No. _____

IN THE
SUPREME COURT OF THE UNITED STATES

ANASTASIO N. LAOUTARIS # 47066-177

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition for a Writ of *Certiorari* to
The United States Court of Appeals
For the Fifth Circuit

Appeal Case No. 16-10516

Criminal No.: 3:11-CR-00386-B-1 (N.D. Tex.)

PETITION FOR A WRIT OF CERTIORARI

ANASTASIO N. LAOUTARIS # 47066-177
ACCC CA-106U
P.O. Box 1600
Washington, MS 39190-1600

PRO SE PETITIONER

QUESTIONS PRESENTED

I. Has the Fifth Circuit erred and its decision is in conflict with this Court's holding in *Jackson v. Virginia*, 443 U.S. 307, 99 S.Ct. 2781, 61 L.Ed.2d 560 (1979), by finding that a rational jury could have found each essential element of the offense of transmitting a malicious code, in violation of 18 U.S.C. § 1030(A)(5)(A) and (C)(4)(B)(I), beyond a reasonable doubt?

II. If the answer to the above question is in the affirmative, was trial counsel ineffective for failing to resubmit a motion for judgment of acquittal at the close of all the evidence pursuant to *Strickland v. Washington*, 466 U.S. 668, 690, 104 S.Ct. 2052, 80 L.Ed.2d 674 (1984), and its progeny?

III. Did the Court of Appeals err in affirming the district court's error applying an obstruction-of-justice adjustment under USSG § 3C1.1 based on finding that Petitioner committed perjury in his testimony at trial, in contravention of his privilege to testify in his own behalf pursuant to *United States v. Dunnigan*, 507 U.S. 87, 95, 113 S. Ct. 1111, 122 L. Ed. 2d 445 (1993)?

IV. Should the Fifth Circuit have reversed the district court's error in increasing Petitioner's base-offense level by applying $1,461,910 in lost revenue to the $235,890 actual loss amount and, as a result of the erroneous calculation, imposing an unreasonable sentence contrary to this Court's decision in *Rita v. United States*, 551 U.S. 338, 127 S.Ct. 2456, 168 L.Ed.2d 203 (2007)?

LIST OF PARTIES

All parties appear on the caption of the case on the cover page.

TABLE OF CONTENTS

PAGES

INDEX TO APPENDICES

IN THE SUPREME COURT OF THE UNITED STATES

PETITION FOR A WRIT OF CERTIORARI

Petitioner respectfully prays that this Honorable Supreme Court issue a writ of certiorari to review the judgment below.

OPINIONS BELOW

The Opinion of the United States Court of Appeals for the Fifth Circuit is unpublished, but cited as *United States v. Laoutaris*, 2018 U.S. App. LEXIS 2102; Case No. 16-10516 (5th Cir. Jan. 29, 2017), on LexisNexis, and also appears at Appendix A (App. 1a) to the petition.

The Order of the United States Supreme Court granting Application for a 60 day extension of time to file this Petition appears at Appendix B (App. 5a).

The Judgment of the United States District Court for Northern District of Texas appears at Appendix C (App. 11a) to the petition.

JURISDICTION

The decision of the United States Court of Appeals for the Fifth Circuit, affirming the Petitioners' convictions and sentences, was issued on January 29, 2018. No petition for a rehearing was filed, but the Supreme Court granted a 60-day extension of time of to file this petition. This petition is submitted within the 60-day extension of time period. Accordingly, the Supreme Court has jurisdiction under 28 U.S.C. § 1254(1) to review this case, and jurisdiction is thus invoked.

CONSTITUTIONAL AND STATUTORY PROVISIONS

The Constitutional and Statutory Provisions cited herein, Appendices E through G, are: U.S. Const. Amend. V (Appendix E, App. a); U.S. Const. Amend. VI (Appendix F, App. a); and Title 18 U.S.C. § 1030.

STATEMENT OF THE CASE

1. Course of Proceedings in the Courts Below

On February 19, 2015, Petitioner was charged in a superseding indictment in the United States District Court for the Northern District of Texas, Case No.: 3:11-CR-00386-B-1, with two counts of computer intrusion causing damage, in violation of 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(B)(i). Each count alleged Laoutaris caused damage to computers owned by Locke Lord Bissell and Liddell, L.L.P. ("Locke"), with count one occurring on or about December 1, 2011, and count two occurring on or about December 5, 2011. (App. 1a). Petitioner pleaded not guilty and went to a jury trial.

Following a seven-day trial, beginning on September 21, 2015, a jury found Petitioner guilty on the two counts of computer intrusion. On each count, the court sentenced Laoutaris, *inter alia*, to a within-Sentencing-Guidelines-term of 115 months' imprisonment, with the terms for each count running concurrently. The court also ordered Laoutaris to pay $1,697,800 in restitution. The Petitioner timely appealed his convictions and sentences to the Fifth Circuit, raising the following:

Regarding his conviction, Petitioner maintains the evidence at trial was insufficient to support the jury's verdict for both counts of conviction because there was no proof he was the person who accessed Locke's network and caused the damage that occurred on

the relevant dates. His related challenge to his conviction is his claim that, due to his trial counsel's failure to preserve this sufficiency challenge for appeal, his trial counsel was ineffective in that regard, with the differing standards of review for preserved and unpreserved sufficiency challenges serving to satisfy the prejudice prong of his ineffective-assistance claim. (App. 2a).

Regarding his sentence, Petitioner contends that the court committed clear error by applying an obstruction-of-justice adjustment under Guideline § 3C1.1 based on finding he committed perjury in his testimony at trial; and by increasing his base-offense level, by including $1,461,910 in lost revenue in the total amount of actual loss for purposes of Guideline § 2B1.1(b)(1). (App. 3a-4a).

On January 29, 2018, the Fifth Circuit affirmed Petitioner's conviction and the district court's judgment in *United States v. Laoutaris*, 2018 U.S. App. LEXIS 2102 (Appendix A), after finding that "there was ample circumstantial evidence identifying him as the perpetrator of these offenses" (App. 3a); and, "because his sufficiency challenge fails even under the preserved-error standard of review, his ineffective-assistance claim also fails on this basis" (*id.*). The Fifth Circuit also affirmed Petitioner's sentence, after finding that "the record shows the court's obstruction finding was plausible in the light of the record as a whole, the finding was not clearly erroneous" (App. 4a); and "because the court's actual-loss finding was plausible in the light of the record as a whole, there was no clear error in this regard" (*id.*).

2. Statement of the Facts

a. The Government's Case at Trial

After opening statements were completed, the government called the first witness, Jerry Clements, Managing Partner of the Locke Lock law firm. He described a day back in the Fall of 2011 in which his lawyers were unable to access emails, communicate with clients, prepare for and effect business transactions and file court papers because their system was basically shut down. (*See* Record on Appeal ("ROA") 679-81).[1] Despite their best efforts, both internally and through contacting external resources, the IT department was unable to identify the problem. (*Id.*). When they determined that it rose to the level of needing outside advice, Clements contacted the FBI in Dallas. (ROA 697). Additionally, Locke Lord hired several security companies to assist them and the ultimate finding was that someone had created a portal into the system and was using it to get in and disrupt their business. (ROA 704).

The next witness called by the government was Jerry McEachern, chief information officer at Locke Lord. (ROA 714). He interviewed and actually hired the Petitioner to work for Locke Lord and had considered him to be a senior level IT engineer and one of the strongest members of the department. (ROA 759-60). In 2011 there were only two approved ways for employees to remotely access the Locke Lord System: VPN and Citrix. However, senior System Engineers would have the authority

---

1 Citings to the Record on Appeal are taken from the parties' appellate briefs because Petitioner has not received a copy of the ROA to make independent references or submit to the Court in the Appendices. Despite the granting of his Application for an Extension of Time of 60 Days by this Court, counsel refused to send it to him in time for submission with this Petition.

and the level of ability to add programs like LogMeIn to their laptops and to the network. (ROA 773). An engineer's credentials as a super user allowed them to do pretty much anything on the network. (ROA 776-777).

On October 20, 2011 a number of user accounts for attorneys, secretaries and IT staff lost connection between their email system and the Active Directory System and attorneys and others could not access their emails, although the emails still existed in the system. (ROA 780-781). The connection was eventually restored. Then two days later, a number of accounts and mailboxes were deleted. In this case the email boxes were actually gone. (ROA 787). This time they called an outside company, Sentinel, to assist. Despite reviewing the system logs they were not able to determine the cause of these incidents. (ROA 793). After these events Locke Lord installed a program entitled Change Order that monitors significant changes in Active Directory and send out notifications. (ROA 795).

The next significant event occurred on December 1, 2011, when a number of Active Directory objects were deleted that created a situation where users were not able to log in and also data on the storage Area Network SAN was "wiped". About half of the firm's desktop's, laptops and servers were deleted, making it impossible to access client files or emails. (ROA 795-97). As before, the data is still there but the account was gone. (ROA 800). When these events occurred, both in October and in December, Petitioner was no longer working with Locke Lord and his active directory account had been deleted. (ROA 805). On December 5, 2011, one of their critical email servers was changed to look like a different server in a different company. (ROA 805-06). As a result

users were unable to get their emails because they could not access the right server. (ROA 808). The emails became associated with another domain – Azafata, which was not related to the firm at all. As a result users were unable to get to their emails because they could not access the right server. (ROA 808).

During cross examination, McEachern stated that for a person to access the Locke Lord system from the outside through VPN they would have had to have a user name, password and perhaps (if they were in use at that time) a token – which is a factor authorization where a device gives the user a special serial number that changes every 30 seconds. (ROA 865-66). However, LogMeIn will not allow access in and of itself. The person would have to have a user id and a password to have access. LogMeIn just allows you to do that remotely. You have to have access to begin with. LogMeIn will not pierce a firewall on its own. (ROA 874-75). Petitioner left the employment of Locke Lord on August 19 2011. His account was disabled and the passwords had been changed and he did not have the ability to get onto the system after he left. (ROA 933).

The next witness was John Paradysz, who in 2011 was the IT director in the Houston office of Locke Lord. (ROA 940) Petitioner was an engineer in his department and reported to him. (ROA 941). He stated that Petitioner was one of the best engineers that he ever worked with. (ROA 943). On August 19, 2011, Petitioner left to take on a new job at another company and in an email left a phone number and an email address at c_hockland@hotmail.com as a way to contact him. (ROA 943). During cross examination, the witness testified that on or before October 21, 2011, based on an email contained in Petitioner's Exhibit ("DE") #3, Petitioner's admin account (NSADM3) was

disabled and was no longer functional. (ROA 981). Locke Lord procedures were that, when an employee leaves the firm, passwords are changed and that individual's account is disabled unless the admin account had jobs or scripts that were running in which case the password would be changed right way and then once all scripts using the admin account were identified, then the admin account would also be deleted. (ROA 985-86). Petitioner's Exhibit ("DE") #8 was admitted into the evidence. The witness identified this Exhibit a short email string dated December 8, 2011, in which witness asked Kenny Bradford, senior engineer at Locke Lord in Dallas if password for NSADM3 (Petitioner) was changed when he left the firm – to which response was absolutely. After Petitioner left the firm the account was gone as it related to him having access. (ROA 1001-02).

The Government then recalled Jerry McEachern, who testified about a report created by Sentinel regarding intrusion into the Locke Lord computer system. Sentinel was looking for intrusion utilizing the program LogMeIn and found that the program was installed on the Houston Office backup server and that someone was using the server as an entry point into the Locke Lord network. (ROA 1040-41). Under cross examination the witness admitted that LogMeIn did not have to be installed from someone physically inside Locke Lord it could have been remotely installed. (ROA 1056-57). There were six or seven other engineers other than the Petitioner who had permission to install such programs. (ROA 1058).

The next witness the called by the Government was Kelly Hurst , director of sales engineering at Softlayer Technologies where he worked with Petitioner. (ROA 1066). He was shown Government's Exhibit ("GE") #85 which was an event log dated October 1,

2011, showing the IP address 75.125.126.8 for Softlayer corporate network utilizing LogMeIn to access a computer designated HOBK01. (ROA 1071-73). He was then shown GE #98 which was an event log for December 1, 2011, showing SVC_GN logging into HOBK01 through LogMeIn.(ROA 1076-77). This was done through the Softlayer Houston Office wifi which would require that the user be in or near a wifi access point within the office. (ROA 1078). He was further shown another Exhibit (#120) which was a similar event log for December 5, 2011. (ROA 1078-80).

The witness stated that Petitioner's was terminated from Softlayer for not badging in (logging in his badge upon arrival at the building) and had not badged in to the building for five or six months. The time frame involved included the period from September through December of 2011. Petitioner had explained that he had been working remotely and had not been in the building and was instructed that this was not acceptable and to physically show up for work at the facility. He complied but later would badge in and then leave within five minutes to an hour later. As a result he was terminated. (ROA 1101-03).

The Government's next witness was Christian Diaz, IT project manager for a commodities trading company named Trafigura. (ROA 1111-12). He hired the Petitioner through a staffing agency to work for Trafigura in August of 2011. (ROA 1113-15). The Witness was shown GE #35 which showed c_hockland@hotmail.com logging into HOBK01 with the user IP address of 74.202.38.20, which shows that someone logged onto the Houston address of 74.202.38.20, which shows that someone logged on the Houston backup server of Locke Lord from the Trafigura IP address. (ROA 1127-28). On

cross examination, it was pointed out that DE #10 shows another Locke Lord employee NSADM2 utilizing the IP address of Trafigura, although he was not actually there.

The witness stated that there is no way to tell where that person was physically located, just that they were using the IP address. The witnessed the concept of spoofing where someone can be doing something and making it appear that they are someone else. It was also brought up that Petitioner left his laptop at the company when he left their employment. That laptop was never analyzed. (ROA 1131-34).

The next witness was Stanley Guzik, senior systems engineer with Locke Lord in Chicago. The witness was shown DE #3 which shows that Petitioner's account was disabled and could no longer log into the Locke Lord network. (ROA 1140). The witness also showed DE #10 which shows on October 7, 2011, through LogMeIn that user NSADM2 (Kenny Bradford – principal engineer from the Dallas Office) logged into the Locke Lord network, which would have been a violation of company policy. The witness agreed that is a person could control Mr. Bradford's account they could control other accounts within Locke Lord if they had credentials. (ROA 1163-64). The Witness testified that he was interviewed by the Secret Service about this case and he stated that he did not think that Petitioner was the perpetrator of these events because he lacked the hands on experience with Cisco Systems or the motivation. (ROA 1178-80).

The next witness was Kenneth R. Bradford, principal engineer at Locke Lord. (ROA 1188). The witness is shown DE #10 which he identifies as a log file showing NSADM2, which he identifies as himself, logging into the Locke Lord Houston Backup server from, based on the IP address from Trafigura on October 7, 2011. He states he did

not do this. (ROA 1190-92). He agreed that someone did log in using his account but that was not his activity. (ROA 1193-94).

During cross examination he agreed that someone looking at it could be deceived and if his account could be controlled in this fashion so could someone else's account. (ROA 1229-30). He then reviewed an email string (DE #8) in December of 2011, stating that the password for NSADM3 (Petitioner) had been changed and that determined that the Petitioner's account was gone, not available for use. (ROA 1229-31). The Exhibit also reflects that he removed the account from the VPN group so that it could not utilize remote access.(ROA 1231-32). As a result anything that occurred on the NSADM3 account would have had to have been done internally in Locke Lord. (ROA 1232-33). The witness stated that after Petitioner left Locke Lord he could only access the firm network if he knew the credentials to another account. If he attempted to access using his old account and password he would not have been able to enter the network. (ROA 1235-36).

The next witness was a witness for the defense. Michael Ger, systems engineer for Locke Lord. He was interviewed by the Secret Service in 2014 and he stated that he did not believe that Petitioner had done what he was accused of doing because he lacked the actual hands-on experience and had just some basic knowledge or superficial knowledge for an engineer. (ROA 1269).

The government then called Dave Petty, an IT engineer who had worked for Sentinel and was tasked with investigating the events described in this case--what happened and come up with a root cause, either a system or an individual. (ROA 1275).

The first event was difficult to analyze because the built in auditing on the mail server was not very robust and the best he could do was recommend that Locke Lord adjust the auditing so that it could capture future events. (ROA 1281-82) The second event occurred about 24 hours later and the user accounts were outrightly deleted. The fact that they happened so close together made him believe that this activity was not accidental. (ROA 1282-83). However, at this point he has not ruled out any possible sources of the problem, including malware and viruses.(ROA 1287). He was brought in again in December when there were further deletions of users and groups. (ROA 1289). This time in looking through the logs he was able to see that a particular user account was causing deletions, SVC_GN which was a general service account. (ROA 1290). On December 5, there was a second event. In analyzing the event he was able to find a session ID and then the client workstation IP address from which they were logging in. (ROA 1296).

Once he traced the contact to the Houston Backup Server, he found the application LogMeIn and his immediate reaction was that he found how the person was getting in. (ROA 1298-99). He disabled it immediately. The witness was shown GE #135, which he identified as a screen shot that he took of the settings window in LogMeIn that was installed on the Houston Backup Server, which showed the computer name that LogMeIn was associated with: c_hockland@ hotmail.com. (ROA 1303-05). Someone in the IT staff recognized this email address as that of the Petitioner. (ROA 1306).

On December 6, 2011, he was monitoring the system and observed attempted connections while he was looking at the server. He turned off the server to prevent the connection. (ROA 1309-10). He was able to see the IP address of 108.214.249.83, which

review of AT&T records (GE #16) shows to be a customer, Violeta Zoeller Laoutaris. (ROA 1312-17).

On cross-examination the witness was shown DE #10, which was a computer shot dated October 7, 2011, source LogMeIn, computer HOBK01, and reads: User Locke Lord NADM2 (Kenny Bradford) has successfully logged on from IP address 74. (ROA 1411). The witness stated that he had never seen this screen-shot before today and wished that he had known of it when he was doing his work back in December 2011, because whoever did this would have had to have that user account name and password, and it is something that he would have pursued. (ROA 1412-14). Even though LogMeIn was an unauthorized program Locke Lord had no technical enforcement of this rule so the written policy was not enforced and if they did not have any detection mechanism for what was installed on the machines then other programs other than LogMeIn could also have been used. (ROA 1415).

The next witness for the Government was Christopher Pogue, senior vice president of Cyber Threat Ananlysis at Nuix. (ROA 1427). At the completion of his investigation he came to the conclusion that the events caused on the Locke Lord system in October and December were caused by interaction with the domain controlled by the user account SVC_GN through the remote administration application LogMeIn. (ROA 1452-53). After describing long string of event which occurred during that session, including the deletion and/or disabling of many user accounts and other events, he stated that these events were generated by user SVC_GN signed on from IP address 75.125.127.4, which they were able to trace back to the Planet. (ROA 1514-15). Because of the interaction

and commands required, he believes the deletions and disabling commands were deliberate and not by a mistake or an accident. Over the space of quite an extremely lengthy exchange, he individually traced numerous incidents of activity to LogMeIn accessed from IP address 70.250.175.91, which he testifies goes to the router in the home of Petitioner's wife from IP address 75.125.126.8, which is registered to the Planet. (ROA 1589-90). He stated the IP address, 70.250.175.91, is assigned to a border router that is physically at the residence of Violeta Zoeller. (ROA 1631). When LogMeIn recorded each of the events occurring on October 13 and 14, 2011, on the HOBK01 server it was the SVC_GN account that generated these events. (ROA 1633).

The events that occurred on October 19 and 21, 2011, through LogMeIn on HOBK01 through SVC_GN account originated from IP address 75.125.126.8, which was assigned to The Planet. (ROA 1633-36-90). Interestingly the events that occurred on November 3, 2011, through LogMeIn on the HOBK01 server generated by SVC_GN came from the IP address of 208.51.212.88, which was assigned to Trafigura located in the city of Amsterdam in the Netherlands. (ROA 1636-37). On November 25, 2011, another similar connection was made from the IP address assigned to Violeta Zoeller. (ROA 1637-38). On December 1 and 5, 2011, access was initiated from the Planet. There was an unsuccessful attempt to connect, initiated on December 6, 2011, from the Zoeller IP address. (ROA 1614). There was a further log in attempt on December 6, 2011, made on the LogMeIn servers from IP address 38.100.85.66, which is located somewhere in Europe. All of these log ins, even those from europe, showed LogMeIn utilizing the email connection of c_hockland@hotmail.com. (ROA 1646-47).

During cross-examination, the witness testified that the planet was a third party provider giving internet connectivity and do not actually provide security protocols. As such they struggle with activity where people rent a server and engage in fraudulent activities. (ROA 1624-25). The identification information with regard to the Planet just provides the IP address, not the user, and he did not cross check Petitioner's hours of employment to see if he was present at the Planet when the activity occurred.(ROA 1727-28) He also testified that he could only connect the activity of the IP address not to the Petitioner or any specific computer. There can be up to 254 computers on a class C router. (ROA 1742-44) He also agreed that it would be very stupid to engage in criminal activity like in this case and leave your own identifying information behind. (ROA 1745-46). He also confirmed that if you did not have the password to get you in the Locke Lord network, LogMeIn will not get you into th network without a password. (ROA 1767-68). Petitioner's email address was entered into LogMeIn by whomever installed it on the Locke Lord backup server. However, no analysis into who (what user) installed LogMeIn on the Locke Lord backup server. (ROA 1770-75).

The next witness called by the Government was Andy Sawyer, Director of Security at Locke Lord. He authenticated GE #195, which is a diagram of Locke Lord's wide area network and access to the internet as it existed in 2011. (ROA 1836). The Government then called Denise Wilkerson where she works as an Associate Director of Asset Protection. (ROA 1851). She Authenticated GE #16, which were billing records for Violeta Zoeller. She also authenticated the U-Verse static IP address of 108.214.249.83, which was applicable to the account of Violeta Zoeller, which was

installed on November 30, 2011. (ROA 1832-36). At the conclusion of this witness' testimony, the Petitioner moved for a judgment of acquittal. (ROA 1860).

b. The Defense's Case at Trial

Petitioner called his first witness William Charles Eastom II, a computer scientist, teacher, consultant and lecturer. (ROA 1890). He was engaged by Petitioner to investigate the case and render conclusions. To do so, he evaluated the logs and emails produced by the Government as well as the other evidence and reviewed Petitioner's resume to determine if he had the skills to do the sort of things that had been alleged. (ROA 1899-1900). He believes that the approach from the Government's expert was to pick a focus, the Petitioner, and to focus the investigation to look for evidence that supports that conclusion. (ROA 1902).

With regard to IP address, the way it works is that a business or a residence has an IP address which is the public or gateway IP address. It was not traced back to an individual source or laptop, device or PC. (ROA 1904). An expert would need to figure out what happened once someone connected to the Houston computer to explain how they were able to knock servers in Los Angeles and San Francisco off line. Further, if he had a suspect in mind he would have to retrieve their computer to analyze it. If they were a previous employee, he would examine the computer that they used at the firm. (ROA 1905). He noticed several issues that caused concern for him.

First, he noticed that LogMeIn entry was coming from lots of places, not just Houston. They were coming from Colorado and Korea.(ROA 1906). Second, he noticed from an email that three servers were detecting LogMeIn but the program was not

actually installed on them. That is a "false positive." Additionally one of their common networking software utilities (SolarWinds) was also triggering false alarms – which means to this expert that it is not possible to know which of the alerts were false and which were real. (ROA 1906-07). When he sees a transaction that says it was a sign from LogMeIn on a particular date he does not feel that he knows that it really was because of the false positives. The only way to be sure would be to look at the actual machines in question and see if they did in fact log in. That was not done. (ROA 1909). Locke Lord had been having issues back to 2009. (ROA 1910).

The witness testified that tracing the IP address back to Softlayer does not tell you anything since it only traces you back to the gateway, not to the machine inside the company that did it. He looked up Softlayer and discovered that it was reported to have 700 employees so you can only narrowed it down to these 700 and it is further possible that someone else has breached their machine and was spoofing the IP address. (ROA 1911). Softlayer is known for having bad security. They have been breached in the past and hackers have used them to attack people. Spammers have used them to send out annoying spam emails. They were on a list of companies in 2011 that were known to have been breached by the Chinese who used their netowrk as what is called "command and control center" to attack other networks. (ROA 1911). Further, LogMeIn is the most commonly breached and misused software in the world. This expert has yet to do a security audit that did not involve someone using LogMeIn. (ROA 1912).

Mr. Easttom was also concerned about the fact that Locke Lord, in 2011, did not have intrusion detection system on their network. (ROA 1912-13). With regard to

Petitioner's email being tied to LogMeIn it is very easy to use or spoof someone else email. You can even go to Google and watch a tutorial on how to do it. (ROA 1914-17). The windows registry saves passwords so we wont have to keep entering them and that makes it easy to steal them because they have terribly weak encryption. The same is true for databases and domain names—the login information is stored. (ROA 1917-18). There are publicly available free tools that can be installed and will extract all the service passwords, wifi passwords, and everything that has ever been used on a machine. (ROA 1918).

He also stated that he disagreed that just because someone entered the Houston Backup Server that it could be assumed that they also took out the other servers. There was no analysis as to how that may have occurred or how did it, if they did. (ROA 1921). He was concerned that emails stated that they imaged three servers but he never saw a report as to what had been discovered or what conclusions were reached and that there was also spyware found on the Locke Lord network. Since the main purpose of spyware is to get passwords, this is very significant since anyone could have had their password compromised. Also the fact that LogMeIn used an email as a user name is of no value unless you track it down to the person's computer to see if they were actually doing it. (*Id.* 1921-22).

The witness doubts that Petitioner has the skill the events that occurred in this case fror several reasons. First, his resume does not demonstrate any education what would relate to hacking or forensic work, which are very specialized. Second, these attacks are coming from multiple IP addresses that are geographically distributed such as jumping

from the Houston server to L.A server to San Francisco Server. (ROA 1963-65). This is what leads the witness to believe that these events are the work of highly skilled Chinese hackers who can go through multiple compromised systems and use those to go after the target and hit them from multiple sources. It would be very hard for a lone individual to do this. (ROA 1970-71).

The witness was asked why the Chinese would want to hack into the Locke Lord's network and he responded that he has been hired by Locke Lord on three times in the past as an expert witness in patent cases and that the law firm is well known as one of the top intellectual property firms with many many clients and the amount of intellectual property store in their servers is staggering. Breaching them would be like breaching the computers of many companies. Hitting the mother lode of intellectual property. (ROA 1992). In redirect examination the witness stressed again that no one ever looked at Petitioner's work machine at Softlayer, or at his work machine at Locke Lord, or at his home computer, so a complete investigation was not done. Thus, neither party can definitely know what happened because you cannot look at the evidence to see what is more probable. (ROA 2071-72)

The next witness was the Petitioner, Nick Laoutaris. He worked at Locke Lord from March 2006 until August 19, 2011. He left Locke Lord because he was going to take a position at Lockheed Martin that was currently on hold so instead he took a contract position at Trafigura that was offered to him to wait for the Lockheed Martin position to open up again. (ROA 2102). At this time, he was also taking classes at Texas A&M in aerospace engineering and the course work was getting very demanding

especially since he lived 100 miles away from campus. (ROA 2103). He denied planting a malicious code or program to try to damage the Locke Lord network. (ROA 2112). In 2010 he noticed problems with regard to his email account. He would have trouble sending and receiving emails.

Also, people would receive emails from him with random links that he did not send. He was force to continue to use it because he had used it for many years and it was the only means of communication between him and recruiters and potential job opportunities. (ROA 2113-14). He was just more careful about what kind of information that he sent through that email and he kept it for business purposes only. (ROA 2115). DE #11 was admitted showing communication from Petitioner to experts-exchange support group trying to solve these problems with his email account. (ROA 2116-17). His emails were redirected to .mirzameginnis1288@ gmail.com (ROA 2117-18). He was also having trouble with his credit cards having unauthorized charges at locations 60 to 70 miles to the south of where he lives. (ROA 2121). DE #63 was admitted, it contained two emails from 2010 showing that spam emails being sent from Petitioner's email c_hockland. (ROA 2150-51).

Petitioner's Exhibit #26 was admitted which was an email string in which it is described that Petitioner sent a USB drive to Christian Kabel at Locke Lord that inadvertently contained personal information from Petitioner (copies of ID, social security, green card, personal accounts and passwords, including his wireless network password and other documents). He requested that it be sent back to him but he never received it. (ROA 2122-2126). DE #55 was admitted showing that even after he had left

the employ of Locke Lord he was still communicating with Locke Lord employees (Christian Kabel) trying to locate and had not yet retrieved the lost USB drive. (ROA 2128-29).

At Locke Lord, Petitioner started out as an IT systems administrator and although his actual title changed several times he did not necessarily get a new set of job responsibilities. (ROA 2131). If any engineer like himself wanted to make a change to the network they would have to get approval at a minimum from Christian Kabel who then might escalate to Chris Gradziel. No one else had "write" access. He had "read" access which means he could look at the configuration but not make any changes. (ROA 2131-33). Changes to the system was monitored by Cisco through a system called Cisco Works. It is a log, so if you make changes you can go back and reference the configuration and remove the changes in case something would break after someone would make a change. Also, every time that someone would make a change to the Cisco configuration, Cisco would automatically generate an alert saying that the configuration was changed at that date and time and by whom so that there could be accountability. (ROA 2134).

Petitioner was then asked to review GE #35 and his attention is called to where the document states under "computer" the designation of "Nick-SLAYER". He stated that he does not recognize that name and says that it definitely is not Softlayer nomenclature which includes the first name, last name, and the LT for laptop or PC for workstation. (ROA 1957) He also asked to look at the designation of Nick LLBL and he states that he does not recognize it. He states that LLBL probably stands for Locke Lord Bissell and

Liddell but an official name from Locke Lord would have been the first name, last name dash Locke Lord and then the type of device LT for laptop and PC for a workstation. (ROA 2158).

He described when secret service agents interviewed him at his house. They stated to him that they wanted to talk to him about Locke Lord. (ROA 2161). The agent had a stack of paper and told him that they already knew everything but were looking for some honesty and to let the Petitioner tell his side of the story. His initial feeling was of suspicion that these men were actually secret service because he thought that secret service only interviewed people accused of threatening the President and also they were dressed casually, with one agent in jeans, tennis shoes and a Hawaiian shirt. (ROA 2160-62). He and his wife were concerned about this visit and Petitioner's wife asked if they were going to arrest Petitioner. They stated that Petitioner is not going anywhere tonight and they just wanted to ask a few questions. Petitioner became very concerned and asked them to allow him to speak to legal counsel because he was not aware of what his rights were. Despite the casual dress he stated that the agents were very polite and professional and gave him a business card and told that he could contact them if he wanted to talk to them and the conversation ended. (ROA 2162-63). There was no mention of computers at that point and no one ever came back to get computers from his house or question him for any reason. (ROA 2165-66).

Petitioner was asked to recall testimony regarding an account called "administrators" on the Locke Lord network. He stated that administrators is not an active directory account on the Locke Lord network the account is actually called

administrator which is a very different entity because there is no "S" on the end. (ROA 2167). He was familiar with LogMeIn because he got a promotional email and signed up for an account because he thought it could be used as a desktop in case he wanted to do a presentation but later on he realized that it was a product that would be against the policy. (ROA 2167-69). Petitioner is then asked to consider DE #1, which is an email dated back in August 10, 2011, from him to Mikhail Ger and Stan Guzik at Locke Lord in Chicago asking about the password of SVC_GN and inquiring if it was changed because he could not get his password to work. Mr. Ger and Mr. Guzik knew that he was leaving the company soon so they did not send him the password. (ROA 2171-74).

Petitioner testified that he did not use SVC_GN after he left Locke Lord. He did not have access to the Locke Lord network after the password was changed they did not give him the new password because they knew he was leaving. (ROA 2176). When he left Locke Lord he surrendered his access badge and the VPN token, which looks like a Zip drive or small key, as well as paperwork and the binder with the projects that he was working on. (ROA 2179). The token has a password that changes every minute so that stops someone from logging in as another person unless they have a token. SVC_GN did not have a token because it is a robotic account and could never leave the premises and therefore did not have remote access. (ROA 2181). Petitioner did not continue to work for Locke Lord after he left. (ROA 2180).

Petitioner was shown DE #10 which shows an event log from Locke Lord's Houston Backup Server 01, dated October 7, 2011, at 7:25 pm, using LogMeIn from the IP address that corresponds to Trafigura. Petitioner worked for Trafigura at that time but

his hours were either 8am to 5pm or 7am to 4pm. The company would close at 5pm. It was a trading company and it closes when Wall Street and the traders would go home and the department would leave. (ROA 2102). Additionally, since Trafigura was a trading company, the network was highly monitored in real-time so LogMeIn would be blocked. (ROA 2104). He denied any connection to the IP addresses that are far away from Houston. (ROA 2105).

He was asked to look at a screen shot of LogMeIn from the Planet on November 25, 2011, which was the Friday after thanksgiving. The Friday after thanksgiving was a holiday for the employees, the company was closed, and he was not at work on that day. (ROA 2193-94). He then testified about his work at Softlayer. LogMeIn was not allowed at Softlayer. He was not an engineer there. He worked for Kelly Hurst supporting the sales department making sure that the customers were served and to help keeping the sales persons honest because it was a high pressure sales environment with emphasis on numbers and quotas. Petitioner stated that after leaving Locke Lord no one from the firm would share their password with him especially not an admin password. (ROA 2195-97). There is no reason for any engineer to share his password with another engineer because every engineer has their own password. If you forgot your password you would be reassigned a new one. (ROA 2197-98). Petitioner was asked if he had animosity toward Locke Lord. He stated that he did not and that it was probably one of the best companies he has ever worked for. (ROA 2204).

On cross-examination, Petitioner confirmed that to access Locke Lord network through VPN one needs to have a token, which Petitioner turned in to his department

when he left the firm. If someone no longer worked at Locke Lord they could not access the computer through VPN because they would not have a VPN token and would need an alternative method. Petitioner was asked if LogMeIn would be an alternative method to enter the Locke Lord network if you no longer had the VPN password. Petitioner replied that if you no longer had the VPN password you could not get into the server, you need a password to do so and if you had a VPN and password you could sign in as SVC_GN and go undetected since the network would recognize you, so there is no need for LogMeIn which would be heard and be highly visible. (ROA 2257-60). After a brief re-direct the witness stepped down and the evidence of the trial concluded. (ROA 2303).

c. The Verdict, PSR and Sentencing

After closing arguments the jury deliberated the case and found Petitioner guilty on both Counts 1 and 2. (ROA 2418). After the preparation of a per-sentencing report ("PSR"), to which the Petitioner filed numerous objections, a sentencing hearing was held on April 14, 2016. Several objections focused on factual assertions in the PSR which did not affect the sentencing guideline range; however, there were three objections that addressed enhancements that added time to the Petitioner's eventual sentence by elevating the guideline range.

The first of these objections was to the enhancement for obstruction of justice. Petitioner asserted to the court that the statements Petitioner made to the court were not false and that he should not be punished for denying the allegations in the indictment as he is basically charged with obstruction because he went to trial and got convicted. (ROA 2442-44). This objection was overruled. (ROA 2449-56). The next objection was

the use of a computer enhancement because the indictment charges transmitting a malicious code and doing so through the use of a computer so this issue has been assessed within the base level of the offense. This objection was also over-ruled. (ROA 2456-58). The court then considered Petitioner's objection to an enhancement for role in the offense and overruled this objection also. (ROA 2501, 2503-05). The court then considered the loss amount attributed to Petitioner.

The PSR found the following damage components all occurred in October and December of 2011:

$198,128 direct expenses from on-site consultants;
$ 6,979 travel expenses; and
$ 30,783 in overtime paid to IT employees; for a
total of $235,890 in actual loss.

However, the PSR went on to find $1,461,910 in "lost revenue" which bring the grand total up to $1,697,800. (ROA 2987). Petitioner objected that the amended PSR increased the loss amount through the inclusion of four computers intrusions with two outside December 2011, which are contained in the superseding indictment. Additionally, the loss amount under 18. U.S.C. § 1030 should include only amounts necessary to restoring data, programs, and systems rather than billable hours that allegedly could have been performed, irrespective of whether the work was available; whether the work would have been done; whether payments would have been collected; and the tax liability on that amount. (ROA 2493-96; 2993-94).

Following the testimony of Allen Shank, forensic accountant hired to testify in support of the damage claim, the court adopted the finding of the PSR on the loss

amount. (ROA 2502). After the court considered the § 3553 factors and Petitioner's sentencing memorandum requesting a downward departure, Petitioner was sentenced to 115 in custody on each account, to run concurrently, and restitution of $1,697,800. (ROA 2519).

Petitioner timely appealed. As shown, *ante*, at pp. 2-4, the Court of Appeals for the Fifth Circuit affirmed the district court's judgment. Petitioner eventually files this writ of certiorari in this Court to review the Fifth Circuit's decision.

REASONS FOR GRANTING PETITION

I. THE FIFTH CIRCUIT ERRED AND ITS DECISION IS IN CONFLICT WITH THIS COURT'S HOLDING IN *JACKSON V. VIRGINIA*, 443 U.S. 307, 99 S.CT. 2781, 61 L.ED.2D 560 (1979), WHEN IT DECIDED THAT A RATIONAL JURY COULD HAVE FOUND EACH ESSENTIAL ELEMENT OF THE OFFENSE OF TRANSMITTING A MALICIOUS CODE, IN VIOLATION OF 18 U.S.C. § 1030(a)(5)(A) AND (c)(4)(B)(i), BEYOND A REASONABLE DOUBT

Although when determining whether there is sufficient evidence to support a conviction the evidence is viewed in the light most favorable to the prosecution and all reasonable inferences are drawn therefrom in its favor, no rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt in this case. *See Jackson v. Virginia*, 443 U.S. 307, 319, 99 S. Ct. 2781, 61 L. Ed. 2d 560 (1979). Even though, "[c]ircumstantial evidence and inferences drawn from it may be sufficient to sustain a conviction[,]" *United States v. Jackson*, 72 F.3d 1370, 1381 (9th Cir. 1995), the prosecution cannot stack inferences upon inferences to achieve that goal. *See In re Winship*, 397 U.S. 358, 364, 90 S. Ct. 1068, 25 L. Ed. 2d 368 (1970) (the Due Process

Clause of the Fifth Amendment protects a Petitioner in a criminal case against conviction "except upon proof beyond a reasonable doubt of every fact necessary to constitute the crime with which he is charged.").

In this case there are huge holes in the prosecution's case in which there was no evidence to bridge the gaps, except the prosecution piled inferences upon inferences into them, a practice that is rejected by this Court since *Winship*, in concern about the injustice that results from the conviction of an innocent person. *Winship*, 397 U.S. at 372 (the "fundamental value determination of our society [is] that it is far worse to convict an innocent man than to let a guilty man go free.") (Harlan, J., concurring); *see Addington v Texas*, 441 US 418, 423, 60 L Ed 2d 323, 99 S Ct 1804 (1979). Thus, although circumstantial evidence is sufficient to prove guilt, the prosecution cannot stack inferences upon inferences to prove that the Petitioner is guilty, which is what was done in this case.

That is so because the evidence shows that Petitioner did not have the password to Locke Lord's computer system and he left their employment and did not have a token that was needed to remotely access Locke Lord's network. Petitioner left the employ of Locke Lord on August 19, 2011. It was uncontested that his account was disabled and the passwords have been changed. *See* Facts, *ante*, at p. 10. Petitioner was not working on any projects and did not have any ability to get on the system after he left. This was confirmed by internal emails from Locke Lord. Petitioner was accused of utilizing the program called LogMeIn to access the Locke Lord network despite the fact that LogMeIn alone would not allow someone to enter the system without the system password and

token. Conversely, if Petitioner had the password and token, utilizing LogMeIn was completely unnecessary since a person could have simply utilized the remote access program already installed on the system rather than LogMeIn which was unauthorized and would attract attention on the system.

In 2011 there were two approved ways for employees to remotely access the Locke Lord system. VPN and Citrix as opposed to other programs like LogMeIn. For a person to access the the Locke Lord system from the outside through VPN they would have had to have a user name, password and perhaps (if they were in use at the time) a token – which is a factor authorization where a device give the user a special serial number that changes every 30 seconds. After the Petitioner left Locke Lord he could only access the firm network if he knew the credentials to another account. If he attempted to access using his old account and password he would not have been able to enter the network.

LogMeIn is not tied exclusively to Petitioner, even if it were, senior system engineers would have had authority and the level of ability to add programs like LogMeIn to their laptops and to the network. Under cross-examination a government witness admitted that LogMeIn did not even have to be installed from someone physically inside Locke Lord, it could have been remotely installed. There were six or seven engineers other than Petitioner who had the ability to install such programs. Government witness Stan Guzik agreed that DE #10 showed that, on October 7, 2011, after the Petitioner had left the employ of Locke Lord, user NASDM2 (Kenny Bradford – principal engineer from the Dallas Office) is recorded as utilizing LogMeIn to log into

the Locke Lord network, which would have been a violation of the policy. If a person could control Mr. Bradford's account then they could control other accounts within Locke Lord provided that they had credentials. Further the witness testified that when he was interviewed by the Secret Service about this case he stated that he did not think Petitioner was the perpetrator of these events because he lacked the hands on experience with Cisco Systems or the motivation. *See* Facts, *ante*, at p. 10

Mr Bradford himself was shown DE #10 which he identified as a log file showing NSADM2, which he acknowledges as himself, logging into the Locke Lord Houston Backup server from, based on the IP address, a company called Trafigura on October 7 2011. He states he did not do this, that someone must have logged using the account NSADM2 and that it was not his activity. During cross-examination he agreed that someone looking at this exhibit could be deceived into thinking it was his activity and that if his account to be controlled in this fashion so could someone else's account. *See* Facts, *ante*, at pp. 10-11. It is very telling that the Government did not share this evidence with his own witness.

Dave Petty was hired by Locke Lord to come up with a root cause for the intrusion of the network. When the witness was shown DE #10 showing Mr. Bradford accessing the system he stated that he had never seen this screen shot before today and wished he had known this when he was doing his work back then. He stated that whoever did this activity would have had to have the user name and password. If he had known this information back in December of 2011 it is something that he would have pursued. LogMeIn alone will not get you onto the Locke Lord network. Mr. Petty agreed that if a

person did not have the password to get you into the Locke Lord network. LogMeIn will not get you into the network without a password. He also agreed that it would very stupid to engage in criminal activity like this case and leave your own identifying information behind for people to discover. *See* Facts, *ante*, at pp. 12-14.

Clearly third parties were utilizing compromised systems to access the Locke Lord systems to access the Locke Lord systems as Log-ins occurred at very close time frames from widely separated geographical locations including other states and foreign countries, which indicates that the intrusion was not the action of the Petitioner. Additionally the network was accessed from a company called Softlayer at times (including Thanksgiving Day evening) in which Softlayer was closed. For example, events allegedly tied to the Petitioner that occurred on November 3, 2011, through LogMeIn on the HOBK01 (Houston Backup Server) generated by SVC_GN, came from IP address of 208.51.212.88, which was assigned to Trafigura located in Amsterdam in the Netherlands. There was a further log in attempt on December 6 2011 which is located somewhere in Europe. Further he noticed that LogMeIn entry was coming from lots of places not just Houston. They were coming from Colorado and Korea. All of these log ins, even those from Europe, showed LogMeIn utilizing the email connection of c_hockland_@hotmail.com, which was Petitioner's email. Also, the fact that LogMeIn used an email as a user name is of no value unless you track down that person's computer to see if they were actually doing it. *See* Facts, *ante*, at pp. 15-18.

With regard to IP address, Petitioner's expert, William Charles Easttom II, testified that a business residence has an IP address which is the public gateway IP address. It is

not tracked to the individual source laptop, device or PC. The only way to actually link this activity to Petitioner would be to look at the actual machines in question and see if they did in fact log in. That was not done. The Government only examined the Locke Lord backup server in Houston and did not examine the Dallas or any other servers, and, even more importantly did not examine Petitioner's computer at work or in his home to determine if he was the source of these alleged intrusions. Tracing the IP address back to Softlayer does not tell you anything since it only traces you back tot he gateway not the machine inside the company that did it. Softlayer is reported to have 700 employees , so you have to narrow it down to these 700 unless someone else has been breached their machine and is spoofing the IP address. Additionally Softlayer is known for having bad security. They have been breached for and hackers have used them to attack other people. Spammers have used them to send out annoying spam emails. They were on a list of companies in 2011 that were known to have been breached by the Chinese and used as what's called a command and control center – using their network to attack other networks. No one ever looked at Petitioner's work machine at Softlayer, at his work machine at Locke Lord, or his home computer. It is therefore impossible to know what happened because no one looked at the actual evidence to see what was more probable. *See* Facts, *ante*, at pp. 19-27.

II. Trial counsel was ineffective for failing to resubmit a motion for judgment of acquittal at the close of all the evidence pursuant to *Strickland v. Washington*, 466 U.S. 668, 690, 104 S.Ct. 2052, 80 L.Ed.2d 674 (1984), and its progeny

As stated above, to prevail on this ineffective assistance claim Petitioner "must establish that (1) his counsel's performance was deficient and (2) the deficient

performance prejudiced his defense." *Strickland v. Washington*, 466 U.S. 688, 687, 104 S.Ct. 2052, 80L.Ed.2d 674 (1984). Based on arguments made above in Reason I, there exists more than a reasonable probability that had counsel moved for judgment of acquittal, the motion would have been granted on the basis of insufficiency of evidence.

III. The Court of Appeals err in affirming the district court's error applying an obstruction-of-justice adjustment under USSG § 3C1.1 based on finding that Petitioner committed perjury in his testimony at trial, in contravention of his privilege to testify in his own behalf pursuant to *United States v. Dunnigan*, 507 U.S. 87, 95, 113 S.Ct. 1111, 122 L.Ed.2d 445 (1993)

The PSR alleged that the Petitioner willfully obstructed or impeded or attempted to obstruct or impeded the administration of justice with respect to the prosecution of the instant offense or conviction and the obstructive conduct related to the Petitioner's offense of conviction and any relevant conduct by testifying untruthfully at trial. Thus, the PSR increased the guideline levels by two points, under USSG § 3C1.1. The PSR set out some testimony provided under direct examination and redirect, where in the Petitioner stated that: (A) the allegations in the indictment against him are false; (B) he registered a LogMeIn account but did not personally utilized the LogMeIn program thereafter because it would not be practical or allowed by most companies; (C) while he request the Locke Lord SVC_GN password, he never received the password; (D) he was not aware the Locke Lord system was down in December 2011; and (E) where he argued that it was technically impossible for the LogMeIn program to be used to access Locke Lord Netowrk. (ROA 2953).

However, § 3C1.1 provides a two level increase in the Petitioner's offense level only if the Petitioner "willfully obstructed or impeded or attempted to obstruct or impede

the administration of justice with respect to the investigation prosecution or sentencing of the instant offense of conviction and this conduct was related to the Petitioner's offense of conviction and any relevant conduct. Examples of such conduct include committing suborning or attempting to suborn perjury." § 3C1.1 cmt. n.4(B). Given the equivocality of the evidence, there is no proof that Petitioner denials were false.

If a Petitioner objects to a sentence enhancement resulting from trial testimony a district court must review the evidence and make independent findings necessary to establish a willful impediment to or obstruction or justice, or an attempt to do the same under the perjury definition. *United States v. Dunnigan*, 507 US 87, 113 S. Ct, 1111, 122L L.Ed.2d 445 (1993); *see also United States v. Storm*, 36 f.3d 1289, 1295 (5th Cir. 1994). A Petitioner commits perjury if, while testifying under oath he gives a false testimony concerning a material matter with the willful intent to provide false testimony. United States v. Como, 53 F.3d 87, 89 (5th Cir. 1995). Separate and clear findings on each element of the alleged perjury "though preferable, not required" *Como*, 53 F3.d at 89; *see also Dunnigan*, 507 U.S at 95 ("the District Court's determination that enhancement is required is sufficient however 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"). Nevertheless, "not every accused who testifies at trial and is convicted will incur an enhanced sentence under 3C.1.1 for committing perjury" *id.* at 95. Petitioner contends following the comments contained in the notes to the Sentencing guidelines that the five instances listed as the basis for the obstructing justice enhancement are either true statements or do not amount to perjury.

Mr Dave Petty, a government witness, agreed that if a person did not have the password to get you into the Locke Lord will not get you into the network without a password, so clearly it would not be practical or effective. This is an example of a government witness agreeing with the statement made by the Petitioner. It should be noted that Mr. Petty also agreed it would be very stupid to engage in criminal activity like in this case and leave your own identifying information behind. In 2011 there were two allowed ways for employees to remotely access the Locke Lord System. VPN and citrix not LogMeIn. Again this is in agreement with the statement of Petitioner, *i.e.*, that Log Me In would not be allowed by most companies. Also these statements are true statements and made pursuant to Petitioner's plea of not guilty. It was established that for a person to access the Locke Lord System from the outside using LogMeIn, they would have had to have a user name, password and a token – which is a factor authentication where a device give a user a special serial number that changes every 30 seconds. After Petitioner left Locke Lord he could only access the firm network if he knew the credentials to another account. If he attempted to access using his old account and password he would not have been able to enter the network. (Facts, *ante*, at pp. 7-11).

Further Petitioner's expert Mr Easttom stressed that no one ever looked at Petitioner's machine at SolftLayer, at his work machine at Locke Lord, or is home computer so a complete investigation was not done so it is impossible to know what happened because you can't look at the evidence to see what is more probable. The fact that LogMeIn uses an email as a user name is of no value unless you track down that person's computer to see if they were actually doing it. You need to see if LogMeIn is

even on that computer, which was not done. The fact that Petitioner requested the Locke Lord SVC_GN password but never received it before he left is well-established by the Government's witnesses and not even contested. Petitioner left the employ of Locke Lord on August 19, 2011. It was uncontested that his account was disabled and the passwords were changed. Additionally this was confirmed by several Government witnesses and by internal emails from Locke Lord (*see* Facts, *ante*, at pp. 10-11); and so goes all the other allegations of perjury.

IV. The Fifth Circuit should have reversed the district court's error in increasing Petitioner's base-offense level by applying $1,461,910 in lost revenue to the $235,890 actual loss amount and, as a result of the erroneous calculation, imposing an unreasonable sentence contrary to this Court's decision in *Rita v. United States*, 551 U.S. 338, 127 S. Ct. 2456, 168 L.Ed.2d 203 (2007)

A determination of the loss amount is a factual finding reviewed for clear error. Under the clearly erroneous standard we will uphold the district court's finding so long as it is plausible in light of the record as a whole. However a finding will be deemed clearly erroneous if based on the record as a whole we are left with the definite and firm conviction that a mistake has been committed. *United States v. Ekanem*, 555 F.3d 172, 175 (5th Cir. 2009) (internal quotation marks and citations omitted). The guidelines provide that in determining the amount of loss, the Trial Court is required to make a reasonable estimate U.S.S.G. 2B.1.1 app in n.3(C). Further, the method used to calculate the amount loss, however must bear some reasonable relation to the actual or intended harm of the offense. A district court cannot impose a sentence enhancement...unless the Government has proven any facts to support the enhancement by a preponderance of the evidence. *United States v. Rodriguez*, 630 F.3d 377, 380 (5th Cir. 2011).

When a sentencing court uses information in the PSR to make a factual determination such as a loss amount, that information generally is presumed reliable and may be adopted...without any further inquiry if the Petitioner fails to demonstrate by competent rebuttal evidence that the information is materially untrue, inaccurate or unreliable. *United States v. Washington*, 480 F3.d 309, 320 (5th Cir. 2007) (internal quotation marks and citations omitted). For this general rule to apply however, the PSR's information must be "bear some indicia or reliability" *United States v. Scher*, 601 F.3d 408, 413 (5th Cir 2010). In other words , the PSR cannot simply include bald assertions in an attempt to "convert" such statements into reliable evidence, without providing any information for the basis of the statements. *United States v. Taylor*, 277 F.3d 721, 724, 726-27 (5th Cir. 2001) (citations omitted). Rather, the PSR's information must have an "adequate evidentiary basis." *United States v. Caldwell*, 448 F3.d 287, 290 (5th Cir. 2006); *United States v. Alford*, 142 F.3d 825, 832 (5th Cir. 1998).

Plain error exists if (1) there is an error, (2) the error is plain....(3) the error affect(s) substantial rights[,] and (4) the error seriously affect[s] the fairness, integrity or public reputation of the judicial proceedings. "United States v. Gordon, 838 F.3d 597, 604 (5th Cir. 2016) To satisfy the third prong of plain error review, the error must have affected the Petitioner's substantial right, which ordinarily requires the Petitioner to show that the error "affected the outcome of the district court proceedings". Any issue that affects the loss amount in the case is crucial because as the Guidelines' commentary explains that under 2B1.1, "loss servers as a measure of the seriousness of the offense and the Petitioner's relative culpability and is a principal factor in determining the offense

level under this guideline. U.S.S.G 2B1.1 cmt Background 2B1.1(b)(1) creates a sliding scale that increases the Petitioner's base offense level by zero to thirty points depending on the amount of loss, so any finding that increases the amount of loss has a direct effect on the sentencing guideline and seriously affects the fairness of the proceeding.

As shown in the facts, the PSR found the following damage components all occurred in October and December of 2011: total actual loss is $235,890. However, the PSR went on to add $1,461,910 in "lost revenue" to bring the grand total up to $1,697,800. (*See* Facts, *ante*, at pp. 29). Basing a damage category on the hours that would have been billed was entirely speculative and presume that the work would have been completed and billed and that the payment would have been collected. Mr Allen Shank a forensic accountant hired to testify at the sentencing hearing about damages in the case, admitted that they did not poll the employees to determine how much time they spent on the phones, taking meetings, taking notes, or how much work they did that did not involve computers. Taking out the lost revenue and leaving only direct expense leaves the loss amount of $235,890 which corresponds to a guideline of 24 and and a sentencing range of 51 to 63 months. *Id.*

Finally, the procedural errors identified in the district court's decision rendered the sentence imposed on Petitioner both procedurally and substantively unreasonable because the district court abused its discretion in weighing the relevant factors by ignoring the relevant § 3553(a) factors. *See, e.g., United States v. Ressam,* 629 F.3d 793, 837-839 (9th Cir. 2010) (vacating sentence because the district court committed procedural errors rendering sentence procedurally and substantively unreasonable, and remanding to different judge for resentencing);

United States v. Ture, 450 F.3d 352, 358-59 (8th Cir. 2006) (vacating and remanding sentence as substantively unreasonable where the § 3553(a) factors did not support the district court's sentence, and where the district court failed to accord significant weight to "the need to avoid unwarranted sentencing disparities"); *United States v. McQueen*, 727 F.3d 1144, 1160-1161 (11th Cir. 2013) (holding that to be correct, a district court must give "some weight to the factors in a manner that is at least loosely commensurate with their importance to the case, and in a way that 'achieve[s] the purposes of sentencing stated in § 3553(a)"); *United States v. McBride*, 511 F.3d 1293, 1297-98 (11th Cir. 2007) (If a district court instead commits a clear error of judgment in weighing the sentencing factors and arrives at a sentence beyond the range of reasonable sentences, the court of appeals is duty bound to vacate and remand for resentencing).

The Fifth Circuit fails to perform its duty in this case. Thus, as instructed by *McBride, supra*, because the district court committed a clear error of judgment in weighing the sentencing factors and arrived at a sentence beyond the range of reasonable sentences, the Fifth Circuit was therefore duty bound to vacate and remand Petitioner's 115 months' imprisonment to the district court for resentencing. Because a district court must be reversed if it "ignored or slighted a factor that Congress has deemed pertinent." *Gall*, 552 U.S. at 68; *Taylor*, 487 U.S. at 337; *United States v. Stewart,* 590 F.3d 93, 167-168 (2nd Cir. 2009). The Fifth Circuit's decision should be reversed by this Court because it left standing a district court's sentence that violated § 3553(a), is reeked of unfairness, and is procedurally and substantively unreasonable.

Accordingly, the sentencing enhancement and increased loss amount were not supported by the facts of this case and, therefore, this Court should reverse and remand this case to the Court of Appeals for it to vacate the Petitioners' sentence and remand to the district for resentencing without the enhancement and to the supported loss amount.

CONCLUSION

Wherefore, based on the foregoing reasons and authorities, Petitioner respectfully prays that the Honorable Supreme Court grant a writ of *certiorari* to the Fifth Circuit in this case.

Dated June 27, 2018

Respectfully submitted,

Anastasio Laoutaris # 47066-177
ACCC CA-106U
P.O. Box 1600
Washington, MS 39190-1600

Pro se Petitioner