

**UNITED STATES DISTRICT COURT  
DISTRICT OF NEW JERSEY**

UNITED STATES of AMERICA

v.

Criminal No. 10-114 (KSH)

KENNETH LOWSON,  
a/k/a “Money”,  
KRISTOFER KIRSCH,  
a/k/a “Robert Woods”,  
JOEL STEVENSON and  
FAISAL NAHDI

**Defendants**

**OPINION**

**Katharine S. Hayden, U.S.D.J.**

**I. Introduction**

Defendants are charged with violations of the Computer Fraud and Abuse Act and the wire fraud statute arising from an alleged scheme to circumvent security measures put in place by Online Ticket Vendors (OTVs) in order to buy large blocks of tickets meant for the general public and then to re-sell those tickets at great profit on the secondary market. Defendants argue that their conduct is not criminal, and that in fact the government seeks to criminalize what otherwise would be a breach of contract action for violating the terms of service for ticket sales on OTVs’ websites. The defendants state, “This Indictment does not seek to punish computer fraud, it inappropriately tries to regulate the legal secondary market for event ticket sales through an overreaching prosecution.” (Moving Br. 5.) The government counters that this case is anything but novel, and that “[e]ach and every step of the way is [a] traditional fraud . . . the

same thing that we see in court every day.” (Oral argument transcript 17:7–11.) The defendants, according to the government, “lied about who they were. They lied about their business model. They lied when they impersonated thousands of individual ticket buyers. And they lied when they established thousands of false email addresses and domain names.” (Opp’n Br. 1.)

The yawning gap between the government’s and the defendants’ positions is not lost on the Court, and it highlights and echoes tensions in other courts’ viewpoints on where the line falls between what is civilly actionable conduct, and what is criminal.

Defendants now move to dismiss the Superseding Indictment (“the indictment”). For the reasons to be discussed, the Court denies the defendants’ motion.

## **II. Legal Standard**

An indictment, if valid on its face and returned by a legally constituted and unbiased grand jury, “is enough to call for trial of the charge on the merits.” *United States v. Vitillo*, 490 F.3d 314, 320 (3d Cir. 2007) (quoting *Costello v. United States*, 350 U.S. 359, 363 (1956)). “An indictment is generally deemed sufficient if it[] (1) contains the elements of the offense intended to be charged, (2) sufficiently apprises the defendant of what he must be prepared to meet, and (3) allows the defendant to show with accuracy to what extent he may plead a former acquittal or conviction in the event of a subsequent prosecution.” *Id.* (quoting *United States v. Rankin*, 870 F.2d 109, 112 (3d Cir. 1989)) (internal quotation marks omitted).

Where an indictment is valid on its face, a motion to dismiss is appropriate only after the government has had an opportunity to present its proofs at trial. *United States v. Forero*, 623 F. Supp. 694, 699 (E.D.N.Y. 1985). In other words, a motion to dismiss an indictment is not a

vehicle for a summary trial on the evidence, *United States v. Winer*, 323 F. Supp. 604, 605 (C.D. Pa. 1971), and any factual assertions related to a charge must be tested at trial. *United States v. Bender*, 2003 WL 282184 (S.D.N.Y. 2003). Moreover, on occasion a defendant's legal contentions may be so bound up with those facts that a court cannot grant a motion to dismiss. *United States v. Shabbir*, 64 F. Supp. 2d 479, 481 (D. Md. 1999).

### **III. The Wire Fraud Counts**

Counts 27-36 and 37-43 of the indictment charge wire fraud by the use of CAPTCHA Challenges (counts 27-36) and e-mails (counts 37-43).

To charge the crime of wire fraud sufficiently, the government must allege three elements of the offense: (1) the defendants' "knowing and willful participation in a scheme or artifice to defraud, (2) with the specific intent to defraud, and (3) the use of the mails or interstate wire communications in furtherance of the scheme." *United States v. Al Hedaithy*, 392 F.3d 580, 590 (3d Cir. 2006); *see also* 18 U.S.C. § 1343 (2006). In addition, the object of the scheme must be a traditionally recognized property right. *Al Hedaithy*, 392 F.3d at 590.

First, the government sufficiently alleges an extensive scheme in which Wiseguys knowingly and willfully engaged to defraud Ticketmaster. The indictment alleges that Wiseguys circumvented computer code and surreptitiously obtained and resold event tickets that online ticket vendors would not otherwise sell to them. According to the indictment, defendants wrote automated software to defeat the vendors' security measures, including CAPTCHA, by opening thousands of connections and using CAPTCHA Bots to quickly solve CAPTCHA challenges. (Superseding Indict. Count 1, ¶¶ 7, 10.) The defendants allegedly acquired source code the vendors used to protect their websites, created a database of CAPTCHA challenges and their answers, and tested means of navigating to ticket "Buy Pages" without having to answer

CAPTCHA challenges at all. (Superseding Indict. Count 1, ¶¶ 9, 11, 12.) Wiseguys also allegedly used various means of deception, including mimicking the steps a human would take when answering CAPTCHA challenges (including making mistakes), using thousands of non-consecutive IP addresses to create the illusion that the addresses were not owned by a single company, using as many as 150 different credit cards to buy tickets, registering for fan clubs under fake names, creating a voicemail system with as many as 1,000 different telephone numbers, renting a mail drop in Las Vegas, renting real estate under an assumed name, and lying to lessors about the nature of their business. (Superseding Indict. Count 1, ¶¶ 14-16, 19, 20, 35-37.)

Second, the indictment sufficiently charges that Wiseguys had the specific intent to defraud the online ticket vendors. First, the alleged deceptive tactics in themselves suggest that the defendants knew what they were doing was wrong. Language in the indictment cites to the defendants' correspondence with each other and with third parties to demonstrate intent to defraud. According to the indictment, the defendants talked about pursuing "non-human" means of buying tickets and finding backdoors at online ticket vendors' websites. (Superseding Indict. Count 1, ¶ 43.) They are charged with discussing the use of "hacks" and breaking CAPTCHA challenges, ignoring Ticketmaster's cease and desist requests, and using tactics like the voicemail system to divert Ticketmaster's efforts to track them down. (Superseding Indict. Count 1, ¶¶ 44, 46.) The indictment also states that Wiseguys also told their employees to keep quiet about what the company did and discussed using "stealth protocol" to go undetected. (Superseding Indict. Count 1, ¶ 47.) Moreover, the indictment alleges that Wiseguys stated that after undermining Ticketmaster's goodwill and position as an exclusive ticket distributor, it intended to become a vendor in the primary market for tickets and attract Ticketmaster's

customers by providing better protection against scalpers. (Superseding Indict. Count 1, ¶¶ 41-42.)

Third, the indictment adequately charges that Wiseguys used interstate wire communications to further their scheme. To wit, counts 27-36 allege that Wiseguys's responses to CAPTCHA challenges and automated ticket purchases generated by CAPTCHA Bots for ten sets of Bruce Springsteen tickets constitute the use of interstate wire communications.

(Superseding Indict. Counts 27-36, ¶ 2.) Counts 37-43 allege that seven emails between the defendants and various individuals regarding Wiseguys' business operations constitute the use of interstate wire communications. (Superseding Indict. Counts 37-43, ¶ 2.)

Finally, the indictment charges that the object of Wiseguys's scheme was to deprive the online ticket vendors of (1) their right to be the exclusive distributor of tickets, (2) their right to define the terms of sale for tickets by refusing to sell to people who use automated programs, and (3) the goodwill value of providing event tickets to the public. (Superseding Indict. Count 1, ¶ 2(c).)

This has led to one of the more hotly debated points in the defendants' motion. While the government describes the online ticket vendors' interests as valuable property rights and this case as a "classic wire fraud case" (Oral argument transcript 28:6-7), the defendants label the government's theory as the tail wagging the dog of secondary-market regulation.

The case law mirrors the opposing positions taken by the parties. While the property right at issue in a wire fraud indictment need not be a tangible one, *United States v. Henry*, 29 F.3d 112, 115 (3d Cir. 1994), the defendants cite to several cases that they claim stand for the proposition that the particular intangible rights asserted by the government in this case are not property rights for purposes of the wire fraud statute. For instance, in *Henry*, the Third Circuit

held that competing banks' right to a fair bidding opportunity to be the depository for toll bridge revenues was not a property right. *Id.* In *United States v. Bruchhausen*, the Ninth Circuit held that a manufacturer's interest in the post-sale destination of its products did not constitute a property right under the wire fraud statute, 977 F.2d 464, 467–68 (9th Cir. 1992), and in *United States v. Alkaabi*, the Third Circuit held that a testing service's interest in maintaining the integrity of its testing process did not constitute a property right. 223 F. Supp. 2d 583, 590 (D.N.J. 2002).

On the other hand, the government points out that a hallmark of a property right is exclusivity, *United States v. Carpenter*, 484 U.S. 19, 26 (1987), and the property right asserted here is tied to the online ticket vendors' interest in being the exclusive distributor of tickets for a given event. Further, in *United States v. Al Hedaithy*, the Third Circuit held that a testing service had a property right in controlling who could take its exam and receive a score report, 392 F.3d 580, 603 (2004), and in *United States v. Alsugair*, the court held that a testing service had a property right in its goodwill. 256 F. Supp. 2d 306, 316 (D.N.J. 2003).

At the motion to dismiss stage, it would be premature for this Court affirmatively to cast its lot with one theory over the other, especially given the broad range of factual situations reflected in the cases cited in the parties' briefs, which are more numerous than those discussed here. For one thing, a court's analysis of a motion to dismiss an indictment must not be converted into a summary trial on the evidence. *United States v. Delle Donna*, 552 F. Supp. 2d 475, 482 (D.N.J. 2008) (“[A]t this stage of the proceedings the indictment must be tested by its sufficiency to charge an offense’ rather than by whether the ‘charges have been established by the evidence.’” (quoting *United States v. Sampson*, 371 U.S. 75, 76, 78–79 (1962))); *United States v. Miller*, 694 F. Supp. 2d 1259, 1267 (M.D. Ala. 2010) (court could not decide, on motion

to dismiss indictment, whether defendant was a “sex offender” within the meaning of a statute because such decision would require the court to look beyond the face of the indictment and rule on the merits). It suffices now to determine whether the government has charged a required element of wire fraud, and it has. Whether the government’s theory is correct is properly decided after it has offered its proofs. The Court’s direct response to the defendants’ strenuous arguments about property rights is simply that, the legal determination of whether the online ticket vendors’ interests alleged constitute property rights under the wire fraud statute is so bound up with the facts of the case that a decision at this stage is premature. *See United States v. Shabbir*, 64 F. Supp. 2d 479, 480 (D. Md. 1999); *United States v. Nanz*, 471 F. Supp. 968, 972 (D. Wis. 1979) (“Trial of the merits of [the] charges would not only be of assistance, but would be indispensable to the proper resolution of the motion.”). It is worth noting that most of the cases cited by both the government and the defense were decided on appeal from a conviction, and one was actually a civil case decided at the summary judgment stage. Here, the alleged facts have not been developed enough for the Court to determine how the online ticket vendors conduct their businesses so as to make a considered judgment about the nature of the property rights they allegedly possessed. On its face, however, the indictment sufficiently specifies property rights that Wiseguys allegedly targeted, such that it must survive the defendant’s motion to dismiss.

#### **IV. The CFAA Counts:**

1. Counts 2 through 10: Obtaining Information from a Protected Computer, 18 U.S.C. §§ 1030 (a)(2)(C) and (c)(2)(B)(i)

Counts 2 through 10 of the indictment charge that defendants Lawson, Kirsch and Stevenson knowingly and intentionally accessed computers without authorization and exceeded authorized access, and using an interstate communication, obtained information from protected computers used in and affecting interstate and foreign commerce and communication, for the purpose of commercial gain. In so doing, the Indictment charges a crime under CFAA § 1030 (a)(2)(C), which prohibits intentionally accessing a computer without authorization or exceeding authorized access, and thereby obtaining information from any protected computer.

The crimes charged under the CFAA—including the two additional CFAA violations alleged in counts 11 to 26—center on the defendants’ alleged unauthorized access of Ticketmaster’s computer network. Throughout their briefs and at oral argument, both the government and the defendants have fiercely contested what constitutes “unauthorized access” for the purpose of a prosecution under the CFAA. The central and recurring question is whether the scheme and conduct alleged here is merely an egregious breach of contract based on violations of the terms of service on Ticketmaster’s website, or something criminal. Defendants assert that the indictment “unambiguously depend[s] upon alleged breaches of contract to establish criminal liability.” (Def. Reply Br. 5.) The government insists that defendants’ conduct amounted to a crime.

The Court is satisfied that the indictment sufficiently alleges the elements of unauthorized access and exceeding authorized access under the CFAA, and sufficiently alleges conduct demonstrating defendants’ knowledge and intent to gain unauthorized access.

The indictment alleges a number of actions taken by defendants to defeat code-based security restrictions on Ticketmaster’s websites. (Although the government’s briefs speak of

unauthorized access of the websites of Online Ticket Vendors in general, the indictment's CFAA charges in counts 2 through 26 reference only the network belonging to Ticketmaster.) A non-exhaustive list of the steps defendants allegedly took to defeat Ticketmaster's code-based security measures includes: circumventing Proof of Work protections; writing automated software to defeat CAPTCHA (itself an extensive process which allegedly involved opening thousands of connections at once and using CAPTCHA Bots to respond to CAPTCHA challenges in fractions of a second); employing optical character recognition to defeat CAPTCHA challenges; testing the vulnerability of security encryption to get directly to "Buy Pages"; and implementing "hacks" and using "backdoors" to enable automated programs to purchase tickets. The defendants also allegedly disregarded cease-and-desist letters and hired programmers, including "contract hackers," to defeat difficult security restrictions. (*See* Superseding Indict. Count 1 ¶¶ 35–40.)

The indictment also sufficiently pleads the other elements of obtaining information from a protected computer under § 1030. The protected computers referenced in the statute are described in the indictment as Ticketmaster's network, which is used in interstate commerce and communication. The elements of commercial advantage and private financial gain are pleaded as 10 separate purchases of tickets for resale to concerts and sports events in 2006 and 2007. (*Superseding Indict. Counts 2 through 10 ¶ 2.*) Finally, the indictment alleges that the "information" obtained by defendants from Ticketmaster's website was a seat-map "built" by CAPTCHA Bots "to seize a number of prize seats," which Wiseguys employees then would "cull through" in order to select and purchase the best ones. (*Superseding Indict. Count 1 ¶¶ 22–25.*)

The Court notes and must take seriously the arguments advanced by the defendants, as well as those made by Amici, regarding whether the unauthorized access alleged here amounts to contract-based violations of Ticketmaster's terms of service that are actionable under civil laws. The Court is aware, for example, that the investigation of Wiseguys, and ultimately these defendants, began after a civil case was successfully prosecuted by Ticketmaster. *See Ticketmaster LLC v. RMG Technologies*, 507 F. Supp. 2d 1096 (C.D. Cal. 2007). Courts have differed over what constitutes unauthorized access under the CFAA and where the line falls between a civil and criminal violation of the statute. Defendants point to *United States v. Drew*, in which a district court dismissed the indictment against a defendant who had been found guilty of a misdemeanor violation of the CFAA for unauthorized access based solely on the defendant's "conscious breach of a website's terms of service." *United States v. Drew*, 259 F.R.D. 449, 467 (C.D. Cal. 2009). To hold otherwise, the *Drew* court stated, would be to transform § 1030 (a)(2)(C) into a law that violates the void for vagueness doctrine by affording "too much discretion to the police and too little notice to citizens who wish to use the [Internet]." *Id.* at 467 (quoting *City of Chicago v. Morales*, 527 U.S. 41, 64 (1999)). Defendants here go further and argue that, under the government's theory, a teenager hypothetically could be prosecuted under the CFAA for violating the age requirement restrictions in the terms of service when using a search engine like Google.

But, as the government goes to pains to stress, and as the indictment makes clear, the unauthorized access charges at the heart of this indictment involve allegations of breaches of both contract- and code-based restrictions. In *Drew*, the conduct charged did not involve allegations of circumvention of code-based restrictions. And significantly, the *Drew* court's decision to dismiss the indictment came *after* trial, which allowed for the full presentation of all

the government's proofs and a development of the factual record in what admittedly is a technology-intensive and unsettled area of the law. This Court is satisfied that a full presentation of the government's proofs is required to determine if the defendants' arguments ring true that the "code-based restrictions . . . are red herrings . . . [and] are inextricably intertwined with the vendors' terms of use." (Def. Reply 3.) For now, the indictment sufficiently alleges conduct supporting the government's theory of distinct code- and contract-based violations, and the government is entitled to the opportunity to fully offer its evidence, subject to cross-examination, as to why the conduct at issue here is criminal. In this case, the facts and the law are so closely related that further development of the record will shed light on crucial questions, such as what exactly the defendants did, how the alleged code-based restrictions worked, and whether the defeat of CAPTCHA challenges and circumvention of Ticketmaster's security measures is indeed distinct conduct from the terms of service violations described in *Drew*. It is only at that point that the Court can examine and rule on the defense theory that the CFAA and wire fraud counts are inextricably entwined, and so if the CFAA counts fall, so must the wire fraud counts.

Defendants also make a vagueness challenge. But as the Supreme Court has noted, "vagueness challenges to statutes which do not involve First Amendment freedoms must be examined in light of the facts of the case at hand." *Drew* at 464 (citing *United States v. Mazurie*, 419 U.S. 544, 550 (1975)). Here, the factual record before the Court remains undeveloped.

In addition, defendants argue that the indictment fails to identify the "information" that defendants "obtained" under counts 2 through 10. They contend that the only things they obtained were tickets, that the "information" at issue was publicly available to "every other member of the public that uses the online vendors' public websites" (Def. Br. 17), and that

“[c]omprehensive seating information was available from numerous other sources.” (Def. Reply 10.) In effect, defendants argue, the government seeks to criminalize obtaining publicly available “information” and, in the process, the government will increase “exponentially” the universe of federal crimes. (Def. Moving Br. 18.) The government, however, argues that the information obtained included a detailed map of “available premium seats for each Event” that was unavailable to individual users and “confidential in the aggregate.” (Opp’n Br. 30–32.) These clashing characterizations of what exactly defendants saw and whether it constituted “obtaining information” within the meaning of the CFAA highlights yet again the need for further factual development of the record. Applying the analysis that is proper at this stage, the Court finds that the indictment does allege sufficient facts to satisfy the element of obtaining information.

2. Accessing a protected computer with intent to defraud, 18 U.S.C. §§ 1030 (a)(4) and (c)(3)(A):

Counts 11 through 20 of the indictment allege that defendants Lawson, Kirsch and Stevenson knowingly, and with intent to defraud, accessed Ticketmaster’s computer network and exceeded authorized access, and by doing so furthered the intended fraud and obtained things of value.

The “things of value” obtained, according to the indictment, were tickets to a July 28, 2008 Bruce Springsteen concert at Giants Stadium. (Superseding Indict. Counts 11 through 20 ¶

2.) The key contested areas in counts 11 through 20 are the issues of unauthorized access (discussed above in counts 2 through 10), and the element of “intent to defraud.”

The “intent to defraud” is demonstrated in the indictment by the defendants’ alleged scheme to, among other things, pose as individual buyers and deceive Ticketmaster into selling tickets to defendants that Ticketmaster otherwise would not sell. (*See e.g.* Superseding Indict. Count 1 ¶¶ 14–21.)

Defendants argue that the charged fraud and access violations are essentially one in the same (Def. Moving Br. 18), while the government contends that the unauthorized access and the fraud are alleged distinctly. According to the government, the unauthorized access consisted of circumventing code restrictions, defeating IP blocking and other conduct. The fraud, the government argues, consisted of the overall scheme to deprive Ticketmaster of its rights to exclusivity and to dictate terms of sale and also of its good will. (Opp’n 28–29.)

The Court finds that the indictment sufficiently pleads facts demonstrating intent to defraud and that the government is entitled to fully present its evidence on this question.

3. Transmitting a program that causes unauthorized damage, 18 U.S.C. § 1030 (a)(5)(A)

Counts 21 through 26 allege that defendants Lawson, Kirsch and Stevenson knowingly caused the transmission of programs, information, code, and commands, and as a result of such conduct, intentionally caused damage without authorization to protected computers, in and affecting interstate and foreign commerce and communication, thereby causing loss to one or more persons during a 1-year period aggregating at least \$5,000 in value.

The indictment pleads a knowledge element demonstrated by allegations that, among other things, defendants discussed and implemented means to purchase tickets automatically without responding to CAPTCHA challenges; to defeat CAPTCHA using optical character

recognition; and to update their CAPTCHA answer base when they encountered new CAPTCHA challenges. The pleaded “transmission” involves defendants’ responses to CAPTCHA challenges and automated ticket purchase requests for six different concerts and other events. (Superseding Indict. Counts 21 through 26 ¶ 2.) The pleaded damage element of at least \$5,000 involves defendants’ blocking out authorized, individual users from the website by using CAPTCHA Bots, which “seized” the best seats for events and made those seats unavailable for purchase or consideration until their release by a Wiseguys employee. (*See* Superseding Indict. Count 1 ¶¶ 2, 25, 56.)

Defendants argue that the conduct at issue in the damage allegation essentially is identical to the conduct underlying the unauthorized access allegations, that the government again is seeking to “criminalize a breach of contract,” and that the indictment as a result contains no valid damage allegation. (Def. Reply 11.) While these arguments fit logically into the defendants’ overall argument that this is a civil and not a criminal matter, the Court is satisfied that, for the purposes of deciding the motion to dismiss, the indictment sufficiently pleads the damage element of counts 21 through 26.

## **V. Conclusion**

This case poses a good example of the complexity of criminal prosecutions under statutes written specifically about, for, and as a result of the Internet—and more, insofar as the parties are wrestling with the always perplexing issue of what constitutes criminal fraud. The challenge is to harmonize the CFAA and the government’s charges of crime in the highly specialized marketplace the defendants operated in, with traditional and, indeed, sacrosanct tenets of the criminal law. The Court—and the parties as well—will be in a far better position to meet that

challenge after the government presents its evidence. The motion to dismiss the Superseding Indictment is denied.

/s/Katharine S. Hayden

Katharine S. Hayden, U.S.D.J.