RECOMMENDED FOR FULL-TEXT PUBLICATION
Pursuant to Sixth Circuit Rule 206

File Name: 09a0394p.06

UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellee,*	]	
	]	No. 09-3053
v.	>	
GABRIEL SCHAFFER, *Defendant-Appellant.*	]	

Appeal from the United States District Court
for the Northern District of Ohio at Cleveland.
No. 08-00097-002—Patricia A. Gaughan, District Judge.

Argued: July 29, 2009

Decided and Filed: November 12, 2009

Before: BATCHELDER, Chief Judge; DAUGHTREY, Circuit Judge; VAN TATENHOVE, District Judge.*

COUNSEL

ARGUED: Richard G. Lillie, LILLIE & HOLDERMAN, Cleveland, Ohio, for Appellant. Daniel R. Ranke, ASSISTANT UNITED STATES ATTORNEY, Cleveland, Ohio, for Appellee. **ON BRIEF:** Richard G. Lillie, Gretchen A. Holderman, LILLIE & HOLDERMAN, Cleveland, Ohio, for Appellant. Daniel R. Ranke, ASSISTANT UNITED STATES ATTORNEY, Cleveland, Ohio, for Appellee.

OPINION

VAN TATENHOVE, District Judge. A grand jury charged Gabriel Schaffer with conspiracy to commit computer fraud and to transport stolen property interstate. Upon Schaffer's motion, the district court dismissed the count charging interstate

---

*The Honorable Gregory F. Van Tatenhove, United States District Judge for the Eastern District of Kentucky, sitting by designation.

transportation of stolen property but denied that motion in all other respects. Schaffer then entered a conditional guilty plea, admitting that he conspired to commit computer fraud. On appeal, Schaffer contends that the indictment should be dismissed due to the omission of essential elements, violation of the statute of limitations, pre-indictment delay, and entrapment as a matter of law. Because the district court correctly rejected each of these arguments, we AFFIRM.

I.

Gabriel Schaffer and his co-defendant Dana Arvidson fell victim to a government sting operation in which they conspired to obtain military secrets and laser missile technology from what they believed was a Department of Defense ("DOD") contractor. The relevant events began on July 31, 2002, when an undercover FBI agent ("UC1") met Arvidson at a hotel in Independence, Ohio, and advised him that he wanted to outsource wireless computer security services to a local Cleveland company. During that meeting, Arvidson indicated that he was the sole owner of SecureNet and had developed proprietary technology which allowed him to intercept wireless computer network traffic from a greater range. Arvidson stated that he had intercepted communications from approximately 500 wireless computer networks in Cleveland, including sensitive information and passwords for employee accounts. He further claimed that he could "spoof" MAC (media access control) addresses, obtain access to computer networks via a WAP (wireless application protocol), and "break" the encryption used to protect the privacy of communications on wireless computer networks.

On October 10, UC1 and Arvidson met in Cleveland. During this meeting, UC1 told Arvidson that he knew an individual in Chicago who was interested in locating someone with expertise in wireless computer networks to obtain information from a DOD contractor. Later that month, Arvidson advised UC1 that "we have developed some new technology that allows us to be more under the radar," and explained that he could now intercept communications "passively" from a significant distance. Arvidson indicated that he was still interested in the "side project."

During the next meeting, on December 3, after Arvidson reiterated his interest in the "side project," UC1 told Arvidson that the target was in Texas and UC1 wanted to "bring up a couple of things . . . to give you (Arvidson) a chance to back out." UC1 then told Arvidson that the target information was "laser missile technology type stuff . . . anything you intercept out of the air . . . is probably going to be illegal . . . it's gonna be a problem if we were to get caught." Arvidson replied, "I'm looking at this as a security audit just like any other security audit . . . capturing data . . . I don't really want to know a whole ton about what I'm capturing . . . I'll be happy to do the job, just as we would any other job." UC1 told Arvidson, "I know you developed a way that can't be traced with this passive technique but if for some reason it did get traced, people can get in trouble. I just want you to know that." Arvidson replied, "Absolutely, well that's the risk premium . . . I'm with you 100 percent."

The next day, Arvidson called UC1 and asked him numerous questions about the location of the target computer system. UC1 gave Arvidson some specifics regarding the company's location and advised that an employee of the target company logged onto the network every night through a wireless access point using his user ID and password. He further explained that there was no guarantee the employee would actually upload files. Arvidson advised UC1 that his first step would be to "go in and decrypt it" and that if he would be "actively infiltrating with the person's password, that changes my risk level." Arvidson stated that if "I do it passively the risk level is, I mean it's high but it's relatively low, if I actually go in and compromise something, I'm still willing to do it but my price is going to be higher." About a month later, Arvidson sent UC1 an email with a list of technical questions about the DOD contractor's computer network.

On February 12, 2003, UC1 and another undercover FBI agent ("UC2") met with Arvidson and Schaffer at a Cleveland hotel. UC2 made it clear that his client was interested in "stealing military secrets and laser missile technology" from a "DOD contractor in El Paso, TX." During this meeting, Schaffer used a notebook computer to demonstrate how their equipment could intercept wireless computer network traffic. Arvidson and Schaffer then detailed how they could similarly intercept wireless

computer network traffic from the DOD contractor, including an employee's login user ID and password. They further explained that after intercepting this information, they would log into the DOD contractor's computer network using the intercepted user ID and password, imitate that employee's physical computer system so they could not be traced, locate the target information, and download it to their computer.

Arvidson told UC2 that they wanted "25" up front for both him and Schaffer, and "50" after completion of the theft. UC2 indicated that he would need a sample of the stolen information to show his client in Chicago. If his client was happy with the stolen information, UC2 would travel to Cleveland and pay the total fee in exchange for all the stolen data. In the event they were unable to acquire the target information in El Paso, UC2 said that he would pay them an hourly rate of $150 per hour for their time. UC2 would also pay for their airfare to and lodging in El Paso. Arvidson and Schaffer agreed.

The trip to El Paso was planned for the last week of February. UC2 told Arvidson and Schaffer that he would mail the plane tickets to Arvidson. Arvidson provided UC2 with a business card that depicted an address for his other Cleveland business, then Schaffer wrote "Gabe Schaffer" on the back of Arvidson's business card.

During a telephone call with Arvidson on February 18, UC1 clarified that Arvidson's fee for the theft, if successful, would be $100,000. One week later, UC2, Arvidson, and Schaffer met in an El Paso, Texas, hotel room which had line-of-sight access to the purported DOD contractor's office. Arvidson and Schaffer connected three antennas to their notebook computer in their attempt to locate the DOD contractor's wireless computer network. After they located the wireless network, Arvidson and Schaffer immediately began intercepting network communications, including the user ID and password of a purported DOD contractor employee. Once the purported employee logged off, Arvidson and Schaffer used the intercepted user ID and password to log onto the purported contractor's network. Arvidson and Schaffer also "spoofed" the purported employee's physical computer system so that their notebook computer would appear to be the employee's computer.

Arvidson and Schaffer downloaded over 6,000 electronic files from two different computer systems on the purported DOD contractor's computer network. Arvidson explained to UC2 that the data on one computer system was contained in sub-directories of a main directory called "proprietary." Arvidson and Schaffer advised that those sub-directories had names like "air force," "army," "navy," "wmsr," and "marketing-data." They also advised that the data stolen from the other computer system was contained in a directory called "000 Sensitive."

Upon completion of the theft, Arvidson and Schaffer copied the stolen data from their notebook computer to an external hard drive, which they encrypted. Arvidson and Schaffer told UC2 that they did not want to get caught with the information, so they gave the external hard drive to UC2. They told UC2 that they would provide the "pass-key" to decrypt the external hard drive when they received the $100,000 payment. Arvidson indicated that he would provide UC2 with a CD-ROM disk containing the pass-key needed to decrypt the external hard drive at their next meeting.

Between March 3 and 13, 2003, UC2 and Arvidson corresponded via email and arranged a meeting wherein Arvidson would provide the decryption key in exchange for $100,000. On March 19, UC1, UC2, Arvidson, and Schaffer met at a Cleveland hotel to exchange $100,000 for the decryption key to the external hard drive. UC2 brought the external hard drive and tendered the $100,000. Schaffer wrote a list of instructions for decrypting the external hard drive. Arvidson provided UC2 with a CD-ROM to be used in conjunction with Schaffer's instructions for decrypting the hard drive and demonstrated the decryption process.

Almost five years later, on February 27, 2008, a grand jury indicted Schaffer and Arvidson. After requesting and obtaining a continuance of the trial date, Schaffer filed several pre-trial motions including a motion for a bill of particulars and a motion to dismiss. He sought dismissal of the indictment based upon pre-indictment delay, statute of limitations, and entrapment. The district court granted part of Schaffer's motion and dismissed the portion of the indictment related to the interstate transportation of stolen property. In all other respects, the district court denied Schaffer's motion to dismiss.

Schaffer then filed a second motion for a bill of particulars.[1] However, before the district court ruled on either of his motions for a bill of particulars, Schaffer entered a guilty plea. Pursuant to his written agreement, Schaffer's plea was conditional, preserving his right to appeal the district court's denial of his motion to dismiss. On January 12, 2009, the district court sentenced Schaffer to three years probation with six months home confinement and ordered him to pay a $5,000 fine and $100 special assessment. As contemplated by the plea agreement, Schaffer appealed.

II.

A.

In his first argument, Schaffer challenges both the factual specificity and sufficiency of the indictment. Schaffer contends that the indictment failed to give him notice of the nature and cause of the allegations against him or an ability to prepare a defense. He argues, as he did in his motions for a bill of particulars, that the indictment lacks details or specifics concerning the computer fraud charge. Schaffer also asserts that the indictment omits essential elements depriving the district court of jurisdiction.

Generally, a valid guilty plea "bars any subsequent non-jurisdictional attack on the conviction." *United States v. Martin*, 526 F.3d 926, 932 (6th Cir. 2008) (quoting *United States v. Pickett*, 941 F.2d 411, 416 (6th Cir. 1991)). Pursuant to Fed. R. Crim. P. 11(a)(2), a defendant may, with the approval of the court and consent from the government, enter a conditional plea of guilty "reserving in writing the right, on appeal from the judgment, to review of the adverse determination of any specified pretrial motion." This rule places an "affirmative duty" on the defendant to preserve any issues collateral to the determination of guilt or innocence by specifying them in the plea itself. *Pickett*, 941 F.2d at 416. "[I]n the absence of a court-approved reservation of issues for appeal, [a defendant pleading guilty] waives all challenges to the prosecution except those going to the court's jurisdiction." *Id.* (citing *Hayle v. United States*, 815 F.2d 879, 881 (2d Cir. 1987)).

[1]It does not appear that the United States responded to either motion.

Here, the parties disagree over the scope and effect of the plea agreement as to whether Schaffer adequately preserved his right to appeal certain issues. Schaffer claims that he properly preserved his challenge to the factual specificity of the indictment in a specific paragraph in his plea agreement and through a reference to his motions for a bill of particulars in a footnote in his motion to dismiss. Despite Schaffer's arguments, we hold that he did not properly preserve his factual specificity argument.

Paragraph Q of the plea agreement states that "[b]y stipulating to the facts contained in paragraphs O and P, the Defendant does not waive his right to contest, on appeal of this Court's Opinion and Order of August 4, 2008, the relevance and applicability of such conduct to the indicted-offense." That paragraph makes no mention of Schaffer's motions for a bill of particulars or the issues raised therein. There is nothing in either of the referenced paragraphs that concerns the factual specificity of the indictment. Instead, this paragraph appears to be related to Schaffer's statute-of-limitations argument. Paragraphs O and P of the plea agreement describe the March 2003 meeting during which the encryption key was exchanged for $100,000. As set forth in a separate argument, Schaffer maintains that the March 2003 meeting cannot be an overt act in furtherance of the conspiracy because the objective of the conspiracy (*i.e.*, obtaining the electronic files) had already been accomplished. Thus, despite his stipulation to those facts, it appears that Schaffer essentially reserved his right to challenge the "relevance and applicability" of that final meeting as an overt act. Paragraph Q of the plea agreement does not, however, allow Schaffer to contest the factual specificity of the indictment.

Schaffer also maintains that he can contest the factual specificity of the indictment because he specifically preserved his right to challenge the denial of his motion to dismiss. In a footnote in that motion, Schaffer indicated that he reserved his right to challenge the specificity of the indictment and, in so doing, referenced his motions for a bill of particulars. Schaffer's attempt to reserve this argument appears to be conditioned upon his "receipt of such Bill of Particulars and detailed charging information from the Government." However, reserving the right to raise an argument

and actually presenting that argument are two different things. Schaffer merely reserved his right to "challenge the elements of charges filed and the details underlying the Indictment," but he did not actually present that argument in his motion to dismiss. The district court's order denying his motion, therefore, did not address that argument and cannot be deemed an adverse ruling on that issue.[2] Schaffer's conditional guilty plea, allowing him to challenge the denial of all issues raised in his motion to dismiss, did not preserve his right to contest the specificity of the indictment to this court. *See Pickett*, 941 F.2d at 416. That argument was waived because it is a non-jurisdictional challenge that was not specifically preserved in his plea agreement.

B.

Schaffer also challenges the sufficiency of the indictment. His failure to raise this argument in the district court or preserve it in his plea agreement is of no consequence because, even if presented for the first time on appeal, claims of jurisdictional defects in the indictment are not waived. *See United States v. Hart*, 640 F.2d 856, 857 (6th Cir. 1981). But when an indictment is not challenged until appeal, as in this case, the indictment must be liberally construed in favor of its sufficiency. *See United States v. Gatewood*, 173 F.3d 983, 986 (6th Cir. 1999) (citation omitted). Moreover, to raise a successful challenge to the district court's jurisdiction, a defendant who enters a guilty plea must establish that the face of the indictment failed to charge the elements of a federal offense. *See United States v. Martin*, 526 F.3d 926, 934 (6th Cir.) (citations omitted), *cert. denied*, ___ U.S. ____, 129 S. Ct. 305 (2008). Schaffer fails to make such a showing here.

An indictment must include "a plain, concise, and definite written statement of the essential facts constituting the offense charged." Fed. R. Crim. P. 7(c)(1). An

[2]The district court noted that the defendants argued for the first time in their reply brief that the computer at issue was not a "protected" computer and claimed to "reserve their right" to challenge that issue. They further alleged that the indictment failed to indicate "what and how 'computer fraud' is being charged." Noting that it was unclear whether the defendants were even seeking dismissal on these grounds, the district court concluded that given the defendants' failure to develop any argument regarding these issues and the fact that they were raised for the first time in their reply brief, dismissal was not appropriate.

indictment is generally sufficient if it "fully, directly, and expressly . . . set[s] forth all the elements necessary to constitute the offense intended to be punished." *United States v. Douglas*, 398 F.3d 407, 411 (6th Cir. 2005) (internal citation and quotation marks omitted). In particular, the indictment must: (1) "set out all of the elements of the charge[d] offense and must give notice to the defendant of the charges he faces[,]" and (2) "be sufficiently specific to enable the defendant to plead double jeopardy in a subsequent proceeding, if charged with the same crime based on the same facts." *Id.* at 413 (internal citation omitted).

Here, the defendants were charged with conspiracy to commit computer fraud in violation of 18 U.S.C. § 371 and 18 U.S.C. § 1030(a)(4).[3] To establish a violation of 18 U.S.C. § 371, the government must allege and prove "an agreement among the conspirators to commit an offense attended by an act of one or more of the conspirators to effect the object of the conspiracy." *United States v. Falcone*, 311 U.S. 205, 210 (1940); *see also United States v. Beverly*, 369 F.3d 516, 532 (6th Cir. 2004). The indictment satisfied these requirements. It alleged that the defendants did "unlawfully, knowingly, and intentionally combine, conspire, confederate, and agree together . . . to commit computer fraud." More specifically, the indictment charged Schaffer with "conspir[ing] to unlawfully access a computer used by a Department of Defense contractor in El Paso, Texas, in order to fraudulently obtain military secrets and laser missile technology . . . ." The indictment also set forth the objective of the conspiracy, the role played by each defendant, the overt actions taken in furtherance of the conspiracy, and the means used to accomplish it. By setting forth the elements of conspiracy and by referencing 18 U.S.C. § 1030(a)(4), the indictment satisfied the requirements of Fed. R. Crim. P. 7(c)(1) and notified Schaffer that he was accused of conspiring to knowingly and with intent to defraud, access a protected computer without authorization to obtain something of value. Thus, the indictment contained sufficient

[3]Title 18 U.S.C. § 1030(a)(4) is violated when one "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value."

information to invoke federal jurisdiction and clearly contained on its face all of the elements necessary to state a federal offense.

Although couched as a jurisdictional argument, Schaffer at least impliedly contends that the conspiracy in this case is a legal impossibility. He notes that the "fake computer accessed by [the defendants] contained bogus information, was located in the pretend office of an alleged defense contractor, was *not* for access exclusively by a financial institution, was *not* used in interstate of foreign commerce or communication, and was *not* used in a manner that affected interstate or foreign commerce or communication." According to Schaffer, the absence of any of these elements precluded the district court's jurisdiction. Schaffer's argument is misplaced.

The basis of the conspiracy charge is the agreement to commit the unlawful act, and not the unlawful act itself. Because the "illegality of the agreement does not depend upon the achievement of its ends," it is irrelevant that it may have been objectively impossible for the conspirators to commit the substantive offense." *United States v. Yang*, 281 F.3d 534, 544 (6th Cir. 2007) (quoting *United States v. Hsu*, 155 F.3d 189, 203 (3d Cir. 1998)). Indeed, it is the mutual understanding or agreement itself that is criminal, and whether the object of the scheme actually is, as the parties believe it to be, unlawful is irrelevant. *See id.* To the extent that Schaffer's jurisdictional argument is based on a claim of legal impossibility, it must fail.

C.

Schaffer next argues that the indictment should have been dismissed because the five-year statute of limitations expired before the indictment was filed. In this case, the indictment was returned on February 27, 2008. According to Schaffer, the last overt act in furtherance of the conspiracy occurred on February 25, 2003, when the defendants traveled to El Paso and obtained the data from the computer system. Because Schaffer also points to that date as the completion of the conspiracy's objective, he contends that the statute of limitations ran prior to the filing of the indictment.

"[N]ormally, the date of the last overt act in furtherance of the conspiracy alleged in the indictment begins the clock for purposes of the five-year statute of limitations." *United States v. Grenoble*, 413 F.3d 569, 574 (6th Cir. 2005) (quoting *United States v. Smith*, 197 F.3d 225, 228 (6th Cir. 1999)); *see also* 18 U.S.C. § 3282. Thus, in the statute of limitations context, "the crucial question . . . is the scope of the conspiratorial agreement, for it is that which determines both the duration of the conspiracy, and whether [an] act . . . may properly be regarded as in furtherance of the conspiracy." *Grunewald v. United States*, 353 U.S. 391, 397 (1957).

Here, the indictment described two overt acts that occurred less than five years before the indictment was returned. First, the indictment alleged that between March 3 and March 13, 2003, an undercover agent corresponded with Arvidson via email to arrange a meeting wherein Arvidson "would provide the decryption key in exchange for $100,000." The indictment also alleged that on March 19, Schaffer and Arvidson met undercover agents at a Cleveland hotel to deliver the decryption key to the external hard drive, which contained the information illegally obtained from the purported DOD contractor's network, in exchange for $100,000.

While Schaffer would have the conspiracy end with the interception of the computer data, neither the record nor common sense supports such a limited interpretation. Nothing in the record suggests that Schaffer agreed to steal military secrets and missile technology for other than a remunerative purpose. Rather, the scope of the conspiracy clearly contemplated the monetary payment in exchange for the data that the defendants obtained. The specific terms of that payment were discussed multiple times. Initially, Arvidson had requested an up-front payment of $25,000 for both him and Schaffer, and $50,000 after completion of the theft. However, it was later agreed that the fee for the theft would be $100,000, if successful. In addition, after Schaffer and Arvidson copied the stolen data to an external hard drive, encrypted it, and gave it to the undercover agent, they explained that they would provide the "pass-key" to decrypt the hard drive when they received the $100,000 payment.

Under these facts, the defendants' participation in the conspiracy was contingent upon the payment. Schaffer and Arvidson essentially negotiated their fee for obtaining the information. By encrypting the hard drive, they maintained constructive control of the stolen information and could prevent others from accessing it until they received payment for their services. The conspiracy in this case, therefore, continued until the anticipated payment for the defendants' efforts was received. Consequently, the defendants' efforts in setting up and attending the meeting to exchange the decryption key for the $100,000 payment constitute overt acts in furtherance of the conspiracy. Indeed, "[c]ase law gives ample support to the proposition that payment is an integral and often final term in a conspiracy." *United States v. Fitzpatrick*, 892 F.2d 162, 167 (1st Cir. 1989) (quoting *United States v. Hamilton*, 689 F.2d 1262, 1270 (6th Cir. 1982), *cert. denied*, 459 U.S. 1117 (1983)). Because the indictment was returned within five years of the last act in furtherance of the conspiracy, no statute of limitations violation occurred.

D.

Schaffer argues that the district court erred in failing to dismiss the indictment based upon pre-indictment delay and resulting prejudice. Pre-indictment delay and post-indictment delay present separate issues. The former is governed by the Fifth Amendment, *see United States v. Rogers*, 118 F.3d 466, 475-76 (6th Cir. 1997), while the latter is a Sixth Amendment matter, *see United States v. Graham*, 128 F.3d 372, 374 (6th Cir. 1997). The Sixth Amendment right to a speedy trial does not come into play until "arrest, indictment or other official accusation." *Doggett v. United States*, 505 U.S. 647, 655 (1992). Moreover, the speedy trial clause does not "require the Government to discover, investigate, and accuse any person within any particular period of time." *United States v. Marion*, 404 U.S. 307, 313 (1971); *see also United States v. Loud Hawk*, 474 U.S. 302, 312 (1986). Because Schaffer was neither arrested for violating federal law nor officially accused of doing so prior to his indictment on February 27, 2008, the protections of the Sixth Amendment were not triggered in this case before that date.

Schaffer's claims about pre-indictment delay must therefore be resolved in the context of the Fifth Amendment.

The Supreme Court recognizes that the Due Process Clause of the Fifth Amendment protects against oppressive pre-indictment delay. *See, e.g.*, *Marion*, 404 U.S. at 324-25; *United States v. Lovasco*, 431 U.S. 783, 789 (1983). In this circuit, dismissal for pre-indictment delay "is warranted only when the defendant shows substantial prejudice to his right to a fair trial and that the delay was an intentional device by the government to gain a tactical advantage." *United States v. Greene*, 737 F.2d 572, 574 (6th Cir. 1984) (quoting *United States v. Brown*, 667 F.2d 566 (6th Cir. 1982) (per curiam)).

Schaffer contends that he was prejudiced because his own recollection of what occurred in 2003 had obviously faded five years later. He also asserts that the Government's evidence failed to "include any record of conversations" he had with Arvidson or "any record of their beliefs and understandings at the time regarding the manner, means, method and content of the information they obtained . . . ." Despite these general allegations, Schaffer points to no examples of actual prejudice. He does not contend that he was unable to assist in his own defense, nor does he suggest that witnesses were unavailable or that specific evidence had been lost or destroyed. Simply put, Schaffer falls far short of demonstrating that he was actually and substantially prejudiced by the delay.

Nonetheless, Schaffer, relying on the Supreme Court's decision in *Doggett v. United States*, 505 U.S. 647 (1992), submits that this court should presume prejudice. According to Schaffer, *Doggett* is "dispositive as to the issue of whether there is a presumption of prejudice in circumstances when the Government fails to act within a reasonable time." However, *Doggett*'s application to the situation at hand is limited at best. In *Doggett*, the Supreme Court held that a lengthy post-indictment delay is presumptively prejudicial to the defendant for the purposes of establishing a Sixth Amendment speedy trial claim. *Id.* at 655.

In *Jones v. Angelone*, 94 F.3d 900 (4th Cir. 1996), the Fourth Circuit addressed an argument virtually identical to the one raised by Schaffer. In that case, Jones urged the court to extend the rule of presumptive prejudice in *Doggett* to pre-indictment delays which potentially give rise to claims under the Due Process Clause of the Fifth Amendment. The Fourth Circuit noted that "[t]he Due Process Clause has never been interpreted so as to impose a presumption of prejudice in the event of lengthy pre-indictment delay." *Id.* at 906. Declining to extend *Doggett* beyond the post-indictment, speedy trial realm, the court concluded that "a rule of presumptive prejudice in [the pre-indictment delay] context would be at odds with established Supreme Court authority." *Id.*

Here, like the defendant's argument in *Jones*, Schaffer's contention that prejudice should be presumed is directly contradicted by Supreme Court precedent. The Supreme Court has repeatedly emphasized that, in order to establish a due process violation, the defendant must show that the delay "caused him *actual* prejudice in presenting his defense." *United States v. Gouveia*, 467 U.S. 180, 192 (1984) (emphasis added); *see also Lovasco*, 431 U.S. at 789 ("[P]roof of actual prejudice makes a due process claim concrete and ripe for adjudication, not . . . automatically valid."); *Marion*, 404 U.S. at 326 ("Events of trial may demonstrate actual prejudice, but at the present time appellees' due process claims are speculative and premature.").

On the record before the court, Schaffer has failed to demonstrate that he was actually prejudiced by the delay. Moreover, "the acceptability of a pre-indictment delay is generally measured by the applicable statute of limitations." *United States v. Atisha*, 804 F.2d 920, 928 (6th Cir. 1986), *cert. denied*, 479 U.S. 1067 (1987); *see also Lovasco*, 431 U.S. at 789 (noting that "statutes of limitations, which provide predictable, legislatively enacted limits on prosecutorial delay, provide 'the primary guarantee against bringing overly stale criminal charges'") (citation omitted). Because the indictment in this case was returned within the five-year limitations period, the pre-indictment delay, absent a showing of actual prejudice, was not fatal.

Schaffer's failure to demonstrate actual prejudice makes it unnecessary to decide whether he established that the delay was an intentional device by the government to gain a tactical advantage. *See Greene*, 737 F.2d at 575 (declining to reach prejudice prong where defendant failed to show that delay was an intentional device). Nonetheless, Schaffer also failed to make the requisite showing that the delay was undertaken by the government to gain a tactical advantage over him. The burden is on the defendant to show "that the delay between the alleged incident and the indictment was an intentional device on the part of the Government to gain a decided tactical advantage in its prosecution." *Id.* at 574. Saying that there could be no valid reason for the Government's delay in bringing this case, Schaffer urges us to presume that the delay was for an improper purpose. The applicable standard, however, neither imputes nor presumes an improper purpose where the defendant simply cannot fathom a valid reason for the delay. Rather, it requires Schaffer to demonstrate that the Government "had no valid reason for the delay." *United States v. DeClue*, 899 F.2d 1465, 1468-69 (6th Cir. 1990). Schaffer wholly fails to make such a showing.

E.

In his final argument on appeal, Schaffer contends that the district court erred in failing to dismiss the indictment based upon entrapment. He insists that, at the time of the instant offense, he was a law-abiding young man who had been educated in computer sciences and was clearly not predisposed to any criminal activity. Absent the repeated and continued enticement of the undercover agents, Schaffer maintains, he would have committed no crime.

It is seldom appropriate to grant a pre-trial motion to dismiss based on an entrapment defense, because the defense focuses on a defendant's state of mind, an evidentiary question. *See United States v. Fadel*, 844 F.2d 1425, 1431 (10th Cir. 1988). To warrant dismissal before trial on the ground that the defendant was entrapped as a matter of law, we have held that "the undisputed evidence must demonstrate a 'patently clear' absence of predisposition." *United States v. Harris*, 9 F.3d 493, 498 (6th Cir. 1993) (quoting *United States v. Barger*, 931 F.2d 359, 366 (6th Cir. 1991)); *see also*

United States v. Osborne, 935 F.2d 32 (4th Cir. 1991) (defense of entrapment may only be resolved prior to trial where there is absolutely no evidence to support it).

Here, Schaffer failed to demonstrate a patently clear absence of predisposition. While he presents arguments in support of his entrapment claim, they are not based on undisputed evidence. In denying Schaffer's argument below, the district court appropriately recognized that it "simply [could] not accept statements made in defendant's brief to establish entrapment as a matter of law." The court also noted that testimony and facts must be undisputed and that the court may not choose between conflicting testimony or make credibility determinations. *See United States v. Pennell*, 737 F.2d 521, 534 (6th Cir. 1984). The district court, therefore, concluded that the entrapment issue could not be resolved until after evidence was presented at trial. The court further denied Schaffer's request for an evidentiary hearing, finding that the entrapment defense "is so central to the general issues in the case that holding a hearing solely on entrapment would be tantamount to two trials."

Consistent with the district court's holding, well-established precedent makes it clear that the question of entrapment is generally one for the jury, rather than for the court. *See, e.g., Mathews v. United States*, 485 U.S. 58, 63 (1988) (citation omitted). In related areas, courts discourage the pre-trial disposition of motions to dismiss that are based on defenses requiring fact finding. For example, in *United States v. Knox*, 396 U.S. 77, 78-79 (1969), the district court dismissed an indictment charging the defendant with knowingly and willfully submitting false tax forms. On appeal, the defendant asserted that the federal tax statutes compelled him to submit the false statements because the statutes provided for penalties if he did not file the forms. *See id.* at 81. In reversing the dismissal of the indictment, the Supreme Court concluded that "the question whether Knox's predicament contains the seeds of a 'duress' defense, or perhaps whether his false statement was not made 'willfully' as required by § 1001, is one that must be determined initially at trial." *Id.* at 83. The Court further noted that Fed. R. Crim. P. 12 "indicates that evidentiary questions of this type should not be determined on such a motion." *Id.*

Therefore, we conclude that the district court committed no error in denying Schaffer's motion to dismiss based upon entrapment as a matter of law. To the contrary, the district court correctly held that such an argument is more appropriately addressed after evidence is presented at trial. Whether Schaffer would have been entitled to an entrapment instruction is a question that cannot be answered on the record before this court because Schaffer waived his right to trial by pleading guilty.

III.

For the foregoing reasons, we AFFIRM the denial of Schaffer's motion to dismiss.