PRESS RELEASES

Printer Friendly

Manhattan U.S. Attorney Announces Seizure Of Additional $28 Million Worth Of Bitcoins Belonging To Ross William Ulbricht, Alleged Owner And Operator Of "Silk Road" Website

FOR IMMEDIATE RELEASE
Friday, October 25, 2013

With This, the Largest Ever Bitcoin Seizure, the Federal Government Has Now Seized Approximately 173,991 Bitcoins Worth Over $33.6 Million

Preet Bharara, the United States Attorney for the Southern District of New York, George Venizelos, the Assistant Director-in-Charge of the New York Office of the Federal Bureau of Investigation ("FBI"), Brian R. Crowell, the Special-Agent-in-Charge of the New York Field Division of the Drug Enforcement Administration ("DEA"), and Toni Weirauch, the Special Agent-in-Charge of the New York Field Office of the Internal Revenue Service, Criminal Investigation ("IRS-CI"), today announced the unsealing of a protective order authorizing the seizure of approximately 144,336 Bitcoins found on computer hardware belonging to ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the alleged owner and operator of "Silk Road," a hidden website designed to enable its users to buy and sell illegal drugs and other unlawful goods and services anonymously and beyond the reach of law enforcement. Along with a prior seizure of approximately 29,655 Bitcoins, federal law enforcement agents have now seized a total of approximately 173,991 Bitcoins in connection with the Silk Road case, which, at today's Bitcoin exchange rate, are worth over $33.6 million.

The Bitcoins have been seized in connection with a civil action previously filed in Manhattan federal court on September 30, 2013, seeking the forfeiture of all assets of Silk Road, including its website and all of its Bitcoins because those assets allegedly were used to facilitate money laundering and constitute property involved in money laundering. Also in connection with that civil action, federal law enforcement agents previously seized the Silk Road website itself. In addition to the civil action, a criminal Complaint against ULBRICHT was filed in Manhattan federal court charging him with one count of narcotics conspiracy, one of count of conspiracy to commit computer hacking, and one count of money laundering conspiracy. ULBRICHT was arrested in San Francisco, California, on October 1, 2013, he was subsequently ordered detained, and he is expected to appear in Manhattan federal court within the next few weeks. ULBRICHT has also been charged in a separate indictment pending in federal court in Baltimore, Maryland.

Manhattan U.S. Attorney Preet Bharara said: "As alleged, Ross William Ulbricht operated Silk Road – a global illegal cyber business designed to broker criminal transactions – protected by a presumed anonymity and motivated by profit. With his arrest and our subsequent seizures of millions of dollars worth of Silk Road's Bitcoins, we have sent a clear message to him and everyone else running criminal enterprises on the dark web: we are determined and equipped to hold you to account."

FBI Assistant Director-in-Charge Venizelos said: "As alleged in court documents, the creator of

Silk Road, Ross William Ulbricht, created a black market bazaar for drugs and illegal services where customer service and anonymity were added value to shoppers and sellers. This market generated millions in illegal profits for Ulbricht in the form of Bitcoins. However, what Ulbricht didn't count on was that Silk Road's coffers would not be out of reach of the FBI and our partners to seize. We want to thank our law enforcement partners here and abroad for their support and work on this case."

DEA Special-Agent-in-Charge Brian R. Crowell said: "The Silk Road underground website was the global venue for drug trafficking and money laundering, producing millions in dirty profits. DEA and others followed the money throughout this investigation, leading to this seizure. The website was used by drug dealers to put illicit drugs into our communities and literally at our doorsteps nationwide. 200,000 people die annually from drug abuse throughout the world, and our investigators worked tirelessly to bring to justice a facilitator who made every effort to hide behind highly encrypted technology while providing 24/7 anonymous services to global drug traffickers and money launderers. Ulbricht's goals were to make millions from drug use and money laundering while protecting the world's criminals from law enforcement. Our goal is to shut these people down and protect our children and DEA will continue to be relentless in this effort."

IRS Special-Agent-in-Charge Toni Weirauch said: "This seizure sends a clear notice to those who think they can commit crimes and conceal the fruits of their criminal activities in digital anonymity. The resolve of the government to uncover criminality and identify criminal proceeds is strong and its investigative capabilities are magnified when different federal agencies, each with its own areas of expertise, unite to achieve a common objective."

According to the allegations in the Complaint, the civil forfeiture action, and the application and protective order unsealed today in Manhattan federal court:

Background on Silk Road and ROSS WILLIAM ULBRICHT

Since approximately January 2011, ROSS WILLIAM ULBRICHT owned and operated the underground website known as Silk Road, which emerged as the most sophisticated and extensive criminal marketplace on the Internet. Throughout the time that ULBRICHT controlled Silk Road, it served as a sprawling black-market bazaar where unlawful goods and services, including illegal drugs of virtually every variety, were bought and sold regularly by the site's users.

During its approximately two-and-a-half years in operation, Silk Road was used by several thousand drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other unlawful goods and services to well over a hundred thousand buyers, and to launder hundreds of millions of dollars derived from these unlawful transactions. All told, the site generated sales revenue of more than 9.5 million Bitcoins and collected commissions from these sales totaling more than 600,000 Bitcoins. Although the value of Bitcoins has varied over time, these figures are roughly equivalent to approximately $1.2 billion in sales and approximately $80 million in commissions, using the Bitcoin exchange rate in effect when the Silk Road website was seized.

ULBRICHT deliberately operated Silk Road as an online criminal marketplace designed to enable its users to buy and sell drugs and other illegal goods and services anonymously and outside the reach of law enforcement. He sought to anonymize transactions on Silk Road in two principal ways. First, ULBRICHT operated Silk Road on what is known as "The Onion Router," or "Tor" network, a special network of computers on the Internet, distributed around the world, designed to conceal the true IP addresses and therefore the identities of the networks' users. The Tor network is designed to make it practically impossible to physically locate the computers hosting or accessing websites on the network. Second, ULBRICHT required that all transactions

on Silk Road be paid with Bitcoins, an electronic currency that is as anonymous as cash. Although Tor and Bitcoins have known legitimate uses, they were intentionally used by Silk Road to further the site's unlawful goals.

The Silk Road website provided a sales platform that allowed vendors and buyers using the site to conduct transactions online. Silk Road is believed to have been visited by hundreds of thousands of unique users from countries across the globe, nearly 30 percent of whom indicated upon registering on the site that they were from the United States. The illegal nature of the items sold on the website was readily apparent to any user browsing through its offerings. Indeed, the vast majority of the items for sale on Silk Road were illegal drugs, which were openly advertised as such on the site. As of September 23, 2013, Silk Road had nearly 13,000 listings for controlled substances, listed under such categories as "Cannabis," "Dissociatives," "Ecstasy," "Intoxicants," "Opioids," "Precursors," "Prescription," "Psychedelics," and "Stimulants." From November 2011 to September 2013, law enforcement agents made more than 100 individual undercover purchases of controlled substances from Silk Road vendors. These purchases included heroin, cocaine, ecstasy, and LSD, among other illegal drugs, and were filled by vendors believed to be located in more than ten different countries, including the United States, Germany, the Netherlands, Canada, the United Kingdom, Spain, Ireland, Italy, Austria and France.

In addition to illegal narcotics, other illicit goods and services were also openly bought and sold on Silk Road. For example, as of September 23, 2013, there were: 159 listings under the category "Services," most of which offered computer-hacking services, such as a listing by a vendor offering to hack into social networking accounts of the customer's choosing; 801 listings under the category "Digital goods," including malicious software, hacked accounts at various online services, and pirated media content; and 169 listings under the category "Forgeries," including offers to produce fake driver's licenses, passports, Social Security cards, utility bills, credit card statements, car insurance records, and other forms of false identification documents.

The only form of payment accepted on Silk Road was Bitcoins, an anonymous, decentralized form of electronic currency, existing entirely on the Internet and not in any physical form. Silk Road's payment system essentially consisted of an internal Bitcoin "bank," where every Silk Road user had to hold an account in order to conduct transactions on the site. Every Silk Road user had at least one Silk Road Bitcoin address associated with the user's Silk Road account. These addresses were stored on wallets maintained on servers controlled by Silk Road. In order to make a purchase on Silk Road, a user had to obtain Bitcoins (typically through a Bitcoin exchanger) and then send those Bitcoins to a Bitcoin address associated with his or her Silk Road account. Once a user's account was funded in this way, the user was free to make purchases on Silk Road. When a purchase was made, the user's Bitcoins were first transferred to an escrow account maintained by Silk Road, pending completion of the transaction. When the transaction was completed, the buyer's Bitcoins were transferred from the escrow account to the Silk Road Bitcoin address of the vendor involved in the sale. Silk Road also used a so-called "tumbler" which, as the site explained, "sen[t] all payments through a complex, semi-random series of dummy transactions…making it nearly impossible to link your payment with any coins leaving the site." Silk Road charged a commission for every transaction conducted by its users. The commission rate varied depending on the size of the transaction, but generally ranged from 8 to 15 percent of the total sales price.

Using the online moniker "Dread Pirate Roberts," or "DPR," ULBRICHT controlled and oversaw every aspect of Silk Road. ULBRICHT, for example, maintained the computer infrastructure and programming code underlying the Silk Road website; determined vendor and customer policies, including deciding what can be sold on the site; managed a small staff of online administrators who assisted with the day-to-day operation of the site; and controlled the enormous profits generated from the operation of the site. ULBRICHT did so while fully aware of the illegal nature

of the enterprise; indeed, he deliberately sought to ensure the anonymity of the drug dealers and other illegal vendors operating on the site, as well as to conceal his own identity as the site's owner and operator.

ULBRICHT was also willing to use violent means to protect the Silk Road enterprise and the anonymity of its users. For example, in March and April 2013, ULBRICHT solicited a murder-for-hire of a Silk Road vendor, known as "FriendlyChemist," who was threatening to reveal the real names and addresses of a long list of Silk Road users unless ULBRICHT paid him $500,000. Upon receiving the threat from "FriendlyChemist" to expose the names of Silk Road users, ULBRICHT wrote to another Silk Road user, telling that user that "FriendlyChemist" is "causing me problems," and adding: "I would like to put a bounty on his head if it's not too much trouble for you. What would be an adequate amount to motivate you to find him? Necessities like this do happen from time to time for a person in my position." ULBRICHT later explained that the threat by "FriendlyChemist" to expose the names of Silk Road users "is unforgivable to me. Especially here on Silk Road, anonymity is sacrosanct." However, there is no record of a homicide at or about that time in the area where "FriendlyChemist" supposedly lived.

The Seizure of Computer Hardware Belonging to ROSS WILLIAM ULBRICHT

ROSS WILLIAM ULBRICHT was arrested in San Francisco, California, on October 1, 2013. At the time of his arrest, ULBRICHT was using a laptop computer, which was seized in connection with his arrest and subsequently searched pursuant to a search warrant. ULBRICHT's residence was also searched on October 1, 2013, pursuant to a search warrant, and federal law enforcement agents conducting that search found several pieces of computer hardware belonging to ULBRICHT (collectively, along with ULBRICHT's laptop, the "computer hardware"). Through forensic analysis of the computer hardware, federal law enforcement agents recovered a Bitcoin wallet containing approximately 144,336 Bitcoins.

* * *

ULBRICHT, 29, of San Francisco, California, is charged with one count of narcotics conspiracy, which carries a maximum sentence of life in prison and a mandatory minimum sentence of 10 years in prison; one of count of conspiracy to commit computer hacking, which carries a maximum sentence of five years in prison; and one count of money laundering conspiracy, which carries a maximum sentence of 20 years in prison.

Mr. Bharara praised the outstanding investigative work of the FBI and its New York Special Operations and Cyber Division, as well as the outstanding investigative work of the DEA's New York Organized Crime Drug Enforcement Strike Force, which is comprised of agents and officers of the DEA, the IRS, the New York City Police Department, U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI), the New York State Police, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the U.S. Secret Service, the U.S. Marshals Service, Office of Foreign Assets Control, and NY Department of Taxation. Mr. Bharara also thanked the Chicago field office of ICE-HSI for its assistance and support, as well as the Department of Justice's Computer Crime and Intellectual Property Section. Additionally, Mr. Bharara praised the foreign law enforcement partners whose contributions to the success of the investigation and prosecution have been invaluable, namely, the Reykjavik Metropolitan Police of the Republic of Iceland and the French Republic's Central Office for the Fight Against Crime Linked to Information Technology and Communication.

Mr. Bharara also noted that the investigation remains ongoing.

The prosecution of this case is being handled by the Office's Complex Frauds Unit. Assistant United States Attorney Serrin Turner is in charge of the prosecution, and Assistant United States Attorney Christine Magdo is in charge of the forfeiture aspects of the case.

The charges contained in the Complaint are merely accusations, and the defendant is presumed innocent unless and until proven guilty.

13-322

Return to Top