



**Department of Justice**

Office of Public Affairs

FOR IMMEDIATE RELEASE

Tuesday, February 8, 2022

## **Two Arrested for Alleged Conspiracy to Launder \$4.5 Billion in Stolen Cryptocurrency**

### **Government Seized \$3.6 Billion in Stolen Cryptocurrency Directly Linked to 2016 Hack of Virtual Currency Exchange**

*View Deputy Attorney General Monaco's Remarks [here](#).*

Two individuals were arrested this morning in Manhattan for an alleged conspiracy to launder cryptocurrency that was stolen during the 2016 hack of Bitfinex, a virtual currency exchange, presently valued at approximately \$4.5 billion. Thus far, law enforcement has seized over \$3.6 billion in cryptocurrency linked to that hack.

"Today's arrests, and the department's largest financial seizure ever, show that cryptocurrency is not a safe haven for criminals," said Deputy Attorney General Lisa O. Monaco. "In a futile effort to maintain digital anonymity, the defendants laundered stolen funds through a labyrinth of cryptocurrency transactions. Thanks to the meticulous work of law enforcement, the department once again showed how it can and will follow the money, no matter what form it takes."

"Today, federal law enforcement demonstrates once again that we can follow money through the blockchain, and that we will not allow cryptocurrency to be a safe haven for money laundering or a zone of lawlessness within our financial system," said Assistant Attorney General Kenneth A. Polite Jr. of the Justice Department's Criminal Division. "The arrests today show that we will take a firm stand against those who allegedly try to use virtual currencies for criminal purposes."

Ilya Lichtenstein, 34, and his wife, Heather Morgan, 31, both of New York, New York, are scheduled to make their initial appearances in federal court today at 3:00 p.m. in Manhattan.

According to court documents, Lichtenstein and Morgan allegedly conspired to launder the proceeds of 119,754 bitcoin that were stolen from Bitfinex's platform after a hacker breached Bitfinex's systems and initiated more than 2,000 unauthorized transactions. Those unauthorized transactions sent the stolen bitcoin to a digital wallet under Lichtenstein's control. Over the last five years, approximately 25,000 of those stolen bitcoin were transferred out of Lichtenstein's wallet via a complicated money laundering process that ended with some of the stolen funds being deposited into financial accounts controlled by Lichtenstein and Morgan. The remainder of the stolen funds, comprising more than 94,000 bitcoin, remained in the wallet used to receive and store the illegal proceeds from the hack. After the execution of court-authorized search warrants of online accounts controlled by Lichtenstein and Morgan, special agents obtained access to files within an online account controlled by Lichtenstein. Those files contained the private keys required to access the digital wallet that directly received the funds stolen from Bitfinex, and allowed special agents to lawfully seize and recover more than 94,000 bitcoin that had been stolen from Bitfinex. The recovered bitcoin was valued at over \$3.6 billion at the time of seizure.

"Cryptocurrency and the virtual currency exchanges trading in it comprise an expanding part of the U.S. financial system, but digital currency heists executed through complex money laundering schemes could undermine confidence

in cryptocurrency,” said U.S. Attorney Matthew M. Graves for the District of Columbia. “The Department of Justice and our office stand ready to confront these threats by using 21st century investigative techniques to recover the stolen funds and to hold the perpetrators accountable.”

The criminal complaint alleges that Lichtenstein and Morgan employed numerous sophisticated laundering techniques, including using fictitious identities to set up online accounts; utilizing computer programs to automate transactions, a laundering technique that allows for many transactions to take place in a short period of time; depositing the stolen funds into accounts at a variety of virtual currency exchanges and darknet markets and then withdrawing the funds, which obfuscates the trail of the transaction history by breaking up the fund flow; converting bitcoin to other forms of virtual currency, including anonymity-enhanced virtual currency (AEC), in a practice known as “chain hopping”; and using U.S.-based business accounts to legitimize their banking activity.

“In a methodical and calculated scheme, the defendants allegedly laundered and disguised their vast fortune,” said Chief Jim Lee of IRS-Criminal Investigation (IRS-CI). “IRS-CI Cyber Crimes Unit special agents have once again unraveled a sophisticated laundering technique, enabling them to trace, access and seize the stolen funds, which has amounted to the largest cryptocurrency seizure to date, valued at more than \$3.6 billion.”

“Criminals always leave tracks, and today’s case is a reminder that the FBI has the tools to follow the digital trail, wherever it may lead,” said FBI Deputy Director Paul M. Abbate. “Thanks to the persistent and dedicated work of our FBI Investigative teams and law enforcement partners, we’re able to uncover the source of even the most sophisticated schemes and bring justice to those who try to exploit the security of our financial infrastructure.”

“Financial crime strikes at the core of our national and economic security. With a hack of this magnitude, public and private sector collaboration is crucial to ensure continued consumer confidence in our financial system,” said Acting Executive Associate Director Steve Francis of Homeland Security Investigations (HSI). “Ilya Lichtenstein and his wife Heather Morgan attempted to subvert legitimate commerce for their own nefarious purposes, operating with perceived anonymity. Today’s action demonstrates HSI’s commitment and ability to work with a collusion of the willing to unravel these technical fraud schemes and identify the perpetrators, regardless of where they operate.”

Lichtenstein and Morgan are charged with conspiracy to commit money laundering, which carries a maximum sentence of 20 years in prison, and conspiracy to defraud the United States, which carries a maximum sentence of five years in prison. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

The investigation was led by IRS-CI Washington, D.C. Field Office’s Cyber Crimes Unit, the FBI’s Chicago Field Office, and HSI-New York. The Ansbach Police Department in Germany provided assistance during this investigation.

The case is being prosecuted by Trial Attorneys Jessica Peck and C. Alden Pelker of the Justice Department’s Computer Crime and Intellectual Property Section and Assistant U.S. Attorney Christopher B. Brown of the U.S. Attorney’s Office for the District of Columbia. Paralegal Specialists Angela De Falco and Brian Rickers and Legal Assistant Jessica McCormick provided valuable assistance. Significant assistance was also provided by Trial Attorney Christen Gallagher of the Office of International Affairs, the U.S. Attorneys’ Offices for the Eastern District of Pennsylvania and Southern District of New York, HSI-Philadelphia, and former Assistant U.S. Attorney Jessica C. Brooks.

*A complaint is merely an allegation, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.*

---

**Attachment(s):**

[Download complaint\\_pacer.pdf](#)

[Download statement\\_of\\_facts\\_pacer.pdf](#)

**Topic(s):**

Cyber Crime

**Component(s):**

Criminal Division  
Criminal - Computer Crime and Intellectual Property Section  
Office of the Deputy Attorney General

**Press Release Number:**

22-105

*Updated February 8, 2022*