

- **Date:** Oct. 25, 2007 - The date of the first document.
- **Case url:** <https://www.courtlistener.com/docket/4208343/united-states-v-yahoo-inc-701-first-avenue-sunnyvale-california/>
- **Case title:** United States v. YAHOO!, INC. 701 FIRST AVENUE SUNNYVALE, CALIFORNIA
- **Crime:** This case basically involves a cyber-crime. A technique named as 'phishing' - The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers (source - google) is used in this case. Some websites and a couple of free web based internet e-mail access that is provided to the public from Yahoo! have been used by the culprits.
- **Investigation:** During March 2007, the Romanian national police (RNP) encountered at the webpage that was spoofed. The webpage was of a Romanian Bank named as BRD bank. The bank's original webpage was <http://www.brd.ro> whereas the spoofed webpage was created at <http://www.brdro.net> created by the culprits. The phishing web page had no legitimate affiliation with BRD bank and the webpage was hosted by Yahoo!. Soon the police found more webpages like this which spoofed BRD bank. All the web-names that were used to spoof the BRD bank webpage were quite similar to the original web-name of the BRD bank. Plenty of spam e-mails were sent to the people saying that something was wrong with their account. To correct it, they had to click on a link provided on the e-mail. And when they used to click on the link provide on the e-mail it would redirect them to a particular web-name that was spoofed.

After all these things happened RNP and FBI contacted Yahoo! and notified about these things. They even asked Yahoo to shut down those websites that were created by the culprits. Then they requested Yahoo! to preserve the existing records on the websites that were used for spoofing and also the related e-mail accounts used in this case. After clear observation, Yahoo! records showed that the web domain accounts used to login were accessed by multiple Romanian internet service providers and with AOL IP address whose location was at the united states. Many of the web domain accounts used for phishing were created by a user who logged into a computer that was the property of a company in Bennington, Vermont. After the FBI people communicated with the company, FBI was allowed to investigate legally in the company's servers to check if some sort of malware was affecting the company server. Then, Yahoo! revealed a list of people who purchased the web hosting service from them by paying with their credit-cards. Unfortunately, the web-names that were hosted were purchased by some stolen credit-cards and fake e-mail addresses. FBI contacted each and every person whose credit card was used to purchase the domains. Everyone's response was same that some unidentified transaction was posted on their credit-card. All the alternative e-mail accounts provided which will be asked while creating an account on Yahoo! were also fake. Then, there was a telephone based scam against customers of Flagstar bank in the Detroit, Michigan area. All the phone calls were pre-recorded and told that they were from the Flagstar bank. The customers were requested to provide their account number and PIN's. The people who did this scam used "voice broadcasting" technology over the internet. The service allowed the users to upload a calling list of numbers and then play the recorded voice message.

These people were linked to the BRD bank phishing scam suspects. Then the court ordered Yahoo! to provide all the tiny details that were linked with BRD bank phishers such as all the information related to the web-names and the e-mail accounts, credit-cards etc., that were used for phishing. A search warrant was issued on October 25th 2007, against the phishers for committing internet auction fraud, phishing scams, identity thefts and money laundering. Most of the people involved in this theft were declared as Romanians committing crimes from Romania. The case papers were legally handed over to the Romanian government authorities and all the obtained materials were shared with the law enforcement authorities of Romania. On November 13th 2007 the Romanian law enforcement authorities charged 22 defendants and arrested 9 defendants and searched over 20 locations connected with this matter.