

EXHIBIT D - REDACTED

Sacramento County Sheriff's Department
North Division (East Area)
5510 Garfield Ave
Sacramento, CA 95841

Report No: NE 2010-0093641

Report Date: 05/28/2010

SUMMARY

Associate Type Information Report
Watch Summary
Occurrence Date Wed 05/26/2010 @ 16:45 Initial Status: Pended
Occurrence address
Reported Date Fri 05/28/2010 @ 18:45

VIOLATIONS

Code Section	Description	Category	Attempt
ZZ INFORMATION	INFORMATION		No

SYNOPSIS OF CRIME

Complainant found a computer next to the trash dumpster in his apartment complex, took it home, and was able to access the harddrive. On the hard drive he found multiple viruses, which when sent out are activated, steal Facebook, and screen names and passwords. Additionally the complainant found an e-mail address, did research online and discovered and that the computer possibly belongs to an individual who is currently involved in a federal lawsuit with Facebook regarding phishing and spamming. The computer was collected as evidence and booked into the evidence room.

ACTIVITY STATUS

Status Date: 5/28/2010 Status: Pended case
Status Set By: Hunt, Bruce
Comment:

PARTICIPANTS

Witness Ricef Male White DOB: 10/9 XREF: 3089797
Operator License Number
Locations Home address Home phone
Employer Full time Health Net

METHOD/CRIME FACTORS

MO	Alarm system	Not applicable
	Surroundings	Residential
	Place of activity	Parking lot
	Structure	Not applicable
IBR	Location Type	Residential, single family house
	Bias Motivation	None
	Suspected of Using	Used computer equipment

VEHICLES

There is no vehicle associated with this report.

PROPERTY

There is no property associated with this report.

EVIDENCE

There is no evidence associated with this report.

INVOLVED PERSONNEL

<i>Involvement</i>	<i>Employee</i>	<i>Badge</i>	<i>Division</i>
Approving Officer	Dean Pai	52	NE
Narrative Officer	Bruce Hunt	1110	NE
Reporting Officer	Bruce Hunt	1110	NE
Transcriber	Lin Katsules		CD

DIST	SECT	SUB	SACRAMENTO SHERIFF'S DEPARTMENT CONTINUATION REPORT		PAGE 3 OF 4	REPORT NUMBER 2010-0093641
LOCATION OF INCIDENT			DATE 05/26/2010	DAY OF WEEK Wed	TIME 16:45	
AUTHORITY / SECTION 22 INFORMATION - INFORMATION						
COMPLAINANT/VICTIM (LIST FIRST VICTIM IF MORE THAN ONE)						

1734 Hours, 05/28/10 (Friday): I, Deputy B. Hunt #1110 (Unit 27D1), was dispatched to a found property call.

The text for the call stated the complainant found a computer discarded next to a dumpster, took it home to use it, and on it found viruses that you can send out which collects Facebook names and passwords and other types of information. The complainant works for a computer software company in the private sector and would like SSD to pick up the computer.

1738 Hours: I arrived and contacted the complainant, [REDACTED] RICE. He related that he had found a computer tower by the trash dumpster and had taken it home to see if he could salvage it.

RICE used a disk to bypass the locked password on the hard drive and gained access. On the hard drive, he found various computer programs for the purpose of breaking in and sending viruses out to collect people's Facebook screen names and passwords. RICE had prepared a handwritten statement and gave it to me. (See attached statement).

RICE handed me a document he printed off of the internet from ZDnet. The title of the document says

"Facebook sues man for allegedly phishing and spamming and lists their names".

One of the names involved in the law suit was a Phillip POREMBSKI. RICE told me he had found an email address on the hard drive; phil420@gmail.com. Additionally, Per POREMBSKI's profile on Facebook, it shows the same email address and he lives in Gold River, CA.

The second document RICE gave me was also printed off of the internet from Justia.com and it indicated that there is currently a lawsuit; Facebook, Inc. vs. FISHER et al. The plaintiff (Facebook) is suing defendants including a Phillip POREMBSKI (case #5:2009 cv 05842) filed December 14, 2009 in the California Northern District Federal Court, San Jose Office. The judge handling the case is Honorable Judge Jeremy Fogel.

I went to the website Justia.com and located additional documents. On the website there was a copy of a Restraining Order filed in the United States District Court of Northern California, San Jose Division. The document shows the plaintiff's attorneys' are: Brian HENNESSEY bar #226721 out of Menlo Park, CA, an attorney Joseph CUTLER, and a law firm Perkins Cloie out of Seattle, WA with a telephone number of (206)359-8000.

I attempted to reach Brian HENNESSEY, but got his voicemail.

I contacted Perkins Cloie law firm in Washington State. I spoke with Joseph CUTLER who indeed stated that he was an attorney that represents Facebook in this matter. I verified that there was a federal civil law suit currently going on and that POREMBSKI was indeed one of the defendants.

I advised him that I had located a computer that may be possibly contain evidence related to his lawsuit and it possibly once belonged to one of the defendants; Phillip POREMBSKI. I advised him

REPORTING OFFICER Hunt	BADGE 1110	DIVISION	APPROVED BY Pal	BADGE 52	DATE AND TIME OF REPORT Fri 05/28/2010 18:45
---------------------------	---------------	----------	--------------------	-------------	---

DIST	SECT	SUB	SACRAMENTO SHERIFF'S DEPARTMENT CONTINUATION REPORT		PAGE 4 OF 4	REPORT NUMBER 2010-0093641
LOCATION OF INCIDENT			DATE 05/26/2010	DAY OF WEEK Wed	TIME 16:45	
AUTHORITY / SECTION 22 INFORMATION - INFORMATION						
COMPLAINANT/VICTIM (LIST FIRST VICTIM IF MORE THAN ONE)						

that it had been found abandoned in an apartment trash dumpster and turned over to law enforcement by a concerned citizen.

CUTLER stated that the computer potentially has thousands and thousands of screen names and passwords to Facebook client's accounts and possibly other sensitive information of similar nature.

I provided him with the Sheriff's Department report number and advised him that if he needed additional information, he will need to obtain a subpoena to get a copy of this report and the computer if it is something Federal Court Judge feels is necessary to their case.

The computer was booked into the Sheriff's North East evidence room as evidence pending the determination of the relevance to the federal case.

FEDERAL COURT CASE INFO:

Facebook, Inc. v. Fisher et al

Plaintiff: Facebook, Inc.
Defendants: Jeremi Fisher, Philip Porembski, Ryan Shimeall, Choko Systems LLC, Harm, Inc., PP Web Services LLC and iMedia Online Services LLC

Case Number: 5:2009cv05842
Filed: December 14, 2009

Court: California Northern District Court
Office: San Jose Office [[Court Info](#)]
County: Santa Clara
Presiding Judge: Hon. Jeremy Fogel
Referring Judge: Magistrate Judge Patricia V. Trumbull

Court house info:

California Northern District Court
San Jose Divisional Office
2112 Robert F. Peckham Federal
Bldg and United States Courthouse
280 South First Street
San Jose, CA 95113-3002
Phone: 408-535-5364

REPORTING OFFICER Hunt	BADGE 1110	DIVISION	APPROVED BY Pai	BADGE 52	DATE AND TIME OF REPORT Fri 05/28/2010 18:45
---------------------------	---------------	----------	--------------------	-------------	---

**SACRAMENTO COUNTY SHERIFF'S DEPARTMENT
PROPERTY RECEIPT/REPORT**

2010-97241
REPORT NUMBER

SEIZED BY SEARCH
WARRANT NO.

ASSET FORFEITURE # OF SUSPECTS

MARK ONE BOX ONLY →

RECOVERED STOLEN

EVIDENCE

CONTRABAND & SEE REMARKS

SAFE KEEPING

FOUND

FILL IN ALL INFORMATION FOR SAFEKEEPING REPORTS

REPORTING DATE: 8-10 DAY: 11 TIME: 12:00 CONNECTED REPORT(S) NUMBER AND TYPE: AUTHORITY AND SECTION:

V NAME (LAST FIRST MIDDLE):
DOB: AGE: SEX: RACE:

CP NAME (LAST FIRST MIDDLE): Rice
DOB: AGE: SEX: RACE:

ITEM NO'S	QUANTITY	NAME OF ITEM (DESCRIBE - SERIAL NO., SIZE, COLOR, MARKINGS, ETC.) WHERE AND HOW WAS PROPERTY RECOVERED: SAFEKEEPING AND FOUND PROPERTY REQUIRE A COMPLETE SYNOPSIS (NO CRIME REPORT REQUIRED UNLESS OTHERWISE DICTATED BY POLICY)	PROPERTY WAREHOUSE USE ONLY
101-1	ONE	Computer monitor 16" monitor Serial # T P 2 B 106 00574 note to 812 * Computer involved in a Federal * Civil lawsuit Facebook vs Fisher Case # 9:2009 cv 05842 C.D. Northern District of S. JOR. Divisional Dist. 408-538-5364	
		* Pull Report for Details *	

I HAVE READ THE REVERSE OF THIS RECEIPT AND ELECT TO:
 EXERCISE MY CLAIM TO ITEMS _____
 WAIVE MY CLAIM TO ITEMS _____
 FILE A FINDERS CLAIM TO ITEMS _____
 SIGNATURE _____

RECOVERED STOLEN PROPERTY - TYPE AND VALUE

A. CURRENCY, NOTES, ETC. \$ _____	C. CLOTHING AND FURS \$ _____	H. HOUSEHOLD GOODS \$ _____
B. JEWELRY AND PRECIOUS METALS \$ _____	E. OFFICE EQUIPMENT \$ _____	I. CONSUMABLE GOODS \$ _____
	F. TV'S, RADIOS, STEREO'S, ETC. \$ _____	J. LIVESTOCK \$ _____
	G. FIREARMS \$ _____	K. MISCELLANEOUS \$ _____

NAME OF OFFICER TAKING PROPERTY (PRINT): _____ BADGE NO.: 1110 DIV: N/A NAME OF SUPERVISOR (PRINT): _____ PAGE OF _____

COMPLETE REVERSE SIDE OF COPY WHEN BOOKING PROPERTY TO: RECORDS - FORWARD REPORT TO: DATE BOOKED: TIME BOOKED:

Blank Page

wednesday around 445 pm found computer ⁱⁿ dumpster of apartments.

brought computer home powered up and found computer in working condition.

operating system is Windows XP

only login was Administrator protected by a password

thursday night used Hiren's Boot CD, specifically Kon-Boot to bypass administrator password.

created another administrator user called "new" - blank password

changed administrator password to 123.45 11 pm

logged into administrator ~~was~~ shortly after

Quickly noticed several suspicious files:

vb program for automatically logging into myspace
hundreds of email addresses with associated passwords

"spam contact" in australia

several "bot" programs used for DDOS, and spam

RDP sessions contained about 15 IP addresses with
user name "WEX"

several adult themed websites

mIRC user

Phil/harm	phil@msain.org
phil420@gmail.com	AKA WEX

majority of last modified dates were 7/24/2007

one file accessed in 2009

no ~~user~~ browser history

no m/RE logs

one folder called "cat & me" contains several pictures
~~with~~.

Searched phil420@gmail.com in facebook. Profile belongs
to Phillip Porembski located in Gold River, CA.

Searched Philip Porembski in google search engine.

1st hit is a case number for facebook vs

Jeremi Fisher, Philip Porembski, Ryan Shineall,
Chico Systems LLC, Harm, Inc PP Web Services,
and iMedia Online.

Case # 5:2009cv05842

December 14, 2009

Blank Page



10-93641

Facebook sues men for allegedly phishing, spamming

Elinor Mills, CNET News.com on December 17th, 2009

Facebook has sued three men, alleging they used phishing techniques to get access to Facebook user accounts and then sent spam from the compromised accounts.

The lawsuit was filed Monday in a federal court in San Jose, California, and named as defendants Jeremi Fisher, Philip Porembski, Ryan Shimeall and the companies associated with them, Choko Systems, Harm, and iMedia Online Services, according to a Facebook statement late on Tuesday. The defendants could not be reached for comment.

The defendants are accused of launching at least four spam campaigns over the last couple of years, the latest in the last three months being responsible for nearly three-fourth of all spam on the site, according to the suit. The latest "escalated attack" included spam offering a colon cleanser, fake messages purporting to show a video of the recipient and offers for recipients to make money through a fake "Google Campaign." Clicking on the spam typically sends a user through various marketing sites before landing them on a page that prompts for their Facebook log in information.

It is unclear exactly how Facebook user log in information, used to send spam to friends, was obtained.

Facebook has spent US\$5,000 combating the spam, according to the suit.

The lawsuit makes claims under the Can-Spam (Controlling the Assault of Non-Solicited Pornography and Marketing) Act, the Computer Fraud and Abuse Act, the California Anti-Phishing Act and the California Computer Data Access and Fraud Act, according to Facebook.

This is the latest legal action the social networking site has taken related to spam. In October, Facebook was awarded US\$711 million in a judgment Thursday against self-described "spam king" Sanford Wallace.

The largest judgment ever under the Can-Spam Act was an US\$873 million award Facebook won in November 2008 against Adam Guerhuez, of Montreal, and his company, Atlantis Blue Capital.

This article was first published as a blog post on CNET News.

URL:<http://www.zdnetasia.com/facebook-sues-men-for-allegedly-phishing-spamming-62060045.htm>

Facebook, Inc. v. Fisher et al

10-93641

Plaintiff: Facebook, Inc.
Defendants: Jeremi Fisher, Philip Poremski, Ryan Shimeall, Choko Systems LLC, Harm, Inc., PP Web Services LLC and iMedia Online Services LLC

Case Number: 5:2009cv05842
Filed: December 14, 2009

Court: California Northern District Court
Office: San Jose Office [Court Info]
County: Santa Clara
Presiding Judge: Hon. Jeremy Fogel
Referring Judge: Magistrate Judge Patricia V. Trumbull

Nature of Suit: Other Statutes - Other Statutory Actions
Cause: 28:1331 Fed. Question: Breach of Contract
Jurisdiction: Federal Question
Jury Demanded By: Plaintiff

Blank Page

1 Brian Hennessy, State Bar No. 226721
2 bhennessy@perkinscoie.com
3 PERKINS COIE LLP
4 101 Jefferson Drive
5 Menlo Park, California 94025
6 Telephone: 650.838.4300
7 Facsimile: 650.838.4350

8 James McCullagh, *pro hac vice application to follow*
9 jmccullagh@perkinscoie.com
10 Joseph Cutler, *pro hac vice application to follow*
11 jcutler@perkinscoie.com
12 PERKINS COIE LLP
13 1201 Third Avenue, Suite 4800
14 Seattle, Washington 98101
15 Telephone: 206.359.8000
16 Facsimile: 206.359.9000

17 Attorneys for Plaintiff
18 FACEBOOK, INC.

19
20
21
22
23
24
25
26
27
28
UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

17 FACEBOOK, INC., a Delaware
18 corporation,

19 Plaintiff,

20 v.

21 JEREMI FISHER; PHILIP POREMBSKI;
22 RYAN SHIMEALL; and JOHN DOES 1-
23 25, individuals; and CHOKO SYSTEMS
24 LLC; HARM, INC.; PP WEB SERVICES
25 LLC, iMEDIA ONLINE SERVICES LLC,
26 and JOHN DOES 26-50, corporations,

27 Defendants.

Case No. C 09-05842 JF

**PLAINTIFF FACEBOOK'S NOTICE OF
MOTION AND MOTION FOR
TEMPORARY RESTRAINING ORDER**

Before: Hon. Jeremy Fogel

TABLE OF CONTENTS

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
NOTICE OF MOTION AND MOTION	1
PLAINTIFF FACEBOOK, INC.'S MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF ITS MOTION FOR TEMPORARY RESTRAINING ORDER	3
I. INTRODUCTION	3
II. REQUESTED RELIEF	4
III. STATEMENT OF FACTS	5
A. Facebook Background	5
B. Defendants' Unauthorized Activities.....	6
IV. ARGUMENT	7
A. Standard for Issuing a Temporary Restraining Order.....	7
B. Facebook Is Likely to Succeed on the Merits and Will Suffer Irreparable Harm if the Defendant Is Not Restrained	8
1. Facebook Is Likely to Succeed on the Merits.....	8
2. Facebook Will Suffer Irreparable Harm if Defendants Are Not Restrained	15
C. Even if There Are Serious Questions on the Merits, the Balance of Hardships Tips Sharply in Facebook's Favor.....	16
D. The Public Interest Favors Facebook's Relief.....	17
E. Minimal Bond Is Appropriate.....	18
V. CONCLUSION.....	18

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

Cases

Aitken v. Commc'ns Workers of Am., 496 F. Supp. 2d 653 (E.D. Va. 2007)9

Amoco Prod. Co. v. Village of Gambell, Ala., 480 U.S. 531 (1987) 17

Diamontiney v. Borg, 918 F.2d 793 (9th Cir. 1990).....8

Facebook v. ConnectU, LLC, 489 F. Supp. 2d 1087 (N.D. Cal. 2007) 11

Fund for Animals, Inc. v. Lujan, 962 F.2d 1391 (9th Cir. 1992).....7

GoTo.com, Inc. v. Walt Disney Co., 202 F.3d 1199 (9th Cir. 2000)7, 16

Midgett v. Tri-County Metro. Transp. Dist., 254 F.3d 846 (9th Cir. 2001).....7

MySpace v. Sanford Wallace, 498 F. Supp. 2d 1293 (C.D. Cal. 2007).....passim

Nat'l Wildlife Fed'n v. Nat'l Marine Fisheries Serv., 235 F. Supp. 2d 1143 (W.D. Wash. 2002).....7

Rent-a-Center, Inc. v. Canyon Television & Appliance Rental, Inc., 944 F.2d 597 (9th Cir. 1991).....15

Stuhlberg Int'l Sales Co., Inc. v. John D. Brush & Co., 240 F.3d 832 (9th Cir. 2001).....15

Tom Doherty Assocs., Inc. v. Saban Entm't, Inc., 60 F.3d 27 (2d Cir. 1995)15

Westlands Water Dist. v. Natural Res. Def. Council, 43 F.3d 457 (9th Cir. 1994).....7

Statutes

15 U.S.C. § 7701 *et seq.*8

15 U.S.C. § 7701(a) 17

15 U.S.C. § 7704(a)(1).....9

15 U.S.C. § 7704(a)(1)(A).....9

15 U.S.C. § 7704(a)(2).....9

15 U.S.C. § 7704(a)(3).....10

15 U.S.C. § 7704(a)(5).....10

15 U.S.C. § 7704(a)(6).....9

15 U.S.C. § 7704(b)(3)10

TABLE OF AUTHORITIES
(continued)

	Page
15 U.S.C. § 7706(g)(1)(A).....	8
18 U.S.C. § 1030.....	10
18 U.S.C. § 1030(a)(2).....	11
18 U.S.C. § 1030(a)(4).....	11
18 U.S.C. § 1030(a)(5)(A)(i)	12
18 U.S.C. § 1030(a)(5)(A)(ii)	12
18 U.S.C. § 1030(a)(5)(A)(iii).....	12
18 U.S.C. § 1030(a)(6).....	10, 12
18 U.S.C. § 1030(g).....	8
Cal. Bus & Prof. Code § 22948.2	14
Cal. Penal Code § 502.....	13
Cal. Penal Code § 502(c)	11
Cal. Penal Code § 502(c)(1)	13
Cal. Penal Code § 502(c)(2)	13
Cal. Penal Code § 502(c)(3)	13
Cal. Penal Code § 502(c)(4)	14
Cal. Penal Code § 502(c)(5)	14
Cal. Penal Code § 502(c)(7)	14
Cal. Penal Code § 502(e)(1)	8
Cal. Penal Code § 503(a).....	17
Regulations and Rules	
Federal Rule of Civil Procedure 65	3
Federal Rule of Civil Procedure 65(b).....	7
Federal Rule of Civil Procedure 65(c).....	18

NOTICE OF MOTION AND MOTION

TO: DEFENDANTS AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE THAT pursuant to Federal Rule of Civil Procedure 65, that on a hearing date set by the Court or as soon as possible, Plaintiff Facebook, Inc. ("Facebook") will move, and hereby moves, for a temporary restraining order against Jeremi Fisher, Philip Porembski, Ryan Shimeall, and Choko Systems LLC, Harm, Inc., PP Web Services LLC, and iMedia Online Services LLC (collectively "Defendants"), restraining and enjoining Defendants' ongoing and escalating phishing and spamming campaign against Facebook and its users. Specifically, Facebook moves to enjoin Defendants, and any of their directors, officers, agents, servants, employees, and persons and entities acting in concert with them, from engaging in the following conduct until the Court may consider Plaintiff's motion for preliminary injunction:

1. Initiating or procuring transmission of unsolicited commercial electronic messages ("spam") on or through Facebook's computers, Facebook's website, Facebook's networks, or to Facebook users;
2. Accessing or attempting to access Facebook's website, networks, data, information, user information, profiles, computers, or computer systems;
3. Soliciting, requesting, or taking any action to induce Facebook users to provide identifying information or representing that such solicitation, request, or action is being done with Facebook's authorization or approval;
4. Retaining any copies, electronic or otherwise, of any Facebook information, including user login information or passwords, obtained through illegitimate or unlawful actions;
5. Engaging in any activity that alters, damages, deletes, destroys, disrupts, diminishes the quality of, interferes with the performance of, or impairs the functionality of Facebook's computers, computer system computer network, data, website, or services;
6. Engaging in any unlawful activities alleged in this action;

1 **PLAINTIFF FACEBOOK, INC.'S MEMORANDUM OF POINTS AND AUTHORITIES**
2 **IN SUPPORT OF ITS MOTION FOR TEMPORARY RESTRAINING ORDER**

3 **I. INTRODUCTION**

4 Plaintiff Facebook, Inc. ("Facebook") respectfully moves the Court, pursuant to Federal
5 Rule of Civil Procedure 65, for an order temporarily enjoining Defendants' ongoing and
6 escalating phishing¹ and spamming campaign against Facebook and its users. Defendants Jeremi
7 Fisher, Philip Porembski, and Ryan Shimeall, individually and through various affiliated
8 corporate entities listed as defendants in this case, continue to target and attack Facebook – the
9 world's largest social network, now with more than 350 million members.

10 Defendants are currently and actively pursuing a sophisticated and multi-faceted attack:

11 [REDACTED]
12 [REDACTED]
13 [REDACTED]

14 Even now, Defendants continue to
15 phish for Facebook user information and send spam to Facebook users despite explicit warnings
16 from Facebook that their activities violate Facebook's Statement of Rights and Responsibilities
17 ("SRR") or any policies, terms, or guidelines governing the use of the Facebook website,
18 network, and the Facebook Platform, and are illegal.

19 In fact, despite these explicit warnings, Defendants' illegal activities have recently and
20 substantially escalated.

21 [REDACTED]
22 [REDACTED]
23 [REDACTED]

24 Due to Defendants' willful disregard of the law and Facebook's warnings, and the recent
25 escalation in their attacks on Facebook and its users, Facebook seeks injunctive relief to prevent
26 further irreparable damage to it and its users. Absent the Court's intervention, Defendants will be

27 _____
28 ¹ "Phishing" describes the attempt to acquire sensitive information such as usernames and
passwords by masquerading as a trustworthy entity in an electronic communication.

1 able to continue and further escalate their illegal activities unfettered, thereby severely harming
2 Facebook and its users.

3 **II. REQUESTED RELIEF**

4 Plaintiff Facebook moves to enjoin Defendants, and any of their directors, officers, agents,
5 servants, employees, and persons and entities acting in concert with them, from engaging in the
6 following conduct until the Court may consider Plaintiff's motion for preliminary injunction:

- 7 7. Initiating or procuring transmission of unsolicited commercial electronic messages
8 ("spam") on or through Facebook's computers, Facebook's website, Facebook's
9 networks, and/or to Facebook users, including messages in the form of Facebook chat
10 messages, Facebook internal messages, Facebook Wall posts, or any other form of
11 messaging available on or through Facebook or the Facebook Platform;
- 12 8. Accessing or attempting to access Facebook's website, the Facebook Platform,
13 Facebook networks, data, information, user information, profiles, computers,
14 computer systems and/or any offices, properties or facilities owned, operated or
15 occupied by Facebook or its employees;
- 16 9. Soliciting, requesting, or taking any action to induce Facebook users to provide
17 identifying information or representing that such solicitation, request, or action is
18 being done with Facebook's authorization or approval;
- 19 10. Retaining any copies, electronic or otherwise, of any Facebook information, including
20 user login information or passwords, obtained through illegitimate or unlawful actions;
- 21 11. Engaging in any activity that alters, damages, deletes, destroys, disrupts, diminishes
22 the quality of, interferes with the performance of, or impairs the functionality of
23 Facebook's computers, computer system, computer network, data, website or services;
- 24 12. Engaging in any unlawful activities alleged in this action;
- 25 13. Disposing of any assets procured through the activities alleged in the Complaint;
- 26 8. Entering or accessing the physical premises or facilities of Facebook or its counsel; or
- 27
28

1 9. Engaging in any activity that violates Facebook's Statement of Rights and
2 Responsibilities, or any policies, terms, or guidelines governing the use of the
3 Facebook website, network, and the Facebook Platform.

4 Facebook further requests that the Court schedule a preliminary injunction hearing at its earliest
5 convenience.

6 **III. STATEMENT OF FACTS**

7 **A. Facebook Background**

8 Facebook owns and operates the widely popular social networking website located at
9 <http://www.facebook.com>. Declaration of Facebook Employee² ("Facebook Decl.") ¶ 2.
10 Facebook currently has more than 350 million active users. *Id.* Users must register with
11 Facebook, agree to its Statement of Rights and Responsibilities ("SRR"), and obtain a unique
12 username and password before being granted full access to the Facebook website. *Id.* ¶ 4. Only
13 registered users may fully utilize Facebook's services, which include accessing user profiles,
14 inviting other Facebook users to be "friends," sending messages on Facebook, and using
15 applications on Facebook's developer platform. *Id.*

16 Facebook users have complete control over those with whom they interact on Facebook.
17 *Id.* ¶ 6. Facebook users have the ability to control access to their user profiles, including the site's
18 various messaging options. *Id.* Privacy controls and secure communications among Facebook
19 users are vital to the integrity of Facebook's proprietary network as well as to the level of
20 confidence that users have in using Facebook. *Id.* ¶ 7. The privacy controls provided by
21 Facebook, Facebook's security measures, and the resulting secure communications between and
22 among Facebook users are key aspects of Facebook's success. *Id.*

23 Facebook does not tolerate or permit the use of its services or website for sending spam.
24 *Id.* ¶ 8. Facebook's SRR, which bind anyone who uses or accesses Facebook's website, explicitly
25 prohibit any unsolicited or unauthorized advertising, solicitations, promotions, junk mail, spam,
26 chain letters, or pyramid schemes. Compl. Ex. A. Facebook's SRR also prohibit, among other

27 _____
28 ² To protect the identity and safety of the employee who handles Facebook's security matters, he
or she will be referred to herein as "Facebook Employee."

1 things, (1) collecting users' content of information or otherwise accessing Facebook using
2 automated means (such as harvesting, bots, robots, spiders, or scrapers) without Facebook's
3 permission; (2) using Facebook in an unlawful manner or in any other manner that could damage,
4 disable, overburden, or impair the Facebook website; (3) providing false personal information on
5 Facebook or falsely stating or otherwise misrepresenting oneself; (4) accessing another Facebook
6 user's account; (5) sending or otherwise posting spam on Facebook; (6) soliciting Facebook login
7 information from Facebook users; and (7) using Facebook profiles for commercial use. *Id.*

8 **B. Defendants' Unauthorized Activities**

9 Defendants are Facebook users and during all relevant times agreed to abide by
10 Facebook's SRR. Facebook Decl. ¶ 5. At no time have Defendants received permission from
11 Facebook to conduct any commercial activity on Facebook's website. *Id.* ¶ 9.

12 Defendants' attack on Facebook is sophisticated, constantly evolving, and quickly
13 escalating. *Id.* ¶ 10.

14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED] *Id.*

18 This escalation is the latest round in a more than yearlong spamming and phishing campaign by
19 Defendants targeted at Facebook and Facebook users. *Id.* ¶¶ 10-11.

20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED] The spam will

24 include a message such as "Hey just wanted to share this with you but I made \$854 today with
25 google, so I thought I'd share this with you just visit <http://profitg00glecash.info>." *Id.* ¶ 15.

26 When a Facebook user receives the spam message and clicks on the embedded link, he or she is
27 then rapidly redirected through a series of websites that pay Defendants for the traffic generated
28 from the link in the spam message. Declaration of Joseph P. Cutler ("Cutler Decl.") ¶ 6.

1 Following this redirection, the user's browser lands at a "phishing" website designed to
2 trick the user into divulging [REDACTED]
3 [REDACTED]. Facebook Decl. ¶ 15. Some of Defendants' websites
4 [REDACTED] while others entice users to [REDACTED] with promises
5 of free computers, colon cleansers, money-making schemes, free ringtones, or IQ tests. *Id.* ¶ 16.

6 [REDACTED]
7 [REDACTED]
8 [REDACTED]. Cutler Decl.
9 ¶¶ 4-5, 7; Facebook Decl. ¶ 15. This cycle then repeats, leading to a rapidly expanding and ever-
10 increasing amount of [REDACTED] and spam.

11 Facebook has explicitly warned Defendants that their activity violates Facebook's SRR
12 and that their activity is illegal. Cutler Decl. ¶¶ 2-3. Despite this warning, Defendants' phishing
13 and spamming has not only persisted, but has escalated. Facebook Decl. ¶ 10.

14 IV. ARGUMENT

15 A. Standard for Issuing a Temporary Restraining Order

16 Federal Rule of Civil Procedure 65(b) authorizes temporary restraining orders, which are
17 governed by the same standards that apply to preliminary injunctions. A plaintiff is entitled to
18 preliminary injunctive relief when it demonstrates either (1) a combination of "probable success
19 on the merits" and "the possibility of irreparable injury," or (2) the existence of "serious questions
20 going to the merits," where the "balance of hardships tips sharply in [the plaintiff's] favor."
21 *GoTo.com, Inc. v. Walt Disney Co.*, 202 F.3d 1199, 1204-05 (9th Cir. 2000) (internal quotation
22 marks and citation omitted).

23 These are not separate tests but a continuum of discretion "in which the required
24 probability of success on the merits decreases as the degree of harm increases." *Nat'l Wildlife
25 Fed'n v. Nat'l Marine Fisheries Serv.*, 235 F. Supp. 2d 1143, 1151 (W.D. Wash. 2002) (quoting
26 *Westlands Water Dist. v. Natural Res. Def. Council*, 43 F.3d 457, 459 (9th Cir. 1994)). Also,
27 where the public interest is involved, courts consider whether the public interest favors the
28 plaintiff's requested relief. *Fund for Animals, Inc. v. Lujan*, 962 F.2d 1391, 1400 (9th Cir. 1992).

1 An adequate showing under either alternative formulation is satisfactory to obtain the
2 requested preliminary relief. *Midgett v. Tri-County Metro. Transp. Dist.*, 254 F.3d 846, 850-51
3 (9th Cir. 2001). Also, the moving party does not need to show actual harm, only the threat of
4 irreparable harm. *Diamontiney v. Borg*, 918 F.2d 793, 795 (9th Cir. 1990). Finally, the federal
5 and state statutes on which Facebook bases its claims expressly allow for injunctive relief. See 15
6 U.S.C. § 7706(g)(1)(A); 18 U.S.C. § 1030(g); Cal. Penal Code § 502(e)(1).

7 In this case, Facebook is entitled to a temporary restraining order because Facebook is
8 likely to prevail on the merits of its claims and will suffer irreparable injury if Defendants'
9 injurious ongoing activity is not immediately enjoined. Even if there are questions on the merits,
10 the balance of hardships tips sharply in Facebook's favor and entitles Facebook to a temporary
11 restraining order. Under either formulation, the public interest favors Facebook's relief.
12 Injunctive relief is also authorized by the statutes that provide the basis for these claims.

13 **B. Facebook Is Likely to Succeed on the Merits and Will Suffer Irreparable Harm if the**
14 **Defendant Is Not Restrained.**

15 **1. Facebook Is Likely to Succeed on the Merits**

16 As Facebook has combated Defendants' illegal and unauthorized actions, it has also
17 tracked and investigated their spamming, phishing, unauthorized access, and monetization
18 activities over the past year. Thus, even prior to discovery, Facebook has assembled sufficient
19 evidence to show Defendants' illegal activities. Based on its collected evidence, as partially
20 detailed in the declarations submitted with this motion and memorandum, Facebook is likely to
21 succeed on the merits of the claims asserted in its Complaint.

22 **a. CAN-SPAM – 15 U.S.C. § 7701, et seq.**

23 The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003
24 ("CAN-SPAM") allows Internet access services to bring actions alleging violations of
25 15 U.S.C. §§ 7701, et seq. [REDACTED]

1 [REDACTED] Facebook Decl. ¶ 10.³ Facebook has
2 gathered evidence of the following violations:

3 (i) 15 U.S.C. § 7704(a)(1) – Materially False Header Information

4 15 U.S.C. § 7704(a)(1) prohibits the transmission of commercial electronic mail messages
5 containing or accompanied by materially false or materially misleading information headers. A
6 header is "materially" misleading if it impairs the ability of the recipient to locate or respond to
7 the person who initiated the message. 15 U.S.C. § 7704(a)(6).⁴ A header that is technically
8 accurate may nevertheless be misleading if the header information was obtained fraudulently.
9 15 U.S.C. § 7704(a)(1)(A).

10 In violation of 15 U.S.C. § 7704(a)(1), Defendants' spam messages contain information
11 headers that are materially false and misleading, because they make it appear as if the spam
12 originated from legitimate Facebook users, when in fact it comes from the Defendants. Facebook
13 Decl. ¶¶ 12, 15-16. A reasonable person viewing Defendants' spam would incorrectly conclude
14 that the user whose name appears on the message was the sender. *Id.* Thus, even though the
15 message technically came from a legitimate Facebook user's account, the headers are materially
16 misleading because Defendants fraudulently [REDACTED]
17 [REDACTED] *Id.*; *MySpace*, 498 F. Supp. 2d at 1301-02 ("hijacking" member
18 accounts to send out mass email messages is prohibited under § 7704(a)(1) even where the header
19 might be accurate).

20 (ii) 15 U.S.C. § 7704(a)(2) – Misleading Subject Headings

21 15 U.S.C. § 7704(a)(2) prohibits the transmission of commercial electronic mail messages
22 to a protected computer (a computer used in interstate or foreign commerce or communication)
23 with misleading subject headings. Defendants' have violated and continue to violate this statute
24 by sending, and continuing to send, spam messages with misleading subject headings. Recipients

25 _____
26 ³ See *MySpace v. Wallace*, 498 F. Supp. 2d 1293, 1301-02 (C.D. Cal. 2007) (holding that
27 electronic mail and related posts using a website's internal account addresses are within the scope of
28 CAN-SPAM).

⁴ See also *Aitken v. Comm'n Workers of Am.*, 496 F. Supp. 2d 653, 667 (E.D. Va. 2007) (finding
that an inaccurate "From:" line that affects an objective recipient's opinion of the value of the message is
materially misleading).

1 are led to believe the messages are about commercial offers for free computers, free ringtones,
2 colon cleansers, money-making schemes, or IQ tests, when in fact they lead recipients to a
3 "phishing" website completely unrelated to the subject headings. Facebook Decl. ¶¶ 16-17.

4 **(iii) 15 U.S.C. § 7704(a)(3) – No "Opt Out" Mechanism**

5 15 U.S.C. § 7704(a)(3) prohibits the transmission of commercial electronic messages to a
6 protected computer that does not provide a means for the recipient to opt out of future messages.
7 In violation of this statute, none of Defendants' [REDACTED] spam messages contain
8 valid opt-out mechanisms. They do not include a return email address or other Internet-based
9 opt-out mechanism as required by statute. Facebook Decl. ¶¶ 10, 15; *MySpace*, 498 F. Supp. 2d
10 at 1302 (finding that use of "hijack[ed]" profiles eviscerates ability to request that no further
11 messages be sent, in violation of § 7704(a)(3)).

12 **(iv) 15 U.S.C. § 7704(a)(5) – No Required Notices**

13 15 U.S.C. § 7704(a)(5) requires (1) clear and conspicuous identification that the message
14 is an advertisement or solicitation, (2) clear and conspicuous notice of the opportunity to decline
15 to receive further commercial electronic mail messages, and (3) a valid physical postal address for
16 the sender. Defendants have violated and continue to violate this statute because their spam
17 messages do not meet any of these three requirements. Facebook Decl. ¶¶ 10, 15-16; *MySpace*,
18 498 F. Supp. 2d at 1303-04.

19 **(v) 15 U.S.C. § 7704(b)(3) – Aggravating Relay and Retransmission**

20 15 U.S.C. § 7704(b)(3) provides that it is an aggravated violation of CAN-SPAM to relay
21 or retransmit unlawful commercial electronic mail messages from Facebook's protected
22 computers and computer network without authorization. [REDACTED]

23 [REDACTED]
24 [REDACTED] Facebook Decl. ¶¶ 10, 14-16, 20.

25 **b. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030**

26 The Computer Fraud and Abuse Act ("CFAA") provides a private right of action for the
27 knowing and unauthorized access of a computer used in interstate commerce that causes loss or
28

1 damage in excess of \$5,000. The CFAA also allows claims based upon attempted violations.
2 18 U.S.C. § 1030(a)(6).

3 Throughout their ongoing cycle of spamming, phishing, unauthorized access, and
4 monetary profit, Defendants have been accessing and continue to access Facebook's computers
5 and network without authorization.⁵ Facebook Decl. ¶¶ 4, 7-8, 9-11, 20. Moreover, Defendants
6 acted and continue to act knowingly, by testing spam, [REDACTED]
7 [REDACTED] sending spam, and collecting payment for these activities. *Id.* ¶¶ 12-17; Cutler Decl.
8 ¶¶ 2-3, 6-7. Facebook has been forced to expend resources in excess of \$5,000 to investigate and
9 attempt to counter Defendants' unauthorized [REDACTED]
10 [REDACTED] Defendants' illegal and unauthorized activities.
11 Facebook Decl. ¶ 18.

12 Facebook has gathered evidence of the following CFAA violations:

13 (i) 18 U.S.C. § 1030(a)(2) – Purposeful Access and Damage

14 18 U.S.C. § 1030(a)(2) prohibits the intentional accessing of protected computers without
15 authorization or exceeding one's authorized access and causing losses of more than \$5,000.
16 Defendants have repeatedly violated this statute by purposefully accessing and continuing to
17 access the Facebook website after violating numerous provisions of Facebook's SRR and [REDACTED]
18 [REDACTED] Facebook Decl. ¶¶ 4, 8, 10-11, 18-19.

19 (ii) 18 U.S.C. § 1030(a)(4) – Knowing Access with Intent to Defraud

20 18 U.S.C. § 1030(a)(4) prohibits knowingly, and with the intent to defraud accessing a
21 protected computer without authorization or exceeding authorized access, to further a fraud and
22 obtain more than \$5,000 in value. Defendants repeatedly accessed, and continue to access,
23 Facebook's protected computers, cloaked as legitimate users, to send fraudulent spam messages
24 designed to lure users to a phishing website and thereafter defraud users through sham incentives
25

26 ⁵ Defendants violated at least seven provisions of Facebook's SRR, triggering the automatic
27 revocation of their license to access Facebook. *See supra* Section III. Therefore, Defendants' use of the
28 Facebook site constitutes unauthorized access. Facebook Decl. ¶ 4, 7-8, 9-11, 20; *Facebook v. ConnectU, LLC*, 489 F. Supp. 2d 1087, 1090-91 (N.D. Cal. 2007) (finding that, under Cal. Penal Code § 502(c), where terms of use prohibit an activity and an individual engages in the activity, the activity is "without permission").

1 specifically designed to trick users into providing [REDACTED]
2 [REDACTED] and third-party pay-per-click websites, where the induced clicks result
3 in additional earnings for defendants. Facebook Decl. ¶¶ 10-16; Cutler Decl. ¶ 6. [REDACTED]

4 [REDACTED]
5 [REDACTED]
6 [REDACTED] See Facebook Decl. ¶ 18-20.

7 (iii) 18 U.S.C. § 1030(a)(5)(A)(i) – **Knowing Malicious Transmission**

8 18 U.S.C. § 1030(a)(5)(A)(i) prohibits knowingly transmitting a program or code and
9 intentionally causing damage without authorization to a protected computer and causing
10 aggregate loss of more than \$5,000. Defendants are knowingly accessing Facebook [REDACTED]
11 [REDACTED] gain unauthorized access to the Facebook network,
12 and send bulk spam through compromised Facebook accounts. Facebook Decl. ¶¶ 10-11, 17.
13 Defendants' clear intent is to continue to violate Facebook's SRR and damage Facebook's
14 relationship with its users. Id. ¶¶ 7, 10-11, 14. In fact, as a result of Defendants' ongoing
15 campaign, [REDACTED]

16 [REDACTED] Id. ¶ 19.

17 (iv) 18 U.S.C. § 1030(a)(5)(B), (C) – **Recklessly Causing Losses**

18 18 U.S.C. § 1030(a)(5)(A)(ii) prohibits intentionally accessing protected computers (a)
19 without authorization, and recklessly causing an aggregate loss of \$5,000 or more, or (b) with
20 authorization and causing aggregate damage or loss of \$5,000 or more. Defendants continue to
21 violate 18 U.S.C. § 1030(a)(5)(B) by repeatedly accessing Facebook's computers without
22 authorization and recklessly causing more than \$5,000 in harm to Facebook. Id. ¶¶ 10, 18. Even
23 if Defendants acted with authorization, they have violated 18 U.S.C. § 1030(a)(5)(C) because
24 they have caused over \$5,000 of aggregated damage to Facebook through their actions. Id. ¶ 18.

25 (v) 18 U.S.C. § 1030(a)(6) – **Trafficking Authentication Credentials**

26 18 U.S.C. § 1030(a)(6) prohibits knowingly, and with the intent to defraud, trafficking, in
27 a way that affects interstate commerce, in passwords or login information through which one can
28 access a protected computer without authorization, and causing losses of more than \$5,000.

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

[REDACTED] and use them to further their fraud on Facebook and its users. Facebook Decl. ¶¶ 11, 14-16. [REDACTED] disguise their identity and masquerade as legitimate Facebook users while sending [REDACTED] spam messages, phishing for [REDACTED], and increasing their payout by driving traffic to third-party websites that pay them for the traffic referred. *Id.* ¶¶ 10-11, 14-16.

c. California Penal Code § 502

The California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502, provides a private right of action for owners of computers, computer systems, computer networks, computer programs, and proprietary data to bring actions for knowing violations. As discussed *supra* in Section IV(B)(1)(b), Defendants have been accessing Facebook's computers and network without authorization or in excess of their authorization [REDACTED]. Defendants have executed and continue to execute their unlawful practices knowingly and with the intent to defraud Facebook's users, damage the Facebook network, and gain personal profit. Facebook Decl. ¶¶ 4, 7-8, 10-11, 13-16; Cutler Decl. ¶¶ 2-3, 6.

Facebook has gathered sufficient evidence to establish the following violations of the California Penal Code:

(i) California Penal Code § 502(c)(1)

In violation of California Penal Code § 502(c)(1), Defendants have manipulated Facebook user data, [REDACTED] and overburdened Facebook's servers with spam messages. Defendants perform these actions as part of their ongoing plan to deceive Facebook users and profit from this deception. Facebook Decl. ¶¶ 10-11, 14-16.

(ii) California Penal Code § 502(c)(2)

Defendants have violated and continue to violate California Penal Code § 502(c)(2) by taking and copying data from Facebook's computers, computer systems, or computer networks, [REDACTED] and using it to execute their attacks. *Id.* at ¶¶ 10-11, 14-16.

1 (iii) California Penal Code § 502(c)(3)

2 Defendants have also abused the Facebook service in violation of California Penal Code
3 § 502(c)(3). Defendants have used and are using the Facebook service to send [REDACTED] false
4 and misleading spam messages, [REDACTED]
5 [REDACTED], and they are profiting from these unlawful actions. Facebook Decl.
6 ¶¶ 10-11, 14-16; Cutler Decl. ¶ 6.

7 (iv) California Penal Code § 502(c)(4)

8 Defendants are violating California Penal Code § 502(c)(4) by altering, damaging, and
9 destroying data, that resides or exists on Facebook's computers, as shown by their [REDACTED]
10 [REDACTED] Facebook Decl. ¶¶ 11, 14.

11 (v) California Penal Code § 502(c)(5)

12 In violation of California Penal Code § 502(c)(5) Defendants have disrupted and continue
13 to disrupt the Facebook service by [REDACTED] To date,
14 Defendants have [REDACTED]
15 [REDACTED] Defendants continue to evolve and escalate their spamming and phishing campaign.
16 Facebook Decl. ¶¶ 10, 20.

17 (vi) California Penal Code § 502(c)(7)

18 Defendants' unauthorized access alone constitutes a violation of California Penal Code
19 § 502(c)(7), which prohibits knowingly accessing a computer network without permission.

20 d. California Bus. & Prof. Code § 22948, et seq.

21 The California Anti-Phishing Act provides:

22 It shall be unlawful for any person, by means of a Web page,
23 electronic mail message, or otherwise through use of the Internet, to
24 solicit, request, or take any action to induce another person to
provide identifying information by representing itself to be a
business without the authority or approval of the business.

25 Cal. Bus & Prof. Code § 22948.2. As seen in some iterations of Defendants' phishing sites,

26 Defendants have incorporated a page that [REDACTED] See
27 Facebook Decl. ¶ 16. This page [REDACTED] is owned

1 and operated by the Defendants and is designed to deceive users into [REDACTED]

2 [REDACTED]. *Id.* ¶¶15-16.

3 e. **Breach of Contract**

4 Use of the Facebook site and Facebook services is governed by and subject to Facebook's
5 SRR, to which all users agree before receiving permission to access Facebook. *Id.* ¶ 4, 7-8. In
6 addition to Defendants' acceptance of Facebook's SRR when they registered, they were also put
7 on specific notice of their violation of the SRR in October 2008. Cutler Decl. ¶¶ 2-3.

8 Facebook has gathered evidence that Defendants have violated at least seven of the
9 provisions in its SRR, including (1) sending or otherwise posting spam on Facebook, (2)
10 collecting users' content or information, or otherwise accessing Facebook, using automated means
11 (such as harvesting, bots, robots, spiders, or scrapers) without Facebook's permission; (3) using
12 Facebook in an unlawful manner or in any other manner that could damage, disable, overburden,
13 or impair the Facebook website; (4) providing false personal information on Facebook or falsely
14 stating or otherwise misrepresenting oneself; (5) accessing another Facebook user's account; (6)
15 soliciting Facebook login information from Facebook users; and (7) using Facebook profiles for
16 commercial use. Facebook Decl. at ¶ 7-8, 11-17.

17 As a result of Defendants' spamming and phishing activities, which breach Facebook's
18 SRR, [REDACTED]

19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED] Cutler Decl. ¶ 6; Facebook Decl. ¶ 18.

23 **2. Facebook Will Suffer Irreparable Harm if Defendants Are Not Restrained**

24 Aside from any economic injuries it has suffered, Facebook has suffered, is suffering, and
25 will continue to suffer injuries such as loss of users, loss of potential users, loss of good will,
26 damage to its reputation, and [REDACTED]. Facebook
27 Decl. ¶¶ 6, 10-11, 18-20. Intangible injuries, such as evidence of threatened loss of customers or
28 loss of good will, support a finding of the possibility of irreparable harm. *Stuhlberg Int'l Sales*

1 Co., v. *John D. Brush & Co.*, 240 F.3d 832, 841 (9th Cir. 2001) (citing *Tom Doherty Assocs., v.*
2 *Saban Entm't, Inc.*, 60 F.3d 27, 37-38 (2d Cir. 1995)); *Rent-a-Center, Inc. v. Canyon Television*
3 *& Appliance Rental, Inc.*, 944 F.2d 597 (9th Cir. 1991); *MySpace*, 498 F. Supp. 2d at 1305-06.

4 Defendants' illegal and unauthorized acts, if allowed to continue unrestrained, have the
5 potential to undermine the core of Facebook's appeal to its users – the ability to interact with
6 friends in a private and secure online community. Facebook Decl. ¶¶ 5-6, 10-11, 14-16, 18-20.

7 [REDACTED]
8 [REDACTED]
9 [REDACTED]

Unless Defendants are restrained, Facebook will be
10 irreparably harmed as a result of the continuing intangible injury inflicted on its ability to attract
11 users, its good will, its users' security, and its reputation.

12 **C. Even if There Are Serious Questions on the Merits, the Balance of Hardships Tips**
13 **Sharply in Facebook's Favor**

14 As shown in Section IV.B., Facebook has established entitlement to a temporary
15 restraining order by showing its probability of success on the merits and the possibility of
16 irreparable injury. Thus, the Court does not need to address the second test, which looks to the
17 existence of "serious questions going to the merits," where the "balance of hardships tips sharply
18 in [the plaintiff's] favor." *GoTo.com, Inc.*, 202 F.3d at 1204-05 (internal quotation marks and
19 citation omitted). Nevertheless, Facebook is also entitled to a temporary restraining order under
20 this test because a balance of the hardships tips sharply in Facebook's favor.

21 Where a social networking site has already spent substantial time and money combating
22 unsolicited electronic mail messages and dealing with user complaints and has had difficulty in
23 curbing ongoing unauthorized and illegal activities, the balance of the hardships tips sharply in
24 that website's favor. *MySpace*, 498 F. Supp. 2d at 1306.

25 If Defendants are allowed to continue, the impact on Facebook and its users will be
26 significant. Every day that Defendants are allowed to continue their abuse of Facebook's
27 networks results in additional [REDACTED]
[REDACTED], send spam to Facebook users, and misuse and abuse Facebook. Facebook Decl.

1 ¶¶ 10, 12, 18-20. Facebook must expend time and resources investigating and countering
2 Defendants' activities in a constant and ever-escalating series of moves and countermoves. *Id.*

3 ¶¶ 10, 20. [REDACTED]

4 [REDACTED] *Id.* ¶¶ 10-11, 14-16, 20. In addition to the
5 monetary damage incurred in combating Defendants and repairing its network, Facebook also
6 suffers the intangible and irreparable injuries described in Section IV.B.2., above.

7 Pending a show cause hearing, Facebook seeks to enjoin Defendants from, among other
8 things, sending unsolicited commercial emails through Facebook computers and the Facebook
9 networks; soliciting and phishing Facebook usernames and passwords from Facebook users; and
10 accessing, with or without authorization, Facebook's website. Almost all of the activities that
11 Facebook seeks to enjoin are illegal, including spamming, phishing, accessing websites without
12 authorization or in excess of authorization, and profiting from illegal actions. Defendants would
13 suffer no hardship from being prohibited from engaging in these illegal activities. *MySpace*, 498
14 F. Supp. 2d at 1306 (finding that the sender of spam experiences no hardship where enjoined
15 from committing further CAN-SPAM violations). Any limitation on Defendants' ability to [REDACTED]
16 [REDACTED], to violate the Facebook SRR, or to profit
17 from their illegal activities is clearly outweighed by Facebook's concerns.

18 **D. The Public Interest Favors Facebook's Relief**

19 With 350 million members of the public as active Facebook users, there is a strong public
20 interest in protecting the privacy and security of Facebook's online community.

21 In evaluating whether the public interest supports a temporary restraining order based on a
22 statutory violation, courts may look to the underlying substantive policy of the governing statute.
23 *Amoco Prod. Co. v. Vill. of Gambell, Alaska*, 480 U.S. 531, 544 (1987). In this case, all four
24 statutes addressed above — CAN-SPAM, the CFAA, California's Comprehensive Computer
25 Data Access and Fraud Act, and California's Anti-Phishing Act — are based upon protecting the
26 public from unscrupulous and harmful activities. *See, e.g.*, 15 U.S.C. § 7701(a) (detailing the
27 public interest in preventing spam); Cal. Penal Code § 502(a) (discussing protection of computers
28 and computer systems as "vital to the protection of the privacy of individuals" and other public

1 and private entities); *MySpace*, 498 F. Supp. 2d at 1306 (noting the public interest in the
2 enforcement of CAN-SPAM). In addition, Facebook's breach of contract claim seeks to prohibit
3 Defendants from engaging in activities that not only breach the SRR but are also illegal under
4 these four statutes. The public interest strongly favors Facebook's requested relief.

5 **E. Minimal Bond Is Appropriate**

6 The Court has the discretion to require no bond or a minimal bond. Fed. R. Civ. P. 65(c).
7 Defendants will suffer no legal cognizable harm from issuance of the requested restraining order,
8 and no bond should be required. Facebook is requesting only that Defendants stop their illegal
9 and unauthorized activities. As such, this is a case where no bond is appropriate. If the Court
10 requires a bond, Facebook submits that, at most, a minimal bond of no more than \$5,000 will be
11 more than adequate and that it be given five days from the date the Temporary Restraining Order
12 is issued to post the bond.

13 **V. CONCLUSION**

14 Defendants' illegal practices, as recounted above, have caused substantial injury to
15 Facebook and to the public. By this application, Facebook seeks to enjoin those practices and to
16 prevent further harm to its reputation, its good will, its relationships with its users, and the
17 security of user login information. This temporary relief is expressly authorized by the federal
18 and state statutes upon which this action is brought. For all of these reasons, Facebook
19 respectfully requests that the Court issue the proposed Temporary Restraining Order.

20 DATED: December 15, 2009

PERKINS COIE LLP

21 By: /s/

22 Brian Hennessey

23 *Attorneys for Plaintiff Facebook, Inc.*