

United States District Court

for the
Western District of New York

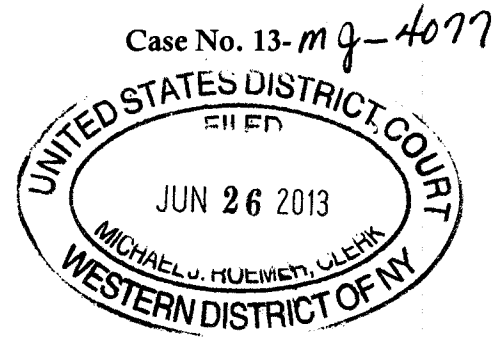
United States of America

v.

Annette Kendrick

Defendant

CRIMINAL COMPLAINT



I, S.A. BARRY W. COUCH, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of April 11, 2013, in the County of Monroe, in the Western District of New York, the defendant violated Title 18, United States Code, Section 1030(a)(5)(A), offenses described as follows:

I respectfully submit that there is probable cause to believe that Annette Kendrick did knowingly transmit a program, information, code, or command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A).

This Criminal Complaint is based on these facts:

Continued on the attached sheet.

Complainant's signature

**BARRY W. COUCH, Special Agent
Federal Bureau of Investigation**

Printed name and title

Sworn to before me and signed in my presence.

Date: June 26 2013

Judge's signature

City and State: Rochester, New York

**HON. MARIAN W. PAYSON
U.S. MAGISTRATE JUDGE**

Printed name and title

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

STATE OF NEW YORK)
COUNTY OF MONROE) ss:
CITY OF ROCHESTER)

13-mj-4077

I, Barry W. Couch, having been first duly sworn, do hereby depose and state as follows:

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI). I have been so employed since November 2008. I am currently assigned to investigations involving computer intrusions, as well as other criminal investigations. As part of my duties as an FBI Special Agent, I investigate crimes related to activity with computers in violation of Title 18, United States Code, Section 1030.

2. This affidavit is submitted for the limited purpose of establishing probable cause to believe that Annette Kendrick, born June 28, 1973, knowingly caused 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, in violation of Title 18, United States Code, Section 1030(a)(5).

3. The statements contained in this affidavit are based on my own personal knowledge and observation, my training and experience, and conversations with other law enforcement officers and witnesses. Because this affidavit is being submitted for the limited purpose of securing a criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause that Annette Kendrick did knowingly violate Title 18, United States Code, Section 1030(a)(5).

4. On April 11, 2013, employees of Iberdrola, a company headquartered in Rochester, New York, reported to me that Iberdrola was the victim of a computer intrusion. On April 4, 2013, someone with valid Iberdrola credentials logged into Iberdrola's computerized job application system, modified a job posting, modified questions on the posting, sent e-mails to agencies about the posting, and sent e-mails to job applicants saying they were no longer being considered for the position. Iberdrola worked with AT&T Forensics and was able to determine that the computer logs showed that the intrusive activity resolved back to an IP address that was assigned to the company, Sutter Health, in Sacramento, California.

5. Iberdrola was of the opinion that the person most likely responsible for the intrusion was Annette Kendrick, a former Iberdrola employee, who had been terminated from her position with Iberdrola. Kendrick had had access to the login id and password of a computer administrator at Iberdrola. Also, the job posting that was defaced and modified was for the Director of Talent and Diversity Inclusion, Kendrick's former position. Out of hundreds of job postings, it was the only one defaced. Iberdrola also believed that Kendrick had been working for a consulting company in Georgia that was being employed by Sutter Health.

6. On April 23, 2013, Iberdrola provided me with documentation that included copies of the job posting referred to in Paragraphs 4 and 5 above prior to the intrusion and after the intrusion and modification. The defaced posting read: "If you are searching for an INNOVATIVE, LONG STANDING, ENVIRONMENTALLY RESPONSIBLE organization to work for . . . GO FUCK YOURSELF! Iberdrola USA Management Corporation (IUMC) an affiliate of Iberdrola S.A. which is the LARGEST RENEWABLE ENERGY COMPANY and one of the top 5 largest energy companies in the world currently has a Director - Talent Management, Diversity & Inclusion opportunity at its Rochester, NY location 'WHICH WILL TOTALLY FUCK YOU IN EVERY ASPECT OF YOUR JOB.' "

7. Iberdrola representatives have advised that they are concerned about the intrusion into the company's computer domain, because the perpetrator would have had access to the personal identifiers for company employees. The Iberdrola computer domain is used to interact with employees and customers of the company in the normal course of its interstate and foreign commerce. As a direct result of the intrusion, Iberdrola chose to notify those individuals whose personal information could have been accessed, as well as credit protection for a year. Iberdrola has estimated the cost of the credit protection and the employment of AT&T Forensics to be between \$200,000 and \$250,000.

8. On June 3, 2013, the company Accenture provided documentation that showed that on April 4, 2013, Annette Kendrick was an employee of Accenture, assigned to a project with Sutter Health in Sacramento, California.

9. On June 7, 2013, the FBI conducted a non-custodial interview with Annette Kendrick in Atlanta, Georgia, at the airport. Kendrick was arriving from Sacramento, California, on a work trip which she stated she routinely takes as her client, Sutter Health, is located in California. Kendrick said she worked currently for Accenture, and prior to that, she worked as the Director of Talent

Management and Diversity at Iberdrola. Kendrick stated that she was given a severance package from Iberdrola due to problems Kendrick had with her Vice President of Human Resources at Iberdrola. Kendrick was advised that the nature of the interview was in reference to a computer intrusion into a computer at Iberdrola. Kendrick then stated she knew that this was most likely in reference to her accessing the Applicant Tracking System (ATS) at Iberdrola. Kendrick said that she developed the ATS system as part of her job duties with Iberdrola. Kendrick said that she utilized the account and password belonging to another Iberdrola employee in order to access the system. Kendrick said she knew the password for the employee because she (Kendrick) created the account for the employee.

10. Kendrick stated that she accessed Iberdrola's computer system approximately two to three months prior from Sutter Health in California while utilizing her Accenture laptop computer. Kendrick was shown a copy of the modified job posting referenced in Paragraph 6 above. Kendrick initially denied any knowledge of the posting being modified by her. She admitted to dropping the job posting and described that as "deleting" it, but did not upload a new job posting in its place. Kendrick stated that you can't just "edit," but you would have to drop and re-add the posting. Upon further questioning, Kendrick recalled writing something similar to

the job posting a long time ago with the intent of possibly sending it to her Iberdrola Vice President, but did not believe she ever sent it. Kendrick then stated that she did not recall uploading a new job posting, but stated that it was possible saying: "Let's say yes."; and: "I may have hit a button". She recalled deleting the posting by hitting an "erase" button and stated she thought she put up a blank posting in its place.

11. Kendrick was then asked the direct question: "Did you cause this to be uploaded?" (referring to the modified job posting), to which Kendrick responded: "Yes.", stating she did not recall how, then adding: "I did it. I admit it. I did it." Kendrick then stated that she used her Accenture computer and Sutter Health's wireless internet in California, to access Iberdrola's computer system, to then modify the job posting. Kendrick stated that she came across the job posting for her former job out of chance, and that it could have caused bad emotions which led her to make the decision to delete and upload the revised job posting. Kendrick offered to look on her Accenture laptop, which she had with her during the interview, to see if she had the modified posting saved. Upon a simple search using the Windows search function within the folder "My Documents", Kendrick was able to pull up a Word document located in her My Documents folder which matched the text posted as the defaced job

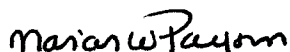
posting to the Iberdrola website.

Based upon the foregoing, your affiant respectfully submits that there is probable cause to believe that Annette Kendrick has violated 18 U.S.C. § 1030(a)(5)(A), which prohibits a person from knowingly transmitting a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization, to a protected computer.



BARRY W. COUCH
Special Agent
Federal Bureau of Investigation

Sworn to before me this
26th day of June 2013.



Hon. Marian W. Payson
United States Magistrate Judge