IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
GREENBELT DIVISION

ASTORNET TECHNOLOGIES, INC.	)	
	)	
Plaintiff,	)	
	)	Civil Action No. 14-cv-547
v.	)	**JURY TRIAL DEMANDED**
	)	
NCR GOVERNMENT SYSTEMS, LLC	)	
	)	
Defendant.	)	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Astornet Technologies Inc. ("Astornet") files this Complaint against Defendant NCR Government Systems, LLC ("NCR"), based upon actual knowledge as to itself and its own actions, and on information and belief as to all other persons and events, as follows:

Parties

1. Astornet is a Maryland Corporation with its principal place of business in Gaithersburg, MD. Astornet is the sole exclusive licensee of, and owns all right, title, and interest to litigate in this matter U.S. Pat. No. 7,649,844 (the '844 patent), referred to below as the '844 Patent.

2. NCR is a Delaware LLC with its principal place of business at 20370 Seneca Meadows Parkway, Germantown, Maryland, 20875. NCR provides government agencies with information technology products and services. NCR may be served with process by service on its registered agent for service, the Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, Delaware, 19801.

NCR's counsel, Kilpatrick Townsend, has been in communication with counsel for Astornet, and has agreed to accept service via email.

Jurisdiction and Venue

3. This claim arises under the United States patent laws, 35 U.S.C. § 1, *et seq*. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

4. NCR has transacted business in Maryland, and has caused tortious injury in Maryland by an act or omission outside Maryland and derived substantial revenue from goods used or consumed in Maryland by establishing its primary offices in Germantown, Maryland.

5. Venue is proper in this District and Division, under 28 U.S.C. §§ 1391 and 1400. NCR resides within this District.

Factual Background

6. Astornet is committed to providing the highest quality of customized products and services that meet the needs of government organizations and corporations. (Ex. 1 at 1). Astornet provides a full range of technology systems and services including software solutions, consulting and system integration. (*Id*. at 2). Astornet's customers include the Federal Aviation Administration, BWI Marshall Airport, the Maryland Department of Education, and the United States Department of Transportation. (*Id*.).

7. BWI in particular retained Astornet in late 2007 to meet new Transportation Security Administration ("TSA") requirements to improve security at the gates, (*id.* at 3), and in particular, develop a system to increase security while maintaining an efficient entry/exit process, (*id.*). For this project, the Astornet team created a touch

screen solution that was able to verify credentials authenticity, perform an instant security check for all persons entering the airport, and deliver a vehicle certificate. (*Id.*). Astornet also provided the airport police with a wireless device capable of authenticating certificates at any point within the airport. (*Id.*). As a result of this work, BWI vehicular gate security was dramatically increased and the system was able to efficiently handle and properly manage entry volume. (*Id.*).

8. On August 27, 2007, Astornet filed a patent application entitled "Airport Vehicular Gate Entry Access System" naming as its sole inventor "Michael A. Haddad." (Ex. 2 at 1).

9. On December 29, 2009, the United States Patent and Trademark Office (the "PTO") granted the '844 patent based on this application (*Id.* at 2), which claims as its invention: "An automated access control system for securing airport vehicular gates and airport sterile areas comprising:" a number of elements, including that "upon a credential reading, the . . . access control system automatically determines the source of the credential data record, and automatically extracts personal information to be checked against a security list, TSA NO-FLY list, SELECTEE list, other alternative credentials" and that the system further "upon the credential authentication, . . . automatically extracts authentication information from the authentication data record, and subsequently displays a warning window, as a result of the individual credentials match and ID forgery risks rating contained in the authentication data record." (*Id.* at col. 4, ll. 67 to col. 5, ll. 37).

10. The PTO Examiner noted that he was granting the '844 patent because none of the prior art considered by the Examiner "discloses" or provided any "reason or motivation" that would render "obvious[]" the invention claimed in the '844 patent. (Ex.

3 at 5). Patents can only be granted by the PTO for new, useful and non-obviousness inventions considered in light of the most relevant "prior art", or technical work that came before the work that is the subject of a patent application. *See, e.g.,* 35 USC § 102; 35 U.S.C. § 103. As the '844 patent itself notes, "[a]irport vehicular entry gates rely on human intervention and manual data entry and are prone to excessive error rates, lower security standards, increased inefficiencies and decreased reliability." (Ex. 2 at 1). Mr. Haddad improved upon BWI's systems markedly by "automatically" performing the steps claimed in the '844 patent, (*id.* at col. 4, ll. 67 to col. 5, ll. 37), something which had never been done before and was not at all "obvious[]" to one of ordinary skill in the art, (Ex. 3 at 5).

11. One of the main difficulties of such a system, for example, was accurately comparing names of passengers that could be translated into English with many different spellings. As a well known example, the one time leader of Libya, Colonel Gaddafi, had his name spelled in newspapers in this form, but also one can find many examples of the same individual having his name spelled as Kadafi and Qaddafi as well. This is not unusual; there is no universally accepted authority for transliterating Arabic names. However, to a human being, all of the spellings of Gaddafi can be seen to be phonetically related. To a computer, by contrast, phoenetic relationships are very difficult to detect. Accordingly, one of the key improvements Astornet made to the state of the art in this area was to develop an arabic language phonetic comparison algorithm that in a number of cases was the difference between catching a match with the TSA no-fly list or not. Astornet's BWI system thus removed human security personnel from the equation but did

so without sacrificing accuracy on phonetic comparisons that can prove crucial to flagging a particular individual on the No Fly list.

12. In June 2009, seeking to build on its success with Astornet's BWI system, Astornet sought to provide its systems in response to TSA requests for bids from government contractors for improved security systems, in particular a system the TSA named the Credential Authentication Technology-Boarding Pass Scanning System (CAT/BPSS). After presenting the TSA with its CAT/BPSS proposal, Astornet was selected for testing and advanced to the next stage of the process. At that stage, the TSA required all of the CAT/BPSS bidders to provide 5 systems in kiosks at a demonstration facility, free of charge. This was a substantial burden on Astornet, as evidenced by the fact that the TSA ultimately purchased 10 systems with five months of support at the earliest stage of the CAT/BPSS program for $1.97 million, or approximately $200,000 a system. (Ex. 4 at 1). Accordingly, participating in this round required an outlay of nearly $1,000,000 in finished systems and support, with no commitment by the TSA to purchase anything.

13. Astornet accordingly attempted to participate in the demonstration with 5 systems in parts, and observed the competing systems being offered by defendant NCR. Unfortunately Astornet was unsuccessful with its bid for the initial CAT/BPSS contracts, at least in part owing to its failure to provide the requisite systems in a kiosk at this demonstration.

14. The CAT/BPSS contracts were instead ultimately awarded to, *inter alia*, defendant NCR. (Ex. 4). In September 2011, NCR was awarded a CAT/BPSS contract providing for orders totaling up to $79 million under its contract (Ex. 4 at A006), as well

as an initial order of 10 systems from each defendant for approximately $2 million, including five months of support, for a pilot program totalling $6 million. (Ex. 5 at 2).

15. Notwithstanding their success in obtaining the initial contract, the initial pilot program with NCR and others did not go well, and in June 2012, the TSA decided to delay procurement of CAT/BPSS. (Ex. 6 at 1). The TSA conducted additional research on the matter in 2013, (Ex. 7 at 1), and re-solicited proposals for a slightly revised CAT/BPSS system, which proposals were due on January 21, 2014. Astornet submitted a proposal for the revised CAT/BPSS sytem, as did NCR.

16. NCR's original and revised CAT/BPSS systems, when used as instructed by NCR, infringe Astornet's '844 patent.

17. NCR's manufacture, sale, and delivery of full and prototype original CAT/BPSS systems to the TSA alone, however, did not result in infringement of Astornet's '844 patent. The sole independent claim of the '844 patent, requires, *inter alia*, "one or more of the following processing" steps to be performed, which processing steps are not performed when NCR's CAT/BPSS system is simply being manufactured, sold, or delivered to the TSA. Instead, these steps are performed when the CAT/BPSS system is being used for its intended purpose to maintain security in sterile areas by, *inter alia*, checking boarding passes against passenger photo identifications and detecting fraudulent identifications. Accordingly, NCR infringed the '844 patent at least by inducing the TSA to use the NCR CAT/BPSS system for these purposes by providing the TSA both with CAT/BPSS prototypes and 10 full CAT/BPSS systems, and instructing the TSA regarding the use of these systems in a manner which infringes the '844 patent as explained in detail below.

NCR Induced the TSA to Infringe Astornet's '844 Patent

18. Claim 1 of the '844 patent first requires "An automated access control system for securing airport vehicular gates and airport sterile areas comprising; a standardized credential reader means for reading a credential encoded with personal identification . . . ." NCR's original and revised CAT/BPSS systems meet this limitation by having readers that can read a boarding pass, which is encoded with personal identification including the passenger's name.

19. Claim 1 next requires this system "be used at entry point into the airport sterile areas." NCR's original and revised CAT/BPSS systems meet this limitation because these systems were to be used on passengers, visitors and transportation workers before entering a sterile/secure area.

20. Claim 1 next requires this system to "automatically collect[] data to build individual real time records." NCR's original and revised CAT/BPSS systems meet this limitation because these systems were designed to scan boarding passes and build the data in real time. TSA specified that in fact no private data should be stored in the system to comply with the Private Individual Information Act.

21. Claim 1 next requires the system to have "a software application for recovering information from the standardized credential reader." NCR's original and revised CAT/BPSS systems meet this limitation because these systems had such software applications; without such applications, NCR could not automate its system as required by CAT/BPSS.

22. Claim 1 next requires a system "wherein one or more of the following processing is performed: real time records are checked searching for a credential

collected information match . . . ." NCR induced the TSA to infringe this limitation at least by instructing the TSA how to use NCR's original and revised CAT/BPSS systems to check a passenger's boarding pass credential information against other credentials provided by the passenger such as a driver's license or a passport.

23. Claim 1 next requires a system wherein "admission is processed as entry or re-entry of the individuals." NCR's original and revised CAT/BPSS systems meet these limitations during operation because these systems do not store any personal information, so all admissions were processed "as entry . . . .of the individuals" as required.

24. Claim 1 next requires "an ID authenticator, wherein a credential to be authenticated is presented." NCR induced the TSA to infringe this limitation by instructing the TSA how to use NCR's original and revised CAT/BPSS systems to check a passenger's boarding pass credential information against other credentials provided by the passenger such as a driver's license or a passport.

25. Claim 1 further requires that the system "analyze" a "credential physical aspect and embedded security features to determine the possibility of any tampering or forgery and provide an authenticity risk rating." NCR induced the TSA to infringe this limitation by instructing the TSA how to use NCR's original and revised CAT/BPSS systems to detect forged identification, using the same commercial ID authenticator found in all of the prototypes submitted to TSA, which authenticator includes an authenticator database that has a record of all state drivers license ID templates, including holographic features, small transparent pictures of the individuals that can only be seen in the infrared, and similar federal passport security features, all of which the authenticator

analyzes to determine the validity of the identification and provide an authenticity risk rating.

26. Claim 1 further requires "said ID authenticator comprises means to read non-encoded credentials. . . ." NCR's original and revised CAT/BPSS systems meet this limitation because the commercial ID authenticator used by NCR is able to accept manual input of credential information on IDs that for whatever reason is non-machine readable, which was also a requirement of the CAT/BPSS specification.

27. Claim 1 further requires "said ID authenticator generates an authentication data record comprising presented credential information and authentication rating . . . " NCR induced the TSA to infringe this limitation by instructing the TSA how to use NCR's original and revised CAT/BPSS system to detect forged identification because the commercial ID authenticator found in all of the prototypes submitted to TSA generates an authentication data record which includes the presented credential information as well as an authentication rating.

28. Claim 1 further requires the system to have "a central processing unit for receiving information from the standardized credential reader and the ID authenticator." NCR's original and revised CAT/BPSS system meets this limitation because without such a central processing unit, these systems would not be automated as required by the CAT/BPSS specification.

29. Claim 1 further requires that "upon a credential reading, the automated access control system automatically determines the source of the credential data record, and automatically extracts personal information to be checked against a security list, TSA No-Fly list, selectee list, other alternative credentials. . . ." NCR induced the TSA to

infringe this limitation by instructing the TSA how to use NCR's original and revised CAT/BPSS system to automatically recognize a boarding pass and automatically extract the personal information from the boarding pass, and check it against "other alternative credentials," i.e. a driver's license or passport.

30. Claim 1 further requires that "upon the credential authentication, the automated access control system automatically extracts authentication information from the authentication data record and subsequently displays a warning window, as a result of the individual credentials match . . ." NCR induced the TSA to literally or equivalently infringe this limitation by instructing the TSA how to use NCR's original and revised CAT/BPSS system to detect forged identification or a credential match failure, because any such detected forgery or failed match would have needed to provide a clear alert to the operator both as a practical matter and as requirement of the CAT/BPSS specification.

31. Claim 1 finally requires there to be an "ID forgery risk rating contained in the authentication data record." NCR's original and revised CAT/BPSS system meets this limitation in operation because NCR's prototype uses the same commercial authenticator as Astornet's prototype, which produces a forgery risk rating in the authentication data record.

32. Accordingly, NCR induced infringement of Claim 1 of the '844 patent by the TSA and/or has committed acts of contributory infringement of the '844 patent.

Count 1 – NCR's Infringement of the '844 Patent

33. Astornet incorporates by reference the material factual allegations above.

34. NCR induced infringement of Claim 1 of the '844 patent by the TSA and/or has committed acts of contributory infringement of the '844 patent.

35. NCR's activities have been without express or implied license from Astornet.

36. NCR will continue to infringe the '844 Patent unless enjoined by this Court. As a result of the NCR's infringing conduct, Astornet has suffered, and will continue to suffer, irreparable harm for which there is no adequate remedy at law. Astornet is entitled to permanent injunctive relief against such infringement, under 35 U.S.C. § 283.

37. As a result of the infringement of the '844 Patent, Astornet has been damaged and is entitled to be compensated for such damages, pursuant to 35 U.S.C. § 284, in an amount to be determined at trial.

Jury Trial Demand

38. Astornet demands a trial by jury on all appropriate issues.

Prayer for Relief

Therefore, upon final hearing or trial, plaintiff Astornet prays for the following relief:

(a) A judgment that NCR has infringed the '844 Patent;

(b) A judgment and order permanently restraining and enjoining NCR, its directors, officers, employees, servants, agents, affiliates, subsidiaries, others controlled by them, and all persons in active concert or participation with any of them, from further infringing the '844 Patent;

(c) A judgment and order requiring NCR to pay damages to Astornet adequate to compensate it for NCR's wrongful infringing acts, in accordance with 35 U.S.C. § 284 and 35 U.S.C. § 289;

(d) A judgment and order requiring NCR to pay to Astornet pre-judgment interest under 35 U.S.C. § 284, and post-judgment interest under 28 U.S.C. § 1961, on all damages awarded; and

//

(e) Such other costs and further relief, to which Astornet is entitled.

Dated: February 24, 2014

Respectfully submitted,

_/s/ Geoffrey Mason, Esq.______________

Geoffrey Mason, Esq., Bar No. 15772
Moarbes, LLP
2200 Pennsylvania Avenue, NW
Fourth Floor, East
Washington, D.C. 20037
Direct: (202) 507-5720
geoff.mason@moarbes.com