

COINBASE WEBSITE SPOOFER STEALS \$37 MILLION IN CRYPTO WITH A DEVIOUS SCHEME



Federal prosecutors have charged Chirag Tomar, a citizen and resident of India, with orchestrating a massive fraud scheme that allegedly stole over \$37 million worth of various cryptocurrencies from hundreds of victims around the globe.

A Web Of Deception – They Employed Every Trick In The Book To Get Their Hands On Stolen Crypto

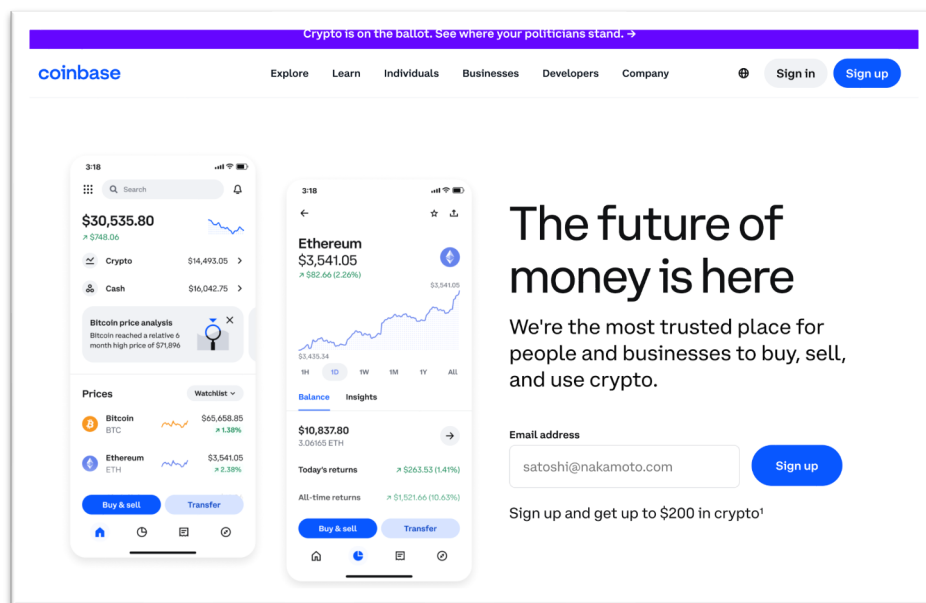
According to the indictment, Tomar and his co-conspirators employed a wide variety of tactics to defraud cryptocurrency owners:

1. **SIM Swapping:** The fraudsters reportedly convinced mobile phone carriers to transfer victims' phone numbers to SIM cards controlled by the conspiracy. This allowed them to bypass two-factor authentication and gain access to victims' cryptocurrency exchange accounts.

2. **Phishing Attacks:** Victims were targeted with sophisticated phishing emails and websites that mimicked legitimate cryptocurrency exchanges, tricking them into entering their login credentials.
3. **Malware Deployment:** The group allegedly used malicious software to infect victims' computers and mobile devices, giving them unauthorized access to cryptocurrency wallets.
4. **Social Engineering:** In some cases, the conspirators posed as customer service representatives from cryptocurrency exchanges, persuading victims to reveal sensitive account information.

A Copycat Crypto Site - Spoofing Coinbase Pro

One of the most insidious tactics allegedly employed by Tomar and his co-conspirators involved the creation of a highly sophisticated fake version of Coinbase Pro, the advanced trading platform offered by Coinbase.



According to investigators, the fraudsters meticulously replicated the look and feel of the legitimate Coinbase Pro website, paying close attention to details such as the user interface, color scheme, and even the responsiveness of trading charts.

His fraudulent site was then promoted through targeted phishing emails and malicious ads, often appearing at the top of search engine results for terms related to cryptocurrency trading. Unsuspecting victims who landed on this spoofed site would enter their login credentials, unknowingly handing over access to their real Coinbase Pro accounts.

The level of detail in this impersonation was so convincing that even experienced traders fell victim to the scam.

How These Spoofed Website Crypto Cases Work – An Example Using A Victim Named Sarah

Step 1 - Creating the Fake Website

Tomar and his team create a near-perfect replica of the Coinbase Pro website, including the login page, trading interface, and account management sections. They register a domain name similar to the real Coinbase Pro, such as "coinbase-pro-secure.com" or "coinbasepro-login.net".

Step 2 - Targeting Victims

The fraudsters purchase email lists of known cryptocurrency investors or scrape public forums for potential targets. They craft a convincing phishing email that appears to be from Coinbase, warning of a security issue and urging users to log in and verify their accounts.

Step 3 – Sending The Phishing Email

The email might read: "Dear Coinbase Pro User, We've detected unusual activity on your account. Please log in immediately to verify your identity and secure your assets. Click here to log in securely." The "Click here" link leads to the fraudulent Coinbase Pro website.

Step 4- Victim Interaction

A victim, let's call her Sarah, receives this email and, concerned about her account security, clicks the link. Sarah arrives at the fake Coinbase Pro login page, which looks identical to the real one.

Step 5 - Credential Theft

Sarah enters her username and password, which are immediately captured by the fraudsters. The fake site may also prompt for two-factor authentication codes, which Sarah provides.

Step 6 - Behind the Scenes

As soon as Sarah's credentials are captured, Tomar or an accomplice immediately logs into Sarah's real Coinbase Pro account. They quickly initiate transfers of Sarah's cryptocurrencies to wallets controlled by the fraudsters.

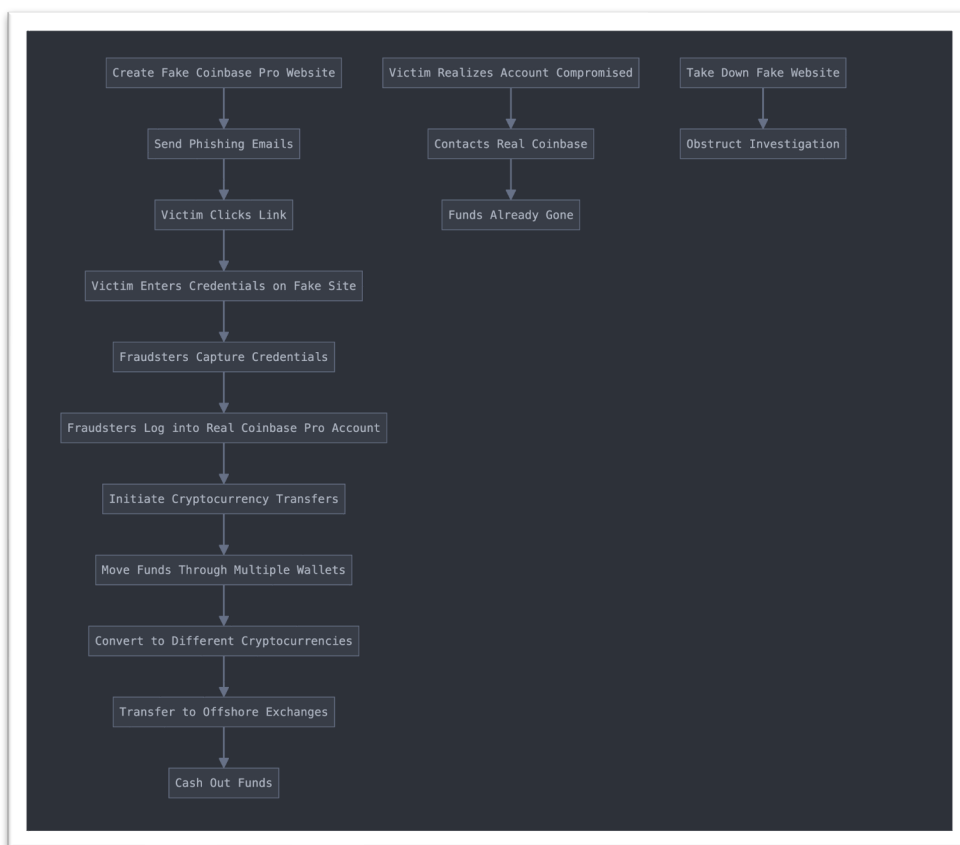
Step 7 - Delay Tactics

To buy time, the fake website shows Sarah a "Processing" or "Verifying" screen for several minutes. It might then display a message like: "Thank you for verifying your account. Your security settings have been updated."

Step 8 - Covering Their Tracks

The fraudsters may use Sarah's stolen credentials to change her email and password on the real Coinbase Pro, locking her out. They might also delete or alter account recovery options to delay Sarah from regaining control.

Here is a helpful diagram of the scheme he concocted.



IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

APR 15 2024
US DISTRICT COURT
WESTERN DISTRICT OF NC

UNITED STATES OF AMERICA)	DOCKET NO. 3:24-CR-76-KDB
)	
v.)	BILL OF INFORMATION
)	
CHIRAG TOMAR)	18 U.S.C. § 1349
_____)	

THE UNITED STATES ATTORNEY CHARGES:

At the specified times and at all relevant times:

Overview

1. At all times relevant to this Information, CHIRAG TOMAR, the defendant, a citizen and resident of the Republic of India, engaged in a conspiracy to steal cryptocurrency from hundreds of victims through fraud. In total, TOMAR and others stole over \$37 million dollars’ worth of various cryptocurrencies from hundreds of victims worldwide.

Cryptocurrency

2. Cryptocurrency is a virtual currency in which transactions are verified and records are maintained by a decentralized system using cryptography, rather than a centralized authority such as a bank or a government. Like traditional fiat currency, there are multiple types of cryptocurrencies, such as Bitcoin, Ethereum, and Tether, among others. Due to its decentralized nature and limited regulation, cryptocurrency allows users to transfer funds more anonymously than would be possible through traditional banking and credit systems. Cryptocurrency owners typically store their cryptocurrency in virtual “wallets,” which are identified by unique electronic “addresses.” Cryptocurrencies can be instantaneously and irreversibly transferred between wallets simply by directing a transfer to the desired recipient wallet address, typically a 26-35-character-long case-sensitive string of letters and numbers.

3. Coinbase, headquartered in San Francisco, California, is one of the largest virtual currency exchanges in the world. Virtual currency exchanges like Coinbase allow customers to buy, sell, or trade cryptocurrencies, and many users store their cryptocurrencies in their virtual currency exchange wallets. When Coinbase users log into their Coinbase accounts, they are able to quickly and easily transfer the cryptocurrencies

held in their Coinbase account wallet to other wallets outside of Coinbase, including to wallets at other exchanges or to so-called “decentralized” wallets, which are not linked to an exchange. Coinbase operated a “Pro” version of its exchange, which was found at the URL “Pro.Coinbase.com.”

The Coinbase Fraud

4. Beginning in as late as June 2021, TOMAR and known and unknown coconspirators stole cryptocurrency in the form of Bitcoin, Ethereum, and Tether from hundreds of victims throughout the United States and elsewhere through the use of a spoofed Coinbase website. Spoofing, as it pertains to cybersecurity, is when a malicious cyber actor disguises an email address, sender name, or website URL—often just by changing one letter, symbol, or number—to convince a victim that the victim is interacting with a trusted source. Here, TOMAR and his coconspirators spoofed the legitimate Coinbase Pro virtual currency exchange website through the use of a similar, but unaffiliated, website URL: “CoinbasePro.com.”

5. When a victim Coinbase customer would inadvertently visit CoinbasePro.com, he or she would be redirected to one of many websites that were intentionally designed to be similar to the legitimate Coinbase log-in website. Misled by the fraudulently designed websites, victims would then attempt to log in with their valid Coinbase credentials, which resulted in the victims’ Coinbase log-in credentials being acquired by the fraudsters. Victims would then be notified that his or her account was locked and prompted to either: (1) call a phone number that was provided in order to speak to a purported Coinbase customer service representative, or (2) use the website’s live chat box feature. The phone number connected the victim to a coconspirator who claimed to be an employee of Coinbase. Typically, at this point in the fraud scheme, a real password-reset link would then be sent to the victim and the fraudulent Coinbase representative would request that the victim provide the real password-reset link in the live website chat. The link provided by the victim was a legitimate link from Coinbase allowing the actor to change the victim’s account password. The purported Coinbase representative would also often cause a two-factor authentication code to be sent to the victim. The fake Coinbase representative would also trick the victim into providing that code to the malicious actors. By tricking victims into providing the password reset link and/or the two-factor authentication code, the actors were able to access and subsequently gain control of the victims’ Coinbase accounts. Alternatively, the fake Coinbase representatives often tricked victims into executing remote desktop software, which allowed the malicious actors to control the victims’ computers and access their Coinbase accounts through the victims’ own computers.

6. After the malicious actors gained unauthorized access to victims’ Coinbase accounts, the actors, without the permission of the victims, transferred the victims’ cryptocurrency holdings from the victims’ wallets at Coinbase to cryptocurrency wallets

in the fraudsters' control. TOMAR controlled many cryptocurrency wallets which received hundreds of transactions of stolen cryptocurrency directly from victim accounts at Coinbase, totaling tens of millions of dollars of cryptocurrency. Upon receipt of the stolen cryptocurrency, TOMAR quickly engaged in cryptocurrency transactions to obfuscate the source of the cryptocurrency, including by: (1) converting the funds into other forms of cryptocurrency, such as from Ethereum to Tether; and (2) moving the stolen funds amongst many wallets controlled by TOMAR and his coconspirators. Ultimately, the stolen cryptocurrency was converted into cash and distributed amongst TOMAR and his coconspirators.

7. In one example, on February 5, 2022, victim R.L., a resident of the Western District of North Carolina, inadvertently attempted to log in to his Coinbase account through CoinbasePro.com. The CoinbasePro spoof site stated that R.L.'s Coinbase account was locked and instructed R.L. to contact a purported Coinbase representative at a phone number provided by the spoof site. Malicious actors involved in the conspiracy described herein tricked R.L. into providing his two-factor authentication code to a fake Coinbase representative. The conspirators then gained access to R.L.'s Coinbase account and stole 5.9 Bitcoin from R.L.'s Coinbase wallet. At the time, Bitcoin was valued at approximately \$41,000 per Bitcoin. Therefore, the loss to R.L. was approximately \$240,000. TOMAR recorded details of the fraudulent transaction in his email account to include, among other things, R.L.'s name, R.L.'s phone number, the date of "5-feb," and the amount of \$230,000.

8. TOMAR and his coconspirators stole over \$37 million dollars' worth of cryptocurrency from hundreds of victims located throughout the United States, including in the Western District of North Carolina. TOMAR used victim funds to fund a lavish lifestyle, and among other things, purchased expensive items such as Rolex and Audemars Piguet watches; engaged in foreign travel such as trips to London, Dubai, and Thailand; and acquired high-end luxury vehicles such as Lamborghinis and Porsches.

[REST OF PAGE INTENTIONALLY LEFT BLANK]

Count One

(18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud)

9. The United States Attorney re-alleges and incorporates by reference herein paragraphs 1 through 8 of this Bill of Information.

10. From at least in or about June 2021, the exact date being unknown to the United States Attorney, until in or about December 2023, in Mecklenburg County and Catawba County, among others, within the Western District of North Carolina and elsewhere, the defendant,

CHIRAG TOMAR,

did knowingly combine, conspire, confederate, and agree with others known and unknown to the United States Attorney, to commit the offense of wire fraud, a violation of Title 18, United States Code, Section 1343.

Object of the Conspiracy

11. *Wire Fraud.* It was a part of and an object of the conspiracy that the defendant and others known and unknown to the United States Attorney, with the intent to defraud, having devised the above-described scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, and by concealment of material facts, and for the purpose of executing and attempting to execute such scheme and artifice, transmitted and caused to be transmitted by means of wire communication in interstate commerce, writings, signs, signals, pictures, and sounds, in violation of Title 18, United States Code, Section 1343.

Manner and Means

12. The defendant and his coconspirators carried out the conspiracy through the manner and means described in Paragraphs 1 through 8 of this Bill of Information, among others.

All in violation of Title 18, United States Code, Section 1349.

NOTICE OF FORFEITURE

Notice is hereby given of 18 U.S.C. § 982 and 28 U.S.C. § 2461(c). Under Section 2461(c), criminal forfeiture is applicable to any offenses for which forfeiture is authorized by any other statute, including but not limited to 18 U.S.C. § 981 and all specified unlawful activities listed or referenced in 18 U.S.C. § 1956(c)(7), which are incorporated as to


proceeds by § 981(a)(1)(C). The following property is subject to forfeiture in accordance with §§ 982 and/or 2461(c):

- a. All property which constitutes or is derived from proceeds of the violations set forth in this Bill of Information; and
- b. If, as set forth in 21 U.S.C. § 853(p), any property described in (a) cannot be located upon the exercise of due diligence, has been transferred or sold to, or deposited with, a third party, has been placed beyond the jurisdiction of the court, has been substantially diminished in value, or has been commingled with other property which cannot be divided without difficulty, all other property of the defendant/s to the extent of the value of the property described in (a).

The following property is subject to forfeiture on one or more of the grounds stated above:

- a. A forfeiture money judgment in the amount of at least \$37,000,000.00, such amount constituting the proceeds of the violations set forth in this Bill of Information.

DENA J. KING
UNITED STATES ATTORNEY



MATTHEW T. WARREN
ASSISTANT UNITED STATES ATTORNEY