Michael Friedland (State Bar No. 157,217)
mfriedland@kmob.com
Boris Zelkind (State Bar No. 214,014)
boris.zelkind@kmob.com
KNOBBE, MARTENS, OLSON & BEAR, LLP
12790 El Camino Real
San Diego, CA 92130
Phone: (858) 707-4000
Facsimile: (858) 707-4001

Attorneys for Plaintiff
SUNPOWER CORPORATION

PSG

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CV 12-00694

SUNPOWER CORPORATION, a Delaware corporation, Plaintiff, v. SOLARCITY CORPORATION, a Delaware corporation; TOM LEYDEN, an individual; MATT GIANNINI, an individual; DAN LEARY, an individual; FELIX AGUAYO, an individual; ALICE CATHCART, an individual, Defendants.	Case No. **MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF PLAINTIFF'S MOTION FOR TEMPORARY RESTRAINING ORDER** Date: TBD Time: TBD Ctrm: TBD

MEM. RE TRO

TABLE OF CONTENTS

TABLE OF CONTENTS
(continued)

Page No.

TABLE OF AUTHORITIES

Page No.

TABLE OF AUTHORITIES
(continued)

Page No.

OTHER AUTHORITIES

Plaintiff SunPower Corporation ("SunPower"), pursuant to Fed. R. Civ. P. 65, respectfully requests the Court to enter a temporary restraining order, and in support states as follows:

I. INTRODUCTION AND SUMMARY OF ARGUMENT

SunPower is a leading manufacturer and distributor of high efficiency solar panels and systems for the residential and commercial solar markets. SunPower's solar panels and systems are now used around the world.

Defendants Tom Leyden ("Leyden"), Matt Giannini ("Giannini"), Dan Leary ("Leary"), Felix Aguayo ("Aguayo"), and Alice Cathcart ("Cathcart") (collectively, the "Former Employees") had been employees of SunPower for years, and SunPower trusted them with its trade secret and proprietary information. All of these Former Employees left SunPower in close proximity to one another, and all began working for defendant SolarCity Corporation ("SolarCity"). SolarCity is a competing distributor of solar panels in the residential market that until recently had not competed with SunPower in the commercial solar market. Despite the fact that all of the Former Employees left SunPower at about the same time and all of them went to SolarCity, SunPower never thought that they would have considered stealing from SunPower. Unfortunately, SunPower was naïve.

In December, 2011, SunPower would learn, by chance, that Aguayo exploited a glitch in SunPower's email system to gain access to SunPower's email system after he left SunPower and forwarded emails to himself containing important SunPower information. After learning of Aguayo's breach of SunPower's email system, SunPower began investigating the Former Employees. The results were alarming: shortly before leaving SunPower, the Former Employees stole tens of thousands of confidential and non-confidential proprietary computer files, including trade secret and confidential customer information, manufacturing cost information, business plans, and market forecasts. Not only did the Former Employees steal massive amounts of SunPower data, their methods were strikingly similar. All the Former Employees connected personal USB devices just days before leaving SunPower and used them to steal important files. Leyden, Aguayo, and Leary

all conducted their theft mainly between the hours of 8:00 p.m. and 2:30 a.m. Often, the file transfers began within seconds of the user connecting their personal USB device.

In this action, SunPower seeks remedies for Defendants' misappropriation of trade secrets, computer hacking, and other causes of action. Before SunPower can proceed with the litigation, however, particularly in view of the Former Employees propensity for stealing and transferring data, SunPower needs this Court's assistance to preserve the evidence.

Accordingly, SunPower respectfully requests that this Court issue a narrowly tailored temporary restraining order requiring Defendants and any person acting in concert with Defendants, to: (1) identify all computers and computer media used by or for the Former Employees at SolarCity; (2) identify all computers and computer media in the Former Employees' possession, custody, or control, including USB devices identified in the Kopelev Decl., ¶ 9, which the Former Employees used to steal SunPower information; (3) produce or otherwise allow a computer forensic expert to forensically mirror the identified computers and computer media; and (4) refrain from using or disclosing any information obtained from SunPower, including SunPower's confidential information and non-confidential proprietary information, to any third party, until a motion for preliminary injunction can be heard by this Court.

II. STATEMENT OF FACTS

SunPower was founded more than a quarter-century ago to generate and deliver sustainable energy. SunPower solar panels and systems meet the highest standards of efficiency and reliability and are used around the world in diverse locations including individual homes, corporations, and large solar power plants. Headquartered in San Jose, SunPower has offices in North America, Europe, Australia and Asia. Bronez Decl., ¶ 2.

The Former Employees were employed by SunPower in various sales positions for years. *See* Bostic Decl., ¶¶ 2-6. While employed by SunPower, each of the Former Employees signed a confidentiality agreement with SunPower. *Id.* at Exs. 1-5. In these agreements, the Former Employees promised not to use any SunPower information for their own or others' benefit or disclose such information to anyone outside SunPower. The

Former Employees also promised to return all SunPower information to SunPower upon the termination of their employment. *Id.* at Exs. 1-5. For a period of two years after their employment with SunPower, the Former Employees also agreed not to solicit, encourage, or cause any employees of SunPower to terminate their employment with SunPower. *Id.*

While the Former Employees were employed by SunPower, SunPower also had various policies in place that limited the use of SunPower computers and computer equipment. Rhodes-Ousley Decl., ¶¶ 10 and 11. These policies require employees to protect SunPower's intellectual property and keep it confidential, prohibit unauthorized access to SunPower confidential information, prohibit use of SunPower information resources in the absence of a job-related need, prohibit connecting non-SunPower-owned equipment to SunPower's network, and prohibit using USB drives to store or transfer files. *Id.* at Exs. 1-4.

SunPower maintains a database to manage sales contacts and data on www.salesforce.com. SunPower employees that are involved in sales, including the Former Employees, regularly access this database as a part of their employment duties. This database includes trade secret and highly confidential and proprietary information regarding past sales activity and potential leads on new sales. The database contains contact information, previously sold products, potential interest in new products, prior sales, potential new sales, and status reports, among other highly confidential information. This information is vital to the success of any employee involved in sales. Bronez Decl., ¶ 3.

SunPower has invested a large amount of resources and employee hours over the past two and a half decades developing the commercial solar industry. As a result, SunPower has gained an enviable position as one of the leading manufacturers and distributors of solar panels in the world. *Id.* at ¶ 4. Much of this success is due to SunPower's extensive research and analysis of the solar market, resulting in invaluable trade secret and proprietary information. *Id.* This information includes market and business forecasts detailing potential target customers, regions, and industries. SunPower has also developed countless tools and models for financial planning and generating customer price quotes. This information is invaluable to the success of a commercial solar sales department. *Id.*

Defendant SolarCity is a distributor of solar panels and systems. Until recently, SolarCity primarily sold solar panels in the residential market and has not had a significant presence in the commercial solar market. *Id.* at ¶ 5. As a result, SolarCity's commercial sales department is much less mature than SunPower's and lacks the information and know-how that SunPower has developed over time. This information would take years to independently develop. *Id.* Rather than spend the time and resources to do so, SolarCity illegally obtained the information through the Former Employees who, on their way out the door, stole tens-of-thousands of SunPower documents and tools comprising SunPower's collective knowledge it has developed over the past quarter of a century.

SolarCity first recruited Tom Leyden, SunPower's Managing Director of East Operations, who was a trusted employee for more than 10 years. *See* Bostic Decl., ¶ 2. On August 23, 2011, Leyden left SunPower and began working for SolarCity. *Id.* Shortly thereafter, Leyden began recruiting other SunPower employees to join SolarCity. Among the employees who left SunPower to work for SolarCity are defendants Giannini, Leary, Aguayo, and Cathcart. *Id.* at ¶¶ 3-6. Every one of them stole vital SunPower information before leaving.

SunPower originally assumed these employees would not steal from SunPower. In December, 2011, SunPower learned that Aguayo exploited a glitch in SunPower's email system to gain access to SunPower's email system after he left SunPower and forward emails to himself containing important SunPower information. Rhodes-Ousley Decl., ¶¶ 2-6. After learning of this breach, SunPower began an immediate investigation of the Former Employees. *Id.* at ¶ 7. The results were staggering: the Former Employees ***all*** had connected personal USB devices and used them to steal tens of thousands of computer files containing SunPower trade secrets, confidential information and non-confidential proprietary information.

Leyden stole approximately 4,300 SunPower files between the hours of 9:40 p.m. and 10:30 p.m. on August 18, 2011, days before leaving SunPower. Kopelev Decl., ¶ 15. Leyden used at least three personal USB devices, including a massive two terabyte external hard

drive, to steal this information. *Id.* at ¶ 9. These files included hundreds of quotes, proposals, and contracts, as well as files containing proprietary and confidential market analyses, business analyses, and forecasts. Bronez Decl., ¶ 6. Leyden targeted critical market summaries and business plans containing the details of targeting potential customers, forecasts, incentives, and overall sales. *Id.* Leyden also stole quote generation tools that contain specific SunPower customer data, costs, and analysis. Several of these files even related to areas of SunPower's business that Leyden was not involved in and would have had no legitimate reason to *ever* have accessed. *Id.*

In addition, on August 17, 2011, days before leaving SunPower, Leyden stole highly confidential data from the SunPower database on www.salesforce.com. This data included information about major SunPower customers accounting for over $100 million of sales throughout 2011. *Id.* at ¶ 7. The data also contained the name of the SunPower employee that was responsible for these major sales. *Id.* Leyden used that information to recruit SunPower employees, including Leary, Aguayo, and Cathcart. All of these employees eventually left SunPower and began working for Leyden at SolarCity—but not before stealing even more of SunPower's computer files.

Aguayo stole approximately 11,000 files between the hours of 9:00 p.m. on October 10, 2011 to 2:30 a.m. on October 11, 2011. Aguayo also stole approximately 12,000 files between the hours of 12:00 a.m. and 1:00 a.m. on October 20, 2011. Kopelev Decl., ¶ 16. Aguayo used at least three personal USB devices to steal this information. *Id.* at ¶ 9. These files included thousands of proposals, contracts, and quotes, as well as hundreds of files containing proprietary and confidential cash flow analysis, market analyses, business analyses, and forecasts. Bronez Decl., ¶ 8. Among these files were critical business plans containing the details of targeted potential customers, forecasts, incentives, and overall sales. Aguayo also stole a proposal generation matrix that forecasts SunPower's manufacturing costs through 2016. *Id.*

Aguayo also stole a large amount of information related to at least one large account he had worked on at SunPower. Far from relationships Aguayo might have developed over

the years, this information contained vital details of SunPower's prior and forecasted dealings with this customer that would allow Aguayo to unfairly compete against SunPower. *Id.* at ¶ 9. Aguayo and SolarCity have already used this information to submit competing bids against SunPower. *Id.*

Leary stole approximately 44,000 files between the hours of 8:00 p.m. and 10:00 p.m. on November 1, 2011—the two hours immediately following Leary connecting his personal USB external hard drive. Kopelev Decl., ¶ 17. Leary used at least two personal USB devices to steal this information. *Id.* at ¶ 9. These files included over 40,000 quotes, contracts, proposals, and deals, as well as hundreds of files containing proprietary and confidential cash flow analysis, market analyses, business analyses, and forecasts. Bronez Decl., ¶ 10. Among these files were critical forecasts, agreements, and several different models used for financial planning. *Id.* Leyden even stole thousands of contracts including engineering procurement and construction contracts, performance guarantee contracts, operations and maintenance contracts, SREC contracts, power purchase agreements, SunPower guarantees for projects, sub-contractor contracts, and customer-executed contracts. These contracts contain extremely sensitive customer information that allows Leary and SolarCity to target SunPower's major accounts. *Id.* Several of these files related to areas of SunPower's business that Leary was not involved in and would have had no legitimate reason to *ever* have accessed. *Id.*

Leary also stole a large amount of information related to at least one large account he had worked on at SunPower. *Id.* at ¶ 11. Additionally, Leyden stole a significant number of files related to this same customer. *Id.* This information contained vital details of SunPower's prior and forecasted dealings with this customer that would allow Leary to unfairly compete against SunPower. *Id.* SunPower employees recently encountered Leary during a walkthrough in preparation to bid on a new solar project for this company. *Id.* at ¶ 12. The information Leary and Leyden stole could allow SolarCity to predict and undermine SunPower's position in submitting its bid. *Id.*

Cathcart stole approximately 1,500 files from November 2, 2011 to November 4, 2011, the final three days of her employment with SunPower. Kopelev Decl., ¶ 18. Cathcart

used at least one personal external hard drive to transfer this information. *Id.* ¶ 9. These files included proposals, contracts, quotes, and deals, as well as files containing proprietary and confidential cash flow analysis, project economics, and market analyses. Bronez Decl., ¶ 13. Several of these files contained critical pricing lists and talking points. At least one of these files was the same proposal generation matrix that Aguayo took, that forecasts SunPower's manufacturing costs through 2016. *Id.* Several of these files even related to areas of SunPower's business that Cathcart was not involved in and would have had no legitimate reason to have accessed. *Id.* Furthermore, the day Cathcart left SunPower, she exported three separate reports from www.salesforce.com which included confidential sales and contact information. *Id.* at ¶ 14.

Giannini stole approximately 500 SunPower files on August 30, 2011. Giannini also stole as many as 350 SunPower files on September 14, 2011, the day before leaving SunPower. Kopelev Decl., ¶ 19. These files included hundreds of quotes, deals, proposals and contracts, as well as files containing proprietary and confidential market analyses, business analyses, and forecasts. Bronez Decl., ¶ 15. The copied files also include critical agreements, contracts, term sheets, and business plans containing the details of targeted potential customers, forecasts, incentives, and overall sales. *Id.* In eight minutes, Giannini connected his personal USB device and transferred more than 180 files from SunPower's network. Kopelev Decl., ¶ 19. Giannini also stole market forecasts for two strategic markets, in which SolarCity has now begun competing. Bronez Decl., ¶ 16.

All of the information the Former Employees copied is extremely valuable to SunPower, any sales person in the solar industry, and SunPower's competitors. This information is valuable because it provides competitive advantage in selecting which markets to pursue, selecting the best market strategies, knowing SunPower's strengths to mitigate and weaknesses to exploit in attacking markets, and competing to win new customer projects. Because SolarCity's large commercial sales group is much less mature than SunPower's, the information also gives SolarCity tools, templates, and knowledge to gain large commercial sales expertise faster than they would without it. *Id.* at ¶ 17.

III. A TEMPORARY RESTRAINING ORDER IS WARRANTED TO PREVENT USE AND DISSEMINATION OF SENSITIVE INFORMATION

The standard for granting a temporary restraining order under Rule 65 is the same as the standard for entering a preliminary injunction. *See Stuhlbarg Int'l Sales Co. v. John D. Brush & Co.*, 240 F.3d 832, 839 n.7 (9th Cir. 2001). To obtain preliminary injunctive relief, a party must show: (1) a likelihood of success on the merits; (2) a likelihood of irreparable harm to the moving party in the absence of preliminary relief; (3) that the balance of equities tips in the favor of the moving party; and (4) that an injunction is in the public interest. *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008). As discussed below, all of these requirements are met.

A. SunPower is Likely to Succeed on the Merits

While SunPower is likely to prevail on all of its causes of action, for judicial efficiency, this motion only addresses the Computer Fraud and Abuse Act and Trespass to Chattels causes of action.

1. Computer Fraud and Abuse Act - 18 U.S.C. § 1030 (a)(2)(C)

The Computer Fraud and Abuse Act is violated by whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030 (a) (2) (C). Furthermore, any person who is damaged may bring a civil cause of action if the "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." 18 U.S.C. § 1030 (g); 18 U.S.C. § 1030 (c) (4) (i) (I).

a. Former Employees Intentionally Accessed Protected Computers

The Former Employees intentionally accessed their SunPower-owned computers every time they logged in to the computers using their assigned usernames and passwords. The term "protected computer" means a computer "which is used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). All of these computers were used to receive email and were connected to the internet. Rhodes-Ousley Decl., ¶ 10. The Ninth Circuit has held that "[a]s both the means to engage in commerce and the method

by which transactions occur, the Internet is an instrumentality and channel of interstate commerce." *U.S. v. Sutcliffe*, 505 F.3d 944, 953 (9th Cir. 2007). Thus, all the computers were used in, and affected, interstate and foreign commerce.

b. The Former Employees Exceeded Authorized Access and Thereby Obtained Information from SunPower's Computers

The phrase "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6); *see also U.S. v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (Defendant exceeded authorized access by obtaining personal information from his employer's computer for a non-business reason, in violation of the employer's policy prohibiting such personal use); *see also U.S. v. John*, 597 F.3d 263, 272 (5th Cir. 2010) (Defendant exceeded authorized access by downloading sensitive customer account information, in violation of her employer's official policy); *see also E.f. Cultural Travel Bv v. Explorica*, 274 F.3d 577, 583 (1st Cir. 2001) (Defendant exceeded authorized access by using proprietary codes obtained while working for their former employer, in violation of a confidential use policy, to design a computer program which extracted publicly available data from the former employer's website much more quickly than possible without the proprietary codes). Thus, an employee who has some authorized access to a computer system "exceeds" that authorized access by accessing information in violation of their employer's written computer use policy.

Here, the Former Employees signed agreements detailing the confidential nature of the information on SunPower's computer system. Bostic Decl., Ex. 1-5. Furthermore, SunPower had several computer use policies in effect during the Former Employees employment at SunPower. Rhodes-Ousley Decl., Exs. 1-4. These policies prohibit employees from using SunPower computer systems when there is no job-related need to do so and prohibits employees from connecting non-SunPower-owned equipment to SunPower's network. *Id.*

///

The Former Employees all violated these policies. They all used SunPower information resources to steal SunPower's confidential information and non-confidential proprietary information—often in the middle of the night. Kopelev Decl., ¶¶ 15-19. They connected multiple personal USB devices to their SunPower-owned computer systems over the course of their employment, including a combined *15* devices in the last 30 days of their employment. *Id.* at ¶ 9. Moreover, many of the Former Employees stole information from other departments, which they would never have had reason to access in the first place. Bronez Decl., ¶¶ 6, 10, and 13. The Former Employees violated SunPower's computer use policy and, therefore, exceeded their authorization under 18 U.S.C. § 1030.[1]

c. The Loss to SunPower Is Well in Excess of $5,000

The term "loss" means "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). Since December, 2011, SunPower has already incurred well over $5,000 in expenses relating to the computer forensic investigation of the Former Employees' breach of SunPower's computer system. Rhodes-Ousley Decl., ¶ 8. Moreover, at least six SunPower employees have spent at least 34 hours investigating the damage. *Id.,* ¶ 9. SunPower has already lost considerably more than $5,000 in the last year.

2. Computer Fraud and Abuse Act - 18 U.S.C. § 1030 (a)(4)

The Computer Fraud and Abuse Act is also violated by any 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 . . ." 18 U.S.C. § 1030 (a) (4). As is the case under 18 U.S.C. § 1030 (a) (2) (c), any person who is damaged may bring a civil cause of action if the "loss to 1 or more

---

[1] Aguayo also accessed SunPower's network without authorization when he accessed SunPower's email system after leaving SunPower and forwarded SunPower information to her personal email account. Rhodes-Ousley Decl. ¶¶ 2-6.

persons during any 1-year period . . . aggregating at least $5,000 in value." 18 U.S.C. § 1030 (g); 18 U.S.C. § 1030 (c) (4) (A) (i) (I).

a. The Former Employees, Knowingly and With Intent to Defraud, Accessed a Protected Computer

As addressed above, the Former Employees intentionally accessed their SunPower-owned computers every time they logged in to the computers using their assigned usernames and passwords. For the purposes of the Computer Fraud and Abuse Act, "'[t]he term 'defraud' . . . simply means wrongdoing and does not require proof of common law fraud." *See Multiven, Inc. v. Cisco Sys.*, 725 F. Supp. 2d 887, 892 (N.D. Cal. 2010) (*citing Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc.*, 556 F. Supp. 2d 1122, 1131 (E.D. Cal. 2008) and *Ebay, Inc. v. Digital Point Solutions, Inc.*, 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009)). A showing of some taking, or use, of information is usually required to prove intent to defraud. *See Id.* (*citing P.C. Yonkers, Inc. v. Celebrations The Party and Seasonal Superstore, LLC*, 428 F.3d 504, 509 (3d. Cir. 2005)).

Here, the Former Employees copied tens of thousands of SunPower files containing SunPower confidential information and non-confidential proprietary information to numerous personal USB devices. Kopelev Decl., ¶¶ 15-19. The repeated copying and deletion of confidential files indicates that information was copied to external devices. *Id.* Defendants clearly took and used a large amount of SunPower data and, therefore, intended to defraud SunPower within the meaning of Computer Fraud and Abuse Act.

b. The Former Employees Exceeded Authorized Access and Thereby Obtained a Thing of Value

As addressed above, the Former Employees repeatedly exceeded their authorized access when they violated SunPower's computer use policy. 18 U.S.C. § 1030(a)(4) requires the defendant obtain "anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period." 18 U.S.C. § 1030 (a) (4). Here, the Former Employees obtained tens of thousands of confidential computer files from SunPower. These files detailed nearly every

aspect of SunPower's business, including confidential and trade secret customer information, manufacturing cost information, business plans, and market forecasts. The information is extremely valuable to Defendants and could allow them to compete unfairly with SunPower for years to come. Bronez Decl., ¶ 17.

c. The Loss to SunPower Aggregates at Least $5,000 in the Last Year

As addressed in section A.1.c. above, SunPower has already lost considerably more than $5,000 in the last year.

3. Trespass to Chattels

Trespass to Chattels occurs where "an intentional interference with the possession of personal property has proximately caused injury." *Thrifty-Tel, Inc. v. Bezenek*, 46 Cal. App. 4th 1559, 1566 (1996). A plaintiff can have a possessory right in intangibles such as computer data. *Id.* The Former Employees stole tens of thousands of SunPower files including files containing non-trade secret proprietary information. Kopelev Decl., ¶¶ 15-19; Bronez Decl., ¶ 17. SunPower had exclusive ownership rights in those files because they were developed by SunPower employees at SunPower's expense. Finally, SunPower was damaged because these files could allow Defendants to compete unfairly in the marketplace. Thus, the Former Employees committed trespass to chattels by their unauthorized copying SunPower's computer files.

B. SunPower Will Suffer Immediate and Irreparable Injury if a Temporary Restraining Order is Not Issued

The files the Former Employees stole from SunPower detail SunPower's business plan for the next several years. These files contain information about important customers, market plans, business plans, cost analysis, and other vital information. These files contain the "keys" to much of SunPower's success and could be used by Defendants to devastate SunPower's ability to compete in the global marketplace. Bronez Decl., ¶ 17. SunPower discovered the theft relatively early and there may still be time to prevent much of the damage if Defendants are ordered to return all the stolen files and ordered not to use, or disclose to third parties, the contents of the stolen files. *See* Rhodes-Ousley Decl., ¶¶ 2-7.

Such an order will prevent Defendants from further damaging SunPower by profiting from the use of SunPower's confidential information and non-confidential proprietary information. In view of the Former Employees deceptive practices of stealing tens-of-thousands of computer files and transferring them amongst highly mobile personal USB devices, it is highly likely Defendants will conceal the stolen computer files unless this Court grants this motion and allows SunPower to copy data from the Former Employees computers. This may be SunPower's only opportunity to obtain this information. SunPower is simply seeking to preserve evidence and to prevent dissemination of its confidential and proprietary information.

SunPower has not delayed in seeking a temporary restraining order. The Former Employees left SunPower between August 23, 2011 to November 4, 2011. Bostic Decl., ¶¶ 2 - 6. SunPower had no reason to believe that these formerly-trusted employees would betray them until they discovered, quite fortunately, that Aguayo had abused a glitch in SunPower's email system to steal information after he left SunPower. Rhodes-Ousley Decl., ¶¶ 2-6. SunPower began an immediate investigation that did not conclude until early February, 2012. SunPower brought suit and moved for a temporary restraining promptly after discovering the full breadth of the Former Employees theft. Accordingly, this factor also supports the granting of a temporary restraining order.

C. <u>The Balance of Equities Tips Strongly in Favor of SunPower</u>

As discussed above, SunPower will suffer immediate and irreparable injury if this motion is not granted. By contrast, Defendants will only be required to allow a computer forensics expert to create a copy of the relevant computer media and be required not to use or disclose any of SunPower's information until a hearing on a motion for preliminary injunction can be heard. Defendants' operations will not be significantly impacted because they will only lose a minimal amount of computer time while the copies are being made. SunPower will treat the preserved information as highly confidential Attorneys' Eyes Only until such time as the Court designates any portion thereof. Accordingly, this factor also supports the granting of a temporary restraining order.

D. An Injunction is in the Public Interest

The public interest analysis requires the court consider "whether there exists some critical public interest that would be injured by the grant of preliminary relief." *Indep. Living Ctr. S. Cal., Inc. v. Maxwell-Jolly*, 572 F.3d 644, 659 (internal citation omitted). "When the reach of an injunction is narrow, limited only to the parties, and has no impact on non-parties, the public interest will be 'at most a neutral factor in the analysis rather than one that favor[s] [granting or] denying the preliminary injunction.'" *Stormans, Inc. v. Selecky*, 586 F.3d 1109, 1138-39 (9th Cir. 2009) (*quoting Bernhardt v. L.A. Cnty.*, 339 F.3d 920, 931 (9th Cir. 2003)). "If, however, the impact of an injunction reaches beyond the parties, carrying with it a potential for public consequences, the public interest will be relevant to whether the district court grants the preliminary injunction." *Id.* at 1139 (*citing Sammartano v. First Judicial Dist. Court*, 303 F.3d 959, 965 (9th Cir. 2002)).

Here, the impact of granting a temporary restraining order is limited to the parties and the general public does not appear to have any significant interest. There is no indication that the impact will reach beyond the parties and injure the public in any fashion. To the extent the public has any interest in this matter, the public interest favors a temporary restraining order. By enacting numerous laws directed to the misuse of computers, Congress and the state legislature have indicated that there is a strong public interest in preventing activities such as Defendants'. Accordingly, this factor also supports the granting of a temporary restraining order.

E. Any Required Bond Should be Minimal

F.R.C.P. 65 provides: "[t]he court may issue a preliminary injunction or a temporary restraining order only if the movant gives security in an amount that the court considers proper to pay the costs and damages sustained by any party found to have been wrongfully enjoined or restrained." As discussed above, all the requirements of a temporary restraining order have been met. However, in the highly unlikely event that Defendants are wrongfully enjoined, the damages will be minimal.

///

As addressed above, Defendants will only be required to allow a computer forensics expert to create a copy of the Former Employees' computer media on site and be required not to use or disclose any of SunPower's information until a hearing on a motion for preliminary injunction can be heard. Defendants operations will not be significantly restrained because they will only lose a minimal amount of computer time while the copies are being made and be required not to use and disseminate computer files (including their contents) that do not belong to them. The preserved information will be treated as highly confidential Attorneys' Eyes Only until such time as the Court designates any portion thereof. Thus, a bond of not more than $5,000 is appropriate.

IV. CONCLUSION

The Former Employees have flagrantly copied tens-of-thousands of SunPower's files and used them for Defendants' benefit. These files detail many aspects of SunPower's business, including important customer information, manufacturing cost information, business plans, and market forecasts. Moreover, the stolen files include not only information that is valuable to individual sales persons, but also broad market and forecast predictions that are incredibly valuable to SolarCity. This information will greatly damage SunPower's global sales by allowing SolarCity to predict SunPower's every movement for years to come. In view of the Former Employees deceptive practices of stealing tens-of-thousands of computer files late at night and transferring them amongst highly mobile personal USB devices, it is highly likely Defendants will conceal the stolen computer files unless this Court grants this motion and allows SunPower to copy data from the Former Employees computers.

Accordingly, SunPower respectfully requests this Court issue a narrowly tailored temporary restraining order requiring Defendants and any person acting in concert with Defendants, to: (1) identify all computers and computer media used by or for the Former Employees at SolarCity; (2) identify all computers and computer media in the Former Employees' possession, custody, or control, including USB devices identified in the Kopelev Decl., ¶ 9; (3) produce or otherwise allow a computer forensic expert to forensically mirror/image the identified computers and computer media; and (4) refrain from using or

disclosing any information obtained from SunPower, including SunPower's confidential information and non-confidential proprietary information, to any third party, until a motion for preliminary injunction can be heard by this Court.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 2-13-2012

By: _____
Michael K. Friedland
Boris Zelkind

Attorneys for Plaintiff
SUNPOWER CORPORATION

12727373
021012