IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

NADER ASGHARI-KAMRANI and **KAMRAN ASGHARI-KAMRANI**,	)	
Plaintiffs,	)	Civil Action No. 2:15-cv-00478-RGD-LRL
v.	)	Hon. Robert G. Doumar
UNITED SERVICES AUTOMOBILE **ASSOCIATION**,	)	
Defendant.	)	

SECOND AMENDED COMPLAINT

Nader Asghari-Kamrani and Kamran Asghari-Kamrani (collectively, "Plaintiffs" or "Messrs. Asghari-Kamrani"), by their attorneys, for their Second Amended Complaint against United Services Automobile Association ("Defendant" or "USAA"), allege as follows:

NATURE OF THE ACTION

1. This is an action for monetary and injunctive relief to recover from the unlawful and unauthorized use of Messrs. Asghari-Kamrani's intellectual property through the infringement of Messrs. Asghari-Kamrani's patent under 35 U.S.C. § 271 by the Defendant USAA. Specifically, Messrs. Asghari-Kamrani complain that USAA infringes at least claims 1-10, 12, 13, 16-26, 28-35, 38-42, 45, 47, 48, 50-52, 54, and 55 of Messrs. Asghari-Kamrani's United States Patent No. 8,266,432 ("the '432 patent"). A true and correct copy of the '432 Patent is attached as Exhibit A.

THE PARTIES

2. Nader Asghari-Kamrani and Kamran Asghari-Kamrani are the inventors of the invention patented by the ’432 patent and are the only owners of the ’432 patent. Both of these inventors and owners live and reside in Fairfax County, Virginia, United States of America.

3. Messrs. Asghari-Kamrani have all right, title, and interest in the ’432 patent and the right to sue for infringement thereof.

4. On information and belief, USAA is an inter-insurance exchange, organized under the laws of the State of Texas, pursuant to the Texas Insurance Code, and its principal place of business is at 9800 Fredericksburg Road, San Antonio, TX 78288.

5. On information and belief, USAA provides a variety of banking, investment, insurance, and consumer products and services in Virginia and throughout the United States and in particular has a place of business in this judicial district of Virginia.

JURISDICTION AND VENUE

6. This action arises under the patent laws of the United States, Title 35, United States Code. The Court has subject matter jurisdiction over this action pursuant to the provisions of 28 U.S.C. §§ 1331 and 1338(a).

7. On information and belief, Defendant conducts substantial business in this judicial district and regularly solicits business from, does business with, and derives revenue from goods and services provided to, customers in this district, and has committed acts of patent infringement in this judicial district. Because Defendant has committed acts of patent infringement in this judicial district, and/or is otherwise present and doing business in this judicial district, this Court has personal jurisdiction over Defendant.

8. This Court has personal jurisdiction over USAA pursuant to provisions of the Virginia Long Arm Statute, VA. Code. Ann. § 8.01-328.1, and the laws of the United States based at least on USAA having committed a tortious injury in this Commonwealth by purposefully utilizing infringing products or services in this judicial district and providing access and continued use to customers and members located in the Commonwealth of Virginia.

9. Venue is proper in this judicial district pursuant to the provisions of 28 U.S.C. §§ 1391, 1400(b), and Local Rule 3(c).

COUNT I: PATENT INFRINGEMENT OF THE '432 PATENT

10. Messrs. Asghari-Kamrani restate, re-plead, and incorporate by reference each and every allegation set forth above as if fully set forth herein. The United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,266,432 on September 11, 2012, to the inventors Nader Asghari-Kamrani and Kamran Asghari-Kamrani. Defendant has directly or indirectly infringed, literally or though the doctrine of equivalents by using and making in this judicial district and elsewhere within the United States apparatuses and methods that are within the scope of at least claims 1-10, 12, 13, 16-26, 28-35, 38-42, 45, 47, 48, 50-52, 54, and 55 of the '432 patent, constituting infringement under 35 U.S.C. § 271. In particular, Defendant used and made its accused technologies to authenticate a user's identity through the use of an authentication system.

11. USAA operates the USAA website at https://www.usaa.com ("the USAA Website") and offers internet-based products and services to its users (e.g., members).

12. USAA is offering internet-based products and services such as Banking, Auto Insurance, Health Insurance, Investments, and Mortgages to its users (e.g., members).

13. On information and belief, USAA requires its users (e.g., members) to first successfully authenticate themselves before the access to their accounts associated with one or more internet-based products and services is authorized.

14. On information and belief, USAA directly and literally infringes the ’432 patent through USAA’s use of at least four technologies as described in the following paragraphs.

I. Infringement Example 1 – USAA’s Use of “Forgot PIN” Technology

15. Claim 1 of the ’432 patent recites “[a] method for authenticating a user during an electronic transaction between the user and an external-entity.” On information and belief, USAA owns, directs, controls, and uses a central-entity (USAA’s authentication system). USAA also owns, directs, controls, and uses an external-entity (USAA’s Web server and banking/application server). USAA uses a method for authenticating a user during an electronic transaction between the user and the external-entity. USAA uses and practices the method recited in claim 1 when a user (USAA member) logs on to the USAA Website (https://www.usaa.com), which is operated by USAA on USAA’s Web server, during an electronic transaction (logon process to, e.g., (i) make a payment from a USAA checking account with USAA Web BillPay or (ii) update a mailing address) between the user (using a Web browser) and the external-entity (USAA’s Web server and banking/application server).

16. Claim 1 recites “receiving electronically a request for a dynamic code for the user by a computer associated with a central-entity during the transaction between the user and the external-entity.” On information and belief, in USAA’s usage, the user enters an Online ID and Password in the USAA Website. The USAA Web server then asks the user to enter his personal identification number (PIN) via the USAA Website. The user clicks on a link labeled “Don’t know your PIN?” The user then clicks on a radio button labeled “Send a temporary pin in a text

message to my mobile device," enter his mobile number, and clicks "Next" in the USAA Website. A computer associated with a central-entity (USAA's authentication system) receives electronically a request for a dynamic code (temporary PIN that is a 4-digit numeric code) during the transaction. More specifically, a computer at USAA's authentication system receives electronically the request for a temporary PIN from USAA's Web server.

17. Claim 1 further recites "generating by the central-entity during the transaction a dynamic code for the user in response to the request, wherein the dynamic code is valid for a predefined time and becomes invalid after being used." On information and belief, in USAA's usage, the central-entity (USAA's authentication system) generates, during the transaction, a dynamic code (temporary PIN that is a 4-digit numeric code) for the user in response to the request. The dynamic code (temporary PIN) is valid for a predefined time (on information and belief, several minutes) and becomes invalid after being used."

18. Claim 1 further recites "providing by the computer associated with the central-entity said generated dynamic code to the user during the transaction." On information and belief, in USAA's usage, the computer associated with the central-entity (USAA's authentication system) provides the generated dynamic code (temporary PIN) to the user during the transaction. More specifically, the computer sends a text message containing the dynamic code (temporary PIN) to the user via his mobile device.

19. Claim 1 further recites "receiving electronically by the central-entity a request for authenticating the user from a computer associated with the external-entity based on a user-specific information and the dynamic code as a digital identity included in the request which said dynamic code was received by the user during the transaction and was provided to the external-entity by the user during the transaction." On information and belief, in USAA's usage, the

central-entity (USAA's authentication system) receives a request for authenticating the user from a computer associated with the external-entity (USAA's Web server and banking/application server) based on a user-specific information (Online ID) and the dynamic code (temporary PIN) as a digital identity included in the request. The dynamic code (temporary PIN) was received by the user during the transaction and was provided to the external-entity (USAA's Web server and banking/application server) by the user during the transaction. More specifically, after the user clicks on a radio button labeled "Send a temporary pin in a text message to my mobile device," enters his mobile number, and clicks "Next" in the USAA Website, the user receives a text message containing the dynamic code (temporary PIN) via his mobile device. The user is told "We have sent you a temporary PIN" and "Please enter it below" by the USAA Website, prompting the user to enter the dynamic code (temporary PIN). The user enters the dynamic code (temporary PIN), which he received via his mobile device during the transaction, in the USAA Website. The dynamic code (temporary PIN) is thereby provided to the external-entity (USAA's Web server and banking/application server). The central entity (USAA's authentication system) then receives, from a computer associated with the external-entity (USAA's Web server and banking/application server), a request for authenticating the user based on a user-specific information (Online ID) and the dynamic code (temporary PIN) as a digital identity included in the request.

20. Claim 1 further recites "authenticating by the central-entity the user and providing a result of the authenticating to the external-entity during the transaction if the digital identity is valid." On information and belief, in USAA's usage, the central-entity (USAA's authentication system) authenticates the user and provides a result of the authenticating to the external-entity (USAA's Web server and banking/application server) during the transaction if the digital identity

is valid. If the digital identity is valid, the USAA Website allows the user to continue to access a restricted area of the USAA Website.

21. On information and belief, USAA also infringes the methods and apparatuses recited in claims 2-10, 12, 13, 16-26, 28-35, 38-42, 45, 47, 48, 50-52, 54, and 55 of the ’432 patent, as described in the claim charts attached hereto as Exhibit B.

22. On information and belief, USAA uses the claimed methods and performs (or directs and controls the performance of) each and every limitation of each of the method claims in the United States.

23. On information and belief, USAA uses and makes the claimed apparatuses within the United States.

24. A copy of a screenshot from USAA’s website (https://www.usaa.com) that further indicates and instructs the user on how USAA proceeds if a user has forgotten his PIN is attached hereto as Exhibit F (with red markings added for emphasis).

25. On information and belief, a USAA Website logon page (https://www.usaa.com/inet/pages/security_take_steps_protect_logon?akredirect=true) states "*What if you forget your Online ID, password or PIN? Don't worry, you can still log on. … Have your online credential sent to you by **email** or **text message** for one-time use.*" *See* Exhibit F.

26. On information and belief, security experts of USAA recommend to its users that for stronger protection of users’ online accounts for password or PIN reset operations, users should enable email or text message options to receive a single-use dynamic code. *See* Exhibit F.

II. Infringement Example 2 – USAA's Use of "Password Recovery" Technology

27. Claim 1 of the '432 patent recites "[a] method for authenticating a user during an electronic transaction between the user and an external-entity." On information and belief, USAA owns, directs, controls, and uses a central-entity (USAA's authentication system). USAA also owns, directs, controls, and uses an external-entity (USAA's Web server and banking/application server). USAA uses a method for authenticating a user during an electronic transaction between the user and the external entity. USAA uses and practices this method when a user (USAA member) logs on to the USAA Website (https://www.usaa.com), which is operated by USAA on USAA's Web server, during an electronic transaction (logon process to, e.g., (i) make a payment from a USAA checking account with USAA Web BillPay or (ii) update a mailing address) between the user (using a Web browser) and the external-entity (USAA's Web server and banking/application server).

28. Claim 1 recites "receiving electronically a request for a dynamic code for the user by a computer associated with a central-entity during the transaction between the user and the external-entity." On information and belief, the user is prompted to enter an Online ID and Password in the USAA Website. The user enters his Online ID and clicks on a link labeled "Forgot Password." The user then clicks on a radio button labeled "Send a temporary password in a text message to my mobile device," enter his mobile number, and clicks "Next" in the USAA Website. A computer associated with a central-entity (USAA's authentication system) receives electronically a request for a dynamic code (temporary password that is an 8-character alphanumeric code) during the transaction. More specifically, a computer at USAA's authentication system receives electronically the request for a temporary password from USAA's Web server.

29. Claim 1 further recites "generating by the central-entity during the transaction a dynamic code for the user in response to the request, wherein the dynamic code is valid for a predefined time and becomes invalid after being used. On information and belief, in USAA's usage, the central-entity (USAA's authentication system) generates, during the transaction, a dynamic code (temporary password that is an 8-character alphanumeric code) for the user in response to the request. The dynamic code (temporary password) is valid for a predefined time and becomes invalid after being used.

30. Claim 1 further recites "providing by the computer associated with the central-entity said generated dynamic code to the user during the transaction." On information and belief, in USAA's usage, the computer associated with the central-entity (USAA's authentication system) provides the generated dynamic code (temporary password) to the user during the transaction. More specifically, the computer sends a text message containing the dynamic code (temporary password) to the user via his mobile device.

31. Claim 1 further recites "receiving electronically by the central-entity a request for authenticating the user from a computer associated with the external-entity based on a user-specific information and the dynamic code as a digital identity included in the request which said dynamic code was received by the user during the transaction and was provided to the external-entity by the user during the transaction." On information and belief, in USAA's usage, the central-entity (USAA's authentication system) receives a request for authenticating the user from a computer associated with the external-entity (USAA's Web server and banking/application server) based on a user-specific information (Online ID) and the dynamic code (temporary password) as a digital identity included in the request. The dynamic code (temporary password) was received by the user during the transaction and was provided to the external-entity (USAA's

Web server and banking/application server) by the user during the transaction. More specifically, after the user clicks on a radio button labeled "Send a temporary password in a text message to my mobile device," enters his mobile number, and clicks "Next" in the USAA Website, the user receives a text message containing the dynamic code (temporary password) via his mobile device. The user is told "We have sent you a temporary password in a text message" and "Please enter the temporary password below" by the USAA Website, prompting the user to enter the dynamic code (temporary password). The user enters the dynamic code (temporary password), which he received via his mobile device during the transaction, in the USAA Website. The dynamic code (temporary password) is thereby provided to the external-entity (USAA's Web server and banking/application server). The central entity (USAA's authentication system) then receives, from a computer associated with the external-entity (USAA's Web server and banking/application server), a request for authenticating the user based on a user-specific information (Online ID) and the dynamic code (temporary password) as a digital identity included in the request.

32. Claim 1 further recites "authenticating by the central-entity the user and providing a result of the authenticating to the external-entity during the transaction if the digital identity is valid." On information and belief, in USAA's usage, the central-entity (USAA's authentication system) authenticates the user and provides a result of the authenticating to the external-entity (USAA's Web server and banking/application server) during the transaction if the digital identity is valid. If the digital identity is valid, the USAA Website allows the user to continue to access a restricted area of the USAA Website.

33. On information and belief, USAA also infringes the methods and apparatuses recited in claims 2-10, 12, 13, 16-26, 28-35, 38-42, 45, 47, 48, 50-52, 54, and 55 of the '432 patent, as described in the claim charts attached hereto as Exhibit C.

34. On information and belief, USAA uses the claimed methods and performs (or directs and controls the performance of) each and every limitation of each of the method claims in the United States.

35. On information and belief, USAA uses and makes the claimed apparatuses within the United States.

36. A copy of a screenshot from USAA's website (https://www.usaa.com) that further indicates and instructs the user on how USAA proceeds if a user has forgotten his PIN is attached hereto as Exhibit F (with red markings added for emphasis).

37. On information and belief, a USAA Website logon page (https://www.usaa.com/inet/pages/security_take_steps_protect_logon?akredirect=true) states "*What if you forget your Online ID, password or PIN? Don't worry, you can still log on. … Have your online credential sent to you by **email** or **text message** for one-time use.*" *See* Exhibit F.

38. On information and belief, security experts of USAA recommend to its users that for stronger protection of users' online accounts for password or PIN reset operations, users should enable email or text message options to receive a single-use dynamic code. *See* Exhibit F.

III. Infringement Example 3 – USAA's Use of "CyberCode Text" Technology

39. Claim 1 of the '432 patent recites "[a] method for authenticating a user during an electronic transaction between the user and an external-entity." On information and belief, USAA owns, directs, controls, and uses a central-entity (USAA's authentication system). USAA also owns, directs, controls, and uses an external-entity (USAA's Web server and

banking/application server). USAA uses a method for authenticating a user during an electronic transaction between the user and the external entity. USAA uses and practices this method when a user (USAA member) logs on to the USAA Website (https://www.usaa.com), which is operated by USAA on USAA's Web server, during an electronic transaction (logon process to, e.g., (i) make a payment from a USAA checking account with USAA Web BillPay or (ii) update a mailing address) between the user (using a Web browser) and the external-entity (USAA's Web server and banking/application server). USAA uses and practices this method if the user has enrolled to participate in "CyberCode Text" technology.

40. Claim 1 recites "receiving electronically a request for a dynamic code for the user by a computer associated with a central-entity during the transaction between the user and the external-entity." On information and belief, in USAA's usage, the user is prompted to enter an Online ID and Password in the USAA Website. The user enters his Online ID and Password and clicks on a link labeled "Log On." A computer associated with a central-entity (USAA's authentication system) receives electronically a request for a dynamic code (temporary PIN that is a 6-digit numeric code) during the transaction. More specifically, a computer at USAA's authentication system receives electronically the request for a temporary PIN during the transaction.

41. Claim 1 further recites "generating by the central-entity during the transaction a dynamic code for the user in response to the request, wherein the dynamic code is valid for a predefined time and becomes invalid after being used." On information and belief, in USAA's usage, the central-entity (USAA's authentication system) generates, during the transaction, a dynamic code (temporary PIN that is a 6-digit numeric code) for the user in response to the

request. The dynamic code (temporary PIN) is valid for a predefined time (on information and belief, several minutes) and becomes invalid after being used.

42. Claim 1 further recites "providing by the computer associated with the central-entity said generated dynamic code to the user during the transaction." On information and belief, in USAA's usage, the computer associated with the central-entity (USAA's authentication system) provides the generated dynamic code (temporary PIN) to the user during the transaction. More specifically, the computer sends a text message containing the dynamic code (temporary PIN) to the user via his mobile device.

43. Claim 1 further recites "receiving electronically by the central-entity a request for authenticating the user from a computer associated with the external-entity based on a user-specific information and the dynamic code as a digital identity included in the request which said dynamic code was received by the user during the transaction and was provided to the external-entity by the user during the transaction." On information and belief, in USAA's usage, the central-entity (USAA's authentication system) receives a request for authenticating the user from a computer associated with the external-entity (USAA's Web server and banking/application server) based on a user-specific information (Online ID) and the dynamic code (temporary PIN) as a digital identity included in the request. The dynamic code (temporary PIN) was received by the user during the transaction and was provided to the external-entity (USAA's Web server and banking/application server) by the user during the transaction. More specifically, after the user clicks on the link labeled "Log On," the user receives a text message containing the dynamic code (temporary PIN) via his mobile device. The user is prompted by the USAA Website to enter the dynamic code (temporary PIN). The user enters the dynamic code (temporary PIN), which he received via his mobile device during the transaction, in the USAA Website. The

dynamic code (temporary PIN) is thereby provided to the external-entity (USAA's Web server and banking/application server). The central entity (USAA's authentication system) then receives, from a computer associated with the external-entity (USAA's Web server and banking/application server), a request for authenticating the user based on a user-specific information (Online ID) and the dynamic code (temporary PIN) as a digital identity included in the request.

44. Claim 1 further recites "authenticating by the central-entity the user and providing a result of the authenticating to the external-entity during the transaction if the digital identity is valid." On information and belief, in USAA's usage, the central-entity (USAA's authentication system) authenticates the user and provides a result of the authenticating to the external-entity (USAA's Web server and banking/application server) during the transaction if the digital identity is valid. If the digital identity is valid, the USAA Website allows the user to continue to access a restricted area of the USAA Website.

45. On information and belief, USAA also infringes the methods and apparatuses recited in claims 2-10, 12, 13, 16-26, 28-35, 38-42, 45, 47, 48, 50-52, 54, and 55 of the '432 patent, as described in the claim charts attached hereto as Exhibit D.

46. On information and belief, USAA uses the claimed methods and performs (or directs and controls the performance of) each and every limitation of each of the method claims in the United States.

47. On information and belief, USAA uses and makes the claimed apparatuses within the United States.

48. Copies of screenshots from USAA's website (https://www.usaa.com) that further indicate and instruct the user on how to utilize the "CyberCode Text" technology are attached hereto as Exhibits G, H, I.

49. A USAA Website logon page (https://www.usaa.com/inet/pages/security_take_steps_protect_logon?akredirect=true) states "*Replace your PIN with a dynamic code that is sent to you by text message each time you log on.*" *See* Exhibit G.

50. A USAA Website logon options page (https://www.usaa.com/inet/pages/security_token_logon_options?wa_ref=SEC_CTR_YourSec_logon_Logonopts), under "CyberCode® Text," states "*CyberCode Text replaces your PIN with a extra security measure (Opens Pop-up Layer). You log on with your Online ID and password as usual but instead of entering a PIN, you'll enter a unique code that you receive by text message.*" *See* Exhibit H.

15. A USAA community website (https://communities.usaa.com/t5/Other/CyberCode-Token/td-p/27522) states "*this logon method allows you to receive a one-time passcode via text message that is unique for each logon*." *See* Exhibit I.

IV. Infringement Example 4 – USAA's Use of "Symantec VIP" Technology

51. Claim 1 of the '432 patent recites "[a] method for authenticating a user during an electronic transaction between the user and an external-entity." On information and belief, USAA directs, controls, and uses a central-entity (Symantec VIP system at Symantec Corporation of Mountain View, California). USAA owns, directs, controls, and uses an external-entity (USAA's Web server and banking/application server). USAA uses a method for

authenticating a user during an electronic transaction between the user and the external entity. USAA uses and practices this method when a user (USAA member) uses an electronic device with a Web browser to log on to the USAA Website (https://www.usaa.com), which is operated by USAA on USAA's Web server, during an electronic transaction (logon process to, e.g., (i) make a payment from a USAA checking account with USAA Web BillPay or (ii) update a mailing address) between the user (using the Web browser) and the external-entity (USAA's Web server and banking/application server).

52. Claim 1 recites "receiving electronically a request for a dynamic code for the user by a computer associated with a central-entity during the transaction between the user and the external-entity." On information and belief, in USAA's usage, the user is prompted to enter an Online ID and Password in the USAA Website. The user enters his Online ID and Password and clicks on a link labeled "Log On." The USAA Web server has JavaScript embedded in the USAA Website's logon page to intercept the ID/Password submission from the user. The USAA Web server sends a request to a Symantec VIP system to perform risk analysis and return a dynamic code (digital ticket) during the transaction. On information and belief, the Symantec VIP system is located at Symantec Corporation of Mountain View, California, and USAA directs and controls the Symantec VIP system. Thus, a computer associated with a central-entity (Symantec VIP system) receives electronically a request for a dynamic code (digital ticket) during the transaction.

53. Claim 1 further recites "generating by the central-entity during the transaction a dynamic code for the user in response to the request, wherein the dynamic code is valid for a predefined time and becomes invalid after being used." On information and belief, in USAA's usage, sometimes the Symantec VIP system judges the risk to be low. In that case, the central-

entity (Symantec VIP system) generates a dynamic code (digital ticket) during the transaction in response to the request. The dynamic code (digital ticket) is valid for a predefined time (on information and belief, several minutes) and becomes invalid after being used.

54. Claim 1 further recites "providing by the computer associated with the central-entity said generated dynamic code to the user during the transaction." On information and belief, in USAA's usage, the computer associated with the central-entity (Symantec VIP system) provides the generated dynamic code (digital ticket) to the user during the transaction. More specifically, the computer associated with the central-entity (Symantec VIP system) sends the digital ticket to the user's electronic device containing the Web browser.

55. Claim 1 further recites "receiving electronically by the central-entity a request for authenticating the user from a computer associated with the external-entity based on a user-specific information and the dynamic code as a digital identity included in the request which said dynamic code was received by the user during the transaction and was provided to the external-entity by the user during the transaction." On information and belief, in USAA's usage, the central-entity (Symantec VIP system) receives a request for authenticating the user from a computer associated with the external-entity (USAA's Web server and banking/application server) based on a user-specific information (Online ID) and the dynamic code (digital ticket) as a digital identity included in the request. The dynamic code (digital ticket) was received by the user via his electronic device during the transaction. The dynamic code (digital ticket) was then provided to the external-entity (USAA's Web server and banking/application server) by the user via his electronic device during the transaction.

56. Claim 1 further recites "authenticating by the central-entity the user and providing a result of the authenticating to the external-entity during the transaction if the digital identity is

valid." On information and belief, in USAA's usage, the central-entity (Symantec VIP system) authenticates the user and provides a result of the authenticating to the external-entity (USAA's Web server and banking/application server) during the transaction if the digital identity is valid.

57. If the digital identity is valid, the USAA Website allows the user to continue to access a restricted area of the USAA Website.

58. On information and belief, USAA also infringes the methods and apparatuses recited in claims 2-10, 12, 13, 16-26, 28-35, 38-42, 45, and 47 of the '432 patent, as described in the claim charts attached hereto as Exhibit E.

59. On information and belief, USAA uses the claimed methods and performs (or directs and controls the performance of) each and every limitation of the method claims in the United States.

60. On information and belief, USAA uses the claimed apparatuses within the United States.

61. On information and belief, USAA utilizes technology patented by the '432 patent for authentication and identification of online/mobile users for a variety of purposes.

62. To the extent any fact finder concludes that Defendant did not literally satisfy any element of the above listed claims of the '432 patent, those elements are met under the Doctrine of Equivalents.

63. Upon information and belief, USAA derives substantial revenue from the cost savings associated with utilizing the infringing products or services covered by the '432 patent.

64. On information and belief, Defendant's acts of infringement have caused damage to Messrs. Asghari-Kamrani, and Messrs. Asghari-Kamrani are entitled to recover from Defendant damages consisting of at least a reasonable royalty.

65. USAA has infringed the ’432 patent as alleged above despite having prior knowledge of the patent at least after the date of the notice letter received by USAA on or about September 9, 2014 and from prior lengthy negotiation sessions, and has acted with willful, intentional, and conscious disregard of the objectively high likelihood that its acts constitute infringement of the ’432 patent.

66. Messrs. Asghari-Kamrani have no adequate remedy at law for Defendant’s continued infringement of the ’432 patent, such that Messrs. Asghari-Kamrani are entitled to injunctive relief from and against Defendant for further acts of infringement.

PRAYER FOR RELIEF

WHEREFORE, Messrs. Asghari-Kamrani request the following relief:

A. Adjudging that Defendant infringes the ’432 patent-in-suit;

B. Adjudging that Defendant’s infringement of the ’432 patent has been willful and deliberate.

C. A judgment awarding Messrs. Asghari-Kamrani damages of at least a reasonable royalty, including but not limited to treble damages, based on any infringement found to be willful, pursuant to 35 U.S.C. § 284, compensatory damages, costs, together with both pre-judgment and post-judgment interest.

D. USAA, and its directors, subsidiaries, affiliates, officers, agents, servants, and employees, and those acting in concert or participation with USAA be preliminarily and permanently enjoined from further infringement of the ’432 patent;

E. A judgment that this case is an exceptional case under 35 U.S.C. § 285, entitling Plaintiffs to an award of its reasonable attorneys' fees for bringing and prosecuting this action;

F. An award of Plaintiffs' costs and expenses in this action; and

G. Such further and additional relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Fed. R. Civ. P. 38(b) and Local Rule 38, Messrs. Asghari-Kamrani demand a trial by jury in this action on all issues triable by jury.

Respectfully submitted,

MEI & MARK LLP

Dated: April 12, 2016

/s/ Krystyna Colantoni
Krystyna Colantoni (VA Bar # 76612)
kcolantoni@meimark.com
Reece Nienstadt (*Pro Hac Vice*)
rnienstadt@meimark.com
MEI & MARK LLP
P.O. Box 65981
Washington, DC 20035-5981
Telephone: 888-860-5678
Facsimile: 888-706-1173

Counsel for Plaintiffs Nader Asghari-Kamrani and Kamran Asghari-Kamrani

CERTIFICATE OF SERVICE

I hereby certify that the foregoing is being electronically filed with the Clerk of Court using the CM/ECF system on April 12, 2016, which will then send a notification of such filing (NEF) to:

Ahmed J. Davis (Va. Bar # 43982)
adavis@fr.com
FISH & RICHARDSON P.C.
1425 K Street, N.W., Suite 1100
Washington, DC 20005

David Francescani (*Pro hac vice*)
francescani@fr.com
Michael T. Zoppo (*Pro hac vice*)
zoppo@fr.com
FISH & RICHARDSON, P.C.
601 Lexington Avenue, 52nd Floor
New York, New York 10022

Matthew Berntsen (*Pro hac vice*)
berntsen@fr.com
David Kuznick (*Pro hac vice*)
kuznick@fr.com
FISH & RICHARDSON, P.C.
One Marina Park Drive
Boston, MA 02210-1878

Counsel for Defendant
United Services Automobile Association

/s/ Krystyna Colantoni
Krystyna Colantoni (VA Bar # 76612)
Email: kcolantoni@meimark.com
Reece Nienstadt (*Pro Hac Vice*)
Email: rnienstadt@meimark.com
MEI & MARK LLP
P.O. Box 65981
Washington, DC 20035-5981
Telephone: 888-860-5678
Facsimile: 888-706-1173