

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY
TRANSPORTATION AUTHORITY

Plaintiff

v.

Civil Action No. No. 08- 11364-GAO

ZACK ANDERSON, RJ RYAN,
ALESSANDRO CHIESA, and the
MASSACHUSETTS INSTITUTE OF
TECHNOLOGY

Defendants

SUPPLEMENTAL DECLARATION OF SCOTT HENDERSON

1. I am the Systems Project Manager for the Automated Fare Collection System for Plaintiff, Massachusetts Bay Transportation Authority ("MBTA").
2. I make this Supplemental Declaration based on my personal knowledge and a review of MBTA business records concerning the matters set out below. I use the term "MIT Students" to refer to Defendants Zack Anderson, RJ Ryan, and Alessandro Chiesa.

**Additional Information Concerning Requests To The MIT Students For
Their DEFCON Presentation Materials**

3. I understand that the MIT Students claim that they were unaware of the MBTA's requests for materials that the MIT Students planned to present at the DEFCON Conference, and that the MBTA's non-receipt of these materials was due to a "misunderstanding." This is incorrect, and I provide additional information concerning my exchanges with Mr. Anderson, below, on these points.



4. I communicated with Defendant Zack Anderson, requesting that he send to the MBTA the materials the MIT Students plan to present at the DEFCON Conference during a phone conversation that I had with him on the afternoon of August 8, 2008.

5. I contacted Mr. Anderson at the request of Joseph Kelley and Jack McLaughlin. Mr. Kelley and Mr. McLaughlin wanted me to talk with Mr. Anderson to find out about the subject matter of the presentation at the DEFCON Conference and to get a copy of the materials that the MIT Students were planning to present at the DEFCON Conference.

6. I called Mr. Anderson on the afternoon of August 8, 2008 after I reviewed the Report. I told Mr. Anderson that there was some interesting material in the Report, but that he had made many assumptions and that it was incomplete. I told him that it was too bad that he did not come to the MBTA to discuss his findings. I then asked Mr. Anderson for a copy of the slide show presentation for the DEFCON Conference. He responded that it wouldn't be a problem to send me a copy and that he would do so shortly.

7. In my initial Declaration, I identified two voicemails that I received from Mr. Anderson on Friday, August 8. These voicemails have been transcribed, and the following is a fair and accurate transcription of these communications from Mr. Anderson. I have retained the sound files for these calls, and will make them available upon request.

8. The voicemail message dated August 8, 2008 at 6:25 PM runs as follows:

Hi Mr. Henderson, This is Zach Anderson. I just wanted to let you know that we're trying to get to an internet connection right now to send you these slides. You should have them probably in the next hour. Feel free to call me though if you want to talk. Again, my number is 310-270-3995. Okay, bye.

9. The voicemail message dated August 8, 2008 at 6:49 PM runs as follows:

Hi Mr. Henderson, this is Zach Anderson. I got to a network connection. But I just spoke to my lawyer and my lawyers are telling me that I should not send the slides at this point. They first wanted to



basically hear the need for the claims that MBTA has filed against us until we send those over. So I guess at this point I'm going to have to hold off. I'm really sorry. I know I said I'd get those over to you. I'm definitely open for a conversation if you want to know just what I'm talking about, I'm open to that, and we're going to keep the communication open over the next couple of days. I guess just my lawyers want to take a look at, uh, you know, what exactly is happening, because they're still kind of in the dark. Feel free to call me if you have any questions. Again, my number is 310-2703995. Okay, bye.

Review Of The MIT Students' Security Analysis Document

10. I am the MBTA leader of a team of MBTA AFC personnel and outside vendors (the "Review Team"), set up to review the document the MIT Students provided on Wednesday evening, August 13, 2008, entitled "A Security Analysis of the Boston T" (the "Security Analysis"). I understand that the Security Analysis was filed under seal, as Docket No. 32. I have signed a non-disclosure and non-use agreement concerning this Security Analysis, as have all other members of the Review Team, to my knowledge.

11. Before receipt of the Security Analysis, as I stated in part in my Declaration (paragraphs 24-25), it was unclear whether the MIT Students were able to, or had, in fact compromised some portion or all of the Fare Media System, and it was not possible to reach these conclusions based on the quality and quantity of materials the MIT Students had provided.

12. Based on the evaluation of the Security Analysis document, conducted by the Review Team, to a reasonable degree of certainty the that MIT Students are able to compromise the security of the CharlieTicket system, and to clone and counterfeit CharlieTickets. Based on the Security Analysis, it appears that the MIT Students have not to date compromised the CharlieCard system.

A handwritten signature in black ink, appearing to be 'Rafel', located in the bottom right corner of the page.

13. In sum, the MIT Students' activities are not a "prank," and represent a real risk to the CharlieTicket system.

**Audit Trail For Illegal Activity
Using CharlieTickets Disclosed In The MIT Students' Presentation**

14. I have reviewed the MIT Students' Presentation entitled "Anatomy of a Subway Hack," which is Compilation Ex. 17, and also Exhibit 7 to the Supplemental Declaration of Ieuan G. Mahony, Docket No. 9 (the "Presentation").

15. The Presentation contains images of CharlieTickets, for example, at Bates Nos. 140. Using the AFC System's Fraud Detection features and related data, I have linked the image of the CharlieTicket used in the Presentation to serial numbers for multiple CharlieTickets (the "Linked Tickets"). I then constructed an audit trail that shows payments, use, other activities surrounding these Linked Tickets.

16. These Linked Tickets were used illegally, and the users of these Linked Tickets obtained MBTA transit services without proper payment.

17. The MBTA's Privacy Policy expressly permits the MBTA to use data to undertake these fraud detection activities, to prevent fraud, and to use the resulting data in legal proceedings. *See* MBTA's Website And Electronic Fare Media Privacy Policy (December 15th, 2006) http://www.mbta.com/customer_support/privacy_policy/#12, at Section 9.3 (Fraud Detection) ("To allow us to detect fraud and system errors, we may compare Ridership Information to Electronic Fare Media information. If, for example, the system shows that anonymous Smart Card no. 1234 was used to enter the Braintree stop, and anonymous Smart Card no. 1234 was also used simultaneously to enter the Wonderland stop, we can assume either (i) that there is a system malfunction, or (ii) that fraudulent activity has taken place"); at Section 12 (Exceptions) ("There are two exceptions to our Privacy Policy. (1) We may release

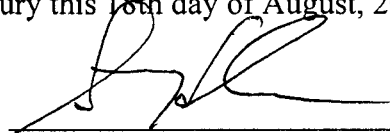


or use Personally Identifiable Information in connection with (a) legal proceedings (such as false reimbursement claims made by MBTA patrons), or contemplated legal proceedings, that directly relate to such information").

AFC System Updating

18. It will take approximately five months to implement security measures that will adequately protect against the activities that the MIT Students have detailed.

Signed under the penalties of perjury this 18th day of August, 2008.



Scott Henderson

5548409_v2

CERTIFICATE OF SERVICE

I, Ieuan G. Mahony, Attorney for the Massachusetts Bay Transportation Authority in connection with the above-captioned proceeding, hereby certify that on this 18th day of August, 2008, the **Supplemental Declaration of Scott Henderson** was served via the ECF system on the following interested parties:

Party

Counsel

Zack Anderson, RJ Ryan,
and Alessandro Chiesa
(the "MIT Undergrads")

Emily Berger, Esquire
Email: emily@eff.org

Jennifer Granick, Esquire
Email: jennifer@eff.org

John Reinstein, Esquire
Email: reinstein@aclum.org

Thomas A. Brown
Email: tbrown@fr.com

Cindy Cohn
cindy@eff.org

Lawrence K. Kolodney
kolodney@fr.com

Marcia Hoffman
marcia@eff.org

Adam J. Kessel
kessel@fr.com

Massachusetts Institute
of Technology ("MIT")

Jeffrey Swope, Esquire
Email: JSwope@eapdlaw.com

/s/ Ieuan G. Mahony_____