

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA

v.

CONOR BRIAN FITZPATRICK,

a/k/a "Pompompurin"

Defendant.

Criminal No. 1:23-cr-119

Honorable T.S. Ellis, III

STATEMENT OF FACTS

The United States and the defendant CONOR BRIAN FITZPATRICK, a/k/a "Pompompurin," agree that the following facts are true and correct, and that had this matter proceeded to trial, the United States would have proven them beyond a reasonable doubt with admissible and credible evidence that:

1. From in or around March 2022 through on or about March 15, 2023, the defendant conspired with other members of the website known as BreachForums, including BreachForums moderators and vendors, to commit and aid and abet the commission of the following offenses:
 - a. To knowingly and with intent to defraud, traffic in and use one or more unauthorized access devices during a one-year period, to wit payment card data, bank routing and account numbers, social security numbers, and login credentials, including usernames and associated passwords intended to be used to access certain online accounts provided by account issuers and other entities in the United States, and by such conduct obtain things of value aggregating \$1,000 or

more during that period, said conduct affecting interstate and foreign commerce, in violation of 18, United States Code, Sections 1029(a)(2) and 2; and

- b. Without the authorization of the issuers of access devices, to knowingly and with the intent to defraud, solicit a person for the purpose of selling unauthorized access devices, to wit payment card data, bank routing and account numbers, social security numbers, and login credentials, including usernames and associated passwords, intended to be used to access online accounts provided by account issuers and other entities in the United States, said conduct affecting interstate and foreign commerce, in violation of Title 18, United States Code, Sections 1029(a)(6) and 2.

2. In addition, FITZPATRICK knowingly falsely registered domain names, including breached.vc, breached.to, breachedforums.com, breachforums.net, breachforums.org, and knowingly used these domain names in the course of committing the offense described in paragraph 1 and charged in Count 1 of the Criminal Information, in violation of 18 U.S.C. § 3559(g)(1).

3. Further, as explained in more detail in paragraphs 26 through 28, from on or about June 28, 2022, through on or about July 6, 2022, in the Eastern District of Virginia and elsewhere, FITZPATRICK knowingly and with the intent to defraud, did aid and abet the solicitation of at least one person for the purposes of offering unauthorized access devices, as defined by 18 U.S.C. § 1029(e)(1) and (e)(3), to wit, bank account and routing numbers and social security numbers, said solicitation affecting interstate and foreign commerce, in that the solicitation occurred via the Internet, and between computers located inside the Commonwealth

of Virginia, and computers located outside of the Commonwealth of Virginia, in violation of 18 U.S.C. §§ 1029(a)(6) and 2.

4. Further, as explained in more detail in paragraphs 37 through 42, on or about March 15, 2023, in the Southern District of New York, FITZPATRICK knowingly possessed and attempted to possess at least one matter containing one or more visual depictions that had been transported using a means and facility of interstate and foreign commerce, and in and affecting interstate and foreign commerce, and which visual depictions were produced using materials which had been mailed and so shipped and transported, by any means including by computer; and the production of such visual depictions involved the use of a minor engaging in sexually explicit conduct and such visual depictions were of such conduct, to wit: videos depicting prepubescent minors and minors who had not attained 12 years of age engaging in sexually explicit conduct, stored on a Dell Inspiron 5593 laptop computer (service tag number B2W9723) with a Samsung 870 QVO 4TB solid state drive (SN S5VYNJ0T405292K).

Overview of BreachForums

5. FITZPATRICK is a 20-year-old citizen of the United States, who resides in Peekskill, New York. On October 26, 2020, FITZPATRICK began using the online moniker “Pompompurin” to post messages on a then-prominent English language data breach forum named “Raidforums.” FITZPATRICK, as “Pompompurin,” developed a reputation amongst Raidforums members by, among other things, posting offers to sell hacked databases.

6. After law enforcement’s public disruption of Raidforums in or around February 2022, FITZPATRICK, as “Pompompurin,”¹ created a data breach website named “Breached”

¹ Unless specified otherwise, all of Fitzpatrick’s conduct on BreachForums was done under the cover of his online persona “Pompompurin.”

that later became widely known as “BreachForums” (collectively, “BreachForums”) to serve as a replacement for Raidforums. From at least March 2022 through March 15, 2023, FITZPATRICK controlled and acted as a lead administrator of BreachForums with the assistance of others, including an evolving “staff” of moderators.

7. While active, BreachForums operated as an illegal marketplace where its members could solicit for sale, sell, and purchase and trade hacked or stolen data and other contraband, including stolen access devices, tools for committing cybercrime, breached databases, and other services for gaining unauthorized access to victim systems. Among other things, BreachForums enabled its members to post solicitations concerning the sale of hacked or stolen data, exchange direct private messages with prospective buyers and sellers, buy access to certain hacked or stolen data that the platform itself controlled, and arrange other services related to the illicit transfer of stolen data and contraband.

8. The purpose of BreachForums, and FITZPATRICK’s intent in operating the forum, was to commit and aid and abet the trafficking of stolen or hacked databases containing, among other things, access devices, and the posting of solicitations to offer databases containing access devices. In particular, FITZPATRICK intentionally ran BreachForums in a manner that made it an attractive marketplace for cybercriminals to frequent in an effort to buy, sell, or trade stolen or hacked access devices. At all relevant times, FITZPATRICK knew and understood that the access devices that BreachForums possessed and helped to traffic were stolen or obtained with the intent to defraud, as defined in 18 U.S.C. § 1029(e)(3).

9. An individual could access the BreachForums website without a membership. However, the website required an individual to sign up for a membership to solicit items for sale

or purchase items. BreachForums offered tiers of membership options, including a “God” membership that offered almost unlimited access to the BreachForums website and features.

10. BreachForums included a “Marketplace” section that was dedicated to the buying and selling of hacked or stolen data, tools for committing cybercrime, and other illicit material, including a “Leaks Market” subsection. Some of the items that were often sold in this section included bank account information, social security numbers, other personal identifying information (PII), and login information for compromised online accounts, such as usernames and passwords to access accounts with service providers and merchants.

11. For instance, on December 18, 2022, a BreachForums user with the moniker “USDoD” posted details of approximately 87,760 members of InfraGard, a partnership between the Federal Bureau of Investigation (FBI) and private sector companies focused on the protection of critical infrastructure. In addition, on January 4, 2023, information obtained from a major U.S.-based social networking site was posted by a user with the moniker “StayMad.” This information included names and contact information for approximately 200 million users. More recently, on March 9, 2023, a BreachForums user with the moniker “denfur” posted a message revealing the PII of tens of thousands of thousands of U.S. citizens. The message included a link to download a file containing names, dates of birth, social security numbers, employment information, and health insurance information compromised from a health insurance exchange.

12. BreachForums also supported additional sections in which users posted stolen or hacked data and discussed tools and techniques for hacking and exploiting that information, including in the “Cracking,” “Leaks,” and “Tutorials” sections. BreachForums further included a “Staff” section that was operated by BreachForums administrators and moderators.

13. In addition, to facilitate transactions amongst BreachForums members, FITZPATRICK offered a “middleman” service in which he acted as a trusted middleman, or escrow, between individuals on the website who sought to buy and sell information. FITZPATRICK’s “middleman” service substantially facilitated and encouraged the dissemination of hacked or stolen data through BreachForums because it enabled purchasers and sellers to verify the means of payment and contraband files being sold prior to executing the purchase and sale. FITZPATRICK’s standardized “middleman” process required members to notify him of the “product” they sought to trade.

14. BreachForums further managed a section titled “Official,” which was described as a “Forum where databases stored on our own servers are kept.” Official databases were available for purchase on BreachForums’ official “content distribution network” (CDN) through a “credits” system that the website administered. Credits were available for purchase on the website or earned through contributing content. BreachForums members seeking to post databases to the official BreachForums content section were required to contact FITZPATRICK directly, and FITZPATRICK personally approved the upload of databases to the CDN.

15. As of March 7, 2023, the official section purported to contain 888 datasets, consisting of over 14 billion individual records. These databases included a wide variety of both U.S. and foreign companies, organizations, and government agencies.

16. BreachForums had approximately 333,412 members as of March 14, 2023. It was the largest English-language data breach forum of its kind at the time it went offline.

FITZPATRICK’s Administration of BreachForums and Middleman Service

17. FITZPATRICK was the founder and lead administrator of BreachForums. FITZPATRICK’s responsibilities in the conspiracy included (i) designing and administering the

website's software and computer infrastructure; (ii) establishing and enforcing the website's rules; (iii) creating and managing sections of the website dedicated to promoting the buying and selling of stolen data; (iv) operating a "middleman" service; (v) approving and uploading breached databases to the BreachForums' official CDN; and (vi) providing other assistance to BreachForums members seeking to buy and sell illicit material on the website, including by investigating and sometimes vouching for the authenticity of stolen data.

18. As part of the administration of BreachForums, FITZPATRICK registered a large volume of domains, including breached.vc, breached.to, breachedforums.com, breachforums.net, breachforums.org, to host or provide access to the BreachForums website. To obscure his identity, FITZPATRICK registered these domains in a manner that prevented the effective identification of him as the person who registered it.

19. FITZPATRICK also hired and managed a "staff" of moderators that helped to ensure BreachForums operated properly and performed traditional administrative activity, such as transmitting messages to warn members of conduct that violated BreachForums' rules. FITZPATRICK compensated staff members for acting as moderators.

20. FITZPATRICK and his co-conspirators gained at least \$698,714 through the relevant conduct alleged in Counts 1 and 2 of the Criminal Information.

Overt Acts in Support of Conspiracy

21. In furtherance of the conspiracy and its objects, the following overt acts, among others, were committed in the Eastern District of Virginia and elsewhere by members of the conspiracy.


A. FITZPATRICK Manages the “Official CDN”

22. On or about September 4, 2022, FITZPATRICK made a post in the “Official” section announcing the process to have data posted to the site’s official content distribution network (“CDN”):

Forum Announcement: How to get your thread added to Official

September 4, 2022, 09:08 PM

[Owner] pompompurin



Bossman

ADMINISTRATOR

Posts: 2,770
Threads: 265
Joined: Mar 2022

Do you want your Database post to be on our Official CDN?

We are always looking for more databases to load onto our Official CDN. The only requirements are these:

- You must know at the very least the Year and Month of the breach (Exceptions can be made if you only know the Year, just ask).
- There must be at least 10,000 Records (Exceptions are always made in special cases, however we prefer loading in only larger breaches). Please tell me the **exact** user-count when messaging me so it's easier for us to put on official.
- It must not already be on our forums.

Additionally, while these are not required it's nice to have:

- A news article talking about the breach OR a disclosure notice from the website.
- The exact day of the breach.
- The person who breached the data initially.
- The vulnerability used (And if the website is still vulnerable).

If your Thread meets these requirements, message me via one of the contact methods listed at <https://bf.hn/contact> and I will load your database onto official. Getting your database on official will get you a lot more credits since people know the links will be active and working, and that the breach is verified.

Your thread will be automatically formatted by our plugin for Official breaches. You don't need to format the Thread for us.

23. On or about May 8, 2022, FITZPATRICK caused the transmission of a message to the moniker “agent” confirming that a customer database from a U.S.-based internet hosting and security services company (“Victim-1”) had been approved and moved to BreachForums’ Official CDN. FITZPATRICK’s approval caused the Victim-1 database to be offered for sale through forum “credits” to individuals on the Internet, including an FBI online covert employee (“OCE”) located in the Eastern District of Virginia who viewed the solicitation. The moniker “agent” had posted a message on BreachForums in or around April 2022 indicating that the Victim-1 database contained names, addresses, phone numbers, usernames, password hashes,

and email addresses for approximately 8,000 customers, as well as payment card information for approximately 1,900 customers.

24. On or about October 27, 2022, the FBI OCE purchased and downloaded this database for 8 credits² from the BreachForums Official CDN. The downloaded archive contained a text file named “Breached_Info.txt,” with the following message:

This file has been downloaded from BreachForums. Please check us out.
Our database list is provided here: <https://breached.co/databases>
> Please do the right thing, if you share this database please mention where it was downloaded from!
At the end of the day with your help the more users we get the more high quality/private databases will be leaked.

25. The downloaded archive also contained 11 text files that included customer names, addresses, phone numbers, usernames, password hashes, email addresses, and credit card information to include card number, expiration date, and card verification value (“cvv”), as described in the BreachForums post.

B. Fitzpatrick’s Middleman Service

26. In a post initially made by pompompurin on BreachForums on July 24, 2022, and later modified on or around November 6, 2022, FITZPATRICK officially announced his middleman service and explained the process for reaching out to him to initiate a transaction. In the post, which is partially reflected in the below image, FITZPATRICK (as pompompurin) stated that he has already performed over \$430,000 in middleman transactions with zero issues.

² As of October 20, 2022, credits cost approximately \$0.25 each, and were available in bundles of 30, 60, 120, 240, and 500. Various forms of cryptocurrency were accepted as payment.

Pom's Official Middleman/guarantor Service
 by pompompurin - Sunday July 24, 2022 at 07:00 PM

July 24, 2022, 07:00 PM. (This post was last modified: November 6, 2022, 04:07 PM by pompompurin.) #1

IF I AM EVER INACTIVE OR SLOW TO REPLY, I SUGGEST <https://breached.vc/Thread-Baphomet-Offi...an-Service>

This thread is for anyone interested in leveraging my Middleman services for transactions with other users on our forum.

Please be aware my contact information will always be available here: <https://bf.hn/contact> | <https://pompur.in>

It's simple. Users interested in a middleman can send me a PM or reach out directly through Telegram/Matrix (Listed on <https://bf.hn/contact>) to initiate the trade. Please provide the following:

BF Usernames (both parties):
Telegram Usernames (both parties):
Thread/Product:
Cryptocurrency being used:
Price:


When all this is provided to me, I will create a group for the middleman deal. When both parties agree to the trade, I will send a wallet address for the funds to be sent to. (I can also MM Deals over Matrix)

Once the funds are in my wallet, and confirmed on the blockchain, I will inform both parties and the seller can release the files to the buyer. The seller will PM the buyer the files directly, so I never even touch the files you're selling.

After the buyer has confirmed the data, and that it is as expected, I will release the funds to the seller. If an issue arises // the data doesn't match, the funds will NOT be sent until confirmation is given by the buyer of the data.

Current MM Fee is 0%. I will never charge users to use a MM. If you want to donate however, it's much appreciated as it keeps the forums running. <https://bf.hn/donate>

I've already middlemanned over \$430k USD in total with zero issues.

pompompurin

 Bossman
ADMINISTRATOR

Posts: 4,143
 Threads: 310
 Joined: Mar 2022
 Reputation: 4,322

27. On July 1, 2022, an OCE located in the Eastern District of Virginia reviewed the BreachForums website and observed a post made by “expo2020” on June 28, 2022, which offered to sell “USA FULLZ. Name.ssn.dob.address.dl.”

28. From July 2, 2022, through July 6, 2022, FITZPATRICK exchanged private messages with an FBI OCE on BreachForums and Telegram in which he agreed to middleman a transaction in which the OCE paid approximately \$5,000 to the user “expo2020” to purchase the PII and bank account information of approximately 15 million U.S. persons, and then helped the parties complete the transaction. FITZPATRICK released the funds for the transaction after the OCE informed FITZPATRICK that the data to be purchased included birth dates, social security numbers, and bank account information, and would be used for conducting financial scams.

29. Likewise, on August 17, 2022, an OCE located in the Eastern District of Virginia reviewed the BreachForums website and observed a post that was made by “jigsaw” on August

10, 2022. In this post, jigsaw attempted to sell “Access to a US healthcare company accounting system (contains US citizens documents).” This information purportedly included credit card numbers, emails, full names, addresses, phone numbers, and other information.

30. On August 18, 2022, the OCE and jigsaw arranged to have pompompurin act as a middleman for the transaction. In a private message on BreachForums, pompompurin contacted the OCE and requested payment via Bitcoin.

31. In a follow-up conversation via Telegram, pompompurin assured the OCE that the funds would not be transferred to jigsaw until the OCE had confirmed his or her access to the U.S. healthcare company’s accounting system:

OCE: hey, just replied to your pm on breached. just curious about how mm works for buying network access...like do i get to confirm that the access actually has the credit card #s and id photographs before the btc gets released to seller? access isnt worth much to me without the data to make my money back lol...its this one with jigsaw
<https://breached.to/Thread-Selling-Access-to-a-US-healthcare-company-accountingsystem-contains-US-citizens-documents>

Pom: Once you confirm you got access and got what was advertised the funds will be released...If any issues arise then it’ll be figured out from there

32. After the OCE confirmed that the funds were sent to FITZPATRICK, as pompompurin, jigsaw provided a link to download files that included a means to gain apparent access to the U.S. health care company’s account system. Jigsaw also provided a file (samples.7z) containing driver’s license photos, insurance cards, and credit card on file paperwork for approximately 13 individuals, that were obtained from the victim network (credit card on file paperwork includes the patient’s name, address, email address, telephone number, signature, and the last four digits of the payment card on file).

33. The credentials provided by jigsaw constitute “access devices,” as defined under 18 U.S.C. § 1029(e)(1), because they are a means of account access that either could have been

“used to obtain money, goods, services, or any other thing of value.” In particular, a malicious actor could change account information so that reimbursement payments could be sent to an account or address controlled by the actor, rather than the medical practice that provided care. Additionally, the PII contained in patient records maintained by the victim can be and is sold on internet sites such as BreachForums.

C. Fitzpatrick Provides Additional Support to BreachForums Members’ Illicit Activity

34. On May 11, 2022, FITZPATRICK sent a private message through BreachForums in which he agreed to delete the registration Internet Protocol (IP) address of a BreachForums user who wanted it deleted because “for privacy reasons, I don’t want cops randomly scouting it for dumb shit I do.”

35. On May 24, 2022, FITZPATRICK sent a private message through BreachForums in which he promised to provide “falsified [registration] information” if law enforcement asked. As part of the reply, FITZPATRICK noted “Sure, although I doubt law enforcement would even bother making legal requests to a hacking forum lmao.”

36. In September 2022, a BreachForums user sought advice on how to monetize a breached e-commerce database that included approximately 16 million records. FITZPATRICK used BreachForums private message to reply that “[’]d try getting money out of them first, and if they refuse try selling it.” FITZPATRICK then explained that he would value the database at about “a few thousand” after the user sought pricing guidance.

FITZPATRICK's Possession of Child Pornography

37. FITZPATRICK knowingly possessed approximately 26 files containing visual depictions of minors engaged in sexually explicit conduct on his Samsung 870 QVO 4TB solid state drive (SN S5VYNJ0T405292K) ("Samsung SSD").

38. FITZPATRICK used his Samsung SSD with his Dell Inspiron 5593 laptop computer (service tag number B2W9723). These devices were seized from FITZPATRICK's home in New York on March 15, 2023, pursuant to a federal search warrant.

39. Law enforcement performed a digital forensic examination of FITZPATRICK's Samsung SSD, which revealed he had saved child pornography in two folders. Many of the files had file names and phrases indicative of child pornography, such as "14yo," "15yo," and "Hebephilia."

40. For example, FITZPATRICK possessed a video file with "13y-fully-nude" in the title. This video depicts a minor female who exposes her genitals and masturbates. FITZPATRICK saved this video file to his Samsung SSD on February 9, 2023. Forensic artifacts show that FITZPATRICK opened this file after he saved it.

41. FITZPATRICK also possessed a video file with "Girl_Hebephilia" in the file title. This video depicts two nude prepubescent females. During the video, the girls expose their genitals to the camera and masturbate. FITZPATRICK saved this video file to his Samsung SSD on February 9, 2023. Forensic artifacts show that FITZPATRICK opened this file after he saved it.

42. The Dell Inspiron 5593 laptop computer and the Samsung SSD were manufactured outside the state of New York, and thus had, at the time of the seizure, been

shipped or transported in interstate or foreign commerce. Moreover, these devices belonged to FITZPATRICK and were used solely by him.

Conclusion

43. The Statement of Facts include those facts necessary to support the defendant's guilty plea. It does not include each and every fact known to the defendant or to the government and it is not intended to be a full enumeration of all the facts surrounding the defendant's case.

44. The actions of the defendant, as recounted above, were in all respects knowing, voluntary, and intentional, and were not committed by mistake, accident, or other innocent reason.

Jessica D. Aber
United States Attorney

Kenneth A. Polite, Jr.
Assistant Attorney General, Criminal Division

Date: July 10, 2023

By: 
Lauren Halper
Assistant United States Attorney

Aarash A. Haghighat
Senior Counsel
Computer Crime and Intellectual Property Section
U.S. Department of Justice, Criminal Division.

Defendant's Signature: After consulting with my attorney, I hereby stipulate that the above Statement of Facts is true and accurate and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

Date: July 1^o, 2023

By: Conor Fitzpatrick
Conor Brian Fitzpatrick
Defendant

Defense Counsel Signature: I am Conor Brian Fitzpatrick's attorney. I have carefully reviewed the above Statement of Facts with him. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.

Date: July 11, 2023

By: 
Peter Katz, Esq.
Counsel for the Defendant