UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

Plaintiff

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, RONALD L. RIVEST, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, SUSAN HOCKFIELD, PHILLIP L. CLAY, and the MIT CORPORATION

Defendants

Civil Action No. _____

MEMORANDUM IN SUPPORT OF PLAINTIFF'S MOTION FOR TEMPORARY RESTRAINING ORDER

Introduction

The plaintiff, Massachusetts Bay Transportation Authority ("MBTA"), seeks a temporary restraining order enjoining the defendants Zack Anderson, RJ Ryan, and Alessandro Chiesa (collectively the "MIT Undergrads") (a) from exploiting security flaws they claim to have discovered in the MBTA's Fare Media System; and (b) from publicizing these flaws in the presentation they are scheduled to give two days from today, on Sunday August 10 at the DEFCON hackers convention in Las Vegas.

Facts

The MBTA's automated fare collection system (the "AFC System" or the "Automated Fare Collection System") relies on so-called CharlieCard passes and CharlieTicket passes for the payment of MBTA fares (among other purposes). Declaration of Joseph Kelley ("Kelley Decl.") ¶¶13-16. The fare media system (the "Fare Media System") contains security features, designed

to prevent unauthorized personnel from manipulating the system, and obtaining free MBTA transit services or causing other harm. Declaration of G. Foster ("Foster Decl.") ¶¶4-5.

The MIT Undergrads (i) claim to have circumvented the security features of the MBTA's computerized CharlieTicket and CharlieCard fare media systems; (ii) publicly offered "free subway rides for life" to interested parties over the Internet; and (iii) plan to allow others to duplicate their claimed "breaking" of the Fare Media's security systems by presenting a paper, releasing software tools, and giving demonstrations at the DEFCON hackers convention this Sunday, August 10, in Las Vegas. Foster Decl. ¶¶10-23.

Despite the MBTA's requests, the MIT Undergrads have declined to provide the MBTA or its system vendors with information concerning the claimed security flaws in the system. Kelley Decl. ¶¶23-26.

If what the MIT Undergrads claim in their public announcements is true, public disclosure of the security flaws – before the MBTA and its system vendors have an opportunity to correct the flaw – will cause significant damage to the MBTA's transit system. Kelley Decl. ¶27; Foster Decl. ¶25.

Argument

I. The MBTA Is Entitled To Immediate Relief

The MBTA is entitled to a temporary restraining order because it has shown: (1) a likelihood that it will prevail on the merits; (2) irreparable harm unless the restraining order is issued; (3) greater harm to it than the adversary's harm resulting from issuance of a temporary restraining order; and (4) the absence of an adverse impact on the public interest. *Esso Standard Oil Co. (Puerto Rico) v. Monroig-Zayas,* 445 F.3d 13, 18 (1st Cir.2006); *McGuire v. Reilly*, 260 F.3d 36. 42 (1st Cir. 2001). Injunctive relief should issue to "prevent a real threat of harm." *Matos ex rel. Matos v. Clinton School District*, 367 F.3d 68, 73 (1st Cir. 2004). As demonstrated

below, if the MIT Undergrads truly have broken the security of the MBTA's Fare Media system, the MBTA will suffer immediate, real harm.

II. The MBTA Has A High Likelihood Of Success On Its Claims Under The Computer Fraud And Abuse Act.

The MBTA is likely to success on the merits of its claims under 18 U.S.C. §1030, the Computer Fraud and Abuse Act (the "CFAA"). First, the systems for storing value and processing payments via CharlieTickets and CharlieCards, including the Fare Gate and the Fare Vending Machine, constitute "computers" within the meaning of 18 U.S.C. §1030(e)(1). These "computers," moreover, are used in interstate commerce or communication due, for example, to the MBTA's services in Rhode Island and Massachusetts. *See* Kelley Decl. ¶7. Accordingly, these are protected computers within the meaning of 18 U.S.C. §1030(e)(2)(B).

Second, based on the Initial and Revised Announcements, it appears the MIT Undergrads knowingly caused the transmission of a program, information, code, or command targeted at MBTA protected computers and, as a result of such conduct, the MIT Undergrads intentionally caused damage without authorization, to these protected computers. Moreover, the MIT Undergrads intentionally accessed MBTA protected computers without authorization, and as a result of such conduct, have caused damage. These damages include a loss aggregating substantially more than the $5,000 amount required under 18 U.S.C. §1030(a)(5)(B)(i), particularly in light of the volume of traffic covered by the CharlieCard and CharlieTicket passes, and the costs of the overall Automated Fare Collection System that relies on the CharlieCard and CharlieTicket passes. *See* Kelley Decl. ¶¶12, 19.

Finally, the damage constitutes a threat to public health or safety, within the meaning of 18 U.S.C. §1030(a)(5)(B)(iv), and also affects a computer system used by a government entity for national security purposes, within the meaning of 18 U.S.C. §1030(a)(5)(B)(v), due to the

role of the MBTA in Homeland Security efforts, and transit services generally. *See* Kelley Decl. ¶¶6, 8-9.

III. Irreparable Harm

"Irreparable injury' in the preliminary injunction context means an injury that cannot adequately be compensated for either by a later-issued permanent injunction, after a full adjudication on the merits, or by a later-issued damages remedy." *Rio Grande Cmty. Health Ctr., Inc. v. Rullan*, 397 F.3d 56, 76 (1st Cir. 2005). The loss of a trade secret is generally found to constitute irreparable harm. *TouchPoint Solutions, Inc. v. Eastman Kodak Co.*, 345 F.Supp.2d 23, 32 (D.Mass. 2004). That is in recognition of the fact that, "once the trade secret is lost, it is gone forever." *Id. (citing FMC Corp. v. Taiwan Tainan Giant Indus. Co.*, 730 F.2d 61, 63 (2d Cir.1984)).

Here, if what the MIT Undergrads claim in their public announcements is true, public disclosure of the security flaws in the Fare Media System – before the MBTA and its system vendors have an opportunity to correct the flaws – will cause significant damage to the MBTA's transit system. Kelley Decl. ¶27; Foster Decl. ¶25. The requested relief, therefore, is necessary to preserve the status quo until a full hearing. *See CMM Cable Rep., Inc. v. Ocean Coast Properties, Inc.*, 48 F.3d 618, 620 (1st Cir.1995)

IV. Reliance On Industry-Recognized "Responsible Disclosure" Practices, There Will Be No Cognizable Harm To The MIT Undergrads.

The temporary halt on the MIT Undergrad's disclosures will not create cognizable harm to the defendants. This is particularly true in light of industry practices, and the so-called "responsible disclosure" doctrine.

The term "responsible disclosure" refers to the method of disclosing a technological vulnerability to the developer so that the developer can fix the vulnerability before the general

public finds out about it. Making a disclosure of the vulnerability to the developer is necessary to obtain a fix. If the discoverer discloses the vulnerability to a broader audience, hackers and other malicious users may be able to exploit the vulnerability before the developer implements a fix. The term "responsible disclosure" is generally used to refer to the process by which (i) the discoverer discloses the vulnerability, (ii) the vulnerability is corrected, and (iii) hackers are prevented from exploiting the vulnerability in the interim.

Microsoft defines the term "responsible disclosure" as follows:

> In a responsible disclosure scenario, the researcher who discovers the vulnerability reports the findings directly to the appropriate vendor, providing a reasonable amount of time for the vendor to investigate, create, and test the necessary update. Only when the update is made available are actual details of the vulnerability made public, with due credit given to the original reporter. (emphasis added).[1]

Google states that "responsible disclosure" is an "industry best practice." Specifically, Google defines the term, and elaborates on the term in its "Security and Product Safety" as follows:

> This process of notifying a vendor before publicly releasing information is an industry-standard best practice known as responsible disclosure. Responsible disclosure is important to the ecology of the Internet. It allows companies like Google to keep users safe by fixing vulnerabilities and resolving security concerns before they are brought to the attention of the bad guys. We strongly encourage anyone who is interested in researching and reporting security issues to observe the simple courtesies and protocols of responsible disclosure. (emphasis added).[2]

---

[1] See Malware Revolution: A Change in Target (published: March 14, 2007), Microsoft Website, located at http://www.microsoft.com/technet/community/columns/secmgmt/sm0307.mspx .

[2] Google Security and Product Safety, located at http://www.google.com/corporate/security.html; see, Symantec Responsible Disclosure Policy (January 2006) (listing 5 steps Symantec commits to follow as part of its "responsible disclosure" procedures), located at http://www.symantec.com/research/Symantec-Responsible-Disclosure.pdf.

A number of industry groups have proposed various "uniform" policies relating to these disclosure issues.[3]

V. The Requested Relief Furthers The Public Interest.

The final factor is the public interest. This factor requires the Court to "inquire whether there are public interests beyond the private interests of the litigants that would be affected by the issuance or denial of injunctive relief." *Friends of Magurrewock, Inc. v. U.S. Army Corps of Engineers*, 498 F.Supp.2d 365, 379 (D.Me.,2007) (quoting *Everett J. Prescott, Inc. v. Ross*, 383 F.Supp.2d 180, 193 (D.Me.2005))

The MBTA provides approximately 1.4 million passenger trips per weekday.[4] The Fare Media System threatened by the MIT Undergrads' conduct governs the majority of this system. It is strongly in the public interest to protect this system in the manner requested, particularly in light of the steps the MBTA has taken to avoid the necessity of requesting relief from this Court.

[3] See, e.g., Rain Forest Puppy - Full Disclosure Policy (RFPolicy) v2.0. located at http://www.wiretrip.net/rfp/policy.html; Organization for Internet Safety Guidelines for Security Vulnerability Reporting and Response, V2.0 (2004) located at http://www.oisafety.org/index.html.

[4] Kelley Decl. ¶6.

Conclusion

THEREFORE, the plaintiff respectfully requests that this Court enter the attached proposed Order.

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

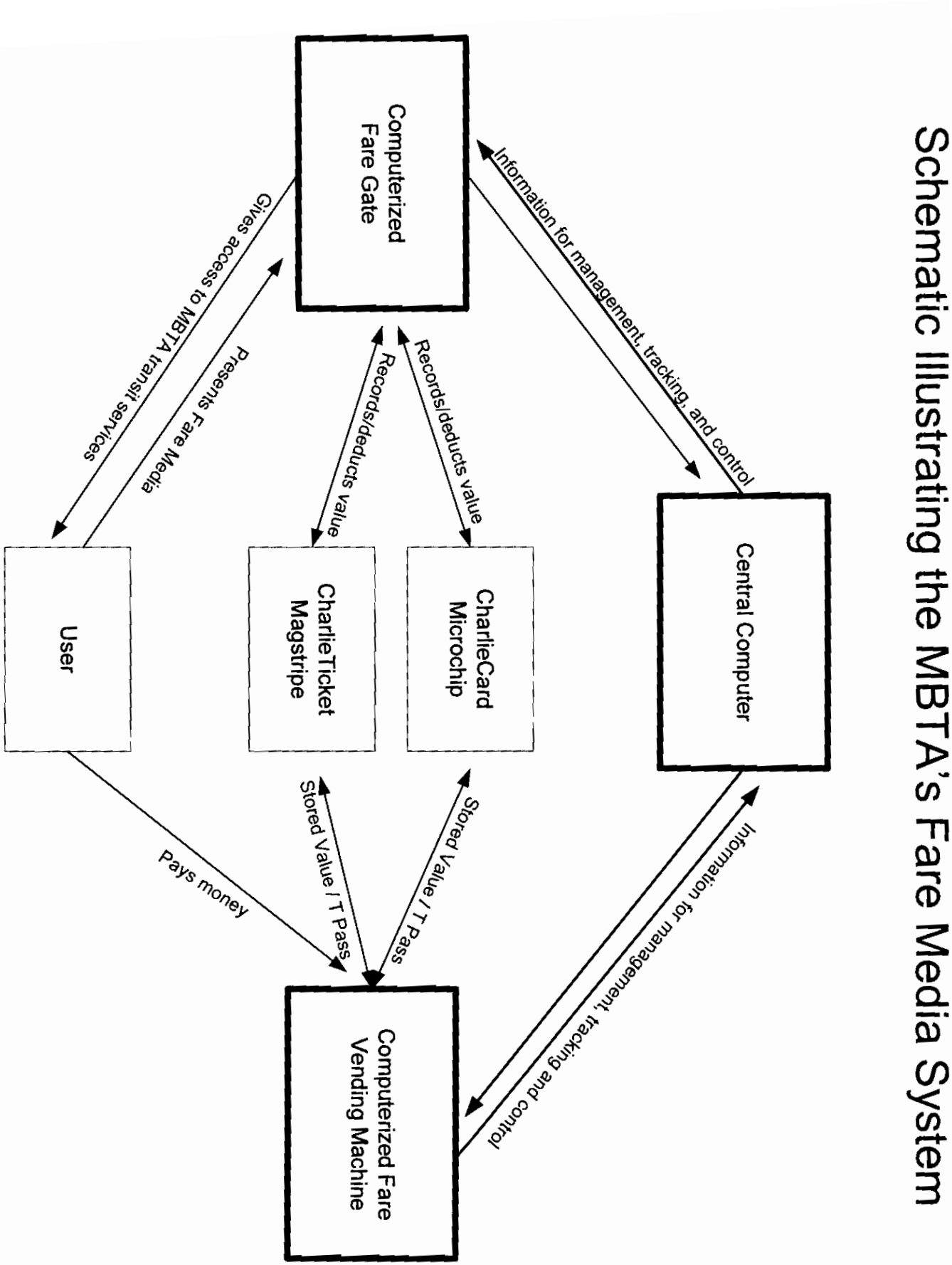
By its attorneys,

Ieuan G. Mahony (BBO #552349)
Maximillian J. Bodoin (BBO # 667240)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

Thomas F.S. Darling III (BBO #558848)
MASSACHUSETTS BAY TRANSPORTATION AUTHORITY
State Transportation Building
7th Floor
10 Park Plaza
Boston, MA 02116
(617) 222-3174

Dated: August __, 2008
Boston, Massachusetts

5530567_v1


Schematic Illustrating the MBTA's Fare Media System
Computerized Fare Gate
Central Computer
User
CharlieTicket Magstripe
CharlieCard Microchip
Computerized Fare Vending Machine
Information for management, tracking, and control
Gives access to MBTA transit services
Presents Fare Media
Records/deducts value
Records/deducts value
Pays money
Stored Value / T Pass
Stored Value / T Pass
Information for management, tracking and control