

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- - - - - x

UNITED STATES OF AMERICA :

SEALED
INDICTMENT

- v. - :

S1 19 Cr. 769

CHRISTIAN ERAZO, :

Defendant. :

- - - - - x

COUNT ONE

(Conspiracy to Commit Wire Fraud)

The Grand Jury charges:

Background

1. At all times relevant to this Indictment, CHRISTIAN ERAZO, the defendant, was a resident of California.

2. At all times relevant to this Indictment, Music Management Company Victim-1 was a U.S.-based international company with offices in New York, New York, among other locations, engaged in the business of managing over twenty influential recording artists and producers around the world.

3. At all times relevant to this Indictment, Music Management Company Victim-2 was a U.S.-based international company with its office in Beverly Hills, California, engaged in the business of managing over forty influential recording artists around the world.

4. At all times relevant to this Indictment, Manager Victim was a music manager who worked for Music Management Company Victim-1 in New York, New York.

5. At all times relevant to this Indictment, Founder Victim was the co-founder of the Music Management Company Victim-2 in Beverly Hills, California.

6. At all times relevant to this Indictment, Producer Victim-1 was an American recording artist and producer based in Los Angeles, California, who was managed by Music Management Company Victim-1, and specifically Manager Victim.

7. At all times relevant to this Indictment, Producer Victim-2 was a Canada-based music producer, who was managed by Music Management Company Victim-1.

8. At all times relevant to this Indictment, Producer Victim-3 was a music producer based in Los Angeles, California, who was managed by Music Management Company Victim-1.

9. At all times relevant to this Indictment, Producer Victim-4 was a music producer based in Los Angeles, California.

10. At all times relevant to this Indictment, Musician Victim-1 was an American musician.

**Overview of Account Takeover and Fraud Scheme to Obtain
Unreleased Music From Music Industry Professionals**

11. As set forth more fully below, from at least in or about late 2016 through at least in or about April 2017, CHRISTIAN ERAZO, the defendant, and others known and unknown, unlawfully obtained unauthorized access to Internet cloud storage service accounts of Music Management Company Victim-1, Music Management Company Victim-2, and Producer Victim-1 by, among other things, using the credentials, or usernames and passwords, of individuals with authorized access to those accounts. From those accounts, ERAZO and his co-conspirators stole music that had not yet been publicly released from over twenty recording artists, as well as usernames and passwords to other online accounts, among other things. ERAZO and his co-conspirators also leaked music that had not yet been publicly released on public online forums, causing financial and reputational harm to Producer Victim-1 and other recording artists.

12. In addition, from at least in or about late 2016 through at least in or about late 2017, CHRISTIAN ERAZO, the defendant, and others known and unknown, unlawfully accessed without authorization a social networking service account belonging to Producer Victim-1, from which ERAZO and a co-conspirator not named as a defendant herein ("CC-1") impersonated Producer Victim-1 and sent private messages to numerous recording

artists to solicit music from them that they had not yet released. ERAZO and CC-1 directed these artists to send their music to a fake email account that ERAZO created that incorporated Producer Victim-1's professional name, which numerous artists did.

13. From in or about December 2016 up to and including in or about late 2017, CHRISTIAN ERAZO, the defendant, and his co-conspirators discussed placing the blame on another individual ("Individual-1") for the hacking activities of ERAZO and his co-conspirators. A co-conspirator not named as a defendant herein ("CC-2") told Manager Victim that Individual-1 was responsible for hacking the Music Management Company Victim-1's file storage account. Furthermore, in a conversation with an individual they believed to be affiliated with Music Management Company Victim-1, but who in fact was an undercover federal law enforcement officer (the "UC"), both ERAZO and CC-2 represented that Individual-1 was responsible for gaining unauthorized access to the Music Management Company Victim-1's file storage account, while omitting that ERAZO, CC-2 and others had engaged in that very conduct. ERAZO materially misrepresented that he was motivated to help Music Management Company Victim-1, Producer Victim-1 and other artists hold the person responsible for hacking them to account, when ERAZO was actually attempting to help himself and the conspiracy avoid detection from law enforcement.

14. In or about late 2017, CHRISTIAN ERAZO, the defendant, voluntarily made statements to law enforcement agents. In substance and in part, ERAZO admitted that he and other co-conspirators unlawfully accessed the cloud storage service accounts of Music Management Company Victim-1 and Producer Victim-1 to steal music that had not yet been publicly released. ERAZO also disclosed that he and CC-1 unlawfully accessed a social networking service account belonging to Producer Victim-1, from which they sent messages to recording artists under false pretenses. ERAZO stated that he used a fake email account that incorporated Producer Victim-1's professional name as part of his scheme to obtain music that had not yet been publicly released from artists. ERAZO acknowledged that he and CC-1 pretended to be Producer Victim-1 so that recording artists would send ERAZO music that he believed they would not otherwise have sent to ERAZO had ERAZO contacted them using ERAZO's real identity and account.

Erazo's Hacking of the Music Management Company Victims

15. Music Management Company Victim-1 maintained an account with a cloud storage service (the "Music Management Company Victim-1 File Storage Account") to store and share music among its artists and management staff. From in or about fall 2016, up to and including at least April 2017, CHRISTIAN ERAZO, the defendant, and others known and unknown, obtained, among

other things, music that had not yet been released to the public from Music Management Company Victim-1 by gaining unauthorized access to the Music Management Company Victim-1 File Storage Account. During this time period, ERAZO and his co-conspirators unlawfully accessed the Music Management Company Victim-1 File Storage Account at least approximately 2,300 times.

16. Music Management Company Victim-2 maintained an account with a cloud storage service (the "The Music Management Company Victim-2 File Storage Account") to store and share music among its artists and management staff. In or about fall 2016, CHRISTIAN ERAZO, the defendant, and others known and unknown, gained unauthorized access to music in the Music Management Company Victim-2 File Storage Account. During this time period, ERAZO and his co-conspirators unlawfully accessed the Music Management Company Victim-1 File Storage Account numerous times.

17. On or about December 30, 2016, CHRISTIAN ERAZO, the defendant, accessed a file in the Music Management Company Victim-1 File Storage Account. The next day, ERAZO sent an online message to CC-1 asking for a password to another account. CC-1 replied that it would be in a file with the same filename, which CC-1 later sent to ERAZO. CC-1 also noted that the file came from the Music Management Company Victim-1. According to Manager Victim, this file contained personal identifiable

information for clients of Music Management Company Victim-1, including their social media login information.

18. On or about February 21, 2017, CC-1 sent an online message to CHRISTIAN ERAZO, the defendant. The message stated that CC-2 sent CC-1 a "[Producer Victim-2] folder from [Music Management Company Victim-1]." CC-1 noted, in substance and in part, that the folder contained three unreleased songs for limited circulation rather than for general public release. On or about March 6, 2017, CC-1 exchanged online messages with ERAZO in which they also discussed content from Producer Victim-2's folder from the Music Management Company Victim-1 File Storage Account.

19. In or about November 2017, CHRISTIAN ERAZO, the defendant, made a voluntary statement to law enforcement agents with respect to the Music Management Company Victim-1 File Storage Account, among other things. ERAZO stated, in substance and in part, that he accessed the Music Management Company Victim-1 File Storage Account between November 2016 and April 2017. ERAZO further stated that he downloaded approximately 50 gigabytes of music, which translated to approximately one hundred high quality songs, including songs that had been released to the public, as well as songs that had not yet been released to the public. ERAZO stated that he shared music with

CC-1, CC-2, and another co-conspirator not named as a defendant herein ("CC-3").

Erazo's Hacking of Producer Victim-1

Erazo's Hacking of Producer Victim-1's File Storage Account

20. Producer Victim-1 maintained an account with a cloud storage service (the "Producer Victim-1 File Storage Account") to store and share music with other artists, producers, and management staff, including Producer Victim-3. From in or about November 2016, up to and including at least December 2016, CHRISTIAN ERAZO, the defendant, and others known and unknown, obtained, among other things, music that had not yet been released to the public from Producer Victim-1 by gaining unauthorized access to the Producer Victim-1 File Storage Account.

21. According to Producer Victim-1 and Producer Victim-3, there were very few people with access to the Producer Victim-1 File Storage Account, and none of them authorized CHRISTIAN ERAZO, the defendant, to access the Producer Victim-1 File Storage Account. In or about December 2016, Producer Victim-3's credentials were used without Producer Victim-3's authorization to access the Producer Victim-1 File Storage Account. Producer Victim-3 was briefly unable to access the Producer Victim-1 File Storage Account, as the email accounts

associated with Producer Victim-3's credentials had been changed.

22. On or about December 24, 2016, CC-1 sent an online message to CHRISTIAN ERAZO, the defendant, in which CC-1 stated that Producer Victim-1 "def got all [Producer Victim-1's] shit on [the cloud storage service used by Producer Victim-1]."

23. In or about November 2017, CHRISTIAN ERAZO, the defendant, made a voluntary statement to law enforcement agents with respect to the Producer Victim-1 File Storage Account, among other things. ERAZO stated, in substance and in part, that he accessed the Producer Victim-1 File Storage Account between November and December 2016 and downloaded approximately ten gigabytes of music, which he claimed is the equivalent of roughly twenty-five to thirty high quality songs, including both released songs and songs not yet released to the public. ERAZO also stated that he used a virtual private network ("VPN") to hide his presence when he accessed the Producer Victim-1 File Storage Account.

24. A forensic analysis of the laptop computer belonging to CHRISTIAN ERAZO, the defendant, revealed that, as of in or about November 2017, it contained over 850 music files from the Music Management Company Victim-1 File Storage Account. Many of these music files belonged to Producer Victim-1, among

other artists managed by Music Management Company Victim-1.

Erazo's Hacking of Producer Victim-1's Social Networking Account

25. Producer Victim-1 maintained, in his professional name, an account with a microblogging and social networking service on which users could post and interact with public and private messages (the "Producer Victim-1 Social Networking Account"). From in or about late 2016, up to and including at least early 2017, CHRISTIAN ERAZO, the defendant, and CC-1 gained unauthorized access to the Producer Victim-1 Social Networking Account and sent private messages purporting to be from Producer Victim-1 to numerous musicians in order to obtain their music under false pretenses.

26. On or about December 24, 2016, CC-1 sent an online message to CHRISTIAN ERAZO, the defendant, telling ERAZO that CC-1's IP address was on the Producer Victim-1 Social Networking Account. ERAZO replied, "OMG well i think it's okay until [Producer Victim-1] notices anything outta ordinary like lay lowkey."

27. On or about December 28, 2016, CHRISTIAN ERAZO, the defendant, exchanged online messages with CC-1. ERAZO stated that he was going to log in to the social networking service used by Producer Victim-1 without a VPN. CC-1 thought that would be "ok also unless they find out we on it. u in LA

already where [Producer Victim-1] usually at." ERAZO noted that they just needed to avoid "doing anything stupid," and that there was "[n]o reason for them to look for us."

28. From on or about December 30, 2016, up to and including January 1, 2017, Producer Victim-2 received several private messages from the Producer Victim-1 Social Networking Account requesting music from Producer Victim-2. Producer Victim-1 did not send or authorize anyone else to send those messages from the Producer Victim-1 Social Networking Account to Producer Victim-2.

29. On or about January 6, 2017, Musician Victim-1 received private messages requesting Musician Victim-1's music from the Producer Victim-1 Social Networking Account, using the Producer Victim-1 username. That same day, CC-1 sent screenshots of the messages between Musician Victim-1 and the Producer Victim-1 Social Networking Account to ERAZO. CC-1 discussed in online messages with CHRISTIAN ERAZO, the defendant, how to respond to Musician Victim-1's messages from the Producer Victim-1 Social Networking Account. ERAZO also deleted a message from Musician Victim-1 from the Producer Victim-1 Social Networking Account so that Producer Victim-1 would not notice it.

30. In or about November 2017, CHRISTIAN ERAZO, the

defendant, made a voluntary statement to law enforcement agents with respect to the Producer Victim-1 Social Networking Account, among other things. ERAZO stated, in substance and in part, that he accessed it from his residence, and sent private messages to numerous artists under the false pretense of pretending to be Producer Victim-1 because artists would not send ERAZO music under his real name and account. ERAZO stated that he and CC-1 participated in this scheme between November 2016 and February 2017. ERAZO stated that he deleted messages he sent from the Producer Victim-1 Social Networking Account after he sent them in order to cover his tracks.

Erazo's Scheme to Defraud Artists
By Impersonating Producer Victim-1

31. From at least in or about December 2016 through at least in or about late 2017, CHRISTIAN ERAZO, the defendant, and CC-1 sent private messages in which they claimed to be Producer Victim-1 from the Producer Victim-1 Social Networking Account to numerous recording artists to solicit from them music that had not yet been released. ERAZO and CC-1 directed these artists to send their music to a fake email account (the "Fake Producer Victim-1 Email Account") that ERAZO created that incorporated Producer Victim-1's professional name, which numerous artists did. The Fake Producer Victim-1 Email Account is substantially similar to the real email account belonging to Producer Victim-1 ("the Real

Producer Victim-1 Email Account"). The Fake Producer Victim-1 Email Account contains one additional letter than the Real Producer Victim-1 Email Account. Producer Victim-1 did not send, receive or have access to any emails from the Fake Producer Victim-1 Email Account or authorize anyone else to do so.

32. On or about December 22, 2016, CHRISTIAN ERAZO, the defendant, devised a plan to "make new [Producer Victim-1] email And give it as [Producer Victim-1's] 'new' email." ERAZO and CC-1 exchanged online messages, and discussed obtaining music from Producer Victim-4 "from a [Producer Victim-1] email" and shared VPN account information. From on or about December 31, 2016, up to and including on or about February 5, 2017, emails were exchanged between the Fake Producer Victim-1 Email Account and Producer Victim-4 in which an individual purporting to be Producer Victim-1 requested music from Producer Victim-4. In response, Producer Victim-4 provided several music files. According to Producer Victim-4, at the time, Producer Victim-4 believed that the emails were in fact from Producer Victim-1 and that the Fake Producer Victim-1 Email Account was a true and correct email account belonging to Producer Victim-1.

33. From on or about December 31, 2016, CHRISTIAN ERAZO, the defendant, and CC-1 exchanged online messages regarding emailing Producer Victim-4 from the Fake Producer Victim-1 Email

Account to request music. CC-1 noted that they were able to get more music from artists by impersonating Producer Victim-1 using the Fake Producer Victim-1 Email Account than by hacking other accounts.

34. On or about January 6, 2017, messages from the Producer Victim-1 Social Networking Account impersonated Producer Victim-1 and directed Musician Victim-1 to send music to the Fake Producer Victim-1 Email Account. From on or about January 7, 2017 up to and including on or about March 2, 2017, emails were exchanged between the Fake Producer Victim-1 Email Account and Musician Victim-1 which continued to impersonate Producer Victim-1 and requested music from Musician Victim-1. In response, Musician Victim-1 provided several music files, the majority of which had not yet been released to the public.

35. On or about August 3, 2017, Producer Victim-2 received a message from the Fake Producer Victim-1 Email Account requesting Producer Victim-2's album. Producer Victim-2 provided consent to the UC to assume Producer Victim-2's online identity using Producer Victim-2's email account. While located in New York, New York, the UC proceeded to pose as Producer Victim-2 from Producer Victim-2's email account and exchange emails with "Producer Victim-1" at the Fake Producer Victim-1 Email Account. The UC posing as Producer Victim-2 replied in

part: "Yo! Just got into Manhattan, I got this exclusive track that didn't make the album but it'll definitely be a club banger. You want me to send that one over?" CC-1, purporting to be Producer Victim-1, responded in part, "send me the finals and that. . .". With the consent of Producer Victim-2, the UC sent a particular track to the Fake Producer Victim-1 Email Account. In response to the UC's request for exclusive unreleased tracks, the Fake Producer Victim-1 Email Account sent several music files to Producer Victim-2's email account.

36. From on or about August 4, 2017, up to and including August 9, 2017, CC-1 exchanged online messages with CHRISTIAN ERAZO, the defendant. CC-1 stated that Producer Victim-2 was responding to emails, and that CC-1 was going to try to get a final album. CC-1 also sent music files to ERAZO in online messages, and they discussed leaking music.

37. Producer Victim-1 did not authorize ERAZO to use Producer Victim-1's name and username in connection with the Fake Producer Victim-1 Email Account. In or about early October 2017, Producer Victim-1 sent an email from the Real Producer Victim-1 Email Account to the Fake Producer Victim-1 Email Account to request that whoever is pretending to be Producer Victim-1 please stop doing so. Shortly thereafter, from on or about October 7, 2017, up to and including October 8, 2017, CC-1 exchanged online

messages with CHRISTIAN ERAZO, the defendant. CC-1 sent screenshots of email exchanges between Producer Victim-1 at the Real Producer Victim-1 Email Account and CC-1 at the Fake Producer Victim-1 Email Account. CC-1 stated, in part, "I cant stop laffin. . . That the funniest shit I done."

38. Music files stolen from the Music Management Company Victim-1 File Storage Account were found in the Fake Producer Victim-1 Email Account.

39. In or about November 2017, CHRISTIAN ERAZO, the defendant, made a voluntary statement to law enforcement agents with respect to the Fake Producer Victim-1 Email Account, among other things. In substance and in part, ERAZO stated that he created this account in December 2016, and that it is not a true email account for Producer Victim-1. ERAZO stated that he provided CC-1 with the password for the Fake Producer Victim-1 Email Account shortly after he created it. ERAZO and CC-1 had access to the Fake Producer Victim-1 Email Account and the Recovery Email Account, which ERAZO also created. ERAZO stated that CC-1 told ERAZO that he had accessed the Fake Producer Victim-1 Email Account in October 2017. ERAZO stated that CC-1 controlled the Fake Producer Victim-1 Email Account as of November 2017. ERAZO used a VPN account to protect himself from detection from law enforcement.

Erazo's Scheme to Defraud Music Management Company Victim-1

40. From in or about December 2016 up to and including late 2017, CHRISTIAN ERAZO, the defendant, discussed with CC-1 in online messages blaming Individual-1 for his and others' hacking activities.

41. On or about January 8, 2017, CC-2 sent an email to Manager Victim stating that Individual-1 had gained unauthorized access to the information stored in the Music Management Company Victim-1 File Storage Account and was selling the information contained therein.

42. On or about January 18, 2017, CHRISTIAN ERAZO, the defendant, and CC-2, called the UC, who was posing as security for Music Management Company Victim-1, at a phone number with a Manhattan area code. The following statements, in substance and in part, were discussed during that call:

a. ERAZO - who identified himself as "Chris," stated that he "assumed you guys were in L.A.," but then noted the UC's "NYC number."

b. When the UC asked what they had, ERAZO stated that "[i]t's a lot of info" and that he was "doing this for the love of the artists, the music and you know what it's a shame, you know honestly it's a shame. You know we don't want no harm done to the artists [Producer Victim-1] in this case [Producer Victim-

1] you know. I'm happy to help out if you need any of the info or anything I could dig up for you guys just let me know and I'm more than happy to help you guys out with this."

c. CC-2 stated that Individual-1 hacked artists and managements to obtain unreleased music, which Individual-1 then sold for \$300 per track. CC-2 stated that Individual-1 distributed other personal identifying information as well. ERAZO stated that they knew this information because they had an inside source close to Individual-1 and were trying to accumulate evidence against Individual-1 for Music Management Company Victim-1.

d. The UC stated that sometimes the UC was in L.A. and sometimes the UC was in New York, and that the UC had no problem flying somebody into New York to talk to them. The UC noted that if music is "going to go big it's worth a lot more money than what you guys are talking about." CC-2 replied, "I know and that's why we wanted to tell you. This is really a fucking disaster for [Music Management Company Victim-1] and for the labels."

e. ERAZO then stated, "Yeah and another thing to why we are going to you guys is we just hate this fucking [person]. Bottom line. We aren't even going to beat around the bush. . .bottom we line is we just hate this fucking [person] and we want to do anything we can do to just like play like double agent or anything to get you guys what you need. I'm here for it. You know?"

f. CC-2 stated that "the only thing that will stop [Individual-1] is if he is legally threatened." ERAZO added that "I know that going through the legal system does not mean anything to you guys but as long as [Individual-1] has the tracks [Individual-1] will continue to send them out."

g. ERAZO stated that they were "probably taking some drastic measures by trying to contact you guys but we don't want this to continue happening and spreading." CC-2 then gave advice regarding increasing the security to the Music Management Company Victim-1 File Storage Account.

h. At no time during this call did ERAZO or CC-2 disclose that ERAZO, CC-2, CC-1, and CC-3 had gained unauthorized access to the Music Management Company Victim-1 File Storage Account, the Producer Victim-1 File Storage Account, or the Producer Victim-1 Social Networking Account, and obtained music and other information from those accounts. Nor did they disclose that they had shared music among themselves, as well as leaked unreleased music on public online forums. Furthermore, neither ERAZO nor CC-2 told the UC about their concerns that they could be detected by law enforcement, and their desire to blame their own conduct on Individual-1.

43. On or about January 25, 2017, CC-1 sent an online message to CHRISTIAN ERAZO, the defendant, regarding having placed

the blame for the hacking on Individual-1. ERAZO replied in part, "this is the perf[ect] cover up."

44. On or about February 16, 2017, CHRISTIAN ERAZO, the defendant, sent an online message to the UC stating that he was seeking to prevent leaks of music associated with Producer Victim-1 on a public online forum (the "Forum") "as a help to you guys and the label." ERAZO did not mention his own role in leaking Producer Victim-1's unreleased music on the Forum, or that he had been contacted on the Forum by Music Management Company Victim-1 to take down the unreleased tracks that ERAZO had posted. ERAZO also omitted that he and others had hacked various online accounts associated with Producer Victim-1 to obtain unreleased music from Producer Victim-1, or that he impersonated Producer Victim-1 in order to obtain unreleased music from other artists.

**Erazo's Scheme Caused Artists to Suffer
Significant Financial Harm**

45. As a result of the theft and leakage of over 100 unreleased songs belonging to Producer Victim-1, Producer Victim-1 suffered substantial financial and reputational harm. Among other things, an entire album that Producer Victim-1 and other collaborators (the "Music Group") worked on for approximately one year was leaked and had to be scrapped since it was already public and would not sell. The Music Group's previous album had grossed roughly \$2 million in sales.

Statutory Allegations

46. From at least in or about late 2016 up to and including at least in or about late 2017, in the Southern District of New York and elsewhere, CHRISTIAN ERAZO, the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated and agreed together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

47. It was a part and an object of the conspiracy that CHRISTIAN ERAZO, the defendant, and others known and unknown, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343.

(Title 18, United States Code, Section 1349.)

COUNT TWO

(Conspiracy to Commit Computer Intrusion)

The Grand Jury further charges:

48. The allegations set forth in paragraphs 1 through 45, are incorporated by reference as if set forth fully herein.

49. From at least in or about late 2016 up to and including at least in or about late 2017, in the Southern District of New York and elsewhere, CHRISTIAN ERAZO, the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit offenses against the United States, to wit, computer hacking, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(a)(4), and 1030(c).

50. It was a further part and an object of the conspiracy that CHRISTIAN ERAZO, the defendant, and others known and unknown, knowingly and willfully would and did intentionally access a computer without authorization and exceed authorized access, and thereby obtained information from a protected computer, and in furtherance of a criminal act in violation of the laws of the United States, to wit, the wire fraud crime charged in Count One of this Indictment, the value of which information exceeded \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(ii) and 1030(c)(2)(B)(iii).

51. It was a further part and an object of the conspiracy that CHRISTIAN ERAZO, the defendant, and others known and unknown, would and did knowingly and with intent to defraud, access a protected computer without authorization and exceed authorized access, and by means of such conduct further the intended fraud and thereby obtain a thing of value, to wit, recording artist information and music that was used in furtherance of wire fraud crime, the value of which information exceeded \$5,000 in a 1-year period, in violation of Title 18, United States Code, Section 1030(a)(4) and 1030(c)(3)(A).

Overt Acts

52. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts were committed in the Southern District of New York and elsewhere:

a. On or about December 25, 2016, CHRISTIAN ERAZO, the defendant obtained unauthorized access to the Music Management Company Victim-1 File Storage Account and downloaded a music file.

b. On or about January 18, 2017, CHRISTIAN ERAZO, the defendant, participated in a telephone call with the UC, who was located in New York, New York, during which ERAZO attempted to avoid detection and further the objective of the conspiracy by placing the blame for the account hacks and takeovers on

Individual-1.

c. On or about August 4, 2017, in response to the UC's request for exclusive unreleased tracks, CC-1 - who was posing as Producer Victim-1 - emailed several stolen music files from the Fake Producer Victim-1 Email Account to the UC, who was located in New York, New York.

(Title 18, United States Code, Section 371.)

COUNT THREE

(Aggravated Identity Theft)

The Grand Jury further charges:

53. The allegations set forth in paragraphs 1 through 45, are incorporated by reference as if set forth fully herein.

54. From at least in or about late 2016 up to and including at least in or about April 2017, in the Southern District of New York and elsewhere, CHRISTIAN ERAZO, the defendant, knowingly did transfer, possess, and use, without lawful authority, a means of identification of another person, during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), to wit, ERAZO used the names, email and social networking accounts, and usernames of other persons during and in relation to the conspiracy to commit the wire fraud

and computer intrusion offenses charged in Counts One and Two of this Indictment.

(Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), and 2.)

FORFEITURE ALLEGATIONS

55. As a result of committing the wire fraud offense alleged in Count One of this Indictment, CHRISTIAN ERAZO, the defendant, shall forfeit to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code Section 2461, any and all property, real or personal, which constitutes or is derived from proceeds traceable to the commission such offense, including but not limited to a sum of money in United States currency traceable to the commission of said offense.

56. As a result of committing the computer intrusion offense alleged in Count Two of this Indictment, CHRISTIAN ERAZO, the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 1030(i), any and all property that was used or intended to be used to commit or to facilitate the commission of said offenses, including but not limited to a sum of money in United States currency representing the amount of proceed traceable to the commission of said offense.

Substitute Assets Provision

57. If any of the above described forfeitable property,


as a result of any act or omission of the defendant:

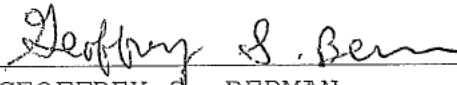
- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third person;
- (c) has been placed beyond the jurisdiction of the Court;
- (d) has been substantially diminished in value; or
- (e) has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 982(b) and Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant up to the value of the above forfeitable property, including but not limited to all of the property set forth above.

(Title 18, United States Code, Sections 981 and 1030; Title 21, United States Code, Section 853; and Title 28, United States Code, Section 2461.)


FOREPERSON

 11/4/19


GEOFFREY S. BERMAN
United States Attorney

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

CHRISTIAN ERAZO,

Defendant.


SEALED INDICTMENT

S1 19 Cr. 769

(18 U.S.C. §§ 371,
1028A(a)(1), 1028A(b), 1349 & 2.)

GEOFFREY S. BERMAN
United States Attorney.

A TRUE BILL

 11/04/19
Foreperson.
