IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v.

DENNIS OWEN COLLINS,
a/k/a "iowa," "owen," "anon5,"
JEREMY LEROY HELLER,
a/k/a "Jeremyhfht," "heelgea,"
ZHIWEI CHEN,
a/k/a "Jack," "TickL," "TickLe," "internets," "Zhiwei,"
JOSHUA S. PHY,
a/k/a "Anonyjosh,"
RYAN RUSSELL GUBELE,
a/k/a "grishnav,"
ROBERT AUDUBON WHITFIELD,
a/k/a "mightymooch,"
ANTHONY TADROS,
a/k/a "Winslow,"
GEOFFREY KENNETH COMMANDER,
a/k/a "jake," "bipto,"
PHILLIP GARRETT SIMPSON,
a/k/a "jikbag,"
AUSTEN L. STAMM,
a/k/a "user_x,"
TIMOTHY ROBERT McCLAIN,
WADE CARL WILLIAMS,
a/k/a "TheMiNd," and
THOMAS J. BELL,

Defendants.

Criminal No. 1:13-cr-383

Count One: 18 U.S.C. § 371

Conspiracy to Intentionally Cause Damage to a Protected Computer

Forfeiture Notice

INDICTMENT

OCTOBER 2013 Term – at Alexandria, Virginia

THE GRAND JURY CHARGES THAT:

COUNT ONE

At all times relevant to this Indictment:

1. Between on or about September 16, 2010 and at least January 2, 2011, defendants DENNIS OWEN COLLINS, JEREMY LEROY HELLER, ZHIWEI CHEN, JOSHUA S. PHY, RYAN RUSSELL GUBELE, ROBERT AUDUBON WHITFIELD, ANTHONY TADROS, GEOFFREY KENNETH COMMANDER, PHILLIP GARRETT SIMPSON, AUSTEN L. STAMM, TIMOTHY ROBERT McCLAIN, WADE CARL WILLIAMS, and THOMAS J. BELL, together with others known and unknown to the Grand Jury, participated in a worldwide conspiracy as part of the online group ANONYMOUS in a campaign dubbed "OPERATION PAYBACK" (or "OPERATION: PAYBACK IS A BITCH,") to engage in a coordinated series of cyber-attacks against victims.

2. OPERATION PAYBACK targeted victims worldwide, including governmental entities, trade associations, individuals, law firms, and financial institutions, which ANONYMOUS claimed opposed its stated philosophy of making all information free for all, including information protected by copyright laws or national security considerations. As a result, the defendants, together with other ANONYMOUS members known and unknown to the Grand Jury, launched, or attempted to launch, cyber-attacks against entities including the Recording Industry Association of America ("RIAA") in the Eastern District of Virginia, the Motion Picture Association of America ("MPAA"), the United States Copyright Office of the Library of Congress, Visa, MasterCard, and Bank of America, and caused significant damage to victims.

3. From on or about September 16, 2010 through on or about January 2, 2011, in the Eastern District of Virginia, and elsewhere, defendants DENNIS OWEN COLLINS, JEREMY LEROY HELLER, ZHIWEI CHEN, JOSHUA S. PHY, RYAN RUSSELL GUBELE, ROBERT AUDUBON WHITFIELD, ANTHONY TADROS, GEOFFREY KENNETH COMMANDER, PHILLIP GARRETT SIMPSON, AUSTEN L. STAMM, TIMOTHY ROBERT McCLAIN, WADE CARL WILLIAMS, and THOMAS J. BELL, each knowingly and intentionally conspired and agreed together and with each other, and with others known and unknown to the Grand Jury, including unindicted co-conspirators known and unknown to the Grand Jury, to commit an offense against the United States, that is, to knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage, and attempt to cause damage, without authorization, to a protected computer, with such damage and attempted damage during the one-year period beginning on or about September 16, 2010 affecting ten or more protected computers and causing loss to victims resulting from the course of conduct affecting protected computers aggregating at least $5,000 in value, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(b), and 1030(c)(4)(B).

MANNER AND MEANS OF THE CONSPIRACY

It was a part of the conspiracy that:

4. Defendants DENNIS OWEN COLLINS, JEREMY LEROY HELLER, ZHIWEI CHEN, JOSHUA S. PHY, RYAN RUSSELL GUBELE, ROBERT AUDUBON WHITFIELD, ANTHONY TADROS, GEOFFREY KENNETH COMMANDER, PHILLIP GARRETT SIMPSON, AUSTEN L. STAMM, TIMOTHY ROBERT McCLAIN, WADE CARL WILLIAMS, and THOMAS J. BELL, as part of ANONYMOUS, planned and executed a

coordinated series of cyber-attacks against victim websites by flooding those websites with a huge volume of irrelevant Internet traffic with the intent to make the resources on the websites unavailable to customers and users of those websites. This method of online attack is known as a Distributed Denial of Service ("DDoS") attack.

5. The weapon of choice for the DDoS cyber-attacks which defendants DENNIS OWEN COLLINS, JEREMY LEROY HELLER, ZHIWEI CHEN, JOSHUA S. PHY, RYAN RUSSELL GUBELE, ROBERT AUDUBON WHITFIELD, ANTHONY TADROS, GEOFFREY KENNETH COMMANDER, PHILLIP GARRETT SIMPSON, AUSTEN L. STAMM, TIMOTHY ROBERT McCLAIN, WADE CARL WILLIAMS, and THOMAS J. BELL, used and, in some cases, publicized and distributed to other ANONYMOUS members, was a freely-available and downloadable network stress testing program known as the Low Orbit Ion Cannon ("LOIC").

6. To generate enough irrelevant Internet traffic to effectively shut down a specific website required the collective firing of many LOIC tools at the same time and at the same website address (the Internet Protocol or IP address). Members of ANONYMOUS, including DENNIS OWEN COLLINS, JEREMY LEROY HELLER, ZHIWEI CHEN, JOSHUA S. PHY, RYAN RUSSELL GUBELE, ROBERT AUDUBON WHITFIELD, ANTHONY TADROS, GEOFFREY KENNETH COMMANDER, PHILLIP GARRETT SIMPSON, AUSTEN L. STAMM, TIMOTHY ROBERT McCLAIN, WADE CARL WILLIAMS, and THOMAS J. BELL, participated in and coordinated these DDoS cyber-attacks – deciding on the next target; publicizing the victim names and IP addresses; announcing dates, times, and relevant instructions; downloading the LOIC tool; and recruiting more attackers – through postings (collectively, "fliers") on web bulletin boards and through social media and dedicated online

chatrooms known as Internet Relay Chat ("IRC") channels. IRC channels used by ANONYMOUS for OPERATION PAYBACK included the #command, #saveTPB, #savethepiratebay, and #operationpayback channels.

7. OPERATION PAYBACK caused damage affecting at least ten protected computers and caused loss aggregating at least $5,000 in value during a one-year period.

OVERT ACTS

In furtherance of the conspiracy and to effect the objects of the conspiracy, the following overt acts, among others, were committed in the Eastern District of Virginia and elsewhere:

8. In or about September 2010, members of ANONYMOUS launched OPERATION PAYBACK to retaliate against the discontinuation of "The Pirate Bay," a Sweden-based file-sharing website dedicated to the illegal downloading of copyrighted material.

9. On or about September 16, 2010, a member of the conspiracy posted a flier on a web bulletin board advertising a cyber-attack against the Motion Picture Association of America ("MPAA") website hosted in California. The flier announced: "We target the bastard group that has thus far led this charge against our websites, like The Pirate Bay. We target MPAA.ORG! The IP is designated at [IP address], and our firing time remains THE SAME." The flier provided the location at which co-conspirators could download the LOIC tool, and gave instructions as follows: "Install the LOIC linked above into any directory you choose, load it up and set the target IP to [IP address] port 80 Method will be TCP, threads set to 10+, with a message of 'Payback is a bitch'... Everything else must be left blank. Once you have the target locked, DO NOT FIRE. REPEAT: DO NOT FIRE! This will be a calm, coordinated display of blood. We will not be merciful. We wil not be newfags. The first wave will be firing in: ONE

DAY: 09/17/2010 9PM EASTERN When it comes time to fire, ignore all warning messages. They mean nothing. Keep firing."

10. On or about September 17, 2010, members of the conspiracy launched the DDoS cyber-attack on MPAA.org. During the DDoS cyber-attack, defendant JEREMY LEROY HELLER repeatedly checked the status of the MPAA.org website.

11. On or about September 18, 2010, defendant ZHIWEI CHEN, as "internets," participated in the DDoS cyber-attack on MPAA.org in a dedicated chat channel for OPERATION PAYBACK.

12. Also on or about September 18, 2010, during the DDoS cyber-attack on MPAA.org, defendant RYAN RUSSELL GUBELE, as "grishnav," monitored the effect of the attack on the victim website and issued warnings that the MPAA.org website was now at a different IP address: "need threads guys! mpaa.org is back! they have a new IP." GUBELE further announced: "new mpaa IP is an anti-ddos service... someone took notice."

13. Also on or about September 18, 2010, during the DDoS cyber-attack on MPAA.org, defendant JEREMY LEROY HELLER, as "Jeremyhfht," announced in #saveTPB that an attack on the Recording Industry Association of America ("RIAA") in the Eastern District of Virginia was scheduled for the following day. HELLER also directed that another member of the conspiracy edit a propaganda flier announcing the attack.

14. As a result of this DDoS cyber-attack by ANONYMOUS, the MPAA suffered at least $5,000 in losses during a one-year period.

15. Also on or about September 18, 2010, a member of the conspiracy posted a flier on a web bulletin board announcing a cyber-attack against the Recording Industry Association of America ("RIAA") website hosted in the Eastern District of Virginia. The flier, captioned

"Operation: Payback (is a bitch)," provided instructions on how to download the LOIC tool, published the target IP address for the RIAA, and declared: "Our first objective was to take down Aiplex, the ones that DDoSed TPB [The Pirate Bay]. Everything had went even better than expected. We selected a new target, MPAA, in just eight minutes after launching the attack, their website suffered another tremendous blow at our Hands. We will be launching a second attack against the RIAA on September 19th, 3:00PM EDT."

16. In connection with the RIAA DDoS cyber-attack, defendant RYAN RUSSELL GUBELE accessed RIAA network resources approximately 150 times.

17. As a result of the DDoS cyber-attacks by ANONYMOUS in September 2010, the RIAA suffered at least $5,000 in losses during a one-year period.

18. During the September 19, 2010 DDoS cyber-attack on RIAA, defendant JEREMY LEROY HELLER, as "Jeremyhfht," led a group vote in #saveTPB to formally name the online group as ANONYMOUS. Co-conspirators in #saveTPB and #savethepiratebay also discussed DDoS cyber-attacks against Davenport Lyons, a British law firm helping clients to protect intellectual property rights, and the British Phonographic Institute ("BPI"), which is a trade association representing the United Kingdom's recorded music industry. HELLER announced the attack on BPI.

19. Also on or about September 19, 2010, a member of the conspiracy posted a flier announcing a DDoS cyber-attack on BPI: "WE ARE ANONYMOUS. For the past 72 hours we have brought down the oppresive RIAA and MPAA. These corperations have fought to restrict our freedoms... We brought them down the same way they brought down The Pirate Bay, with a distributed denial of service... There is one corperation that has so far escaped our notice. BPI, the British Phonographic Industry... So what can you do to help? Download LOIC or

JavaLOIC, charge your lazahs, and point them at [IP address]' ... Remember, don't start shooting until 4:00 GMT Monday September 20."

20. That day, September 19, 2010, members of the conspiracy launched a DDoS cyber-attack against the BPI website hosted in the United Kingdom.

21. During the attack on BPI on or about September 19, 2010, defendant ZHIWEI CHEN, as "TickL," coached other co-conspirators in #savethepiratebay how to specifically use the LOIC tool to accomplish the DDoS cyber-attack.

22. On or about September 20, 2010, during the DDoS cyber-attack on BPI, members of the conspiracy agreed in #saveTPB in which defendant JEREMY LEROY HELLER was a channel operator to attack the RIAA next. A member of the conspiracy posted a flier announcing another DDoS cyber-attack on the RIAA in the Eastern District of Virginia that same day at 8 p.m. An unindicted co-conspirator also used the social media platform Twitter to announce "RAID ON THE RIAA OCCURING AT 0000 GMT," and included a link to an announcement for the attack. That same day, members of the conspiracy also scheduled another attack on the MPAA for September 21, 2010. Defendant JOSHUA S. PHY participated in these discussions.

23. Also on or about September 20, 2010, members of the conspiracy changed the DDoS cyber-attack target from BPI to AiPlex Software Pvt.Ltd. ("AiPlex"), an anti-piracy company based in the Republic of India. In connection with this attack, a member of the conspiracy posted a flier publishing the IP address of AiPlex and instructing LOIC users to include the message "Payback is a bitch" in the irrelevant Internet traffic aimed at the AiPlex website.

24. On this day, defendant JOSHUA S. PHY, as "Anonyjosh," also identified AiPlex as a current target and told members of the conspiracy to "FIRE NOW!" On or about September 21, 2010, PHY, in #saveTPB, posted a link to "An Open Letter from Anonymous" describing the OPERATION PAYBACK campaign of DDoS cyber-attacks against MPAA and RIAA in the Eastern District of Virginia. The letter vowed that "[t]hese successful attacks on MPAA and RIAA's servers shall continue."

25. Also on or about September 21, 2010, defendant JEREMY LEROY HELLER, as "heelgea," and defendant JOSHUA S. PHY, as "Anonyjosh," in #saveTPB, announced a DDoS cyber-attack on MPAA, and members of the conspiracy launched a DDoS cyber-attack against MPAA. During this attack, HELLER coached co-conspirators on how to most effectively use the LOIC tool, admitted to coordinating the DDoS cyber-attacks, and solicited more DDoS cyber-attacks.

26. Also on or about September 21, 2010, during the attack on RIAA in the Eastern District of Virginia, members of the conspiracy planned DDoS cyber-attacks on ACS:Law, a British law firm helping clients to protect intellectual property rights, and Anti-piracy.nl, the website for the BREIN foundation, a Dutch trade association fighting intellectual property theft. Once defendant JEREMY LEROY HELLER announced the new targets, members of the conspiracy launched DDoS cyber-attacks against the websites of ACS:Law and the BREIN foundation.

27. During the DDoS cyber-attacks against ACS:Law and the BREIN foundation on or about September 21, 2010, members of the conspiracy agreed to attack the Australian Federation Against Copyright Theft ("AFACT") next.

28. While OPERATION PAYBACK was targeted at ACS:Law on or about September 22, 2010, defendants JEREMY LEROY HELLER, as "heelgea," and ZHIWEI CHEN, as "TickL," in #saveTPB and #savethepiratebay announced the current DDoS target as ACS:Law, identified A.C., the main partner of the firm, individually as a target, and posted A.C.'s home address. HELLER stated that, "WE WILL MAKE HIS COFFEE TASTE LIKE AIDS."

29. Also on or about September 22, 2010, during the DDoS cyber-attack on ACS:Law, members of the conspiracy launched a DDoS cyber-attack on AFACT.

30. Also on or about September 22, 2010, during the DDoS cyber-attacks on ACS:Law and AFACT, members of the conspiracy planned and launched additional DDoS cyber-attacks on Davenport Lyons and the Association of Commercial Audiovisual of Portugal ("ACAPOR"), a film and music anti-piracy association, and attempted a DDoS cyber-attack against Trident Media Guard, a French anti-piracy company seeking to prevent unauthorized copying of files over the Internet.

31. On or about September 23, 2010, conspirators planned and launched a second DDoS cyber-attack on Davenport Lyons.

32. Also on or about September 23, 2010, defendant ZHIWEI CHEN, as "TickL," in #savethepiratebay directed the testing of a new version of the LOIC tool. CHEN then posted a link to this new version of the LOIC tool with instructions on how to use it and stated, "we will begin our mass attacks on friday."

33. On or about September 24, 2010, during the DDoS cyber-attack on Davenport Lyons, members of the conspiracy planned and launched additional attacks on AiPlex and ACS:Law. The related OPERATION PAYBACK flier announced ACS:Law as a new target "in

our movement against anti-piracy organizations across the globe," provided the IP address for the law firm's website, gave instructions on how to download and use the LOIC tool, and provided the exact time for the attack in various time zones.

34. On or about September 25, 2010, during the DDoS cyber-attacks on AiPlex and ACS:Law, members of the conspiracy planned another attack on AFACT. Defendant JEREMY LEROY HELLER, as "heelgea," in #savethepiratebay stated, "Our next target will suffer just as much as ACS law. WE WILL NOT STOP."

35. Also on or about September 25, 2010, during the DDoS cyber-attacks on AiPlex and ACS:Law, a member of the conspiracy posted a link to a flier entitled "Payback is a bitch, isn't it?" The flier explained that organizations supportive of copyright laws, such as the MPAA, the RIAA, BPI, AFACT, and BREIN, were engaged in "propaganda" and that "[i]n the end, our DDoS efforts have been compared to waiting for a train. What do we have to do to be heard? To be taken seriously? Do we have to take to the streets, throwing molitovs, raiding offices of those we oppose? Realize, you are forcing our hand by ignoring us. You forced us to DDoS when you ignored the people, ATTACKED, the people, LIED TO THE PEOPLE!"

36. Also on or about September 25, 2010, during the DDoS cyber-attacks on AiPlex and ACS:Law, members of the conspiracy publicly posted the personal identifying information of various individuals associated with the target entities of OPERATION PAYBACK. Such personal identifying information included home addresses, the names of spouses, credit card details, personal email addresses, dates of birth, and other private information.

37. On or about September 26, 2010, during the DDoS cyber-attacks on AiPlex and ACS:Law, a member of the conspiracy in #savethepiratebay posted a link to an attack list which included as upcoming targets additional anti-piracy groups in Australia, Belgium, and Brazil, and

another member of the conspiracy posted a flier entitled "OPERATION PAYBACK." The flier cited to the DDoS attacks against AiPlex, MPAA, RIAA, ACS:Law, and Davenport Lyons, and claimed: "We took down their websites... Our next target will suffer just as much as ACS law. Every swine is destined for a stick with two pointed ends, and Anonymous is the usher that leads these swine to their fate."

38. Also on or about September 26, 2010, members of the conspiracy began launching a DDoS cyber-attack against AFACT, and on or about September 27, 2010, a member of the conspiracy posted a link to a flier announcing the attack against AFACT, recruiting new attackers, and pointing them to where to get the LOIC tool: "We will not stop, because we are Anonymous. We cannot be stopped, because we are the face of the Internet. The time to rise is now. You know why you are here. You know why you have kept reading this. You know why you are angry. Now ACT on it. Get in the IRC."

39. On or about September 27, 2010, defendant JEREMY LEROY HELLER, as "heelgea," in #savethepiratebay urged his co-conspirators to keep firing at AFACT to keep up the DDoS cyber-attack.

40. On or about September 29, 2010, members of the conspiracy launched DDoS cyber-attacks on the websites of Web Sheriff, a British company providing anti-piracy services, and DGLegal, a British legal consulting firm. As part of the attack, a member of the conspiracy posted a recruiting flier online under the OPERATION PAYBACK banner. The flier listed targets hit as RIAA, AiPlex, and BPI, showed the current target as "WebSheriff.com," pointed readers to #savethepiratebay and the LOIC tool, and proclaimed: "Anonymous needs You. The hour of Vengeance has come.... We will keep the DDoS down as long as possible. Lets do this, Anons."

41. On or about September 30, 2010, during the attack on DGLegal, members of the conspiracy planned a DDoS cyber-attack on the U.S. law firm of DunlapWeaver, which provides intellectual property services and has offices in Leesburg and Richmond, Virginia in the Eastern District of Virginia.

42. Also on or about September 30, 2010, defendant ZHIWEI CHEN, as "TickL," identified the current target as DGLegal and cautioned co-conspirators not to target WebSheriff with a DDoS cyber-attack but rather directed the co-conspirators to a Web Sheriff link if they "want to harm WebSheriff." On or about October 2, 2010, CHEN also advised co-conspirators that "unless you are DoS'ing from a closed internet source (like north korea) or from a closed insititution (school, prison, ect), YOU WILL NOT BE CAUGHT."

43. Between on or about October 1, 2010 and on or about October 3, 2010, during the DDoS cyber-attack on DGLegal and thereafter, members of the conspiracy planned attacks on Hadopi, a French institution dedicated to the protection of intellectual property rights; the Ministry of Sound, a British record label; and Gallant MacMillan LLP, a British law firm helping clients to protect intellectual property rights. Members of the conspiracy posted fliers announcing the attack: "We, the people, will be DDoSing www.gmlegal.co.uk [IP address] on 3 October, 7PM GMT / 3PM EDT."

44. On or about October 3, 2010, because Gallant MacMillan's website went down before the attack, ANONYMOUS abandoned the campaign, and instead launched a multi-day DDoS cyber-attack on the Ministry of Sound. During this attack, members of the conspiracy suggested a DDoS cyber-attack on the Spanish General Society of Authors and Publishers ("SGAE").

45. On or about October 6, 2010, a member of the conspiracy posted a flier captioned "OPERATION PAYBACK" advertising the date and time of the upcoming DDoS cyber-attack on SGAE: "After GMlegal taking down their own site before the countdown ended, effectively surrendering, we changed target to MinistryOfSound.com and brought them down within minutes, along with their sales page, for about 24h. Now it's time for a new target: www.sgae.es [IP address]." The flier further gave instructions on where and how participants could download the LOIC tool for the attacks.

46. Also on or about October 6, 2010, members of the conspiracy launched a DDoS cyber-attack on SGAE; planned a cyber-attack on the Business Software Alliance ("BSA"), an anti-piracy trade association headquartered in Washington, D.C.; and planned and launched attacks on the Spanish Ministry of Education, Culture, and Sport ("MCU") and Promusicae, a Spanish trade group representing the interests of the Spanish recording industry. In connection with planning various DDoS cyber-attacks, members of the conspiracy posted fliers captioned "OPERATION PAYBACK" and claimed that: "We sick and tired of these corporations seeking to control the internet in their pursuit of profit. Anonymous cannot sit by and do nothing while these organizations stifle the spread of ideas and attack those who wish to exercise their rights to share with others."

47. From on or about October 9, 2010 to on or about October 12, 2010, members of the conspiracy launched DDoS cyber-attacks on the Federal Italian Music Industry (fimi.it), the Italian branch of the International Federation of Phonographic Industry (ifpi.it), and an Italian directory of Pro Music, an Italian directory of sites offering music products legally (pro-music.it). During this time, ANONYMOUS planned and launched another attack on Gallant MacMillan.

48. From on or about October 13, 2010 to on or about October 15, 2010, during the DDoS cyber-attack on Gallant MacMillan, certain members of the conspiracy planned and launched DDoS cyber-attacks on the websites of Gene Simmons, an American performer who has spoken out against music piracy, and Access Copyright, a Canadian copyright licensing agency, and discussed attacking the website of Lily Allen, a British pop music singer and songwriter who has reportedly stated that illegal file-sharing hurts emerging artists. Fliers captioned "Operation: Payback (is a bitch)" advertising the attack against Gene Simmons stated that "Mr. Simmons shares the same ideology as ACS:Law and many of our other targets. Thusly his website has been targeted."

49. On or about October 16, 2010, members of the conspiracy suggested a DDoS cyber-attack on the website of the Australian Communications and Media Authority (ACMA.gov.au), the government entity responsible for the regulation of broadcasting, the Internet, radio, and telecommunications, and planned and launched a DDoS cyber-attack on the British Intellectual Property Office (IPO.gov.uk), the official government body responsible for granting intellectual property rights in the United Kingdom. OPERATION PAYBACK fliers advertising the attack stated that the reason for attacking the British Intellectual Property Office was because it was "[p]erpetuating the system that is allowing the exploitative usage of copyrights and intellectual property."

50. Between on or about October 17, 2010 and on or about October 19, 2010, during the attack on the British Intellectual Property Office, members of the conspiracy planned and launched DDoS cyber-attacks on Gene Simmons's websites. During the attack, defendant DENNIS OWEN COLLINS, as "iowa," in #savethepiratebay, monitored the effectiveness of the

attack on the Gene Simmons sites. Also on or about October 17, 2010, COLLINS, as "anon5," taught another member of the conspiracy how to use the LOIC tool in a DDoS cyber-attack.

51. On or about October 19, 2010, during the ongoing DDoS cyber-attacks on the British Intellectual Property Office and Gene Simmons's websites, members of the conspiracy planned an attack on Hadopi. As a result of the DDoS cyber-attacks by ANONYMOUS, Gene Simmons suffered at least $5,000 in losses during a one-year period.

52. Between on or about October 20, 2010 and on or about October 23, 2010, members of the conspiracy launched a DDoS cyber-attack on the websites of Satel Film, an Austrian movie production company, and Hustler, an American adult magazine.

53. On or about October 23, 2010, defendant DENNIS OWEN COLLINS, as "iowa," in #savethepiratebay, provided a link to the LOIC tool to another member of the conspiracy.

54. On or about October 25, 2010, members of the conspiracy discussed a DDoS cyber-attack on the Swiss Anti-Piracy Association ("SAFE") and planned and launched a DDoS cyber-attack on the Copyright Information and Anti-Piracy Centre in Finland (AntiPiracy.fi).

55. On or about October 26, 2010, during the attack on the Copyright Information and Anti-Piracy Centre in Finland, members of the conspiracy planned additional DDoS cyber-attacks on the websites of RIAA in the Eastern District of Virginia, and later also planned another attack on Hadopi.

56. On or about October 27, 2010, defendant DENNIS OWEN COLLINS, as "iowa," participated in the DDoS cyber-attack on RIAA by confirming the time for the attack, and a member of the conspiracy posted a flier captioned "OPERATION PAYBACK" advertising the RIAA attack. The flier declared that: "Limewire [a peer-to-peer file-sharing program] has been shut down by the RIAA. We cannot ignore this. They have f----- us over far too many times...

Be against the massive power of copyright labels. We must take revenge. It's time for payback... DDoS riaa.org on the 29th October 2010 9 PM EST." The flier additionally encouraged participants to harass the chairman and CEO of RIAA and his wife and listed their home address in Fairfax Station, Virginia, in the Eastern District of Virginia: "Send pizza and other crap. Get creative. Prank Call and black faxes for maximum lulz and Payback... We are Anonymous We are Legion We do not forgive We do not forget Expect Us."

57. Also on or about October 27, 2010, defendant DENNIS OWEN COLLINS, as "iowa," advised co-conspirators how to configure the LOIC tool, encouraged them to "steal your neighbors wireless," and provided a link to the LOIC tool to another member of the conspiracy.

58. On or about October 29, 2010, during a countdown to the planned DDoS cyber-attack on RIAA, defendant DENNIS OWEN COLLINS as "iowa" and other members of the conspiracy posted fliers advertising the upcoming planned attack on RIAA as part of OPERATION PAYBACK. One flier stated: "The Recording Industry Association of America, a private corporation, has crossed a line. In shutting down Limewire, they have exercised more control than any private entity should be allowed. Globally, these corporations are trying to censor the internet, a place without borders, a place where millions freely share ideas and information. If Limewire is gone today, what will we lose tomorrow?... When does this stop? Anonymous says it stops right now... Be against censorship. Be against private corporations having more rights than the average citizen. Be against the massive power of copyright labels. We must fight back. No more shall we wait. It is time for action. If they dare to take down Limewire, then we shall take down the RIAA in kind." Members of the conspiracy then launched a DDoS cyber-attack on RIAA.

59. On or October 31, 2010, members of the conspiracy launched a multi-day DDoS cyber-attack on the website of the U.S. Copyright Office of the Library of Congress located at www.copyright.gov. According to the website of the U.S. Copyright Office: "Copyright law is the engine of free expression in our society and a major building block of the U.S. economy. Our national system of copyright law, which the Office administers, plays an essential role in the creation, promotion, and dissemination of American works of authorship throughout the world, and sustains businesses large and small in the information, entertainment, and technology sectors. The Office's legal and policy functions help shape the future of copyright on a global scale, while the Office's copyright registration system provides an authoritative record of American creativity. The Office oversees statutory licensing programs for certain types of copyrighted works, and enriches the Library of Congress's collections by ensuring that authors provide copies of their works to the Library in connection with the Copyright Act's mandatory deposit provisions."

60. On or about November 1, 2010 and on or about November 3, 2010, defendants DENNIS OWEN COLLINS, as "iowa," and ROBERT AUDUBON WHITFIELD, as "mightymooch," participated in the DDoS cyber-attack on the website of the U.S. Copyright Office, in concert with their co-conspirators, by using the LOIC tool to flood the website of the U.S. Copyright Office with requests in an effort to make the website inoperable.

61. On or about November 3, 2010, a member of the conspiracy posted a flier advertising the DDoS cyber-attack on the website of the U.S. Copyright Office and directing participants to the LOIC tool, and members of the conspiracy launched the planned attack on the U.S. Copyright Office that day. As a result of this DDoS cyber-attack by ANONYMOUS, the U.S. Copyright Office suffered at least $5,000 in losses during a one-year period.

62. On or about November 4, 2010, during the attack on the U.S. Copyright Office, members of the conspiracy planned and launched a DDoS cyber-attack on Hadopi.

63. From on or about November 4, 2010 to on or about November 5, 2010, during the attack on Hadopi, members of the conspiracy planned and launched a DDoS cyber-attack on the Ireland National Federation against Copyright Theft ("INFACT").

64. On or about November 7, 2010, defendant DENNIS OWEN COLLINS, as "iowa," in #operationpayback stated that he had created a "recruit channel," posted a link to the LOIC tool, and provided explicit instructions to another member of the conspiracy as to the settings for the LOIC tool to allow one to join a DDoS cyber-attack.

65. Between on or about November 7, 2010 and on or about November 11, 2010, members of the conspiracy launched another DDoS cyber-attack on INFACT, while planning and launching a multi-day DDoS cyber-attack on the Irish Recorded Music Association ("IRMA").

66. On or about November 18, 2010, defendant DENNIS OWEN COLLINS, as "iowa," posted a message in #operationpayback suggesting that the conspiracy should target websites to "temporarily shut off income."

67. On or about November 19, 2010, the Pirate Party of both the UK and the USA posted an online letter to OPERATION PAYBACK. The letter called on ANONYMOUS to "immediately cease your Distributed Denial-of-Service (DDoS) attacks and to instead seek out a legal method to express your frustration . . . . By continuing Operation: Payback attacks, you will hamper those who promote copyright reform and curtailment of abuses of copyright, but who do so within the bounds of the law." The next day, members of ANONYMOUS posted a response letter signed OPERATION PAYBACK stating that "we refuse to halt our actions."

68. Between on or about November 23, 2010 and on or about November 24, 2010, members of the conspiracy planned and launched a DDoS cyber-attack on the website of The Fight Piracy Organization (fightpiracy.org) in Cyprus.

69. On or about November 26, 2010, members of the conspiracy launched a DDoS cyber-attack on the website of the International Federation of the Phonographic Industry (IFPI.org) in the United Kingdom, and defendant DENNIS OWEN COLLINS, as "iowa," identified the current target at IFPI.org. A flier advertising the IFPI.org attack directed participants to the LOIC tool, announced that "[t]he time has come to show these rich corporate IFPI bastards that the internet should always be an uncontrolled territory" and urged potential participants to "Get the F--- In Here."

70. On or about November 27, 2010, during the DDoS cyber-attack on IFPI.org, members of the conspiracy discussed launching a DDoS attack and other cyber-attacks on the website of the U.S. Immigration and Customs Enforcement ("ICE") located in the Eastern District of Virginia.

71. Between on or about November 27, 2010, and on or about November 28, 2010, during the multi-day DDoS cyber-attack on IFPI.org, members of the conspiracy planned and launched a multi-day attack on the website of Warner Brothers, an American movie studio.

72. On or about November 28, 2010, during the DDoS cyber-attacks on IFPI.org and Warner Brothers, a member of the conspiracy posted a link to a flier declaring "war on the US government" and encouraging DDoS attacks on websites including that of the Central Intelligence Agency ("CIA") in the Eastern District of Virginia.

73. Also on or about November 28, 2010, during the DDoS cyber-attacks on IFPI.org and Warner Brothers, members of the conspiracy, including defendant WADE CARL

WILLIAMS, as "TheMiNd," planned an attack on the website of a copyright compliance agent (copyright-compliance.com).

74. On or about November 29, 2010, during the DDoS cyber-attacks on IFPI.org and Warner Brothers, members of the conspiracy discussed targeting United States government websites for DDoS cyber-attacks, including the websites for The White House, the Central Intelligence Agency, the Internal Revenue Service, the Department of Justice, and the Federal Bureau of Investigation. In addition, members of OPERATION PAYBACK discussed moving domain registration overseas to avoid seizure by Immigration and Customs Enforcement (ICE).

75. On or about December 2, 2010, members of the conspiracy continued the ongoing DDoS cyber-attacks on IFPI.org and Warner Brothers.

76. On or about December 3, 2010, members of the OPERATION PAYBACK conspiracy discussed possible new targets related to WikiLeaks, the organization which had released U.S. State department confidential diplomatic cables in late November 2010. A draft statement by OPERATION PAYBACK stated in response to the question "what does [WikiLeaks] have to do with censorship and Operation Payback?" that ""While we don't have much of an affiliation with WikiLeaks, we fight for the same reasons. We want transparency and we counter censorship."

77. On or about December 4, 2010, members of the conspiracy in #operationpayback planned DDoS cyber-attacks on the websites of entities that were either critical of WikiLeaks or had refused to process payments for WikiLeaks, including Amazon and United States Senator Joseph Lieberman.

78. On or about December 6, 2010, members of the conspiracy in #operationpayback planned an attack on MasterCard and planned and launched a DDoS attack on PostFinance, a Swiss payments, e-finance, and electronic account management organization.

79. On or about December 7, 2010, during the DDoS cyber-attack on PostFinance, members of the conspiracy planned and launched DDoS cyber-attacks on the Swedish prosecutor's office; everydns.com; and Borgström and Bodström, a Swedish law firm; and planned DDoS cyber-attacks on the websites of the British court system and the Metropolitan Police in London, all in connection with arrest warrants for sexual crimes issued for the founder of WikiLeaks.

80. On or about December 8, 2010, members of the conspiracy launched a DDoS cyber-attack on the website of MasterCard. Defendants ANTHONY TADROS, as "Winslow," GEOFFREY KENNETH COMMANDER, as "bipto," PHILLIP GARRETT SIMPSON, as "jikbag," AUSTEN L. STAMM, as "user_x," TIMOTHY ROBERT McCLAIN, and THOMAS J. BELL participated in the DDoS cyber-attack on MasterCard, in concert with their co-conspirators, by using the LOIC tool to flood the website of MasterCard with requests in an effort to make the website inoperable.

81. Also on or about December 8, 2010, defendant WADE CARL WILLIAMS, as "TheMiNd," focused members of the conspiracy on the current target, stating that "we need to be hitting the companies who are subverting wikileaks in the pocketbooks IMO."

82. As a result of this DDoS cyber-attack by ANONYMOUS, MasterCard suffered at least $5,000 in losses during a one-year period.

83. Also on or about December 8, 2010, members of the conspiracy planned and launched DDoS cyber-attacks on websites of entities including Visa. In connection with these attacks, members of the conspiracy posted fliers captioned "Operation: Payback."

84. On or about December 9, 2010, a member of the conspiracy posted an online document which expressed and re-confirmed the manner and means and object of the conspiracy, while members of the conspiracy planned a DDoS cyber-attack on the website of Amazon.com. Various fliers advertising the DDoS cyber-attacks provided step-by-step instructions on how to use the LOIC tool to "DDoS like a Pro."

85. Also on or about December 9, 2010, members of the conspiracy planned and launched a DDoS cyber-attack on Moneybookers.com, an online payment service.

86. Also on or about December 9, 2010, defendant WADE CARL WILLIAMS, as "TheMiNd," stated that "take out internet transactions you hurt amazon, you hurt... visa, MC... you get the attention of everyone."

87. On or about December 10, 2010, after the DDoS cyber-attack on Moneybookers.com, a member of the conspiracy posted a link to an online document encouraging new participants to join OPERATION PAYBACK and to engage in DDoS cyber-attacks without getting caught. Advice included: "F------ MAGNETS won't DELETE F------ EVERYTHING unless they're exposed directly to the harddrive for a few minutes. Do not use the recycle bin to dump data!... Microwave works wonders on CDs, also on HDDs, pen drive and most electronics."

88. Also on or about December 10, 2010, members of the conspiracy launched a DDoS cyber-attack on the website of the Recording Industry of South Africa ("RISA").

89. On or about December 11, 2010, after the attack on RISA, members of the conspiracy launched another planned DDoS cyber-attack on the website of MasterCard.

90. On or about December 12, 2010, during the attack on MasterCard, members of the conspiracy on #operationpayback launched a DDoS cyber-attack on the website of Amazon.

91. On or about December 13, 2010, a member of the conspiracy posted a flier which warned members of the conspiracy about a planned "sweep of ARRESTS" and suggested that individuals "SECURELY DELETE YOUR LOGS (if you were stupid enough to keep any)."

92. On or about December 16, 2010, members of the conspiracy launched a DDoS cyber-attack on the website of Arbor Networks, a DDoS mitigation firm.

93. On or about December 18, 2010, members of the conspiracy planned and launched a multi-day DDoS cyber-attack on the websites of Bank of America.

94. On or about December 22, 2010, members of the conspiracy launched another DDoS cyber-attack on SGAE.

95. Also on or about December 22, 2010, during the attack on SGAE, a member of the conspiracy posted a link to online documents designed to recruit new members to the conspiracy.

96. On or about December 24, 2010, members of the conspiracy launched additional DDoS cyber-attacks on the websites of RIAA in the Eastern District of Virginia and MPAA. During the ongoing attacks on RIAA and MPAA, a member of the conspiracy posted a flier captioned "Operation: Payback," referenced the previous DDoS attacks on entities including MasterCard and Visa, and announced the ongoing attacks on RIAA and MPAA.

97. Between on or about December 25, 2010 and on or about December 27, 2010, during the attacks on RIAA and MPAA, members of the conspiracy continued to plan and then

launch a DDoS cyber-attack on Bank of America. Members of the conspiracy posted fliers captioned "Operation: Payback" which announced Bank of America as a target.

98. On or about December 27, 2010, following the attack on Bank of America, members of the conspiracy launched another DDoS cyber-attack on BREIN.

99. On or about December 29, 2010, in #operationpayback, defendant WADE CARL WILLIAMS, as "TheMiNd," posted a link to flier which identified the CEO of Bank of America and his wife by their names, home address, and phone number, for harassment.

100. On or about January 1, 2011, members of the conspiracy in #operationpayback discussed an FBI operation in which the FBI seized servers used in DDoS cyber-attacks.

(All in violation of Title 18, United States Code, Section 371.)

FORFEITURE NOTICE

Pursuant to Rule 32.2(a), each defendant is hereby notified that, if convicted of the offense alleged in Count One above, he shall forfeit to the United States, pursuant to18 U.S.C. §§ 982(a)(2)(B) and 1030(i), any property, real or personal, constituting or derived from any proceeds the defendants obtained directly or indirectly as a result of the offense, and all personal property that was used or intended to be used to commit or to facilitate the offense.

Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b) and 1030(i)(2), the defendant shall forfeit substitute property if, by any act or omission of the defendant, the property described above, or any portion thereof, cannot be located upon the exercise of due diligence; has been transferred, sold to, or deposited with a third party; has been placed beyond the jurisdiction of the Court; has been substantially diminished in value; or has been commingled with other property which cannot be divided without difficulty.

(In accordance with Title 18, United States Code, Sections 982 and 1030; and Rule 32.2(a), Federal Rules of Criminal Procedure.)

A TRUE BILL:

Pursuant to the E-Government Act, the original of this page has been filed under seal in the Clerk's Office.

Foreperson of the Grand Jury

DANA J. BOENTE
ACTING UNITED STATES ATTORNEY

Jay V. Prabhu
Alexander T.H. Nguyen
Assistant United States Attorneys

MYTHILI RAMAN
ACTING ASSISTANT ATTORNEY GENERAL
U.S. Department of Justice
Criminal Division

Richard D. Green
Trial Attorney, U.S. Department of Justice
Computer Crime & Intellectual Property Section