No JS-6

**UNITED STATES DISTRICT COURT**

**CENTRAL DISTRICT OF CALIFORNIA**

TYAN, INC.,

Plaintiff,

v.

YOVAN GARCIA,

Defendant.

Case No. CV 15-05443- MWF (JPRx)

**FINDINGS OF FACT AND CONCLUSIONS OF LAW**

This matter came on for trial before the Court sitting without a jury on January 10, 2017. Following the presentation of evidence and the parties' closing arguments, the matter was taken under submission.

Having carefully reviewed the record and the arguments of counsel, as presented at the trial and in their written submissions, the Court now makes the following findings of fact and reaches the following conclusions of law under Rule 52 of the Federal Rules of Civil Procedure. Any finding of fact that constitutes a conclusion of law is also hereby adopted as a conclusion of law, and any conclusion of law that constitutes a finding of fact is also hereby adopted as a finding of fact.

The following witnesses were called and examined by the parties in the order recited below:

All testimony was given on **January 10, 2017**. Joseph S. Fischbach and Andrew Zelus appeared on behalf of Plaintiff Tyan, Inc., d/b/a Security Specialists ("Tyan") and gave an opening statement. Defendant Yovan Garcia appeared *in pro se* and gave an opening statement.

Mr. Fischbach first examined **Nick Tsotsikyan**, founder, owner, and Director of Operations of Security Specialists. Mr. Tsotsikyan's sworn declaration was submitted in lieu of a full direct examination. Mr. Garcia cross-examined Mr. Tsotsikyan.

Mr. Fischbach next examined **Steve Leon**, Operations Manager of Security Specialists. Mr. Leon's sworn declaration was submitted in lieu of a full direct examination. Mr. Garcia cross-examined Mr. Leon.

Mr. Fischbach recalled **Mr. Tsotsikyan** for redirect examination. Mr. Garcia recross-examined Mr. Tsotsikyan.

Mr. Zelus next examined Defendant **Yovan Garcia** regarding Defense Exhibit A.

Mr. Zelus then examined **Junior Arana**, a Patrol Officer for Security Specialists. Mr. Arana's sworn declaration was submitted in lieu of a full direct examination. Mr. Garcia cross-examined Mr. Arana.

Mr. Zelus examined **Ken Hagopian**, a principal in Digital Synergy Consulting, Inc., the company that provides IT support for Security Specialists. Mr. Hagopian's sworn declaration was submitted in lieu of a full direct examination. Mr. Garcia cross-examined Mr. Hagopian. Mr. Zelus conducted a redirect examination; Mr. Garcia conducted a recross examination. Mr. Zelus conducted a second redirect examination; Mr. Garcia conducted a short, second recross examination.

Mr. Zelus next examined Defendant **James Caspari**, a former Patrol Officer for Security Specialists. Mr. Caspari's sworn declaration was submitted in lieu of a full direct examination. Mr. Garcia cross-examined Mr. Caspari. Mr. Zelus conducted a short redirect examination of Mr. Caspari; and Mr. Garcia conducted a recross examination.

Mr. Zelus conducted a second redirect examination of Mr. Caspari; Mr. Garcia conducted a second recross examination.

Mr. Zelus examined **Denis Rybalka**, a Field Training Officer for Security Specialists. Mr. Rybalka's sworn declaration was submitted in lieu of a full direct examination. Mr. Garcia cross-examined Mr. Rybalka.

**Mr. Garcia** then took the stand and testified in his own defense. Mr. Zelus cross-examined Mr. Garcia.

Finally, Mr. Fischbach examined **Mr. Tsotsikyan** a third time, as a rebuttal witness. Mr. Garcia cross-examined Mr. Tsotsikyan.

At the end of the day, Mr. Fischbach made his closing argument for Plaintiff. Mr. Garcia made his own closing argument.

## I. FINDINGS OF FACT

### A. Background

1. Nick Tsotsikyan founded Security Specialists, a private security patrol company, in 1999. Since then, Security Specialists has provided security services throughout Southern California.

2. At some point, Tsotsikyan realized that the typical reporting process used by most security companies could be updated and streamlined with modern technology. Tsotsikyan purchased FileMaker Pro, a software that enables users to develop custom, proprietary databases. Tsotsikyan taught himself to use FileMaker Pro and began to develop a set of custom databases for use by Security Specialists.

3. Eventually, Tsotsikyan developed a unique set of forms and databases that, in his opinion, set Security Specialists apart from the competition. Each patrol car is equipped with a laptop computer, from which Patrol Officers can access Security Specialists' central database over the internet. Patrol Officers can then generate their daily reports as they patrol. The reports are emailed or faxed directly to clients as a .pdf. In an

industry where carbon copy reports are still common, Tsotsikyan believes that his custom forms helped Security Specialists to distinguish itself from its competitors.

4. Tsotsikyan also used FileMaker Pro to develop databases to store confidential client information and employee records. All of Security Specialists' databases were protected by username and password. Only administrators — *i.e.*, Steve Leon and Tsotsikyan — were authorized to edit the reporting software and access the confidential client and employee databases.

5. Tsotsikyan averred that he spent 5,000 hours over the course of 15 years developing the forms and databases that Security Specialists uses. In 2009–2010, Tsotsikyan hired Dina Torok, a certified FileMaker developer, to help him continue developing the custom files. Torok charged $170 per hour, and Tsotsikyan believes that this is a fair hourly rate.

**B. Inconsistencies in Garcia's Payroll Records**

6. Yovan Garcia began working for Security Specialists as a Patrol Officer sometime in or around 2012.

7. On July 24, 2014, Steve Leon noticed something odd about Garcia's payroll records. Although Garcia's schedule reflected that he had worked typical eight-hour days during the previous two-week pay period, the payroll program indicated that Garcia had worked twelve hours per day, and thus was owed 40 hours of overtime pay.

8. At first, Leon thought that perhaps the payroll program was not adding properly. Then, he noticed that someone had tampered with the program's "Lunch" field. Four hours had been added into the lunch field each day, which accounted for the unexplained extra 40 hours of overtime in Garcia's records. The hours had been entered in black text on a black background, in one-point font. As a result, the alterations to Garcia's hours would not have been noticeable to the casual observer. The alterations resulted in Garcia's being paid wages for overtime that, presumably, he did not work.

9. His curiosity piqued, Leon pulled the paystub server log, which tracks all attempts to log into the payroll database. The paystub server log was admitted into

evidence as Exhibit 3. The log indicated that just the night before, on July 23, 2014 at about 9:00 p.m., someone logged into the payroll program from Garcia's patrol laptop. The individual used an administrative username and password. As a Patrol Officer, Garcia was not authorized to access the payroll database and was never given the username or password.

10. Leon eventually figured out that Garcia's hours had been artificially inflated since at least January 2014. Garcia's paystubs for each of those pay periods, along with his corresponding schedule for that pay period, was admitted into evidence as Exhibit 2.

11. As an example of how Garcia's hours were altered, in the first pay period of the year, Garcia's paystub shows that he worked 80 hours of regular scheduled time, 20.5 hours of overtime, and 8 hours of holiday time. Garcia's schedule for that same period shows that he only actually worked 80 hours of regular scheduled time (including one 8-hour day of holiday time) and three hours of overtime. The discrepancy meant that Garcia was overpaid by $371.67 that month.

12. Garcia's hours were similarly inflated for each subsequent pay period. No other employee's records reflected a similar discrepancy. Leon testified that, as a Patrol Officer, Garcia was not authorized to access or alter the scheduler program, and was never given the supervisor password that would have allowed him to do so.

13. Leon testified competently and knowledgeably about this incident. The Court credits his testimony.

14. Leon discussed the issue with Tsotsikyan. He then tried to call Garcia to ask him about the discrepancy. Leon left a message asking Garcia to come into the office for a meeting, but Garcia never arrived. Instead, Garcia called someone he considered to be a friend at Security Specialists, long-time employee Denis Rybalka, and asked to meet.

15. Rybalka had the day off, and had spent the day washing his car. He tried to avoid Garcia's calls. Rybalka had just finished hand waxing his car when he received yet another call from Garcia, and finally decided to answer.

16. Garcia was in a panic. He was speaking "gibberish," and was talking too fast for Rybalka to follow. Rybalka thought he heard Garcia say, "they found out;" Garcia was worried that he had been fired. Garcia asked to meet because he didn't feel like he could talk about what had happened over the phone.

17. Rybalka hung up and immediately called Leon. Leon asked Rybalka to meet with Garcia — and to record the conversation for Security Specialists' benefit. Rybalka had worked at Security Specialists for more than a decade, and he was intensely loyal to the company and to Leon in particular. Rybalka set his cell phone to record and drove his freshly waxed car to a nearby McDonald's to meet with Garcia.

18. The audio recording that Rybalka made was admitted, along with a transcript, as Exhibit 4. Rybalka spoke slowly and clearly while testifying. He did not hesitate to answer questions and appeared confident in his answers. Based on his manner when testifying and other factors, the Court credits Rybalka's testimony.

19. During the meeting, Garcia told Rybalka that Garcia suspected Leon wanted to meet with him because he had been receiving inflated paychecks for the past few months. Garcia told Rybalka the following story:

20. Garcia began by explaining that he has some skill with computers. A few months prior, someone from Security Specialists' competitor, PTS Security Services ("PTS"), had asked him to come take a look at a broken laptop. While working on the computer, Garcia noticed a file labelled "Security Specialists." Curious, he opened the file, only to find what he recognized to be confidential client records. Garcia saved the file to his own device, deleted it from the laptop, and said nothing to his contact at PTS.

21. A little while later, Richard Balint, a former employee of Security Specialists and current employee of PTS, contacted Garcia. Balint told Garcia that he knew Garcia had seen the "Security Specialists" file on the laptop. He asked Garcia not to say anything to his employer about the file — and promised that Garcia would be well compensated for staying quiet. Garcia said nothing, and soon after started receiving the inflated paychecks.

22. Rybalka tried to convince Garcia to tell his story to Leon. Rybalka emphasized to Garcia that accepting the extra money had been wrong; but said that he believed Garcia that it was PTS who inflated the paychecks. Rybalka thought that if Garcia would only explain what happened to Leon, Garcia would be able to keep his job.

23. Garcia was reluctant. He was afraid, he said. He had a family and was worried for their safety. Besides, Garcia did not like Leon and thought that he and Tsotsikyan would probably just try to blame the whole thing on Garcia. Instead, Garcia wanted Rybalka to tell Leon and Tsotsikyan what had happened. Garcia thought that the two higher-ups would be more receptive to his story if they heard it from Rybalka first.

24. Eventually, Rybalka convinced Garcia to meet with Leon and Tsotsikyan. Rybalka arranged the meeting.

25. Leon, Tsotsikyan, Rybalka, and Garcia all met later that evening at a North Hollywood gas station. This time, it was Leon who recorded the conversation. The audio recording and a transcript were admitted as Exhibit 6.

26. At the gas station, Leon aggressively confronted Garcia about the inflated paychecks. Garcia told the assembled men his story about fixing the laptop for PTS and the offered reward in exchange for his silence about the Security Specialists file. Garcia explained that he thought there was a "mole" inside the company who was altering his hours. Over and over, Garcia repeated that he had only acted to protect the company and his friends who worked there.

27. Leon immediately started pressing Garcia for names. He and Tsotsikyan thought that even if Garcia did not have the administrative password, he must know who did. At first Garcia was reluctant to name any names, citing a vague fear for his family's safety. Eventually, after being assured that the company would not press charges against him for the inflated paychecks — or even ask for the money back — Garcia talked. By the end of the meeting Garcia named several Security Specialists employees who he claimed were agents of PTS. All of them were subsequently fired.

28. Leon also confronted Garcia about the entries in the paystub server log indicating that Garcia logged into the management system from his patrol laptop the night before Leon discovered the inflated wages. Garcia denied having used the administrator password to log in.

29. Garcia also emailed the client information that he said he found in the Security Specialists file to Leon. The email contained a spreadsheet with entries for several clients, and included their phone numbers, addresses, as well as other confidential information. The attachment was admitted as Exhibit 7 at trial. Leon testified that Garcia was never authorized to access this sort of client information, nor did Security Specialists ever give Garcia a username or password that would have allowed him to access this information.

**C. Garcia's Firing**

30. A few months later, in September 2014, management at Security Specialists began to notice something odd about towing patterns at the properties in Garcia's patrol area. While a Patrol Officer would typically tow one or two cars in any given day, Garcia was regularly towing between five and ten cars per day. Moreover, most of the cars were being towed by one particular company, L&M Towing.

31. Tsotsikyan and Leon became concerned that Garcia was towing cars in exchange for illegal kickbacks from L&M Towing. To test this theory, the pair decided to transfer Garcia to a different patrol area, presumably one that L&M Towing did not service, to see whether his towing patterns would change.

32. On September 29, 2014, Leon informed Garcia that he was being reassigned to a different patrol area. Right away, Garcia became very upset. In Leon's retelling, Garcia argued with Leon to be put back in his old patrol area. When Leon refused, Garcia insisted that Security Specialists was pushing him out. Leon explained that was not true, that the company was just reassigning Garcia to a different patrol area. Eventually, Garcia told Leon he was quitting; Leon told Garcia to put it in writing. In Garcia's retelling, the reassignment was Security Specialists' way of pushing him out of the company and

forcing him to quit. Either way, Garcia submitted a handwritten note to Security Specialists that day, stating simply "I Yovan Garcia quit Security Specialist[s]," signed Yovan Garcia. The note was admitted as Exhibit 45.

33. The day he was fired, Garcia texted Rybalka. At first, Garcia seemed only to want to rant, complaining that he'd given two years of his life to a company that never really cared about him. Then, Garcia began to talk about how ungrateful Security Specialists was for the protection he had provided them. Garcia texted Rybalka a picture of a client file on one of Security Specialists' proprietary forms, as an example of the "protection" he provided. Later on, Garcia texted Rybalka a picture of Leon's employee personnel file, also a confidential document.

34. Rybalka showed the messages to Leon and Tsotsikyan. Leon testified that the two images Garcia sent were of confidential files that Garcia never had authorization to access. Without an administrative username and password, Garcia should not have been able to see them, let alone store copies on his phone.

**D. The Security Specialists Hack**

35. On October 14, 2014, Security Specialists' company servers were hacked. The hacker targeted Tsotsikyan's archived emails, company server files, accounting software, and databases used for accounting, invoices, and payroll. Security Specialists' custom-made FileMaker Pro databases were also targeted. The company lost files used to schedule employees, generate and store field security reports, record and search client information, and store service location instructions and service records. Security Specialists' backup files were also deleted or corrupted and the hacker was in the process of reformatting the company's various drives when the intrusion was discovered and the servers disconnected from the internet. Tsotsikyan testified that the damage was extensive and debilitating.

36. Junior Arana, a Security Specialists Patrol Officer, testified that he was on patrol the night of the hack. While Arana was in the field, he noticed that his patrol laptop had been accessed remotely. Arana watched as a number of files were accessed and

deleted, including Yovan Garcia's reprimand file. Arana told his supervisor, Petros Dertsakyan, what he had seen, and at some point drafted a short statement to the same effect. The statement was admitted as Exhibit 11.

37. Although Arana is still employed by Security Specialists, and thus has a motive to testify favorably to his employer, he also appeared to answer questions honestly and to the best of his ability. Arana told a consistent story in Exhibit 11, his declaration, on direct examination, and during cross examination. The Court credits Arana's testimony based on its content and plausibility, and also on Arana's demeanor while testifying.

38. A few hours before the hack, former employee and Defendant Richard Balint — the same former employee who, according to Garcia, offered Garcia a reward for keeping quiet about the Security Specialists file on the PTS laptop — called Security Specialists. Petros Dertsakyan, a Security Specialists employee, answered the call. Dertsakyan stated that Balint called to ask how things were going at Security Specialists. At some point later, Dertsakyan typed up his recollection of the phone call as a signed statement; exactly when the statement was created is unclear, as it is undated. The statement was admitted as Exhibit 17.

39. Balint called Security Specialists a second time on October 17, 2014, just three days after the hack. Gevorg Dertsakyan, another Security Specialists employee, answered the call. Later that day, Dertsakyan typed up his recollection of the phone call, which was admitted as Exhibit 18. The statement was dated October 17, 2014 and signed by Dertsakyan. Dertsakyan stated that Balint identified himself before asking "How is your system, I heard it was down?" Balint asked, "Someone hacked it, did you check out the website?" Dertsakyan asked Balint who had told him that Security Specialists had been hacked; Balint replied, "a little birdy."

40. Security Specialists' website was also vandalized that same week. The website's header was changed to read "Are you ready" along with the date December 1, 2014, and a string of five digits. Leon testified that these numbers were the first five

digits of his Social Security Number. The website had also been edited to include a particularly unflattering picture of Leon. Leon and Tsotsikyan took the vandalism as a threat, both to Security Specialists generally and Leon specifically.

**E. Garcia's Connection to the Hack**

41. Whoever vandalized the website solicited further embarrassing stories and photos related to Security Specialists. The hacker left an email address where he or she could be contacted: theAnonygroup@gmail.com.

42. In an effort to figure out who had hacked the website — and perhaps also Security Specialists' network — Security Specialists served Google with a subpoena for the account information. Google responded with a few pages of information, admitted as Exhibit 13.

43. Included in Google's response was an IP address associated with the "theAnonygroup" email address. Ken Hagopian, Security Specialists' IT contractor, testified that in October 2014 he ran a web search using several independent online IP tracker tools to determine the approximate location of the user who had been assigned the IP address. Screenshots of the search were admitted as Exhibit 14. Hagopian traced the IP address to a neighborhood in North Hollywood, about a block from where Garcia lives.

44. James Caspari, a former Patrol Officer for Security Specialists, testified about a phone call he received from Garcia in September or October 2014. Caspari had quit working for Security Specialists about six months before, on March 10, 2014. Caspari was taking classes and working on building his own security company. Caspari testified that Garcia called him to offer some computer software for his security company. When Garcia came by, Caspari realized that the software was very similar to the software that Security Specialists used. Garcia offered the software to Caspari in exchange for agreeing to serve as Qualified Manager in the security company that Garcia was in the process of developing. Caspari agreed to take a look, but felt that something was off about the software. When Caspari expressed his concerns, Garcia told Caspari that he had developed Security Specialists' software, and that he thus owned the software rights.

Caspari was not convinced, especially because Garcia refused to give Caspari the administrative password.

45. Nevertheless, Caspari agreed to serve as Garcia's Qualified Manager in exchange for the software. Caspari began using the software in his own business. He testified that, in practice, the software operated remarkably similarly to Security Specialists' software.

46. Caspari testified that he eventually stopped using the software Garcia gave him. Caspari testified that not only did the software never work particularly well, but his suspicions about the true ownership of the software continued unabated. Eventually, Caspari concluded that the software was not necessary to run his business. He has since resigned as Garcia's Qualified Manager.

47. While testifying, Caspari appeared nervous and ill at ease. He asked to review his declaration before testifying and could not answer a single question without referencing his declaration first. Caspari essentially testified directly from the declaration, paragraph by paragraph, rather than speaking extemporaneously about any of the above events. Caspari required prompting from his declaration for even the smallest details. It was not clear whether Caspari actually remembered ***any*** of the above events, to which he nevertheless testified. Moreover, given that Caspari was also named as a defendant in this action, and faced similar liability for his role in the hack before settling separately with Security Specialists, Caspari had some motivation to avoid any indication of his own involvement with, and potential responsibility for, the hack. Therefore, the Court gives his testimony little weight.

**F. Garcia's Version of Events**

48. Garcia denies that he ever hacked Security Specialists. After starting to work for the company in about 2012, Garcia soon realized that it was not as professional as its client-facing image implied. Management was paranoid about competitors and regularly fired employees for possible collusion. Management was particularly concerned with

PTS, which had been started by a former employee and Defendant Mher Uzunyan, and with whom run-of-the-mill business competition had become personal.

49. The day Leon discovered the inflated payroll checks, Garcia had worked the night shift. He got off work at 4:30 a.m.; Leon then asked him to come in to talk about the checks at 9:00 a.m. Garcia explained that he had to take care of his daughter and, in any case, fell asleep. He slept through the meeting. Garcia later got a phone call from one of his colleagues at Security Specialists, who told Garcia that he had been taken off the schedule. Garcia understood this news to mean that he had been fired. It was then that he called Rybalka to arrange a meeting.

50. Once Garcia got to the McDonald's for the meeting, it became clear to him that Rybalka was recording him. Garcia testified that when he went to get a hamburger, Rybalka followed. When he went to the bathroom, Rybalka followed. So, knowing that he was being recorded, Garcia decided to play a game: Garcia made up the story about fixing the laptop for PTS just to see how Rybalka would react. Garcia did the same in his second meeting, with Tsotsikyan and Leon, because he knew that it would upset them. Garcia testified that, in reality, none of the events he relayed in either meeting ever actually occurred.

51. Even taking Garcia at his word that he lied to Rybalka, Tsotsikyan, and Leon, Garcia never explained what had really happened. That is, Garcia never explained why his payroll numbers were inflated and how he came to be in possession of Security Specialists' confidential client information. The evidence that Garcia had obtained unauthorized access to Security Specialists' confidential files was thus unrebutted.

52. Garcia also flatly denied ever hacking Security Specialists or its website. Garcia admitted to giving Caspari FileMaker Pro files that were very similar to those used by Security Specialists. But he said he did so as a favor to Caspari, and that he had developed the files himself. Garcia testified that FileMaker software is not difficult to buy or learn, and said he had created his own files at some point during or right after his employment with Security Specialists. However, Garcia could not explain the similarities

in filenames or layout between Security Specialists' forms and the forms Garcia gave to Caspari, other than to say that similar templates are easy to find online. The Court thus discounts Garcia's implausible testimony and finds that Garcia obtained the files through the hack.

53. Garcia also contested Hagopian's conclusion that the IP address traced to a physical address close to where Garcia lives in North Hollywood. Garcia used several websites to trace the same IP address a few weeks before trial, and found it was associated with an address in Sherman Oaks.

54. Hagopian testified in response that IP addresses are not tied to a specific location "in perpetuity." Rather, searching for the physical referent for an IP address at one point in time may yield a different result than searching for the physical location of the same IP address at a different point in time.

55. The Court infers from Hagopian's testimony that an IP search is more likely to be accurately traced to an individual's location the sooner after a particular incident involving that IP address it is searched. Therefore, because Hagopian's search of the IP address associated with the October 2014 hack was conducted sooner after the hack than Garcia's search, the results of Hagopian's search are more likely to actually represent where the hacker was during the incident than Garcia's search.

56. Tsotsikyan also testified that Garcia had access to information in Tsotsikyan's personal email that Garcia otherwise had no way to know. Garcia told Caspari about a car that Tsotsikyan had bought. Garcia testified that he had seen the car at Security Specialists' offices the day he quit. But, according to Tsotsikyan, the car was not delivered until after Garcia had quit. However, Tsotsikyan had arranged for the car's delivery over email, before the hack. Therefore, it appears likely that Garcia read about the vehicle's impending delivery in Tsotsikyan's email, rather than actually seeing it for himself at Security Specialists.

57. In sum, the Court does not find Garcia's testimony to be credible. Not only did Garcia himself admit to being capable of creating complex lies on short notice (for

example, when he testified that he made up the whole story about PTS), Garcia's testimony failed to explain key aspects of his involvement with the various computer hacking and website attacks at issue in this action. And Garcia himself testified that he is good with computers — he can reformat drives, create FileMaker Pro files, and knows some html.

58. Garcia also told internally contradictory and easily disproved lies while testifying. The story about the car provides one example; another came when Garcia presented what he said was a letter of commendation from Security Specialists, but which later testimony indicated was in fact a compliment delivered by Garcia himself, who pretended to be a client and emailed the "compliment" to Tsotsikyan through a spoofed email address. Throughout his testimony, Garcia appeared nervous, spoke quickly, and tended to talk himself in circles.

**G. The Court's Findings**

59. Based on the foregoing testimony and evidence, the Court finds as follows:

60. Garcia personally hijacked Security Specialists' website. Garcia also accessed Security Specialists' network without authorization and increased the number overtime hours he had worked, so that he was paid overtime wages he had not earned.

61. Furthermore, Garcia was involved in a conspiracy to hack Security Specialists' network. Although the specifics of the conspiracy are not clear from the testimony, there is sufficient evidence to support a finding that Garcia worked with at least one other individual to steal confidential files from Security Specialists and destroy the servers and hardware that hosted Security Specialists' information. Even before the hack, Garcia was able to access Security Specialists' network from his patrol car, using an administrative password that he had never been given, to change his reported number of hours. Additionally, it is clear from the text messages that Garcia sent to Rybalka that Garcia had at some point acquired confidential files that he was never authorized to access. And soon after the hack, the evidence indicates, Garcia came into possession of Security Specialists' proprietary FileMaker Pro forms. Whether or not Garcia himself was

the hacker, the evidence indicates that in the hack, Garcia obtained Security Specialists' confidential and proprietary materials that he otherwise had no authorization to access.

62. As evidenced by Garcia and Caspari's subsequent attempts to solicit Security Specialists' customers, the aim of this conspiracy was twofold: first, to damage Security Specialists in an effort to reduce its competitive advantage; and second, to obtain access to those files that gave Security Specialists its advantage, and use them to solicit Security Specialists' clients. Garcia copied portions of Security Specialists' promotional materials for the security company he later developed, and created sample reports using the stolen FileMaker Pro forms. Using these stolen materials, Garcia successfully poached several of Security Specialists' clients, as discussed in more detail below.

**H. Damages**

63. Plaintiff requests the following damages, as set forth in Tsotsikyan's declaration:

a. Garcia's unworked overtime pay: $6,071.49
b. Payroll taxes and insurance costs on Garcia's unworked overtime pay: $1,214.29
c. Invoices for work by Digital Synergy, Ken Hagopian's IT company, for work to repair damage from the hack: $83,260.37
d. Miscellaneous data recovery costs: $3,187.27
e. Recovery of domain name: $500
f. Increased payroll costs for recovery: $20,000
g. Loss of proprietary files: $425,000
h. Lost profits: $346,111.66
i. Attorneys' fees: $64,446.50
j. Litigation costs: $5,857.62

64. Plaintiff also requests punitive damages, which are available under the California Uniform Trade Secrets Act ("CUTSA"). *See* Cal. Civ. Code § 3426.3(c).

Finally, Plaintiff requests attorneys' fees and costs, available under California Penal Code section 502(e)(2).

**1. Costs related to Garcia's inflated checks**

65. The Court has found that Garcia was involved in a scheme to access his payroll records and artificially inflate the number of overtime hours he earned. Accordingly, as explained below, Plaintiff is entitled to collect damages for Garcia's excess pay.

66. Plaintiff submitted paystubs indicating that Garcia was paid $6,071.49 more than he was owed for the number of hours he worked between January 2014 and July 2014, when the scheme was discovered. Garcia's pay stubs, pay checks, and schedules were admitted as Exhibit 2, and adequately support Plaintiff's request.

67. Plaintiff submitted no records to prove it spent $1,214.29 in payroll taxes and insurance costs on the inflated wages. Tsotsikyan averred that payroll taxes and insurance costs were "typically" 20% of what the employee was paid, but did not provide any more detail as to how he reached that conclusion, or any evidence to show that the 20% figure was representative of what Security Specialists typically paid on ***Garcia's*** wages.

68. Accordingly, the Court finds that Plaintiff has failed to meet its burden to show its entitlement to payroll taxes and insurance costs. The proposed method of calculation is too speculative and is unsupported by the evidence. The Court awards **$6,071.49** in damages related to Garcia's inflated checks.

**2. Repair Costs**

69. Ken Hagopian testified about his efforts after the hack to repair the damage to Security Specialists' network and email. Tsotsikyan called Hagopian in as soon as he realized something was wrong with the servers. After directing that the servers be disconnected from the internet, Hagopian began to assess the damage. In Hagopian's opinion, the hacking resulted in a near total loss. The company server files, sage software, Outlook Exchange email database files, and FileMaker Pro server files had all been

deleted. To do damage this extensive, Hagopian reasoned, the hacker must have used an administrative username and password.

70. Although he could not remember the exact timeline of the effort, Hagopian testified that he undertook a "protracted project" to make Security Specialists functional again. He tried to recover the deleted information, but was largely unsuccessful. Instead, Hagopian had to rebuild all of the servers from scratch. Hagopian scanned every one of Security Specialists' computers for viruses (including all of the laptops in all of the patrol cars), wiped them clean, and reinstalled all of the programs and data. Some hardware and software had to be replaced entirely.

71. In support of his testimony, Hagopian submitted invoices for the project totaling $83,260.37. The invoices were admitted as Exhibit 22. The Court reviewed the invoices and discovered that many did not appear to bill for services provided in connection with the hack. Most obviously, several of the invoices were dated August and September 2014, months before the hack occurred. The invoices also listed items as late as October 2015 for routine services, like determining why Outlook was running slowly on a particular day, or purchasing annual licenses. Moreover, many of the billing records are so heavily redacted that the Court was unable to determine what service was performed, let alone whether it was provided in connection with the hack.

72. Having gone through the records, the Court finds that only a portion of the invoices can be tied with any certainty to the October 2014 hack. These invoices include hardware purchased in late October and early November 2014, as well as all service invoices tagged "Server down issues" (Ticket No. 10976), "Server Rebuild – Ticket 2" (Ticket No. 12001), and "Server issues ticket 3" (Ticket No. 12444). Together, these invoices total **$53,017.11.** The Court finds this sum to be an appropriate amount of compensation for Hagopian's hack-related services.

73. Tsotsikyan also testified that, after Security Specialists' website was hijacked, he had some trouble convincing the hosting company to release the domain name back to Security Specialists. Tsotsikyan eventually paid $500 for a notarized letter

from the company to which the website had been transferred. The letter instructed the web host to return the domain name to Security Specialists. A copy of the letter was admitted as Exhibit 15. The Court finds this testimony sufficient to show Plaintiff's entitlement to **$500** for the recovery of Security Specialists' domain name.

74. Plaintiff additionally requests $3,187.27 in what it calls "miscellaneous data recovery costs." Tsotsikyan explained that after the hack, Security Specialists sent its hard drives to an offsite file recovery company in an attempt to recover the erased files. Security Specialists was also forced to buy replacement hardware. Exhibit 23 includes credit card records that have been redacted to show only charges related to the hack. The records adequately support Plaintiffs' request and the Court finds **$3,187.27** to be a reasonable amount to pay in data recovery services.

75. Plaintiff also requests $20,000 in increased payroll costs to the company for hours that Tsotsikyan, Leon, and other employees spent working overtime to address issues raised by the hack. Tsotsikyan testified that for at least thirty days after the incident, he and other Security Specialists employees worked many extra hours rebuilding databases and records, including the payroll database. The Court finds this to be a reasonable amount to expend on payroll to return Security Specialists to some semblance of functionality during the month following the hack. Accordingly, Plaintiff is awarded **$20,000** in extra payroll costs for the month following the hack.

76. Finally, Plaintiff requests compensation for the loss of its proprietary FileMaker Pro files. Tsotsikyan explained that he spent in excess of 5,000 hours developing the databases and forms that were attacked. Tsotsikyan once paid an experienced FileMaker Pro software developer $170 per hour to consult on developing the database, and believes $170 per hour to be a reasonable rate. Multiplying the proposed reasonable hourly rate by the number of hours he spent on software development, Tsotsikyan estimated that the proprietary files he had developed over the years were worth approximately $850,000. Tsotsikyan added that other security providers paid $1 million to implement an inferior database platform. Tsotsikyan further testified that he lost about

half of the work he had done to create his proprietary database in the hack. Therefore, Plaintiff asks for $425,000 in damages for the loss of the FileMaker Pro files.

77. The Court does not agree that the above method is an appropriate method for valuing the loss of Security Specialists' proprietary files. For one thing, Tsotsikyan was admittedly an amateur, a self-taught developer who had to learn the program on the go. He is unlikely to be able to charge the same hourly fee as an experienced professional. Similarly, because Tsotsikyan was learning the program as he went, all 5,000 hours are unlikely to be billable. Any professional would be expected to cut out billing inefficiencies resulting from inexperience or redundant efforts.

78. Finally, the Court notes that Tsotsikyan was already paid his regular wages for the hours he spent developing the program in the first place, and Plaintiff will be compensated for the time Tsotsikyan spent rebuilding what was lost. To also pay Tsotsikyan an hourly wage for developing the program in the first place would result in his being paid twice for the same work.

79. The Court recognizes that the proprietary files likely had some value independent of Tsotsikyan's pay while developing them, or while rebuilding the database. That is, the confidential information and proprietary forms would likely be worth some sum to an objective buyer hoping to open his or her own security company in the greater Los Angeles area. But the cost to develop the proprietary information is not the same as the cost to resell it. The Court doubts that Plaintiff's proprietary files would be worth $425,000. The Court places the likely resale value of what was lost at **$100,000**, and awards Security Specialists that sum in addition to the increased payroll costs for rebuilding the various databases and files.

**3. Lost Income**

80. Finally, Plaintiff requests $346,111.66 in lost profits. Plaintiff believes, and the Court concludes below, that the goal of the hack was to cripple Security Specialists and use its proprietary files to lure away its clients. Plaintiff submitted as Exhibits 24 and 25 examples of solicitation emails sent by Garcia and Caspari to Security Specialists'

clients, which utilize stolen promotional materials and forms to convince the clients to change providers. Plaintiff submitted as Exhibit 21 a list of clients that it believes it lost due to the hack, along with the date the client became "inactive" and the monthly revenue each client provided.

81. The first entry, for client Santiago Estates, appears to have been included in error, as its inactive date is July 11, 2014 — three months before the hack. As for the remaining clients, the latest inactive date is June 15, 2015. The emails soliciting clients using stolen materials date to April 2015, and Plaintiffs provide evidence that Garcia continued to solicit Security Specialists' clients through at least September 2015. Plaintiff has met its burden of proof to show lost profits from November 2014 through June 2015.

82. In his declaration, Tsotsikyan states that the company lost $329,630.16 in annual revenue from clients who left Security Specialists due to the hack. Tsotsikyan appears to have based its valuation on the sum of the total monthly revenue provided by each client, which includes the monthly income from Santiago Estates. Plaintiff multiplied the monthly loss by 12 to arrive at $329,630.16 in annual lost revenue.

83. Tsotsikyan assumes that 35% of the annual lost revenue would be profit. He also explains that according to industry standards, the usual valuation of a client contract is three years' worth of profit. Multiplying the annual lost revenue by 35%, and multiplying that sum by three years, Tsotsikyan arrived at $329,630 in lost profits due to the hack.

84. The Court finds that this method significantly overvalues Plaintiff's likely lost profits. Plaintiff's proposed sum assumes that each client's contract would have provided three years' of profits from the date that client left Security Specialists. The Court finds that estimate to be overly optimistic. The testimony of Tsotsikyan and Leon shows that Security Specialists is in a competitive business. Even if the hack had not occurred, presumably at least some of Security Specialists' clients would have been lured away within six months of October 2014 by competitors' promises of cheaper or more professional service. Even assuming some of the contracts would have lasted another

three years from the time they became inactive, other clients likely would have left at the same time anyway, or would have left in fewer than three years.

85. Accordingly, the Court finds that a 1.5 year valuation, or half of the industry standard, is more appropriate. The Court also finds that the annual lost revenue must be calculated without the annual revenues of Santiago Estates, which as previously explained became inactive months before the hack. Without Santiago Estates, the total monthly lost revenue due to the hack is $21,569.18. Multiplied by 12 months, the Court finds that Security Specialists' annual lost income is $258,830.16. Assuming 35% of that is profit, and valuing the likely remaining term of the each contract at 1.5 years, the Court awards Security Specialists **$135,885.83** in lost profits.

86. In total, the Court awards Plaintiff **$318,661.70** in actual damages.

**4. Attorneys' Fees**

87. Because the litigation in this action is not yet concluded, the Court declines to award any attorneys' fees at this point. Counsel for Plaintiff may submit a separate request for fees after the final judgment is entered. The request shall be properly noticed under the Local Rules and supported by an attorney declaration and billing records.

## II. CONCLUSIONS OF LAW

1. The Court concludes that Defendant Garcia is liable for the following four claims: violation of the Computer Fraud Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(4); violation of the Stored Communications Act, 18 U.S.C. § 2701(a); violation of the California Computer Data Access and Fraud Act, California Penal Code section 502; and violation of the California Uniform Trade Secrets Act ("CUTSA"), California Civil Code section 3426, *et seq.* Much of this liability arises from the same factual nexus. By accessing Security Specialists' protected network to artificially inflate his hours and by participating in a conspiracy to hack into Security Specialists' password protected, confidential databases, Garcia incurred civil liability on all four claims.

### A. Claim One: Violation of the Computer Fraud Abuse Act, 18 U.S.C. § 1030(a)(4)

2. "The CFAA prohibits acts of computer trespass by those who are not authorized users or who exceed authorized use." *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1065 (9th Cir. 2016). Under § 1030(a)(4), a person who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value[,]" with some exceptions not relevant here, violates the CFAA. A plaintiff may pursue a civil claim under the statute if the harm exceeds $5,000 in value during a one-year period. *Id.* § 1030(g); *Facebook*, 844 F.3d at 1066. The civil plaintiff is limited to economic damages on this claim. *Id.*

3. Therefore, "[t]o bring an action successfully under § 1030(g) based on a violation of § 1030(a)(4), [Plaintiff] must show that [Garcia]: (1) accessed a protected computer, (2) without authorization or exceeding such authorization that was granted, (3) knowingly and with intent to defraud, and thereby (4) furthered the intended fraud and obtained anything of value, causing (5) a loss to one or more persons during any one-year period aggregating at least $5,000 in value." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132 (9th Cir. 2009) (internal quotation marks and citations omitted) (citing *P.C.*

*Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504, 508 (3d. Cir.2005); *Theofel v. Farey–Jones*, 359 F.3d 1066, 1078 (9th Cir.2004)).

4. Here, all of the elements of § 1030(a)(4) are met.

5. A "protected computer" is one that "is used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). This has been construed to include computer networks and databases. *United States v. Nosal*, 844 F.3d 1024, 1058 (9th Cir. 2016) ("*Nosal II*") ("The CFAA's restrictions have been applied to computer networks, databases and cell phones."). Protected computers are "effectively all computers with Internet access." *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012) ("*Nosal I*"). The databases and computers at issue in this action were connected via the Internet and thus were protected as defined by the statute.

6. Whether Garcia had authorization to access Plaintiff's computers turns on whether Security Specialists gave him permission to use them. *See Nosal II*, 844 F.3d at 1028 ("[W]e conclude that 'without authorization' is an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission."); *LVRC Holdings*, 581 F.3d 1133 ("an employer gives an employee 'authorization' to access a company computer when the employer gives the employee permission to use it."). As the Court previously found, Garcia never had permission to access any of the files that were hacked. Garcia was not a supervisor and neither Tsotsikyan nor Leon ever gave Garcia the administrative username and password.

7. The intent element of the statute is defined with reference to the criminal standard. *See Nosal II*, 844 F.3d at 1032 (approving use of Ninth Circuit model jury instructions to define "intent to defraud" under the CFAA). Intent to defraud is defined in the Ninth Circuit model jury instructions as "the intent to deceive or cheat." Instruction 8.121. When Garcia accessed the Security Specialists payroll files to alter his hours, he acted with intent to defraud Security Specialists by cheating the company out of wages that he never earned.

8. Garcia was also involved in a conspiracy to hack the Security Specialists network with a username and password that he was unauthorized to use. The hacker accessed the files without Security Specialists' permission or knowledge, making illegitimate use of a legitimate password. The conspiracy thus acted with intent to defraud Security Specialists.

9. Garcia's personal actions furthered the payroll fraud to the extent that he was able to collect more than $6,000 in unworked overtime pay. Additionally, the proprietary data the hackers obtained was worth at least $100,000, and the hack itself succeeded in damaging Security Specialists' network to such an extent that it took at least a month to get the various databases and systems back in working order.

10. Finally, the CFAA defines "losses" to include "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service . . . ." 18 U.S.C. § 1030(e)(11). As discussed above, Security Specialists incurred significant costs in assessing the damage, restoring the data, and in lost revenue.

11. Therefore, the Court concludes that Garcia was a participant in a conspiracy to hack Security Specialists, and that the hack violated the CFAA.

**B. Claim Two: Violation of the Stored Communications Act, 18 U.S.C. § 2701(a)**

12. "The Stored Communications Act provides a cause of action against anyone who 'intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage.'" *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004) (quoting 18 U.S.C. §§ 2701(a)(1), 2707(a)). "Like the tort of trespass, the Stored Communications Act protects individuals'

privacy and proprietary interests." *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004). Section 2707 provides for civil liability under the statute.

13. The hack, as described above, included an effective attack on Security Specialists' email servers as well as the data stored in its network and backup drives. Tsotsikyan was unable to access his email during the hack, and many emails were simply lost. This result was one of the intended purposes of the hack. Accordingly, the Court concludes that the conspiracy to hack Security Specialists also violated the Stored Communications Act.

**C. Claim Three: Violation of the California Computer Data Access and Fraud Act, California Penal Code Section 502**

14. California Penal Code section 502 imposes civil liability on a person who "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network." *Id.* § 502(c)(2); *see also id.* § 502(e)(1) (permitting a plaintiff to bring a civil action for a violation of any provision of section 502(c), for compensatory, injunctive, and equitable relief). Garcia violated section 502 when, without permission, he accessed Security Specialists' payroll system from his patrol laptop and altered his payroll records. He was also involved in the conspiracy to hack Security Specialists, and through that conspiracy obtained proprietary files and databases, including Leon's confidential employee personnel file and the FileMaker Pro forms that he gave to Caspari.

15. Accordingly, the Court concludes that Garcia violated section 502.

**D. Claim Four: Violation of the CUTSA, California Civil Code section 3426, *et seq.***

16. "Trade secret misappropriation occurs whenever a person . . . discloses or uses, without consent, another's trade secret that the person '[u]sed improper means to acquire knowledge of' . . ." *Altavion, Inc. v. Konica Minolta Sys. Lab. Inc.*, 226 Cal. App.

4th 26, 41–42, 171 Cal. Rptr. 3d 714 (2014) (quoting Cal. Civ. Code § 3426.1(b)(2)(A)). "Improper means includes theft, . . . misrepresentation, . . . or espionage through electronic or other means." *SASCO v. Rosendin Elec., Inc.*, 207 Cal. App. 4th 837, 844, 143 Cal. Rptr. 3d 828 (2012), *as modified on denial of reh'g* (Aug. 7, 2012) (quoting Cal. Civ. Code § 3426.1(a)). A trade secret is defined as "information, including a . . . program . . . that: (1) [d]erives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) [i]s the subject of efforts that are reasonable under the circumstances to maintain its secrecy." *Id.* (quoting Cal. Civ. Code § 3426.1(d)).

17. The California Supreme Court has emphasized that "the primary purpose of California's trade secret law . . . is to promote and reward innovation and technological development and maintain commercial ethics." *DVD Copy Control Ass'n, Inc. v. Bunner*, 31 Cal. 4th 864, 878, 4 Cal. Rptr. 3d 69 (2003), *as modified* (Oct. 15, 2003) (internal quotation marks omitted).

18. Plaintiff has met its burden to show that its confidential client databases and FileMaker Pro files were trade secrets. Tsotsikyan testified that the FileMaker Pro forms he developed, such as the forms that allowed Security Specialists Patrol Officers to send reports to clients instantly from the field, gave Security Specialists a competitive edge. Indeed, Garcia himself recognized the independent value of Security Specialists' files and databases when he offered Caspari access to the forms in exchange for Caspari's willingness to help Garcia by taking a position in Garcia's fledgling security company. *Cf. Direct Techs., LLC v. Elec. Arts, Inc.*, 836 F.3d 1059, 1071 (9th Cir. 2016) (affirming grant of summary judgment in favor of the defendant where a putative trade secret had "no actual or even potential value to [the plaintiff] outside of a single ephemeral project for a single customer.").

19. Additionally, Security Specialists made reasonable efforts to keep these materials secret by authorizing only its two highest ranked and most trusted employees, Tsotsikyan and Leon, to edit its FileMaker Pro files and confidential client information.

20. Finally, Garcia's later use of Security Specialists' client list and FileMaker Pro files to poach clients constitutes misappropriation under the statute. Garcia was never authorized to access the files, let alone use them to his advantage and to Security Specialists' great expense. *See, e.g.*, *Reeves v. Hanlon*, 33 Cal. 4th 1140, 1155, 17 Cal. Rptr. 3d 289 (2004) (internal citations omitted) ("A violation of the [CUTSA] occurs when an individual misappropriates a former employer's protected trade secret client list, for example, by using the list to solicit clients or to otherwise attain an unfair competitive advantage."). By participating in a conspiracy to steal Security Specialists' confidential files and databases by accessing Plaintiff's network without authorization — and then personally using those files to undercut Security Specialists' competitive standing by soliciting its clients while it worked to repair the damage from the hack — Garcia misappropriated Plaintiff's trade secrets.

**E. Claim Five: Civil Conspiracy**

21. Allegations of civil conspiracy cannot constitute a separate claim for relief under California law. *See, e.g.*, *Moran v. Endres*, 135 Cal. App. 4th 952, 954, 37 Cal. Rptr. 3d 786, 788 (2006) ("Conspiracy is not a cause of action, but a legal doctrine that imposes liability on persons who, although not actually committing a tort themselves, share with the immediate tortfeasors a common plan or design in its perpetration.") (internal quotation marks and citation omitted); *Ram v. Wachovia Mortgage, FSB*, No. CIV S-10-1834 LKK DAD PS, 2011 WL 1135285, at *9 (E.D. Cal. Mar. 25, 2011) ("No cause of action for conspiracy exists unless the pleaded facts show some wrongful act that would support a cause of action without the conspiracy.") (quoting *Jones v. Wells Fargo Bank*, 112 Cal. App. 4th 1527, 1541, 5 Cal. Rptr. 3d 835 (2003)); Haning, Flahavan & Kelly, Cal. Practice Guide: Personal Injury (The Rutter Group) ¶ 2:946 ("A civil conspiracy is not itself an actionable tort."). Therefore, the Court interprets Plaintiff's fifth claim for relief as an alternative basis for holding Garcia liable for the forgoing torts. Where the Court has concluded that Garcia is liable under a theory of civil conspiracy, the Court has so noted in the above discussion.

**F. Remedies**

22. Under the CFAA, an injured plaintiff may collect as damages "'any reasonable cost . . . including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.'" *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d at 1066 (quoting 18 U.S.C. § 1030(e)(11)). As calculated above in the Findings of Fact, the Court awards Plaintiff damages for Garcia's unworked overtime pay, the various costs to recover and repair Security Specialists' lost and damaged files, the fair value of the FileMaker Pro files, and Security Specialists' lost profits as a result of the hack. The same damages suffice to compensate Plaintiff for its injuries under the Stored Communications Act, Penal Code section 502, and the CUTSA.

23. Additionally, the CUTSA permits an injured plaintiff to obtain "exemplary damages in an amount not exceeding twice any" damages award for willful and malicious misappropriation. Cal. Civ. Code § 3426.3(c); *see also Mattel, Inc. v. MGA Entm't, Inc.*, 705 F.3d 1108, 1110 (9th Cir. 2013) (explaining that the CUTSA permits an award of punitive damages for willful and malicious trade secret misappropriation). However, California requires specific evidence of the defendant's financial condition to award punitive damages. *See Vacco Indus., Inc. v. Van Den Berg*, 5 Cal. App. 4th 34, 46 n.11, 6 Cal. Rptr. 2d 602 (1992), *as modified* (Apr. 14, 1992) (holding that, under *Adams v. Murakami*, 54 Cal.3d 105, 116, 123, 284 Cal. Rptr. 318 (1991), "substantial evidence of [a defendant's] financial condition" is required to award a plaintiff punitive damages pursuant to the CUTSA). California courts consider "evidence of the defendant's financial condition" to be "***essential*** for evaluating whether the amount of punitive damages actually awarded is appropriate." *Robert L. Cloud & Assocs., Inc. v. Mikesell*, 69 Cal. App. 4th 1141, 1151 n.8, 82 Cal. Rptr. 2d 143 (1999), *as modified* (Feb. 11, 1999) (emphasis added).

24. Here, Plaintiff presented no evidence of Garcia's financial condition. Garcia's paystubs from 2014 indicate that he was at that time earning less than $15 per hour as a Patrol Officer for Security Specialists. Plaintiff has presented no evidence as to Garcia's current financial condition. Accordingly, the Court cannot award Plaintiff punitive damages under California law.

## VERDICT

The Court **FINDS** and **RULES** as follows:

On Plaintiff's Claim One for violation of the CFAA, Defendant Garcia knowingly accessed Security Specialists' payroll system, and altered his records to reflect that he worked more overtime hours than he really did. Additionally, Defendant Garcia participated in a civil conspiracy to knowingly access without authorization Security Specialists' network, with the intent to defraud, and thereby obtained Security Specialists' valuable, proprietary information. The Court thus finds in favor of Plaintiff.

On Plaintiff's Claim Two for violation of the Stored Communications Act, Defendant Garcia participated in a civil conspiracy to intentionally access and cripple, without authorization, Security Specialists' email servers. The Court thus finds in favor of Plaintiff.

On Plaintiff's Claim Three for violation of California Penal Code section 502, Defendant Garcia knowingly and without permission accessed Security Specialists' payroll system and altered his records to reflect that he worked more overtime than he really did. As a result, Defendant Garcia was paid thousands of dollars more in overtime wages than he was really owed. Additionally, Defendant Garcia participated in a civil conspiracy to knowingly access without authorization Security Specialists' network, with the intent to defraud, and thereby obtained Security Specialists' valuable, proprietary information. The Court thus finds in favor of Plaintiff.

On Plaintiff's Claim Four for violation of the CUTSA, Garcia participated in a conspiracy to steal, and subsequently used, Security Specialists' confidential databases

and files to undercut Security Specialists' competitive advantage. The Court thus finds in favor of Plaintiff.

On Plaintiff's Claim Five for civil conspiracy, the Court concludes that civil conspiracy is not a separate claim for relief under California law, but rather an alternative means of finding liability. As a technical matter the Court finds in favor of Defendant Garcia on this claim, but the Court has previously noted where it has found Defendant Garcia liable for the foregoing claims on a theory of civil conspiracy.

In total, Plaintiff is awarded **$318,661.70** in damages. As the prevailing party, Plaintiff may be entitled to statutory attorneys' fees, in a sum to be calculated at a later date.

Plaintiff has pending claims against one other Defendant in this action, Mher Uzunyan. The Court will enter a separate judgment pursuant to Federal Rules of Civil Procedure 54 and 58(b) once those claims are resolved and the entire action is concluded.

Dated: May 2, 2017.

MICHAEL W. FITZGERALD
United States District Judge