

E-FILING

ADR

ORIGINAL

1 Michael Friedland (State Bar No. 157,217)  
mfriedland@kmob.com

2 Boris Zelkind (State Bar No. 214,014)  
boris.zelkind@kmob.com

3 KNOBBE, MARTENS, OLSON & BEAR, LLP  
12790 El Camino Real  
4 San Diego, CA 92130  
Phone: (858) 707-4000  
5 Facsimile: (858) 707-4001

FILED

FEB 13 2012

RICHARD W. WIENING  
CLERK, U.S. DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

6 Attorneys for Plaintiff  
SUNPOWER CORPORATION

PSG

8 IN THE UNITED STATES DISTRICT COURT  
9 FOR THE NORTHERN DISTRICT OF CALIFORNIA

CV 12-00694

10 \_\_\_\_\_  
11 SUNPOWER CORPORATION, a  
Delaware corporation,

) Case No.

12 Plaintiff,

) MEMORANDUM OF POINTS AND  
) AUTHORITIES IN SUPPORT OF  
) PLAINTIFF'S MOTION FOR  
) TEMPORARY RESTRAINING ORDER

13 v.

14 SOLARCITY CORPORATION, a  
15 Delaware corporation; TOM LEYDEN, an  
individual; MATT GIANNINI, an  
16 individual; DAN LEARY, an individual;  
FELIX AGUAYO, an individual; ALICE  
17 CATHCART, an individual,

) Date: TBD  
) Time: TBD  
) Ctrm: TBD

18 Defendants.  
\_\_\_\_\_

19  
20  
21  
22  
23  
24  
25  
26  
27  
28

TABLE OF CONTENTS

1		<u>Page No.</u>
2		
3	I. INTRODUCTION AND SUMMARY OF ARGUMENT .....	1
4	II. STATEMENT OF FACTS .....	2
5	III. A TEMPORARY RESTRAINING ORDER IS WARRANTED TO	
6	PREVENT USE AND DISSEMINATION OF SENSITIVE	
7	INFORMATION .....	8
8	A. SunPower is Likely to Succeed on the Merits .....	8
9	1. Computer Fraud and Abuse Act - 18 U.S.C. § 1030	
10	(a)(2)(C) .....	8
11	a. Former Employees Intentionally Accessed	
12	Protected Computers.....	8
13	b. The Former Employees Exceeded Authorized	
14	Access and Thereby Obtained Information from	
15	SunPower’s Computers .....	9
16	c. The Loss to SunPower Is Well in Excess of	
17	\$5,000 .....	10
18	2. Computer Fraud and Abuse Act - 18 U.S.C. § 1030	
19	(a)(4) .....	10
20	a. The Former Employees, Knowingly and With	
21	Intent to Defraud, Accessed a Protected	
22	Computer .....	11
23	b. The Former Employees Exceeded Authorized	
24	Access and Thereby Obtained a Thing of Value .....	11
25	c. The Loss to SunPower Aggregates at Least	
26	\$5,000 in the Last Year .....	12
27	3. Trespass to Chattels .....	12
28	B. SunPower Will Suffer Immediate and Irreparable Injury if a	
	Temporary Restraining Order is Not Issued .....	12
	C. The Balance of Equities Tips Strongly in Favor of SunPower .....	13
	D. An Injunction is in the Public Interest .....	14
	E. Any Required Bond Should be Minimal .....	14

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

TABLE OF CONTENTS  
(continued)

Page No.

IV. CONCLUSION..... 15

TABLE OF AUTHORITIES

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Page No.

*Bernhardt v. L.A. Cnty.*,  
339 F.3d 920 (9th Cir. 2003) ..... 14

*E.f. Cultural Travel Bv v. Explorica*,  
274 F.3d 577 (1st Cir. 2001)..... 9

*Ebay, Inc. v. Digital Point Solutions, Inc.*,  
608 F. Supp. 2d 1156 (N.D. Cal. 2009)..... 11

*Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc.*,  
556 F. Supp. 2d 1122 (E.D. Cal. 2008) ..... 11

*Indep. Living Ctr. S. Cal., Inc. v. Maxwell-Jolly*,  
572 F.3d 644 ..... 14

*Multiven, Inc. v. Cisco Sys.*,  
725 F. Supp. 2d 887 (N.D. Cal. 2010)..... 11

*P.C. Yonkers, Inc. v. Celebrations The Party and Seasonal Superstore, LLC*,  
428 F.3d 504 (3d. Cir. 2005) ..... 11

*Sammartano v. First Judicial Dist. Court*,  
303 F.3d 959 (9th Cir. 2002) ..... 14

*Stormans, Inc. v. Selecky*,  
586 F.3d 1109 (9th Cir. 2009) ..... 14

*Stuhlberg Int’l Sales Co. v. John D. Brush & Co.*,  
240 F.3d 832 (9th Cir. 2001) ..... 8

*Thrifty-Tel, Inc. v. Bezenek*,  
46 Cal. App. 4th 1559 (1996) ..... 12

*U.S. v. John*,  
597 F.3d 263 (5th Cir. 2010) ..... 9

*U.S. v. Rodriguez*,  
628 F.3d 1258 (11th Cir. 2010) ..... 9

*U.S. v. Sutcliffe*,  
505 F.3d 944 (9th Cir. 2007) ..... 9

*Winter v. Natural Res. Def. Council, Inc.*,  
555 U.S. 7 (2008)..... 8

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

TABLE OF AUTHORITIES

(continued)

Page No.

OTHER AUTHORITIES

18 U.S.C. § 1030..... 8, 9, 10, 11

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

4 **I. INTRODUCTION AND SUMMARY OF ARGUMENT**

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

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

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

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

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

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

## 18 **II. STATEMENT OF FACTS**

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

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

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

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

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

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



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

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

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

26 Leyden stole approximately 4,300 SunPower files between the hours of 9:40 p.m. and  
27 10:30 p.m. on August 18, 2011, days before leaving SunPower. *Kopelev Decl.*, ¶ 15. Leyden  
28 used at least three personal USB devices, including a massive two terabyte external hard

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

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

17 Aguayo stole approximately 11,000 files between the hours of 9:00 p.m. on October  
18 10, 2011 to 2:30 a.m. on October 11, 2011. Aguayo also stole approximately 12,000 files  
19 between the hours of 12:00 a.m. and 1:00 a.m. on October 20, 2011. Kopelev Decl., ¶ 16.  
20 Aguayo used at least three personal USB devices to steal this information. *Id.* at ¶ 9. These  
21 files included thousands of proposals, contracts, and quotes, as well as hundreds of files  
22 containing proprietary and confidential cash flow analysis, market analyses, business  
23 analyses, and forecasts. Bronez Decl., ¶ 8. Among these files were critical business plans  
24 containing the details of targeted potential customers, forecasts, incentives, and overall sales.  
25 Aguayo also stole a proposal generation matrix that forecasts SunPower's manufacturing  
26 costs through 2016. *Id.*

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

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

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

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

27 Cathcart stole approximately 1,500 files from November 2, 2011 to November 4,  
28 2011, the final three days of her employment with SunPower. Kopelev Decl., ¶ 18. Cathcart

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

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

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

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

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

11 **A. SunPower is Likely to Succeed on the Merits**

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

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

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

22 **a. Former Employees Intentionally Accessed Protected Computers**

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

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

4 **b. The Former Employees Exceeded Authorized Access and Thereby**  
5 **Obtained Information from SunPower’s Computers**

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

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

28 ///

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

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

11 The term “loss” means “any reasonable cost to any victim, including the cost of  
12 responding to an offense, conducting a damage assessment, and restoring the data, program,  
13 system, or information to its condition prior to the offense, and any revenue lost, cost  
14 incurred, or other consequential damages incurred because of interruption of service.” 18  
15 U.S.C. § 1030 (e) (11). Since December, 2011, SunPower has already incurred well over  
16 \$5,000 in expenses relating to the computer forensic investigation of the Former Employees'  
17 breach of SunPower's computer system. Rhodes-Ousley Decl., ¶ 8. Moreover, at least six  
18 SunPower employees have spent at least 34 hours investigating the damage. *Id.*, ¶ 9.  
19 SunPower has already lost considerably more than \$5,000 in the last year.

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

21 The Computer Fraud and Abuse Act is also violated by any person who “knowingly  
22 and with intent to defraud, accesses a protected computer without authorization, or exceeds  
23 authorized access, and by means of such conduct furthers the intended fraud and obtains  
24 anything of value . . .” 18 U.S.C. § 1030 (a) (4). As is the case under 18 U.S.C. § 1030 (a)  
25 (2) (c), any person who is damaged may bring a civil cause of action if the “loss to 1 or more

26 \_\_\_\_\_  
27 <sup>1</sup> Aguayo also accessed SunPower's network without authorization when he accessed  
28 SunPower's email system after leaving SunPower and forwarded SunPower information to  
her personal email account. Rhodes-Ousley Decl. ¶¶ 2-6.

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

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

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

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

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

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



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

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

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

8 3. **Trespass to Chattels**

9 Trespass to Chattels occurs where "an intentional interference with the possession of  
10 personal property has proximately caused injury." *Thrifty-Tel, Inc. v. Bezenek*, 46 Cal. App.  
11 4th 1559, 1566 (1996). A plaintiff can have a possessory right in intangibles such as  
12 computer data. *Id.* The Former Employees stole tens of thousands of SunPower files  
13 including files containing non-trade secret proprietary information. Kopelev Decl., ¶¶ 15-19;  
14 Bronez Decl., ¶ 17. SunPower had exclusive ownership rights in those files because they  
15 were developed by SunPower employees at SunPower's expense. Finally, SunPower was  
16 damaged because these files could allow Defendants to compete unfairly in the marketplace.  
17 Thus, the Former Employees committed trespass to chattels by their unauthorized copying  
18 SunPower's computer files.

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

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

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

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

19 **C. The Balance of Equities Tips Strongly in Favor of SunPower**

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

1 **D. An Injunction is in the Public Interest**

2 The public interest analysis requires the court consider “whether there exists some  
3 critical public interest that would be injured by the grant of preliminary relief.” *Indep. Living*  
4 *Ctr. S. Cal., Inc. v. Maxwell-Jolly*, 572 F.3d 644, 659 (internal citation omitted). “When the  
5 reach of an injunction is narrow, limited only to the parties, and has no impact on non-parties,  
6 the public interest will be ‘at most a neutral factor in the analysis rather than one that favor[s]  
7 [granting or] denying the preliminary injunction.’” *Stormans, Inc. v. Selecky*, 586 F.3d 1109,  
8 1138-39 (9th Cir. 2009) (quoting *Bernhardt v. L.A. Cnty.*, 339 F.3d 920, 931 (9th Cir. 2003)).  
9 “If, however, the impact of an injunction reaches beyond the parties, carrying with it a  
10 potential for public consequences, the public interest will be relevant to whether the district  
11 court grants the preliminary injunction.” *Id.* at 1139 (citing *Sammartano v. First Judicial*  
12 *Dist. Court*, 303 F.3d 959, 965 (9th Cir. 2002)).

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

21 **E. Any Required Bond Should be Minimal**

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

28 ///

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

#### 10 IV. CONCLUSION

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

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

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

4 Respectfully submitted,

5 KNOBBE, MARTENS, OLSON & BEAR, LLP

6  
7 Dated: 2-13-2012

8 By: 

Michael K. Friedland  
Boris Zelkind

9 Attorneys for Plaintiff  
10 SUNPOWER CORPORATION

11 12727373  
12 021012

13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28