping security for all websites, again at the cost of significant staff time.

52. NNAF held in-person meetings, workshops, and webinars throughout the following year to support funds who were impacted at significant expense and staff time.

53. NNAF hired an IT Security Manager who spent a great deal of time providing security and IT related support to affected funds. The hiring cost alone was almost $2,000. These ongoing costs were significant and have yet to be finalized.

EASTERN MASSACHUSSETS ABORTION FUND ("EMAF")

54. EMAF is located in Cambridge, Massachusetts. The fund is committed to access to reproductive justice and focuses on serving the population of Eastern Massachusetts.

55. In 2016, EMAF used the NNAF Bowl-A-Thon site to register participants and collect donations.[2]

56. On or around April 11, 2016, EMAF realized they could not access its Bowl-A-Thon fundraising website and emailed NNAF.

57. On or around April 11, 2016 EMAF had to send an internal email to its staff, informing them that the website was down. Staff scrambled to come up with a plan to

[2] Instead of bowling, EMAF organizes what it calls a "triathlon" for participants who raise funds.

inform donors of the situation and to provide an alternative means to process donations.

58. Later, EMAF sent an email to Bowl-a-Thon participants informing them that the website was not working and gave them an alternative donation site to use until the problem could be fixed.

59. Two days later, on April 13, 2016, an EMAF staff member learned that an individual trying to donate through the website had received a message from Google that the site was "unsecured". As a result, the donor could not complete the donation.

60. By the evening of April 13th, EMAF staffers became aware that the website was being labeled as unsecured whenever a user attempted to access it from the Google Chrome browser.

61. On April 14, 2016, EMAF staff and Bowl-A-Thon participants received a spoofed email with a picture of a fetus. This email caused emotional distress in its recipients and discouraged participation in the Bowl-a-Thon.

62. On April 14, 2016, NNAF informed all of its participating member funds, including EMAF, that the website was down and that a hacker had sent spoofed emails.

63. On April 15, 2016 at 6:05 AM, EMAF notified its fundraiser participants of the attack.

64. EMAF was eventually informed that the personally identifying information of a number of their donors had been stolen.

65. EMAF had to notify its donors that had their information had been compromised in the attack.

66. EMAF estimates that at least 50 staff and/or volunteer hours were spent responding to the hack.

67. EMAF has not been able to calculate the reputational cost of the attack.

68. EMAF's ability to provide access to abortions is contingent upon the time its staff and volunteers can dedicate to effectuating that goal. The Bowl-A-Thon attack caused EMAF

material harm because it had to redirect resources away from fundraising and towards crisis response.

GATEWAY WOMEN'S ACCESS FUND ("GWAF")

69. GWAF is an abortion access fund located in St. Louis, Missouri. It serves Missouri residents receiving care in Missouri, Illinois, and Kansas.

70. GWAF participated in the Bowl-A-Thon for the first time in 2016.

71. When GWAF volunteer staff and board members learned of the security breach in April 2016, they were very distressed.

72. GWAF became aware of the impersonating email sent out by Defendant(s), and needed to take on a number of responsive measures to reassure and calm their donors.

73. GWAF had to send out an email to their listserve about the spoofed email, and advised everyone not to open the email.

74. A number of GWAF's donors had their personal information compromised and GWAF had to notify those donors about their stolen information.

75. GWAF had to expend a significant number of hours in order to respond to the attack.

76. GWAF has not been able to calculate the reputational cost of the attack.

77. GWAF's ability to provide access to abortion is contingent upon the time its staff and volunteers can dedicate to effectuating that goal. The Bowl-A-Thon attack caused GWAF material harm because it had to redirect resources away from fundraising and towards crisis response.

KENTUCKY HEALTH JUSTICE NETWORK ("KHJN")

78. KHJN is an abortion fund located in Louisville, KY that is committed to providing access to reproductive justice in the state of Kentucky. Their abortion access programs currently assist approximately a dozen individuals per week statewide.

79. On April 11, 2016, NNAF informed KHJN that there had been an issue with the Bowl-A- Thon website, but that the website was back up again.

80. On April 13, 2016, NNAF provided more details about the attack and that changes were being made to enhance security.

81. On or around April 14, 2016, KHJN donors and participants received the spoofed email.
That same day, NNAF notified participating funds of the spoofed email.

82. The attack required KJHN to expend staff time by sending out additional communications to donors and participants. KJHN had to send out communiqués to alert donors and participants about the spoofed email (April 14, 2016), to inform them how they could still make donations (April 18, 2016), and when the Bowl-A-Thon site was restored (April 25, 2016).

83. After the attack, KHJN had to switch to accepting Bowl-A-Thon donations through PayPal, which was more complicated to track and administer.

84. The attack also created additional work for KHJN in May 2016 for reporting donation data to NNAF, because NNAF could not rely on its usual tracking systems.

85. On or around May 27, 2016, NNAF provided information to KHJN about the number of donors whose personally identifying information was stolen.

86. At least eleven of KHJN's donors had their information compromised.

87. On or around May 30, 2016, KHJN sent out individualized emails to the eleven donors that had their information compromised in the attack.

88. On or around June 1, 2016, KHJN distributed a list of frequently asked questions about the attack to its board members and others.

89. In October 2016, KHJN participated in a Technology and Security Assessment for NNAF in preparation for 2017 Bowl-A-Thon.

90. A significant number of KHJN staff and volunteer hours were spent

responding to the attack.

91. KHJN depends on fundraising to support its work in facilitating access to abortion. Between 2013-2017 KHJN provided assistance to only about one third of requests they received through their hotline, for a total of 1850-1900 people served.

92. The attack had a substantive impact on KHJN's fundraising in fiscal 2016. KHJN had raised a net total of $4,730 from the 2014 Bowl-A-Thon. It raised $13,025.64 the following year, for an increase of 175.4%. In 2016, as a result of the attack on Bowl-A-Thon, KHJN was only able to raise $11,841.54, a 9% annual decrease.

93. In 2016, KHJN's Bowl-a-Thon fundraiser went live on February 14th. From that date to April 11th, the fund received $7,283.54 in donations.

94. The DDoS attack on April 11, 2016, forced KHJN to move its fundraising platform to PayPal. Between April 12th and April 22nd when the Bowl-A-Thon website was restored, KHJN raised money on PayPal. Generally fundraising rises as the Bowl-A-Thon event approaches however during this ten-day period in 2016, the fund raised only $1,355, a marked decrease from previous years.

95. The extent to which the year-on-year decrease was anomalous is illustrated by KHJN's 2017 Bowl-A-Thon fundraising number - $30,278.45. KHJN has no explanation for the year on year decrease in 2016 other than the effects of the attack.

96. KHJN has not been able to calculate the reputational cost of the attack.

97. KHJN's ability to provide access to abortion is contingent upon the time its staff and volunteers can dedicate to effectuating that goal. The Bowl-A-Thon attack caused KHJN material harm because it had to redirect resources away from fundraising and towards crisis response.

NORTHWEST ABORTION ACCESS FUND ("NWAAF")

98. NWAAF is an abortion access fund committed to reproductive justice that is located in Eugene, Oregon. Between 2014-2017 the hotline received 4,041 calls and the fund disbursed 1,257 grants. It serves the areas of Washington, Oregon, Idaho, and Alaska.

99. The Bowl-A-Thon is the premier annual fundraising event for NWAAF. Each year they have seen a significant increase in funding over the prior year.

100. In 2016, NWAAF used the NNAF Bowl-A-Thon site to register bowlers and receive donations. The attack completely interrupted its capacity to fundraise during the time that the NNAF site was down.

101. To make matters worse, the attack occurred at the height of NWAAF's fundraising momentum. As with other funds, a significant percentage of all donations to Bowl-A-Thon are raised in the final ten days of the event. Because NWAAF's Bowl-A-Thon event took place on April 23, 2016 the attack had a major impact on their fundraising during this crucial period.

102. NWAAF had to send information to redirect donors to its home donation page. Because NWAAF's website lacked the same tools as the NNAF donation site, staffers at NWAAF had to expend additional time notifying participants in the event that they had received donations.

103. Upon information and belief, the April 14, 2016 spoofed emails went to everyone registered as a NWAAF participant or a donor through the NNAF site.

104. After the email, NWAAF had to send follow up communications to tell recipients explaining what had occurred and to keep them apprised of the situation and its consequences as they unfolded.

105. The interruption made it very difficult for NWAAF to match donations to participants. Participants also could not see their donation totals, a motivational tool for

NWAAF's fundraisers, and were therefore not motivated to outperform each other.

106. At least seven NWAAF donors had their credit card information stolen as a result of the attack.

107. NWAAF board members devoted significant time to addressing the consequences of the breach. The President of NWAAF's board alone spent at least forty hours on the matter.

108. As a result of the disruption of their fundraising activities, NWAAF's annualized year over year growth in fundraising from Bowl-A-Thon from 2015 to 2016 lagged substantially behind other years.

109. NWAAF has not been able to calculate the reputational cost of the attack.

110. NWAAF's ability to provide access to abortion is contingent upon the time its staff and volunteers can dedicate to effectuating that goal. The Bowl-A-Thon attack caused NWAAF material harm because it had to redirect resources away from fundraising and towards crisis response.

PRETERM ACCESS FUND ("PRETERM")

111. Preterm is a full-service reproductive healthcare provider dedicated to reproductive justice located in Cleveland, Ohio.

112. It provides financial assistance for abortion patients through its Preterm Access Fund.

113. For Preterm, the attack occurred around 10 days before their Bowl-a-Thon event. Historically, Preterm has raised about a third of its donations during the final ten (10) days of the Bowl-a-Thon leading up to the final event.

114. Before the attack, Preterm was on track to meet its fundraising goal, but in the end, they did not reach it.

115. As a result of the attack, Preterm saw a smaller number of donations in 2016 than it had in 2015; in 2015 Preterm had 1,036 total donations, while in 2016 it only received 770.

116. Preterm saw a smaller increase in the total amount it raised during Bowl-A-Thon than it had anticipated. From 2013 to 2014, Preterm's Bowl-A-Thon fundraising total grew from $17,888 to $36, 796 (an increase of $18,908). From 2014 to 2015, fundraising increased to $45,011 (an increase of $8,215). However, from 2015 to 2016 Preterm saw only a $3,123 increase in fundraising. The following year it would return to its historical growth rate, of $10,018).

117. At least eight of Preterm's donors had their information compromised.

118. NNAF advised Preterm of those whose information was compromised.

119. Preterm notified donors who had their information compromised in the attack.

120. Preterm also told the participants whom those donors had supported, and it shook the confidence of the donors and participants, for example one of the donors whose information was stolen, contacted Preterm recently to ask whether a current credit card problem they were experiencing could be linked back to the Bowl-A-Thon.

121. It was highly damaging for Preterm to reach out to their supporters, as they were individuals with whom Preterm had previously maintained strong relationships with.

122. Preterm staff had to create a workaround while the website was down, which was very time-consuming.

123. Preterm has not been able to calculate the reputational cost of the attack.

124. Preterm's ability to provide access to abortion is contingent upon the time its staff and volunteers can dedicate to effectuating that goal. The Bowl-A-Thon attack caused Preterm material harm because it had to redirect resources away from fundraising and towards crisis response.

FIRST CAUSE OF ACTION
Violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030

125. Plaintiffs re-allege and incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

126. Defendant(s) violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq.* by intentionally accessing a protected computer without authorization or exceeding authorized access with the intent to obtain information, further a fraud, or damage the computer or its data.

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

128. Defendant(s) knowingly and intentionally accessed Plaintiffs' computers without authorization or in excess of authorization.

129. After gaining unauthorized access to Plaintiffs' Bowl-a-Thon platform, Defendant(s) obtained and used valuable information from Plaintiffs' protected computers, including credit card and personal identifying donor information.

130. Defendant(s) damaged the data stored on protected computers by organizing a DDoS attack, which disabled the fundraising website for several hours.

131. Defendant(s) knowingly, willfully, and with intent to defraud routed Plaintiffs' donors to a fraudulent web page to harvest donors' information and sent spoofing emails impersonating Plaintiff NNAF.

132. Defendant(s)' conduct has caused a loss to Plaintiffs during a one-year period well in excess of $5,000.00. Plaintiffs have been damaged by Defendant(s)' actions, including decreased fundraising, being forced to expend resources to respond to the attack, pay for forensic investigators, and the cost of staff dealing with the crisis.

133. Plaintiffs also suffered irreparable and incalculable harm and injuries resulting from Defendant(s)' conduct in the form of lost and interrupted donations, the distress from receiving Defendant(s)' racist and anti-Semitic messages, and damages to donors' goodwill and trust.

134. Plaintiffs have been damaged by Defendant(s)' actions, including being forced to expend resources and staff time in investigating and responding to the attack.

135. As a result of Defendant(s)' violations of the CFAA, Plaintiffs seek compensatory and equitable relief.

FIRST CAUSE OF ACTION
Violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(a)(2)(C)

136. Plaintiffs re-allege and incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

137. Defendant(s) violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(2)(C), by intentionally accessing a protected computer without authorization, or exceeding authorized access, and thereby obtaining information.

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

139. Defendant(s) intentionally accessed Plaintiffs' computers without authorization or in excess of authorization.

140. After gaining unauthorized access, or exceeding their authorized access, to Plaintiffs' Bowl-a-Thon platform, Defendant(s) obtained and used valuable information from Plaintiffs' protected computers, including credit card and personal identifying donor information.

141. Defendant(s)' conduct has caused a loss to Plaintiffs during a one-year period well in excess of $5,000.00. Plaintiffs loss from Defendant(s)' actions includes decreased fundraising, being forced to expend resources to respond to the attack, pay for forensic investigators, and the cost of staff dealing with the crisis.

142. Plaintiffs also suffered irreparable and incalculable harm and injuries resulting from Defendant(s)' conduct in the form of lost and interrupted donations, the distress from receiving Defendant(s)' racist and anti-Semitic messages, and damages to donors' goodwill and trust.

143. Plaintiffs have been damaged by Defendant(s)' actions, including being forced to expend resources and staff time in investigating and responding to the attack.

144. As a result of Defendant(s)' violations of the CFAA, Plaintiffs seek compensatory and equitable relief.

SECOND CAUSE OF ACTION
Violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(a)(5)(A)

145. Plaintiffs re-allege and incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

146. Defendant(s) violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(5)(A) by knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caused damage, without authorization, to a protected computer.

147. Defendant(s) damaged the protected computers through their actions, including implementing a DDoS attack, which disabled the fundraising website for several hours, as well as running malicious scripts on Plaintiffs' computers.

148. Defendant(s)' conduct has caused a loss to Plaintiffs during a one-year period well in excess of $5,000.00. Plaintiffs loss from Defendant(s)' actions include decreased fundraising, being forced to expend resources to respond to the attack, pay for forensic investigators, and the cost of staff dealing with the crisis.

THIRD CAUSE OF ACTION
Violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(a)(5)(B)

149. Plaintiffs re-allege and incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

150. Defendant(s) violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(5)(B) by intentionally accessing a protected computer without authorization, and as a result of such conduct, recklessly caused damage.

151. Defendant(s)' conduct has caused a loss to Plaintiffs during a one-year period well in excess of $5,000.00. Plaintiffs loss from Defendant(s)' actions include decreased

fundraising, being forced to expend resources to respond to the attack, pay for forensic investigators, and the cost of staff dealing with the crisis.

FOURTH CAUSE OF ACTION
Violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(a)(5)(C)

152. Plaintiffs re-allege and incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

153. Defendant(s) violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(5)(C) by intentionally accessing a protected computer without authorization, and as a result of such conduct, caused damage and loss.

154. Defendant(s)' conduct has caused a loss to Plaintiffs during a one-year period well in excess of $5,000.00. Plaintiffs loss from Defendant(s)' actions include decreased fundraising, being forced to expend resources to respond to the attack, pay for forensic investigators, and the cost of staff dealing with the crisis.

FIFTH CAUSE OF ACTION
Violations of the Freedom of Access to Clinic Entrances Act,
18 U.S.C. § 248(a)(1) and § 248(a)(3)

155. Plaintiffs re-allege and incorporate by reference the allegations in the foregoing paragraphs of this complaint as though fully set forth herein.

156. Defendant(s) have violated the Freedom of Access to Clinic Entrances Act ("FACE") because they "intentionally damage[d] or destroy[ed] the property of a facility, or attempt[ed] to do so, because such facility provides reproductive health services…".

157. Plaintiffs have standing to bring this suit because they are "persons" seeking to provide access to reproductive health services or are in fact facilities that provide reproductive health services.

158. Plaintiffs are considered to be "facilities" within the meaning of the statute because they offer access to "reproductive health services."

159. "Reproductive health services" is defined in the statute to include, "counselling or

referral services relating to the human reproductive system, including services relating to pregnancy or the termination of pregnancy."

160. Plaintiffs offer referral services related to the termination of pregnancies, and at least one of the Plaintiffs, Preterm, provides abortions onsite.

161. Defendant(s)'actions – the hacking and phishing, creation and distribution of racist and violent imagery – all intimidated or interfered with, or attempted to intimidate or interfere with Plaintiffs' services relating to pregnancy or the termination of pregnancy.

162. Defendant(s) damaged or destroyed Plaintiffs' property when they redirected Plaintiffs' web traffic to a fraudulent donations page, thereby damaging the donor lists that belonged to Plaintiffs and depriving Plaintiffs of donations they otherwise would have received.

163. Defendant(s) damaged and destroyed Plaintiffs' property by forcing Plaintiffs' Bowl- a-Thon website offline through waves of fake donations on April 11, 2016, thereby depriving Plaintiffs of donations they otherwise would have received.

164. Defendant(s)' actions were motivated by their desire to intimidate or interfere with access to reproductive health services. This was demonstrated by the Anti-abortion rhetoric that Defendant(s) sent to Plaintiffs' donors in the emails sent under the names "Adolph Hitler" and Info@NNAF.org.

165. As a result of Defendant(s)' violations of the FACE Act, Plaintiffs seek punitive and compensatory damages, as well as the cost of suit, attorney's fees, and expert witness fees in an amount to be determined by the Court.

JURY DEMAND

166. Plaintiff demands a trial by jury on all issues pursuant to the Seventh Amendment to the United States Constitution and Rule 38 of the Federal Rules of Civil Procedure.

WHEREFORE, Plaintiffs pray that the court:

1. Enter judgment in favor of Plaintiffs and against Defendant(s).

2. Enter a preliminary and permanent injunction enjoining Defendant(s) and their officers, directors, principals, agents, servants, employees, successors and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein.

3. Enter judgement ordering the disgorgement of all data obtained by Defendant(s) during the course of the activity complained of herein, and ordering Defendants not to distribute any such data and to destroy any copies thereof.

4. Enter judgment awarding compensatory damages in an amount to be proven at trial, and other equitable relief, as provided in 18 U.S.C. § 1030(g).

5. Enter judgement awarding compensatory and punitive damages in an amount to be proven at trial, as well as the costs of suit and reasonable fees for attorneys and expert witnesses, or in lieu of actual damages and at Plaintiffs' election, an award of statutory damages in the amount of $5,000 per violation, as provided in 18 U.S.C. § 248(c)(1)(B);

5. Enter judgement awarding attorneys' fees and costs, and

6. Order such other relief that the court deems just and reasonable.

Dated: March 28, 2018

Respectfully submitted,

/s/Mitchell Matorin
Mitchell J. Matorin (BBO# 649304)
Matorin Law Office, LLC
18 Grove Street, Suite 5
Wellesley, MA 02482
(781) 453-0100
mmatorin@matorinlaw.com

/s/ *Carrie Goldberg*
Carrie Goldberg
Aurore DeCarlo
Adam Massey
C.A. Goldberg PLLC
16 Court Street, Suite 2500
Brooklyn, NY 11241
(646)666-8908
carrie@cagoldberglaw.com
Pro Hac Vice Motions Pending