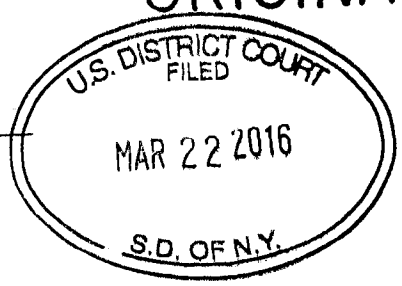
ORIGINAL



16 MAG 1906

Approved: _____
SIDHARDHA KAMARAJU / ANDREW K. CHAN
Assistant United States Attorneys

Before: HONORABLE SARAH NETBURN
United States Magistrate Judge
Southern District of New York

DOC #

UNITED STATES OF AMERICA - v. - DAVID W. KENT, Defendant.	**SEALED COMPLAINT** Violation of 18 U.S.C. §§ 371, 1343, and 2 COUNTY OF OFFENSE: NEW YORK

SOUTHERN DISTRICT OF NEW YORK, ss.:

EVELINA ASLANYAN, being duly sworn, deposes and says that she is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE
(Conspiracy)

1. From at least in or about October 2013, up to and including at least in or about February 2016, in the Southern District of New York and elsewhere, DAVID W. KENT, the defendant, and others known and unknown, willfully and knowingly, did combine, conspire, confederate, and agree together and with each other to commit offenses against the United States, to wit, violations of Title 18, United States Code, Sections 1030(a)(2)(C) and 1343.

2. It was a part and an object of the conspiracy that DAVID W. KENT, the defendant, and others known and unknown, intentionally would and did access a computer without authorization and exceed authorized access and thereby obtain information from a protected computer, which offense would be committed for purposes of commercial advantage and private financial gain, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B).

3. It was further a part and an object of the conspiracy that DAVID W. KENT, the defendant, and others known and unknown, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343.

OVERT ACTS

4. In furtherance of said conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed, in the Southern District of New York and elsewhere:

a. On or about February 6, 2014, DAVID W. KENT, the defendant, accessed client information from the database of a website ("Website-1") owned by a company ("Company-1") without authorization.

b. On or about April 4, 2014, KENT caused an unsolicited email solicitation to be sent to a member of Website-1 who appears to reside in the Southern District of New York.

c. On or about January 20, 2015, a co-conspirator not named herein ("CC-1") accessed information from a Google Analytics account owned by Company-1 without authorization. CC-1 then emailed the information to KENT.

d. On or about December 8, 2015, KENT joined a conference call with representatives of Company-1 and attempted to persuade Company-1 to acquire a website owned by KENT.

e. On or about December 11, 2015, KENT attempted to access client information from the database of a website owned by Company-1 without authorization.

f. On or about January 20, 2016, KENT met with representatives of Company-1 in the Southern District of New York and attempted to persuade Company-1 to acquire a website owned by KENT.

(Title 18, United States Code, Section 371.)

COUNT TWO
(Wire Fraud)

5. From at least in or about October 2013, up to and including at least in or about February 2016, in the Southern District of New York and elsewhere, DAVID W. KENT, the defendant, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme and artifice, to wit, KENT sent emails and phone calls to Company-1 to persuade Company-1 to invest in or acquire a website, the membership of which was increased after KENT illegally accessed client information from the database of a website owned by Company-1.

(Title 18, United States Code, Sections 1343 and 2.)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

6. I have been a Special Agent with the FBI for approximately four years. I am currently assigned to a squad responsible for investigating computer network intrusions. I have participated in investigations of such offenses, and have made and participated in arrests of individuals who have committed such offenses.

7. The information contained in this Complaint is based upon my personal knowledge, as well as information obtained during this investigation, directly or indirectly, from other sources, including, but not limited to: (a) business records and other documents, including records of electronic communications; (b) publicly available documents; (c) conversations with, and reports of interviews with, law enforcement and non-law-enforcement witnesses; (d) conversations with, and reports prepared by, other FBI agents; (e) documents provided by

employees of Company-1. Because this Complaint is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions and statements of and conversations with others are reported herein, they are reported in substance and in part. Where figures, calculations, and dates are set forth herein, they are approximate, unless stated otherwise.

Summary of the Scheme to Defraud

8. As set forth below, there is probable cause to believe that DAVID W. KENT, the defendant, agreed with CC-1 and others to access information belonging to Website-1 without authorization and to defraud Company-1. KENT accessed a database maintained by Website-1 without authorization and stole customer information, including information from over 500,000 unique resumes. KENT then exploited this information by inviting many of Website-1's members to join a new website he had created called Oilpro.com ("Oilpro"). Similarly, CC-1 accessed information in Website-1's Google Analytics account without authorization and forwarded the information to KENT. In the meantime, KENT attempted to defraud Company-1 by misrepresenting that his new website had increased in membership through standard marketing methods. In furtherance of this scheme, KENT caused emails and telephone calls to be sent to the CEO of Company-1.

Background

9. Several Internet-based businesses operate websites that provide professional networking services. These websites typically allow employees, employers, and recruiters to create online profiles that contain personal and professional information. Depending on their privacy settings, users can then view each other's profiles, connect with colleagues, or try to establish new professional contacts.

10. Professional networking websites also frequently offer job-placement services for job-seekers, recruiters, and employers. Professional networking websites allow job-seekers to upload their resumes as part of their user profiles, which can be used to apply for job openings posted by recruiters and employers. Similarly, recruiters and employers—who also usually create their own profiles—can also solicit employees directly for job opportunities. For these reasons, the size of the website's user database—and especially the number of resumes and

jobs in the database—can make the website more attractive to job-seekers, recruiters, and employers.

11. Professional networking websites can generate revenue by selling advertising space on their website. The desirability and pricing of such space is driven, in part, by the number of users who visit the website and the number of page views by users. Thus, professional network websites attempt to generate increased web traffic by encouraging users to create online profiles and visit the website on a regular basis. Websites will also solicit membership through emails directed at potential users.

12. Professional networking websites can also generate revenue by offering premium accounts for a fee that allow additional services or functionality. For example, some professional networking websites will offer premium accounts to recruiters or employers, allowing them to post potential job opportunities or access the user database. Just as with advertising revenue, the size of a website's user database can have an impact on the revenues from premium accounts.

13. At all times relevant to this Complaint, Company-1 was a publicly-traded company in the online professional networking industry headquartered in New York, New York.

14. In or about March 2000, DAVID W. KENT, the defendant, launched Website-1. Website-1 provides, among other things, networking services to professionals working in the oil and gas industry. Website-1 allows its members to create profiles, which includes personal and professional information. As part of their profiles, members can also upload their resumes, which are assigned unique numerical identifiers ("Resume ID numbers"). The profiles are contained in a database maintained by Website-1 (the "Members Database"). Members are assigned login credentials (i.e. usernames and passwords) when they create their profiles. Members use these login credentials to access their profiles.

15. Recruiting agencies and employers pay Website-1 for access to the Members Database, which allows them to solicit job-seekers for available positions. Website-1 also derives revenue from selling advertising space on its website.

16. In or around August 2010, Company-1 acquired Website-1 from DAVID W. KENT, the defendant, for approximately $51 million. Company-1 retained an accounting firm to conduct an analysis of the value of Website-1's assets. According to this

analysis, the Members Database was worth approximately $6 million at that time.

17. On or about August 9, 2010, DAVID W. KENT, the defendant, entered into an employment agreement with Company-1 (the "Employment Agreement"), agreeing to continue to serve as President of Website-1 after the acquisition. As part of the Employment Agreement, KENT agreed to not participate in any business that competes with Website-1 while employed by Company-1. KENT also agreed to refrain from competing with Company-1 if he left Company-1, until the expiration of the latter of three years after the signing of the Employment Agreement, or two years after leaving the employ of Company-1 (the "Non-Compete Period").

18. In or around September 2011, DAVID W. KENT, the defendant, left Website-1. In or around October 2013, shortly after the earliest possible expiration of the Non-Compete Period, DAVID W. KENT, the defendant, announced that he had founded Oilpro.com ("Oilpro"), which also provides networking services to professionals working in the oil and gas industry. Oilpro is headquartered in Houston, Texas.

19. CC-1 is an employee at Oilpro who previously worked for Website-1. KENT has stated that the Oilpro employees own approximately 15 percent of the Oilpro business. For this reason, CC-1 stands to financially benefit from Oilpro's success.

20. Like other professional networking websites, the financial success of Oilpro depended in part on the number of users and resumes in the Oilpro database. On or about April 1, 2015, CC-1 emailed DAVID W. KENT, the defendant, and other Oilpro employees a document entitled "Operation Resume Hoard - Part 1" (the "Resume Hoard Document"). The Resume Hoard Document stated: "Objective: Increase number of searchable resumes in the back end for recruiters and build the [Oilpro database] . . . Goals/Outcomes: Add 100,000 resumes to the [Oilpro database] and Convert 40,000 new members over the 9 months."

21. On or about April 24, 2014, DAVID W. KENT, the defendant, wrote to the CEO of Company-1 and stated: "My original mission was to build something that [Company-1] would be interested in acquiring. It seemed to work for all parties before."

22. By January 2016, the Oilpro database had grown to at least 500,000 members. In communications with the CEO of Company-1, DAVID W. KENT, the defendant, attributed the growth of the Oilpro database to emailing invitations to contacts of Oilpro members, traditional marketing methods, and "network effects."

The First Round of Hacks

23. Based upon my review of documents and records maintained by Company-1, conversations with representatives of Company-1, my review of other records, and my review of publicly available information, I have learned in part the following:

a. On or about February 26, 2014, an individual who had created a member profile with Website-1 ("Member-1") contacted Website-1's customer support line. Member-1 stated, in sum and substance, that Member-1 had received an email solicitation from Oilpro to use Oilpro's services even though Member-1 had never provided any information in the past to Oilpro.

b. An internal review of Website-1's computer systems revealed no evidence that any employee of Oilpro had viewed Member-1's profile using an account created through Website-1.

c. To determine if the Members Database was being accessed improperly, employees of Company-1 created two fictitious member accounts and populated them with names and email addresses that were only available through Website-1's Members Database.

d. On or about April 14, 2014, the email accounts associated with the fictitious member accounts each received email communications from an employee at Oilpro ("Employee-1"). The communications solicited the fictitious members to create profiles on Oilpro. An internal review of Website-1's systems revealed no records of Employee-1 viewing the fictitious member accounts on Website-1. Further, there was no record that any single user of Website-1 had accessed both of the fictitious member accounts.

e. A review of Website-1's computer systems showed that, between on or about October 17, 2013 and on or about April 15, 2014, approximately 100,000 suspicious hypertext transport protocol ("HTTP") requests were made to Website-1's Members

Database over the Internet (the "First Round of Hacks"). An HTTP request is a computer code command transmitted to a website over the Internet. Based on my experience and training, the speed with which the HTTP requests related to the First Round of Hacks were submitted suggests very strongly that they were sent using an automated computer program, rather than using manual submissions.

f. The HTTP requests related to the First Round of Hacks contained a computer command that directed the Website-1 Members Database to give the user access to specific resumes (the "Get Resume Command"). The Get Resume Command was crafted to exploit a piece of source code unique to Website-1 known only to a few individuals, including DAVID W. KENT, the defendant.

g. In total, the First Round of Hacks involved the unauthorized access of information from approximately 96,000 resumes belonging to members of Website-1, at least several of whom appear to reside in the Southern District of New York.

h. Following the First Round of Hacks, web traffic to Oilpro increased dramatically, and appears to correlate with the severity of the intrusions into the Website-1 Members Database. Additionally, thousands of Website-1 members affected by the First Round of Hacks created profiles on Oilpro.

The Second Round of Hacks

24. Based upon my review of documents and records maintained by Company-1, conversations with representatives of Company-1, my review of other records, and my review of publicly available information, I have learned in part the following:

a. On or about July 20, 2015, an employee for Company-1 who began-but did not complete-the process of creating a member profile with Website-1 ("Member-2") reported receiving an email solicitation from Oilpro. Because the profile was incomplete, Member-2's information was never published in the Website-1 Members Database.

b. A review of Website-1's computer systems showed that, between on or about June 17, 2015 and on or about August 2, 2015, approximately 750,000 suspicious HTTP requests were made to the Website-1 Members Database over the Internet (the "Second Round of Hacks"). Based on my experience and training, the speed with which the HTTP requests related to the Second Hack were submitted suggests very strongly that they were sent

using an automated computer program, rather than using manual submissions.

c. Unlike the First Round of Hacks, the Second Round of Hacks exploited a file on Website-1 called resume_writer.asp. Only a person with intimate knowledge of how resume_writer.asp works and how Website-1 catalogued each resume in the Website-1 Members Database would be able to submit the appropriate commands to extract such a large quantity of resumes in such a short period of time.

d. In total, the Second Round of Hacks involved the unauthorized access of information from approximately 700,000 resumes belonging to members of Website-1, at least several of whom appear to reside in the Southern District of New York.

Evidence Linking the Scheme to KENT and CC-1

25. Based upon my review of documents and records maintained by Company-1, conversations with representatives of Company-1, my review of other records, my review of records obtained in response to search warrants, and my review of publicly available information, I have learned in part the following:

a. Each of the HTTP Requests related to the First Round of Hacks and Second Round of Hacks was submitted to Website-1 using a computer that was associated with an Internet Protocol address ("IP address"). The same IP address, however, was not used to submit all of the HTTP requests. Rather, approximately 23 different IP addresses were involved in submitting the approximately 100,000 HTTP Requests related to the First Round of Hacks. An additional 10 different IP addresses were involved in submitting the approximately 750,000 HTTP requests related to the Second Round of Hacks.[1] In my training and experience, it is common for individuals engaged in computer or wire fraud to switch between IP addresses to try to avoid detection by law enforcement.

b. Of the approximately 23 IP addresses relating to the First Round of Hacks, approximately 22 were registered to a company based in the United Kingdom that provides services to obscure a user's true originating IP address ("Company-2").

[1] 660,323 HTTP requests were submitted by IP addresses beginning with the numbers 104.128.21.XXX. I am counting this as one unique IP address.

Similarly, of the 10 different IP addresses relating to the Second Round of Hacks, at least two of them were also registered to Company-2 (collectively, the "Masked IP Addresses").

c. On or about February 6, 2014, February 7, 2014, April 3, 2014, and April 15, 2014, certain of the Masked IP Addresses were used to log into a social media website account registered to DAVID W. KENT, the defendant. On those same days, the Masked IP Addresses were also used to submit unauthorized HTTP Requests to Website-1.

d. An email address associated with KENT was used to register and pay for an account with Company-2. Around the time of the First Round of Hacks, KENT received emails from Company-2 regarding his username and password.

e. Among the IP addresses relating to the First Round of Hacks, at least one IP address ("IP Address-1") was not registered to Company-2. Among the IP addresses relating to the Second Round of Hacks, at least one IP address ("IP Address-2") was not registered to Company-2. Instead, IP Address-1 and IP Address-2 were registered to SIOPCO, an Internet-based business that was also co-founded by KENT in or about April 2012.

f. Between the First Round of Hacks and the Second Round of Hacks, approximately 796,000 accounts in the Website-1 Members Database were accessed without authorization (the "Hacked Website-1 Accounts"). The Hacked Website-1 Accounts contained approximately 586,560 unique email addresses (the "Hacked Website-1 Email Addresses"). As of January 2016, approximately 17.7 percent of the Hacked Website-1 Email Addresses received email invitations to join Oilpro after the accounts were accessed without authorization. Approximately 35.7 percent of the Hacked Website-1 Email Addresses who received email invitations eventually joined Oilpro. In total, over 111,000 of the Hacked Website-1 Accounts have joined Oilpro.

g. Between on or about April 4, 2014 and on or about April 6, 2014, approximately 13,000 accounts in the Website-1 Members Database were accessed (the "April Hacked Website-1 Accounts"). On or about April 14, 2014, almost all of the April Hacked Website-1 Accounts received email invitations to join Oilpro.

h. On or about April 24, 2014—shortly after the completion of the First Round of Hacks—KENT contacted the CEO of Company-1 via email. In sum and substance, KENT stated that

Oilpro had received an unsolicited offer for investment. KENT also stated that his original mission with Oilpro was to build something that Company-1 would be interested in acquiring. This email was received by the CEO of Company-1 in the Southern District of New York.

i. On or about June 11, 2015—shortly before the beginning of the Second Round of Hacks—KENT contacted CC-1 with a link to the resume of an individual claiming to be a "freelancer for web scraping / crawling / automated data extraction solutions." KENT stated to CC-1: "We should hire him and ask him if he can scrape job boards including resume databases . . . He might find backdoors, etc." CC-1 responded to KENT: "Might be worth a conversation at the least. But yea, if he can find a backdoor to full CVs... boom." Based on my participation in this investigation, I believe that "web scraping" and "crawling" refers to automated programs that extract large amounts of data from websites.

j. On or about October 25, 2015—shortly after the completion of the Second Round of Hacks—KENT contacted the CEO of Company-1 via email. In sum and substance, KENT stated that Oilpro had taken on an investor the previous year. KENT further stated that there were few better fits for the software platform of Oilpro than Website-1.

The Google Analytics Hack

26. Based on my conversations with representatives of Company-1, my review of records obtained from Company-1, my review of other records, and my personal participation in this investigation, I know in part that:

a. Google Analytics is a service used by websites to collect data on a variety of statistics relating to user engagement, including: (1) number of visits to the website; (2) number of new users; (3) pages viewed per visit; and (4) average duration of each visit. Every Google Analytics account is password-protected, including the Google Analytics accounts associated with Website-1.

b. On or about January 20, 2015, DAVID W. KENT, the defendant, contacted CC-1 via email and provided a link to Google Analytics data relating to Oilpro. KENT wrote to CC-1: "How do this compare to our friends site...." CC-1 replied to KENT via email and provided a link to data relating to a different website (the "January 2015 Data").

c. Based on the formatting of the January 2015 Data and conversations with representatives of Company-1, I know that: (i) the January 2015 Data came from a password-protected Google Analytics account associated with Website-1; and (ii) CC-1 did not have authority to access any password-protected Google Analytics account associated with Website-1 any time after CC-1 left Company-1 on or about November 27, 2013.

d. On or about January 21, 2015, KENT replied to CC-1 and stated: "Very interesting . . . Can we identify the paths on the website that are leading to high [page views]/Session for them? Then we can look at our own and identify our deficiency." CC-1 replied to KENT via email and stated: "Yeah sort of. Their page path's are a bit harder to follow due to the various links, but we can determine the landing pages, second pages etc. and come to an educated guess. FYI we hit 345,000 [page views] yesterday, they got 409k. Pretty close." Based on my conversations with representatives of Company-1, I know that Website-1 had approximately 409,000 page views on January 20, 2015. Based on my participation in this investigation, I believe that KENT asked CC-1 to determine which pages on Website-1 receive high web traffic. CC-1 then responds that it is possible to make an "educated guess" about which pages on Website-1 are popular. CC-1 then provides non-public information about the number of page views on January 20, 2015 for Website-1 and Oilpro.

e. On or about June 10, 2015, CC-1 contacted KENT via email and provided two links to data relating to a website (the "June 2015 Data"). CC-1 wrote to KENT: "So, I'm trying to scratch the engagement on Rusty[2] a bit and noticed that the folks searching their jobs are 75% return users regardless of the source." KENT replied to CC-1 via email and stated: "So... we don't have enough jobs... and our job search sucks. Solution 1. Get Hannah scraping full-time until we have equal if not more jobs posted per day than Rusty." Later that day, KENT contacted CC-1 via email and stated: "Why don't we just hire someone to post all the Rusty jobs? Brute force?" Based on my participation in this investigation, I believe that CC-1 informed KENT that 75 percent of the users looking for jobs on

[2] On or about December 8, 2014, KENT wrote an email to several employees of Oilpro and stated: "Rusty = [Website-1]. Much easier to say and conveys [Oilpro] is the new, non-rusty solution to all of your oil & gas data needs. Also protects my feelings because at one point, that was a product I loved... it has just gotten a bit rusty."

Website-1 were users who previously had visited Website-1. This information was not publicly available. KENT responds that Oilpro's website does not have enough jobs and Oilpro's tools for searching for jobs "sucks." KENT proposes to have an Oilpro employee engage in "scraping" for jobs on other websites. KENT later suggests that Oilpro hire an employee to re-post all of the jobs on Website-1 onto Oilpro.

f. Based on the formatting of the June 2015 Data and conversations with representatives of Company-1, I know that: (i) the June 2015 Data came from a password-protected Google Analytics account associated with Website-1; and (ii) CC-1 did not have authority to access any password-protected Google Analytics account associated with Website-1 any time after CC-1 left Company-1 on or about November 27, 2013.

Kent's Sales Pitch to Company-1 and the Attempted Third Hack

27. Based on my conversations with representatives of Company-1, my review of records obtained from Company-1, my review of other records, and my personal participation in this investigation, I know in part that:

a. On or about October 28, 2015, DAVID W. KENT, the defendant, contacted the CEO of Company-1 via email. Relating to the membership of Oilpro, KENT stated: "Our membership has grown to 540,000 members . . . I believed the LinkedIn style growth hacks we applied to [Oilpro] can work in any other market as well. These so-called growth hacks require a social network to be effective." Based on my involvement in this investigation and as further described in subparagraphs b, c, e, and i of this paragraph, I believe that "LinkedIn style growth hacks" refer to asking Oilpro members to upload their contacts from LinkedIn.com ("LinkedIn"), another professional networking website, into the Oilpro database. All of these contacts from LinkedIn are then invited to join Oilpro, and the process repeats itself. However, KENT did not mention the First Round of Hacks or Second Round of Hacks in this communication.

b. On or about November 5, 2015, KENT contacted the CEO of Company-1 via email. In response to questions from the CEO of Company-1 regarding the growth of Oilpro's membership, Kent stated: "We have consistently generated between 20,000 and 50,000 new members per month. The buildup is lumpy just depending on the marketing strategy in place during a given month . . . For the first three months, our contacts downloaded LinkedIn contacts for invites to [Oilpro]. This sparked the membership growth and the network effect . . . I don't think our

growth was dependent on our existing relationships . . . With the contacts that [Company-1] has, we could grow faster than [Oilpro] . . . We did not do anything unique to [Oil & Gas] to achieve our growth. We have a half dozen strategies that work well and are repeatable." Based on my involvement in this investigation, I believe that KENT is reiterating that Oilpro's primary marketing strategy is inviting Oilpro members to upload their contacts from LinkedIn. KENT also denies that the growth of Oilpro can be attributable to existing relationships in the oil and gas industry. KENT further states that Oilpro uses marketing strategies that are repeatable in other industries. However, KENT fails to mention the First Round of Hacks or the Second Round of Hacks.

c. On or about November 11, 2015, KENT contacted the CEO of Company-1 via email. In response to a question from the CEO of Company-1 regarding the growth of Oilpro's membership and marketing approaches used, KENT stated: "From a membership development front, we have several marketing tactics. LinkedIn is one of them but we also use traditional marketing methods such as Indeed[3] (if you can call Indeed traditional). Of late, we have pulled back on ad spend which caused the lumpiness." Based on my involvement in this investigation, I believe that KENT is reiterating that one of Oilpro's marketing strategies was inviting Oilpro members to upload their contacts from LinkedIn. KENT also may be referring to posting advertisements on another website, Indeed.com. However, KENT fails to mention the First Round of Hacks or the Second Round of Hacks.

d. On or about November 25, 2015, KENT contacted the CEO of Company-1 via email. In response to a question from the CEO of Company-1 regarding a valuation expectation for an acquisition of Oilpro, KENT replied: "Last year, we took on [an energy venture capital firm] as an investor. They invested $3MM at a $20MM valuation." Based on my involvement in this investigation, I believe that KENT is telling Company-1 that Oilpro was worth $20 million in 2014. As a result, KENT is implying that Company-1 would need to offer at least $20 million—if not more—to purchase Oilpro.

e. On or about December 8, 2015, the CEO, CFO, and General Counsel for Company-1 had a conference call (the "Conference Call") with KENT to further discuss KENT's proposal

[3] Based on publicly available information, I know that Indeed.com is a website where job-seekers and employers can search for and post resumes and job opportunities.

to sell Oilpro to Company-1. During the Conference Call, KENT stated that the "number one" strategy for growing the membership of Oilpro was asking recruiters and other contacts to upload their LinkedIn contacts to Oilpro. Oilpro then invited these contacts to join Oilpro. KENT also attributed the growth of Oilpro to "effort" and the fact that oil and gas is a "safe haven industry." At the end of the Conference Call, the CEO of Company-1 expressed interest in scheduling a follow-up conversation to further discuss the practical details of a potential merger or acquisition. KENT responded that he would "prefer" to have a transaction with Company-1 rather than any other potential investors. KENT did not mention the First Round of Hacks or the Second Round of Hacks during the Conference Call.

f. A review of Website-1's computer systems showed that, on or about December 11, 2015, at least five suspicious HTTP requests were made to access Website-1's Members Database over the Internet (the "Attempted Third Hack"). Like the Second Hack, the HTTP requests were made to Website-1's Members Database using the resume_writer.asp file. The Attempted Third Hack sought to extract the next Resume ID Number in the Members Database following the last resume that had already been extracted during the Second Round of Hacks. Because the resume_writer.asp file had been modified after the Second Round of Hacks, however, the Attempted Third Hack did not result in the extraction of any real resumes from the Members Database.

g. At least one of the IP addresses used to access the Members Database during the Attempted Third Hack ("IP Address-3") was registered to Company-2. At the time of the Attempted Third Hack, IP Address-3 was assigned to the Company-2 account associated with KENT. At the time of the Attempted Third Hack, the Company-2 account associated with KENT was accessed by an IP Address that was assigned to SIOPCO.

h. On or about December 13, 2015—two days after the Attempted Third Hack—the Company-2 account associated with KENT was accessed by an IP address that was assigned to KENT's home in Spring, Texas.

i. On or about January 20, 2016, KENT traveled to Manhattan for a meeting to discuss a potential acquisition of Oilpro by Company-1 (the "January Meeting"). In describing the dramatic growth of Oilpro, KENT stated that the "main mission" for Oilpro employees at the outset was calling friends and asking them to upload their contacts from LinkedIn. Oilpro would then send emails to these LinkedIn contacts, invite them

to join Oilpro, and then invite them to upload their contacts from LinkedIn. KENT stated that this "network effects" strategy was the "core way" and "enough" to grow Oilpro to over 500,000 members in a short period of time. KENT later stated that Oilpro had the "ability" to increase its membership growth in any given month by putting "effort" into rolling out new features for Oilpro. KENT did not mention the First Round of Hacks, the Second Round of Hacks, or the Attempted Third Hack during the January Meeting.

j. On or about January 27, 2016, KENT emailed a spreadsheet to the CEO of Company-1 with figures and charts describing the growth in membership and number of resumes in the Oilpro members database (the "Spreadsheet"). According to the Spreadsheet:

i. Oilpro gained approximately 3,085 new members in December 2013 and approximately 4,486 new members in January 2014. Oilpro then gained approximately 12,131 new members in February 2014. As mentioned above in subparagraph a of paragraph 23, Member-1 reported receiving an email solicitation to join Oilpro on or about February 26, 2014.

ii. Oilpro gained approximately 28,763 new members in April 2014. As mentioned above in subparagraph d of paragraph 23, the fictitious member accounts in Website-1 received email solicitations to join Oilpro on or about April 14, 2014.

iii. Oilpro gained approximately 45,936 new members in June 2014, which was shortly after the First Round of Hacks was completed. KENT attributes the membership growth in June 2014 to a "Recruiter Directory" and "'Most Jobs' + Indeed Campaign."

iv. Oilpro gained approximately 45,823 new members in September 2015, which was shortly after the Second Round of Hacks was completed. KENT attributes the membership growth in September 2015 to a "LinkedIn Campaign."

v. KENT did not mention the First Round of Hacks, the Second Round of Hacks, or the Attempted Third Hack in the Spreadsheet.

WHEREFORE, I respectfully request that an arrest warrant be issued for DAVID W. KENT, the defendant, and that he be arrested and imprisoned or bailed, as the case may be.

EVELINA ASLANYAN
Special Agent
Federal Bureau of Investigation

Sworn to before me this
23rd day of March 2016

HONORABLE SARAH NETBURN
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK