16-10516

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

ANASTASIO N. LAOUTARIS,
Defendant-Appellant.

On Appeal from the United States District Court
For the Northern District of Texas
Dallas Division
District Court No. 3:13-CR-386-1

BRIEF FOR THE UNITED STATES

John R. Parker
United States Attorney

J. Nicholas Bunch
Assistant United States Attorney
Texas Bar No. 24050352
1100 Commerce Street, Third Floor
Dallas, Texas 75242-1699
Telephone: (214) 659-8836
nick.bunch@usdoj.gov

Attorneys for Appellee

STATEMENT REGARDING ORAL ARGUMENT

The government does not recommend oral argument. The issues are discrete and adequately addressed in the briefs such that the decisional process would not be significantly aided by oral argument. *See* Fed. R. App. P. 34(a)(2)(C).

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Federal Cases **Page(s)**

Federal Cases (continued) **Page(s)**

Federal Statutes and Rules

Federal Sentencing Guidelines

STATEMENT OF JURISDICTION

This is a direct appeal of a conviction and sentence. The district court had jurisdiction under 18 U.S.C. § 3231. This Court has jurisdiction under 28 U.S.C. § 1291 and 18 U.S.C. § 3742(a). The district court entered judgment on April 15, 2016. (ROA.373.) Laoutaris timely filed a notice of appeal on April 27, 2016. (ROA.380.)

STATEMENT OF THE ISSUES

1. Was the evidence sufficient to convict Laoutaris on Counts One and Two of the Superseding Indictment?

2. Did the district court clearly err in applying a two-level enhancement for obstruction of justice after making specific factual findings of instances of perjury based on the defendant's testimony at trial?

3. Did the district court err in making a reasonable estimate of the lost revenue of the victim as a result of Laoutaris's unlawful intrusions that shut down the firm for multiple days?

STATEMENT OF THE CASE

Defendant-Appellant Anastasio ("Nick") Laoutaris (hereinafter, "Laoutaris") was convicted after a week-and-a-half jury trial of two counts of intentionally causing computer damage, in violation of 18 U.S.C. § 1030(a)(5) and (c)(B)(iv).

1. Between October and December 2001, Locke Lord LLP was the victim of a series of computer hacks causing significant damage and disruption to the firm's business.

October 20, 2011, was a day like no other for Locke Lord L.L.P., an international law firm with its headquarters in Dallas, Texas. (ROA.676-77.) The firm's managing partner, Jerry Clements, woke up in San Francisco, where she was planning to attend a conference for the American College of Trial Lawyers. (ROA.677.) Like all mornings, she opened her laptop and went to check her email. (ROA.677.) Almost immediately, she knew there was a problem: "I hadn't gotten any emails overnight. It was two hours earlier in California, so I knew we were already doing business in Texas and other parts of the country where we have offices. And I knew if I hadn't gotten any emails incoming, there was probably something wrong." (ROA.677.) She tried her phone, her iPad, and her back-up laptop—nothing worked. "[A]ll three devices resulted in the same situation, which was a nonfunctioning email system." (ROA.678.)

With nearly 1,000 attorneys and approximately 1,800 additional staff spread across the United States and abroad, the firm depends on ready and reliable access to a computer network in order to manage client business, communicate with each other and third parties, and conduct the business of the firm. (ROA.685-86.) That morning, with numerous employees unable to access the email server, panic set in quickly. (ROA.679, 693.) Clements testified:

> [W]ithin about an hour or so, I began getting phone calls from a number of the lawyers in our firm, particularly our partners, who were very alarmed about the fact that when they got in that morning their email systems were down and they couldn't communicate with their clients, with one another; they couldn't transmit documents to their clients, many of whom had either closings going on that day or were trying to file papers and documents in federal court or state court under very important time-sensitive deadlines that were critical to both our lawyers and our clients.

(ROA.679-80.)

Unfortunately for Locke Lord, that day in October was just the beginning of the problem. The firm's IT staff worked nonstop to remediate the problem, bringing in outside experts and consultants from Microsoft and Sentinel, a security company. (ROA.694-696, 784-91, 815-17.) Just as the IT staff had the system and network back up and running, it was attacked again. (ROA.694.) More remediation efforts followed, and Locke Lord had no idea why the firm's network had crashed. (ROA.696-697.)

Things quieted down, for a while. Locke Lord continued to employ third-party experts to try and determine what caused the outages and how to prevent it from occurring again. (ROA.1271-89.) But on December 1, 2011, the network crashed again. (ROA.795-800.) This time, the intruder deleted user accounts in Microsoft's Active Directory program, an application used to manage accounts on a computer network. (ROA.727, 1289-95.) After nonstop remediation efforts by the IT staff and third party entities, a fourth attack occurred on December 5, 2011. (ROA.1295-99.) That day, the intruder compromised an email server by changing passwords, renaming the server, and making the server inaccessible to the firm. (ROA.1295-99.)

Locke Lord brought in several different entities to assist in remediation. One of those was Dave Petty, an IT contractor with Sentinel. After the December 5 attack, Petty reviewed the server logs and determined that the intruder gained access to the Locke Lord system through a backup server in Houston called HOBK01. (ROA.1296-1301.) Petty logged into the backup server and reviewed the applications on it. (ROA.1296-98.) There, he saw, for the first time, the program LogMeIn, which is a software application that allows a user to connect to a network over the internet without going through any security measures, such as a firewall. (ROA.1297.) "My

immediate reaction was, you know, I figured out how the person was getting [into the Locke Lord network]." (ROA.1299.)

LogMeIn is a client/server application where a software application is installed on two different computers—a server and a client, with LogMeIn creating the bridge between the two. (ROA.845-53.) Petty immediately disabled LogMeIn so that it could no longer be used as a means to access the Locke Lord network. (ROA.1307-08.) Petty had access to one side of the relationship (the HOBK1 server) and brought up the server-side application. (ROA.1304-06.) Within the application, Petty was able to identify the registered user—the person who installed the application on the server. (ROA.1306.) The email address of the user who setup LogMeIn on the Locke Lord network was "c_hockland@hotmail.com." (ROA.1305-06.) Petty shared the email address with others on the Locke Lord staff, who immediately recognized it as belonging to Anastasio "Nick" Laoutaris, an IT engineer who abruptly left the firm a few months before the outages. (ROA.1306.) At that point, Clements and the Locke Lord firm contacted law enforcement. (ROA.696-98.)

2. Circumstantial evidence in the form of computer logs and other records presented at trial confirm that Laoutaris was the actor behind the series of unauthorized intrusions into the Locke Lord network.

A grand jury charged Laoutaris with two counts of computer intrusion causing damage, in violation of 18 U.S.C. § 1030(a)(5)(A), relating to the December 1 [Count One] and December 5 [Count Two] intrusions. At trial, the government presented a substantial volume of circumstantial evidence identifying Laoutaris as the intruder. Logs created by the servers on the Locke Lord network showed that the intruder on December 1 and December 5 connected to the network using LogMeIn, which was installed on the HOBK01 backup server in Houston, and accessed the network using the credentials of a Windows "master services account" called svc_gn and its associated password. (ROA.1463-1515, 2835-47.) The IP address of the intruder on December 1 and December 5 was 75.125.127.4. (ROA.2768, 2835.)

That IP address was assigned to The Planet. (ROA.1077-79.) Laoutaris was an employee of The Planet at the time. (ROA.1068-70; *see also* ROA.2635-83.) Kelly Hurst, Laoutaris's supervisor at The Planet, testified that the IP address was The Planet's public wireless network at the Houston corporate office, which employees would be able to use while working out of The Planet's corporate office. (ROA.1077-78.)

Laoutaris was also associated with the LogMeIn software running on the Houston backup server. The software program was installed by a person who identified his email address as "c_hockland@hotmail.com." (ROA.1304-07, 2848.) Records from Microsoft established that the account was created by "A.N. Laoutaris." (ROA.2587.) Further, several Locke Lord employees testified that "c_hockland@hotmail.com" was an email address they knew to be associated with Laoutaris. (ROA.1306.) Additionally, Laoutaris's personnel file included his resume, where he used the email address, and an email he sent on his last day providing c_hockland@hotmail.com as his forwarding email address. (ROA.2550.) Even after he quit, Laoutaris used that email address to send a message to a former colleague at Locke Lord making disparaging comments about the firm and his former supervisor. (ROA.2559-60.) Laoutaris continued using the email address as recently as July 2014, after he was indicted. (ROA.2681.)

The government also presented evidence establishing that Laoutaris had the password for the "svc_gn" account. The "svc_gn" account was the "master of all masters" account that had "no limits" on what it could do within the Locke Lord network. (ROA.1147.) IT engineers at Locke Lord explained that all of the engineers would from time to time use the "svc_gn" account when performing various tasks on the network and that all the

engineers had the password. (ROA.1147.) The jury heard evidence that Laoutaris asked for, and received, the password for the "svc_gn" account shortly before quitting the law firm. On August 10, 2011, a few days before Laoutaris quit, he requested the password from Michael Ger and Stan Guzic, two of the other IT engineers at Locke Lord. (ROA.2556-57.) Guzic testified that Laoutaris "constantly asked us for the password" and thus "to help him remember it, we used his name within the password itself"—specifically, "4nick8." (ROA.1151.)

Not only was Laoutaris specifically tied to the December 1 and December 5 attacks, the government presented evidence tying him to at least 12 unauthorized intrusions into the Locke Lord network through LogMeIn. (ROA.2703-16, 2746, 2756, 2758, 2760, 2762, 2764, 2766, 2768, 2835, 2849.) Each of those intrusions originated from an IP address that was tied back to Laoutaris—either his home or his place of employment. (ROA.2703-16.)

3. Laoutaris testified in his own defense, denying any involvement with the series of attacks at Locke Lord, and presented an expert witness, who suggested the attacks came from China.

Laoutaris took the stand at trial. He denied attacking the Locke Lord network or having the motivation to do so. (ROA.2112.) Laoutaris offered a variety of reasons why some of the circumstantial evidence pointed at him. Among other things, he suggested that his email account had been

compromised, despite his continued use of it. (ROA.2112-18.) He further noted that he had provided colleagues at Locke Lord a flash drive containing sensitive personal information, which he never got back, suggesting that someone could have used that information to make it appear as if Laoutaris committed the offenses. (ROA.2122-27.) He also testified about LogMeIn. While he acknowledged that he created the account, he denied ever using it, despite all of the connections between places associated with him. (ROA.2167-69.) And finally he denied ever receiving the password to the "svc_gn" account that was used in the attacks. (ROA.2171-73.)

Laoutaris also presented an expert witness, Charles Easttom, who was hired just about a week before trial. Easttom criticized the thoroughness of the government's forensic investigation, (ROA.1901-02), and suggested that attacks on the Locke Lord firm could have come from state actors in China. (ROA.2071-72, 2077.)

4. Over Laoutaris's objections to enhancements for obstruction of justice and to the loss amount, the district court sentenced Laoutaris to 105 months' imprisonment.

The PSR determined Laoutaris's base offense level was 24, which included six base-level points (USSG § 2B1.1(a)(2)), 12 levels for losses greater than $250,000 but less than $550,000 (USSG § 2B1.1(b)(1)(G); 4 levels for convictions under 18 U.S.C. § 1030 (USSG § 2B1.1(b)(18)(A)(ii)), and 2 levels

for obstruction of justice (USSG § 3C1.1). (ROA.2955.) Laoutaris's initial guideline range was 51 to 63 months. (ROA.2963.)

The government filed an objection to PSR, seeking a two-level enhancement under USSG § 3B1.3 for use of a special skill (ROA.2968-71), which the probation officer adopted. (ROA.2981.) The defendant filed several objections to the PSR including, relevant here, the two-level enhancement for obstruction of justice and the calculation of the loss amount. (ROA.2973-79.)

In an addendum to the PSR, the probation officer noted that she received additional information from the victim concerning the loss amount that was not included in the original PSR. (ROA.2988.) The victim provided information establishing losses in excess of $1.6 million, which included approximately $1.4 million in lost revenue. (ROA.2988.) That change resulted in an additional 4 levels under USSG § 2B1.1(b)(1)(I) and increased Laoutaris's offense level to 30, with an advisory guideline range of 97 to 121 months. (ROA.2989-90.)

At sentencing, the district court, after review of Laoutaris's trial testimony, made general and specific findings of perjury. The district court also based her findings on Laoutaris's "demeanor" while testifying. (ROA.2451.) The court acknowledged that Laoutaris is a "very intelligent individual, highly educated," who "simply spun a tale of how this happened,

by his own testimony and then use of an expert to buffet that, if you will, in a way the jury didn't buy and the Court didn't buy." (ROA.2452.) Put directly, Laoutaris "concocted a pretty sophisticated idea of . . . Chinese hackers, at least, as a possible scenario that may have committed this horrendous attack on the Locke Lord system on more than one occasion." (ROA.2452.) The district court further acknowledged that Laoutaris "pos[ed] himself as somewhat of an expert in the field, almost to the extent where he was maybe coming across a bit arrogant, as to how the jury should understand it happened [Laoutaris's] way . . and how the prosecution's substantial circumstantial case was flimsy and had no meaning to it and had no substance to it." (ROA.2453.) The district court made clear that Laoutaris' s false testimony was not the result of "confusion, mistake or faulty memory." (ROA.2453.)

The district court also identified specific instances of false testimony concerning material matters made with willful intent. First, the district court pointed to Laoutaris's testimony that the allegations in the indictment against him were "false." (ROA.2453-54.) The court noted that it was "perjured testimony at its essence," directly contradicted by the evidence presented by the government linking Laoutaris to the series of unauthorized attacks on the Locke Lord network. (ROA.2454.) Second, the district court pointed to Laoutaris's testimony concerning LogMeIn. (ROA.2454-55.) The defendant

testified that he set up an account simply to learn about it as a possible tool for doing presentations but ultimately never used it. (ROA.2167-69.) The Court found that was willfully false because LogMeIn was "an integral part of his steps toward attacking the system." (ROA.2455.) Laoutaris's effort to say he was connected with "but didn't use it because it wasn't going to work for him was certainly perjured testimony." (ROA.2455.) Third, the district court pointed to Laoutaris's denial of having the password for the "svc_gn" account. (ROA.2455-56.) The evidence established that Laoutaris requested the svc_gn password shortly before he quit Locke Lord (ROA.2455, 2556), that it was provided to him (ROA.1147-51), that it was specifically tailored to be something he could remember (ROA.1151, 2557), and that Locke Lord did not immediately change the password until after the December 1 and December 5 intrusions. (ROA.1315.) The district court further adopted other specific instances of perjured testimony outlined in the presentence report and the addendum, although the Court noted that "if there's a shortcoming in the presentence report addendum, it's that it doesn't recount all of the instances where [the defendant] perjured himself on the witness stand with regard to this case." (ROA.2452.)

With respect to the calculation of loss, the government presented testimony from a former controller at Locke Lord, Allen Shank, who testified

regarding the firm's lost revenue and other losses associated with the intrusions. Relevant here, concerning the firm's lost revenue, Mr. Shank gathered data on each timekeeper at the firm from January 1, 2011, through November 30, 2011. (ROA.2469-70.) A timekeeper, Mr. Shank explained, was "anybody who could bill" a client, including attorneys, paralegals, and some secretarial staff. (ROA.2470.) For each timekeeper, Mr. Shank determined that person's fees worked through November 30, 2011—in other words, the total hours billed multiplied by the timekeeper's hourly rate. (ROA.2470.) From there, Mr. Shank calculated each timekeeper's average daily fees based on a six-day work-week. (ROA.2471-72.) Mr. Shank used a six-day work week to reflect that many of the employees of the firm often worked on the weekend and it resulted in a smaller, per-day average than had he used a five-day work week. (ROA.2471-72.)

For each of the outages, Mr. Shank consulted with Locke Lord's IT staff to determine the severity of the outage. (ROA.2472-74.) Using that information, Mr. Shank made a subjective estimate of how impactful the outage was on the firm's ability to conduct business. (ROA.2474.) Mr. Shank further analyzed the data based on the location of the affected attorneys. (ROA.2476.) For each of the outages, Mr. Shank determined the percentage of hours impacted, taking into account the different time zones of Locke Lord

attorneys. (ROA.2476-78.) Mr. Shank took the average daily fees and multiplied it by the degree of severity, adjusted for the number of hours the computer systems were impacted and adjusted further by time zone. (ROA.2476-78.) For each attack, Mr. Shank looked at when the attack started and when it ended and made a qualitative assessment, after consulting with others at the firm, of the attack's severity. (ROA.2477.)

Mr. Shank also made adjustments based on the percentage of hours actually billed by the firm to clients. (ROA.2478-80.) In other words, Mr. Shank recognized that even if a lawyer may have worked a certain amount of time, the firm may not have billed all of it to the firm's client. (ROA.2478-80.) Mr. Shank also reduced the lost revenue by the firm's historical realization rate. (ROA.2478-80.) Using historical data, Mr. Shank looked at how much money the firm actually received based on the percentage of collections over time. (ROA.2478-80.)

The district court overruled the defendant's objections to the obstruction enhancement and the loss calculation. (ROA.2456, 2501-03.) The court sentenced Laoutaris to 115 months' imprisonment and a three-year term of supervised release. (ROA.2519.) Laoutaris was also ordered to pay $1,697,800 in restitution to the victim. (ROA.2520.)

SUMMARY OF THE ARGUMENT

This Court should affirm Laoutaris's convictions and sentence. Laoutaris's challenge to the sufficiency of the evidence is reviewed under the "manifest miscarriage of justice standard" because he did not renew the Rule 29 motion at the close of all the evidence. The primary dispute at trial was the identity of the perpetrator of a series of attacks on the Locke Lord computer network. All the evidence in the case pointed at one individual, Laoutaris, and the jury rejected his effort to present an alternative perpetrator—the People's Republic of China—for the intrusions into the firm's computer network.

The district court did not clearly err in applying a two-level enhancement for obstruction of justice based on the defendant's perjured testimony at trial. The district court's obstruction finding was based on her observation of Laoutaris's demeanor at trial. The court reviewed the trial transcript and made general and specific findings of perjury on the record at the sentencing hearing. Each specifically identified statement related to a material matter in the trial and the court's factual findings encompassed all the elements of perjury, as required by *United States v. Dunnigan*, 507 U.S. 87 (1993).

The district court did not clearly err by including Locke Lord's lost revenue from the series of outages caused by the damage to its network by the defendant. Expressly called for in the commentary to USSG § 2B1.1, the

district court properly included the law firm's lost revenue in the loss calculation. The district court's factual finding was supported by the testimony of a forensic accountant from the victim, who explained his methodology and presented a detailed summary exhibit that established approximately $1.4 million in lost revenue from the series of computer attacks by Laoutaris.

ARGUMENT AND AUTHORITIES

1. The evidence was sufficient to support Laoutaris's convictions on Counts One and Two of the superseding indictment [responsive to Laoutaris's Issues 1 and 2].

Standard of Review

Laoutaris concedes that while he moved for acquittal at the close of the government's case, he did not renew the motion at the end of the trial. (App. Br. at 35.) This Court, therefore, reviews the sufficiency of the evidence "for a manifest miscarriage of justice." *United States v. Dowl*, 619 F.3d 494, 500 (5th Cir. 2010) (internal quotation marks omitted); *see United States v. Pringler*, 765 F.3d 445, 449 (5th Cir. 2015). Under the manifest-miscarriage-of-justice standard, the Court will find the evidence lacking only if the record is "devoid of evidence pointing to guilt, or the evidence on a key element of the offense is so tenuous that a conviction would be shocking." *United States v. Brown*, 727 F.3d 329, 335 (5th Cir. 2013) (internal quotation marks omitted).

Laoutaris also contends that trial counsel was ineffective for failing to re-urge a motion for acquittal at the close of all the evidence, despite conceding that such a claim "is generally not reviewed on direct appeal." (App. Brief at 41-43.) This Court has evaluated an ineffective-assistance claim where the record is sufficiently developed. *United States v. Rosalez-Orozco*, 8 F.3d 198, 1999 (5th Cir. 1993); *United States v. Almaguer*, 246 F. App'x 260, 261 (5th Cir. 2007). To prevail, Laoutaris must demonstrate (1) deficient performance by counsel that (2) prejudiced the defense. *Strickland v. Washington*, 466 U.S. 668, 687 (1984). To establish prejudice, Laoutaris "must show that there is a reasonable probability that, but for counsel's unprofessional errors, the result of the proceeding would have been different." *Rosalez-Orozco*, 8 F.3d at 200. That requires this Court to evaluate "the sufficiency of the evidence as if counsel had moved for judgment of acquittal at the close of the evidence." *Id.* In that circumstance, this Court determines whether "viewing the evidence and the inferences that may be drawn from it in the light most favorable to the verdict, a rational jury could have found the essential elements of the offense beyond a reasonable doubt." *Id.* (quotation omitted).

Discussion

The evidence was sufficient to support Laoutaris's convictions on Counts One and Two of the superseding indictment, regardless of whether trial

counsel moved for judgment of acquittal at the close of the evidence or not. Laoutaris was charged with two counts of computer intrusion causing damage, in violation of 18 U.S.C. § 1030(a)(5) and (c)(B)(iv). (ROA.76-80.) To sustain a conviction on each count, the government must prove (a) that Laoutaris knowingly caused the transmission of a program, information, code or command; and (b) that by doing so, Laoutaris intentionally caused damage to a protected computer without authorization. (*See* 18 U.S.C. § 1030(a)(5)(A); ROA.345-46.) If both elements are met, the government must also prove one or more of the elements in section 1030(c)(4)(A)(i) for purposes of determining the maximum punishment. (ROA.346.) Here, the government alleged, and proved, that the computer intrusions caused loss aggregating at least $5,000 in value (18 U.S.C. § 1030(c)(4)(A)(i)(I)) and damage affecting 10 or more protected computers during any 1-year period (18 U.S.C. § 1030(c)(4)(A)(i)(VI)). (*See* ROA.78-79 (superseding indictment); ROA.345-46 (jury charge).)

A. For both Count One and Two, the government introduced evidence that Locke Lord's network was damaged by an unauthorized access.

With respect to count one of the superseding indictment, the government introduced evidence that someone accessed the Locke Lord network using LogMeIn on December 1, 2011, at approximately 9:34:44 PM. (ROA.2768.)

The intruder's IP address was 75.125.127.4. (ROA.2768) The intruder used the "svc_gn" account at Locke Lord. (ROA.2768.) Once the intruder accessed the HOBK01 server, he moved through the network until he accessed the domain controller that ran Active Directory, a Microsoft product that manages accounts on a network. (ROA.1463-515.) Within Active Directory, the intruder transmitted a series of commands and instructions that caused damage to approximately 496 desktop and laptop accounts, 359 user accounts, 78 distribution and security groups, 105 server accounts, 18 network administrator accounts, and 6 service accounts. (ROA.1462-63, 2771-883.) Locke Lord spent more than $5,000 to remediate the intrusion. (ROA.2561-77.)

With respect to count two of the superseding indictment, the government introduced evidence that someone accessed the Locke Lord network using LogMeIn on December 5, 2011, at approximately 7:36 PM. (ROA.2835.) The intruder's IP address was 75.124.127.4. (ROA.2835.) The intruder used the svc_gn account at Locke Lord. Once the intruder accessed the HOBK01 server, he took one of the firm's mail servers off the network and made it into a separate domain. (*See* ROA.2835-47.) The result of that action was that anyone who had an email account on the server would no longer be able to access their email, and any email sent to that user would not be received.

(ROA.1519-48.) The transmission of the code, commands, and instructions to remove the mail server resulted in damage to the firm's network and over $5,000 in remediation costs. (ROA.2561-77.)

B. All the circumstantial evidence in the case pointed to Laoutaris as the perpetrator of the attacks on the Locke Lord network.

The central issue at trial was the identity of the intruder. "Identity may be established by 'inference and circumstantial evidence.'" *United States v. Alaniz*, 726 F.3d 586, 606 (5th Cir. 2013) (quoting *United States v. Seals*, 987 F.2d 1102, 1110 (5th Cir. 1993)) (citations and internal quotation marks omitted); *United States v. Garza*, 591 F. App'x 259, 260 (5th Cir. 2015) (finding sufficient evidence where no witness identified the defendant's voice on a recording). The government introduced a variety of evidence from different sources and in different forms all confirming that the intruder into the Locke Lord network was Laoutaris.

First, all the Internet Protocol ("IP") addresses involved in the attacks were associated with Laoutaris—either his personal residence or one of his employers. The IP address of the intruder on December 1 and December 5 was 75.125.127.4 (ROA.2768, 2835), which was assigned to The Planet at the time. (ROA.1077-79.) Laoutaris was an employee of The Planet at the time. (ROA.1068-70; *see also* ROA.2635-83.) Further, the government presented

testimony from Kelly Hurst, Laoutaris's supervisor at The Planet, who testified that the IP address was The Planet's public wireless network at the Houston corporate office, which employees would be able to use. (ROA.1077-78.)

In addition, the government introduced evidence showing at least 12 unauthorized intrusions into the Locke Lord network through LogMeIn. (ROA.2703-16, 2746, 2756, 2758, 2760, 2762, 2764, 2766, 2768, 2835, 2849.) Each of those intrusions originated from an IP address that was tied back to Laoutaris. Several of them were from an IP address assigned to Laoutaris's home. Up until November 30, 2011, Laoutaris had a dynamic IP address through a "DSL" internet access with AT&T. (ROA.1851-56.) The dynamic IP address changed from time to time. AT&T records, however, showed that at the applicable time, the IP address was assigned to Laoutaris's personal account (albeit in his wife's name). (ROA.2578-86.) Further, beginning on November 30, 2011, Laoutaris had a static IP address (i.e., one that does not change, as opposed to a dynamic IP address) through AT&T. (ROA.2578-86.) One of the unauthorized intrusions—on December 6, 2011—was from the IP address assigned specifically to Laoutaris's residence. (ROA.2580, 2849.) Likewise, several of the unauthorized intrusions came through an IP address associated with another company where Laoutaris went to work after he quit the law firm. (ROA.1120-29.)

Second, the user who installed LogMeIn on the Locke Lord server was identified by the "c_hockland@hotmail.com" email address. Evidence presented at trial tied Laoutaris to that email address. Records from Microsoft established that the account was created by "A.N. Laoutaris." (ROA.2587.) Further, several Locke Lord employees identified "c_hockland@hotmail.com" as an email address they knew to be associated with Laoutaris. (ROA.1306.) Laoutaris's personnel file included his resume (where he used the email address) and an email he sent on his last day providing it as his forwarding email address. (ROA.2550.) Even after he abruptly quit, Laoutaris sent emails to a former colleague at Locke Lord in which he made disparaging comments about the firm and his former supervisor. (ROA.2559-60.) And Laoutaris continued using the email address as recently as July 2014, after he was indicted in October 2013. (ROA.2681.)

Third, the jury heard evidence that Laoutaris asked for, and received, the password for the "svc_gn" account shortly before quitting the law firm. On August 10, 2011, a few days before Laoutaris quit, he requested the password from Michael Ger and Stan Guzic, two of the other IT engineers at Locke Lord. (ROA.2556-57.) Guzic testified that Laoutaris "constantly asked us for the password" and thus "to help him remember it, we used his name within the password itself." (ROA.1151.)

Fourth, the LogMeIn records introduced at trial corroborated the event logs recovered from the Houston backup server. Records from LogMeIn showed every use by the "c_hockland@hotmail.com" account. (ROA.2703-16.) Not only did those records corroborate the event logs from Locke Lord's servers, but they further showed that all the uses tied back to Laoutaris. Among other things, the LogMeIn records showed connections from Laoutaris's home to HOBK01; from The Planet to HOBK01; from Laoutaris's home to The Planet; and from The Planet to Laoutaris's home. (ROA.2703-16.) In addition, after Laoutaris's quit Locke Lord, he worked at Trafigura (while also working at The Planet), a commodities trader in the Houston area. (ROA.1112.) LogMeIn records further showed connections from Trafigura to HOBK01; from Trafigura to Laoutaris's home; and from Trafigura to The Planet. (ROA.2703-16.) What was clear to the jury was that Laoutaris was using LogMeIn at various locations where he worked or lived as a means to remotely access networks. As much as Laoutaris wants to suggest the attacks were from some other person or entity, he cannot ignore all the connections using LogMeIn, which was installed using his email account, between locations that he frequented.

Fifth, the jury heard evidence that Laoutaris was well educated and knowledgeable about the Locke Lord network, including the vulnerabilities.

This evidence, coupled with Laoutaris disdain for the firm and his former supervisor, established motive and opportunity to commit the crime. In a series of emails after he quit with a colleague, Laoutaris, using the "c_hockland@hotmail.com" email address, disparaged his former firm and former supervisor. (*See* ROA.2559-60.)

Taken together, the jury was presented with overwhelming circumstantial evidence connecting Laoutaris to each of the charged intrusions into the Locke Lord computer network.

C. Laoutaris rehashes the same arguments on appeal that the jury has already rejected concerning the identity of the hacker.

Laoutaris essentially rehashes the same arguments regarding the identity of the intruder that the jury and district court rejected. As discussed above, the evidence was more than sufficient for a rational jury to convict him on both counts, and nothing about the circumstantial evidence suggests, let alone establishes, a manifest miscarriage of justice or even that the jury was irrational in finding him guilty. *Brown*, 727 F.3d at 335; *Rosalez-Orozco*, 8 F.3d at 200.

First, Laoutaris asserts that he "did not have the password to Locke Lord's computer system after he left employment . ." (App. Br. at 35-36.) Laoutaris maintained that position during his testimony at trial, and it was one of the bases identified by the district court to support the obstruction

enhancement. (*See* ROA.2455-56.) But his testimony was contradicted by the testimony of one of his former IT colleagues, Stan Guzick (ROA.1151), emails showing Laoutaris requesting the password for that account (ROA.2556-57), and the use of a password that would be easy for him to remember. (ROA.1151.) The jury was free to reject Laoutaris's self-serving testimony in view of the other evidence.

Second, Laoutaris asserts that he "did not have the [] token that was needed to remotely access Locke Lord's network." (App. Br. at 35-36.) That was a true statement but it miscomprehends the nature of the attack. Locke Lord had two authorized means of accessing the network remotely—the software application Citrix and through a virtual private network (VPN). (ROA.768-71.) To use the latter, the employee would need a token—a special code that randomly changes as a security measure. (ROA.768-69.) Laoutaris no longer had access to Citrix or a token after he quit the firm, but he was able to access the Locke Lord network using an unauthorized means—LogMeIn, which establishes a connection so long as the software is running on a server. (ROA.1297.) Once the connection was established with LogMeIn, Laoutaris still needed credentials to log onto the network, which he did using the "svc_gn" username and the password that was provided to him before he quit. (ROA.1270-98.)

Third, Laoutaris contends that another IT engineer, Kenny Bradford, accessed the Locke Lord network through LogMeIn. (App. Br. at 38.) Laoutaris tries to use this event to suggest that other engineers at Locke Lord were using LogMeIn and thus not all LogMeIn entries were necessarily him. As an initial matter, Laoutaris's argument fails because the alleged Bradford login using LogMeIn occurred on October 7, 2011, which was not one of the dates charged in the indictment. (ROA.1190-92.) Even if true that it was Bradford, it does not change the evidence establishing that Laoutaris was the intruder behind the December 1 and December 5 attacks.

The bigger problem with Laoutaris's argument is that it entirely ignores Bradford's testimony that he never accessed Locke Lord using LogMeIn and never worked at Trafigura. (ROA.1192-94.) And it ignores testimony of a Trafigura representative who corroborated Bradford on these points. (ROA.1123-24.) The jury was free to resolve this credibility choice against him. *See United States v. Grant*, 683 F.3d 639, 642 (5th Cir. 2012) (noting that the jury "retains the sole authority to weigh any conflicting evidence and to evaluate the credibility of the witnesses").

Moreover, the government presented evidence that the login using Bradford's account was from an IP address assigned to Trafigura, which was

one of Laoutaris's employers at the time. The government called Christian Diaz, Laoutaris's supervisor at Trafigura, who testified that only employees of Trafigura could access that IP address by connecting directly to the Trafigura internal corporate network. (ROA.1123-24.) Diaz further testified that he did not know Bradford and that Bradford did not work for Trafigura. Bradford, likewise, testified that he had never worked for Trafigura, had never been to Trafigura's office, and had never logged into a Trafigura computer. (ROA.1123-24.)

The jury made a rational decision to convict Laoutaris based on the evidence, and its decision should not be disturbed on appeal.

2. The district court did not clearly err in applying a two-level enhancement for obstruction under USSG 3C1.1 based on Laoutaris's perjured testimony at trial.

Standard of Review

Laoutaris objected to the obstruction-of-justice enhancement under USSG § 3C1.1. (ROA.2976-78.) This Court reviews the district court's legal interpretations *de novo* and its factual findings for clear error. *United States v. Como*, 53 F.3d 87, 89 (5th Cir. 1995). Under the clearly-erroneous standard, this Court "will uphold a finding so long as it is plausible in light of the record as a whole." *United States v. Miller*, 607 F.3d 144, 148 (5th Cir. 2010). This Court "give[s] particular deference to findings that are based on credibility

determinations." *United States v. Smith*, 804 F.3d 724, 737 (5th Cir. 2015) (citing *United States v. Powers*, 168 F.3d 741, 743 (5th Cir. 1999)).

Discussion

The district court did not clearly err in applying a two-level enhancement under USSG § 3C1.1 based on Laoutaris's perjured testimony at trial. Section 3C1.1 provides for a two-level enhancement "[i]f (1) the defendant willfully obstructed or impeded, or attempted to obstruct or impede, the administration of justice with respect to the . . prosecution . . of the instant offense of conviction, and (2) the obstructive conduct related to (A) the defendant's offense of conviction and any relevant conduct[.]" USSG § 3C1.1. "Though the court may not penalize a defendant for denying his guilt as an exercise of his constitutional rights, a sentence may be enhanced if the defendant commits perjury." *Como*, 53 F.3d at 89 (citing *United States v. Laury*, 985 F.2d 1293, 1308 (5th Cir. 1993)). Federal law defines perjury as giving false testimony concerning a material matter with the willful intent to provide false testimony rather than as a result of confusion, mistake, or fault memory. *United States v. Dunnigan*, 507 U.S. 87, 94 (1993) (citing 18 U.S.C. § 1621(1)).

The Supreme Court recognizes, however, that "not every accused who testifies at trial and is convicted will incur an enhanced sentence under § 3C1.1 for committing perjury." *Id.* at 95. Because there are reasons why a defendant

may testify falsely without committing perjury, "if a defendant objects to a sentence enhancement resulting from [his] trial testimony, a district court must review the evidence and make independent findings necessary to establish a willful impediment to or obstruction of justice, or an attempt to do the same, under the perjury definition [the Supreme Court has] set out." *Id.* Although it is "preferable" for the district court to address each element of perjury, the district court's application of the enhancement is sufficient if "the court makes a finding of an obstruction of, or impediment to, justice that encompasses all of the factual predicates for a finding of perjury." *Id.*

Here, the district court reviewed Laoutaris's trial testimony and made both general and specific findings that he committed perjury. (ROA.2449-56.) The district judge based her findings on Laoutaris's "demeanor" while testifying. (ROA.2451; *see Smith*, 804 F.3d at 737.) She acknowledged that Laoutaris is a "very intelligent individual, highly educated," who "simply spun a tale of how this happened, by his own testimony and then use of an expert to buffet that, if you will, in a way the jury didn't buy and the Court didn't buy." (ROA.2452.) Put directly, Laoutaris "concocted a pretty sophisticated idea of . . . Chinese hackers, at least, as a possible scenario that may have committed this horrendous attack on the Locke Lord system on more than one occasion." (ROA.2452.) The district court further acknowledged that

Laoutaris "pos[ed] himself as somewhat of an expert in the field, almost to the extent where he was maybe coming across a bit arrogant, as to how the jury should understand it happened [Laoutaris's] way . . and how the prosecution's substantial circumstantial case was flimsy and had no meaning to it and had no substance to it." (ROA.2453.) The district court also made clear that the "material matter" was that Laoutaris did not commit the attacks, and that his testimony to that effect was "with willful intent to provide false testimony to obscure his involvement in the case, and it was in no way" the result of "confusion or faulty memory." (ROA.2453.)

The district court then identified several specific instances of false testimony. First, the district court pointed to Laoutaris's testimony that the allegations in the indictment against him were "false." (ROA.2453-54.) The court noted that it was "perjured testimony at its essence," directly contradicted by the evidence presented by the government linking Laoutaris to the series of unauthorized attacks on the Locke Lord network. (ROA.2454.) Laoutaris suggests that this is tantamount to punishing him for entering a "not guilty" plea (App. Br. at 45) but that is wrong. A "not guilty" plea is simply an assertion that the government has not proven its case. Laoutaris's testimony, by contrast, was a flat denial of the allegations. *See United States v. Flores*, 640 F.3d 638, 644 (5th Cir. 2011) (affirming obstruction enhancement where

defendant testified he had "no involvement" with the drugs or the coconspirators "on the weekend in question"); *United States v. Smith*, 804 F.3d 724, 737-38 (5th Cir. 2015) (rejecting argument that the obstruction enhancement for perjured testimony "amounts to punishing [the defendant] for exercising his constitutional right to testify").

Second, the district court pointed to Laoutaris's testimony concerning LogMeIn. (ROA.2454-55.) Laoutaris told the jury that he set up an account simply to learn about it as a possible tool for doing presentations but ultimately never used it. (ROA.2167-69.) The Court found that was willfully false because LogMeIn was "an integral part of his steps toward attacking the system." (ROA.2455.) Laoutaris's effort to say he was connected with "but didn't use it because it wasn't going to work for him was certainly perjured testimony." (ROA.2455.) Laoutaris cannot deny that the records from LogMeIn established that each of the IP addresses associated with the "c_hockland@hotmail.com" email account were connected to places known to be associated with Laoutaris: his residence and his employers. (*See* ROA.2703-16.) The LogMeIn records further confirmed that Laoutaris used LogMeIn to establish the connection to the Houston backup server (HOBK01) that was the entry point for the subsequent damage to the computer network. *See Flores*, 640 F.3d at 644 (finding that the defendant's assertion was "not worthy of

credence" because it was "flatly contradicted by other witnesses").

Third, the district court pointed to Laoutaris's denial of having the password for the "svc_gn" account. (ROA.2455-56.) The evidence established that Laoutaris requested the svc_gn password shortly before he quit Locke Lord (ROA.2455, 2556), that it was provided to him (ROA.1147-51), that it was specifically tailored to be something he could remember (ROA.1151, 2557), and that Locke Lord did not immediately change the password until after the December 1 and December 5 intrusions. (ROA.1315.)[1] Laoutaris's testimony was plainly false, and the district court was correct to rely upon it in applying the obstruction enhancement. *United States v. Montelongo*, 539 F. App'x 603, 606 (5th Cir. 2013) (finding district court's factual finding not clearly erroneous in light of directly contradictory testimony).

The district court did not clearly err in applying the two-level enhancement for obstruction of justice.

[1] The district court further adopted other specific instances of perjured testimony outlined in the presentence report and the addendum, although the Court noted that "if there's a shortcoming in the presentence report addendum, it's that it doesn't recount all of the instances where [the defendant] perjured himself on the witness stand with regard to this case." (ROA.2452.)

3. The district court did not clearly err in calculating the reasonably foreseeable lost revenue to the victim that was caused by Laoutaris's network attacks.

Standard of Review

Laoutaris objected to the district court's loss calculation. (ROA.2978, 2993-94.) This Court reviews *de novo* the district court's method of determining the loss. *United States v. Harris*, 597 F.3d 242, 251 (5th Cir. 2010); *United States v. Roussel*, 705 F.3d 184, 197 (5th Cir. 2013). Loss calculation is reviewed for clear error. *United States v. Scher*, 601 F.3d 408, 412 (5th Cir. 2010). "A factual finding is not clearly erroneous as long as it is plausible in light of the record read as a whole." *United States v. Krenning*, 93 F.3d 1257, 1269 (5th Cir. 1996). The district court has wide latitude to determine the amount of loss. *United States v. Cothran*, 302 F.3d 279, 287 (5th Cir. 2002).

Discussion

Pursuant to USSG § 2B1.1(b)(I), the district court applied a 16-level enhancement based on the testimony of the former corporate controller of the victim concerning the firm's losses as a result of Laoutaris's unlawful intrusions into the computer network. (ROA.16.10516.2989.) Of the $1.6 million in actual loss, Laoutaris only objects to approximately $1.4 million in lost revenue to the firm. (*See* App. Br. at 51-53.)

As an initial matter, it is well established that USSG § 2B1.1 provides for an offense-level increase based on the loss, defined as "the greater of actual loss or intended loss." USSG § 2B1.1 cmt. N. 3(A). Actual loss is "the reasonably foreseeable pecuniary harm that resulted from the offense." *Id.* n.3(a)(i). The district court is only required to make a "reasonable estimate" of the loss based on a preponderance of the evidence. *Id.* n.3(C); *United States v. Bazemore*, 839 F.3d 379, 389 (5th Cir. 2016).

In computer-intrusion cases, such as this one, the district court's inclusion of lost revenue is specifically called for by the guidelines. The commentary to USSG § 2B1.1 expressly notes that in section 1030 cases, the pecuniary harm includes "any revenue lost . . because of the interruption of service." USSG § 2B1.1, comment n.3 (A)(v)(III) (emphasis added); *see United States v. Pok Seong Kwong*, 237 F. App'x 966, 969 (5th Cir. 2007) (affirming inclusion of lost revenue based on victim representative testimony in computer-intrusion case); *United States v. Schuster*, 467 F.3d 614, 617 (7th Cir. 2006) (affirming actual loss that included "lost productivity" of the victim company).

The district court's loss calculation was based on testimony presented by the government from Allan Shank, the Director of Accounting, Finance, and Risk for Locke Lord at the time of the attacks. The district court found that

Mr. Shank, a "forensic accountant who is educated in this area," presented "credibl[e]" testimony concerning a "conservative estimate" as to the firm's losses, including lost revenue, as illustrated in Government's Sentencing Exhibit 2. (ROA.16-15106.2562; Sent. Exh. 2.)

With respect to the firm's lost revenue, Mr. Shank gathered data on each timekeeper at the firm from January 1, 2011, through November 30, 2011. (ROA.2469-70.) A timekeeper, Mr. Shank explained, was "anybody who could bill" a client, including attorneys, paralegals, and some secretarial staff. (ROA.2470.) For each timekeeper, Mr. Shank determined that person's fees worked through November 30, 2011—in other words, the total hours billed multiplied by the timekeeper's hourly rate. (ROA.2470.) From there, Mr. Shank calculated each timekeeper's average daily fees based on a six-day work-week. (ROA.2471-72.) Mr. Shank used a six-day work week to reflect that many of the employees of the firm often worked on the weekend and it resulted in a smaller, per-day average than had he used a five-day work week. (ROA.2471-72.)

For each of the outages, Mr. Shank consulted with Locke Lord's IT staff to determine the severity of the outage. (ROA.2472-74.) Using that information, Mr. Shank made a subjective estimate of how impactful the outage was on the firm's ability to conduct business. (ROA.2474.) Mr. Shank

further analyzed the data based on the location of the affected attorneys. For each of the outages, Mr. Shank determined the percentage of hours impacted, taking into account the different time zones of Locke Lord attorneys. (ROA.2476.) Mr. Shank took the average daily fees and multiplied it by the degree of severity, adjusted for the number of hours the computer systems were impacted and adjusted further by time zone. (ROA.2476-78.) Mr. Shank did not include timekeepers who were in offices not affected by the attacks. (ROA.2477.)

Mr. Shank made adjustments based on the percentage of hours actually billed by the firm to clients. (ROA.2478-80.) In other words, even if a lawyer may have worked a certain amount of time, the firm would not necessarily bill all of that time to the firm's client. (ROA.2478-2480.) Mr. Shank also reduced the lost revenue by the firm's historical realization rate. (ROA.2478-80.) Using historical data, Mr. Shank looked at how much money the firm actually received based on the percentage of collections over time. (ROA.2478-80.)

Despite Mr. Shank's detailed analysis, Laoutaris contends that relying on "hours that could have been billed" was "speculative" because it presumes that work was available, that it would have been completed and billed, and that payment would have been collected. (App. Br. at 52.) But Laoutaris's argument is directly contradicted by Mr. Shank's testimony. (ROA.2477-80.)

Laoutaris further argues that Mr. Shank's analysis is faulty because Locke Lord did not "poll the employees" to determine whether they were able to conduct firm business in other ways. (App. Br. at 52.) Mr. Shank's severity analysis significantly discounted each timekeeper's average daily fees based on the nature of the attack, taking into account the degree to which each attack impacted the lawyers at the firm. (ROA.2474.) For each of the attacks, Mr. Shank did not assume the timekeepers were completely unable to work but only impacted by the attack to a certain degree. (ROA.2474.)

Finally, Laoutaris contends that attorneys could have made up the lost time by working later in the evening or on the weekends. (App. Br. at 53.) Mr. Shank made clear that attorneys at Locke Lord work extensive hours, a fact not lost on the experienced trial judge, and that the attorneys likely would have billed during the days of the outage *as well as* the corresponding weekends and evenings. (ROA.2492-93.)

In short, Mr. Shank's analysis was conservative, and the district court did not clearly err in relying on it as a "reasonable estimate" of the losses suffered by Locke Lord during four separate computer intrusions by the defendant. Certainly, Laoutaris has not satisfied his burden on appeal to show that the district court's loss calculation was implausible based on the record as a whole. *Krenning*, 93 F.3d at 1269).

CONCLUSION

The Court should affirm Laoutaris's conviction and sentence.

Respectfully submitted,

John R. Parker
United States Attorney

/s/ J. Nicholas Bunch
J. Nicholas Bunch
Assistant United States Attorney
Texas Bar No. 2405032
1100 Commerce Street, Third Floor
Dallas, Texas 75242-1699
Telephone: (214) 659-8836
nick.bunch@usdoj.gov

CERTIFICATE OF SERVICE

I certify that this document was served on Laoutaris's attorney, Chris McCaffrey, through the Court's ECF system on July 13, 2017, and that: (1) any required privacy redactions have been made; (2) the electronic submission is an exact copy of the paper document; and (3) the document has been scanned for viruses with the most recent version of a commercial virus scanning program and is free of viruses.

/s/ J. Nicholas Bunch
J. Nicholas Bunch
Assistant United States Attorney

CERTIFICATE OF COMPLIANCE

1. This document complies with the type-volume limit of Fed. R. App. P. 32(a)(7)(B) because, excluding the parts of the document exempted by Fed. R. App. P. 32(f), this document contains 8,044 words.

2. This document complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because this document has been prepared in a proportionally spaced typeface using Microsoft Word 2016 in 14-point Calisto MT font.

/s/ J. Nicholas Bunch
J. Nicholas Bunch
Assistant United States Attorney
Date: July 13, 2017