IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SMART AUTHENTICATION IP, LLC	)
	)
Plaintiff,	)
	) Civil Action No. _____
v.	)
	) **JURY TRIAL DEMANDED**
PERSONAL CAPITAL CORPORATION	)
	)
Defendant.	)
	)

COMPLAINT

For its Complaint, Smart Authentication IP, LLC ("SAIP"), by and through the undersigned counsel, alleges as follows:

THE PARTIES

1. SAIP is a Texas limited liability company with a place of business located at 1400 Preston Road, Suite 400 Plano, Texas 75093.

2. Defendant Personal Capital Corporation is a Delaware company with, upon information and belief, a place of business located 999 18th Street, Suite 800, Denver, Colorado 80202.

JURISDICTION AND VENUE

3. This action arises under the Patent Act, 35 U.S.C. § 1 *et seq.*

4. Subject matter jurisdiction is proper in this Court under 28 U.S.C. §§ 1331 and 1338.

5. Upon information and belief, Defendant conducts substantial business in this forum, directly or through intermediaries, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct and/or deriving substantial revenue from goods and services provided to individuals

in this district.

6. Venue is proper in this district pursuant to 28 U.S.C. § 1400(b).

BACKGROUND

7. On December 20, 2011, U.S. Patent No. 8,082,213 (the "'213 patent"), entitled "Method and System for Personalized Online Security," was duly and lawfully issued by the U.S. Patent and Trademark Office. A true and correct copy of the '213 patent is attached hereto as Exhibit A.

8. Jarlath Lyons invented the technology claimed in the '213 patent.

9. SAIP is the assignee and owner of the right, title and interest in and to the '213 patent, including the right to assert all causes of action arising under said patent and the right to any remedies for infringement of it.

10. The inventions of the '213 Patent generally relate to methods and systems for multi-factor authentication of users over multiple communications mediums.

11. The '213 patent discloses an Authentication Service Provider ("ASP"), which "is generally implemented above a software and hardware platform or platforms . . . that include operating systems, lower-level applications, and computer-server hardware." Ex. A at col. 4, ll. 13-16. "In many embodiments, the ASP . . . is a software implemented service that runs on one or more computer systems interconnected by various communications media with both ASP clients and users." *Id.* at col. 2, ll. 47-50. In certain embodiments, the "ASP may interact with the user via two different communications media, such as a combination of the Internet and a cell phone." *Id.* at col. 3, ll. 23-25.

12. In another example of disclosed embodiments, "[t]he [] third interface 208 allows the ASP to interface with user devices through alternative communications media, such as a cell

phone, fax machine, telephone, or other communications devices. The third interface 208 allows the ASP to interface with virtually any network enabled resource through an appropriate medium, including both physical devices such as a cell phone, fax machine, telephone, or other communications devices, and also soft devices, such as an instant messaging account, or an email account." *Id.* at col. 3, ll. 37-46.

13. As one example of an asserted claim, the '213 Patent recites a novel method of authenticating a user of an authentication service where an authentication-service client communicates with the user through a first communication medium. The authentication service receives user-identifying information from the authentication-service client, and uses the received user-identifying information to carry out an authentication procedure to authenticate the user by sending information to the user through a communications medium different from the first communications medium. The authentication result is then returned to the authentication service client.

14. In another example of an asserted claim, the '213 Patent recites the novel method described above, wherein the user authentication service further uses electronically-encoded information about the user to retrieve all stored user authentication policies for the user, and conducting the user authentication procedure as permitted by the stored policies. The authentication result is then returned to the authentication service client.

15. Defendant offers computer-aided products and services to customers related to financial tools for financial planning. Defendant's products and services use two-factor authentication over multiple communications mediums by first requiring the user to enter a username (e.g., e-mail address) and password through the Internet via a browser, mobile, or desktop app, and then by requiring the user to verify his or her identity by entering a one-time

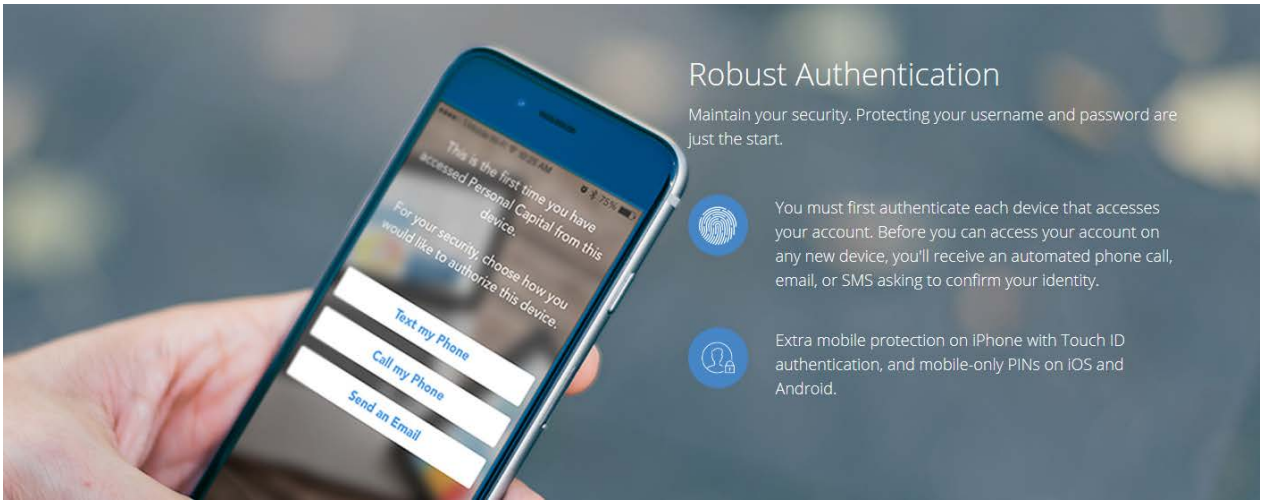
code received by means of text message (SMS), voice call, or e-mail.

16. During the two-factor authentication process, Defendant also uses the electronically- encoded information about the user to retrieve all authentication-related policies for that user. For example, the user may set up several methods of receiving the one-time verification code. Once the authentication-related policies are retrieved, Defendant conducts the authentication procedure and returns the authentication results.

COUNT I – INFRINGEMENT OF U.S. PATENT NO. 8,082,213

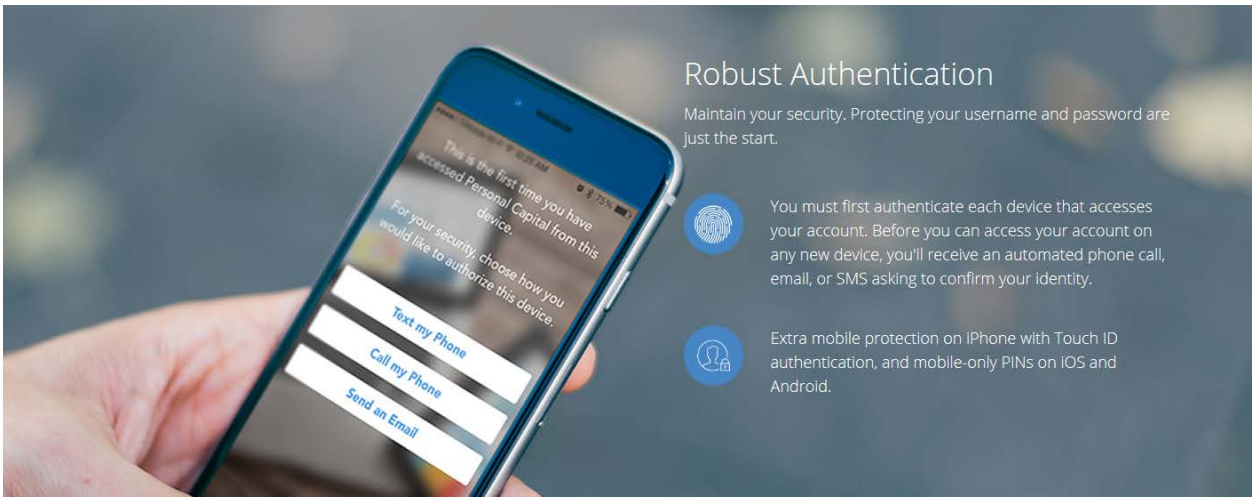
17. SAIP repeats and realleges the allegations of paragraphs 1 through 16 as if fully set forth herein.

18. Without license or authorization and in violation of 35 U.S.C. § 271(a), Defendant is liable for infringement at least claims 1-5, 7-10 and 12-16 of the '213 patent by making, using, importing, offering for sale, selling and/or hosting methods for financial planning software and apps that require two-factor authentication to access such software and apps.

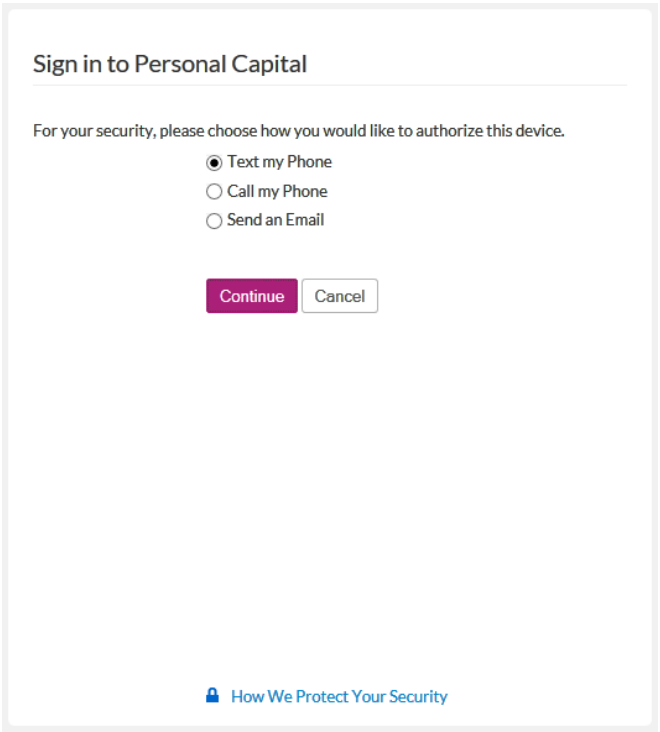


https://www.personalcapital.com/financial-software/security.

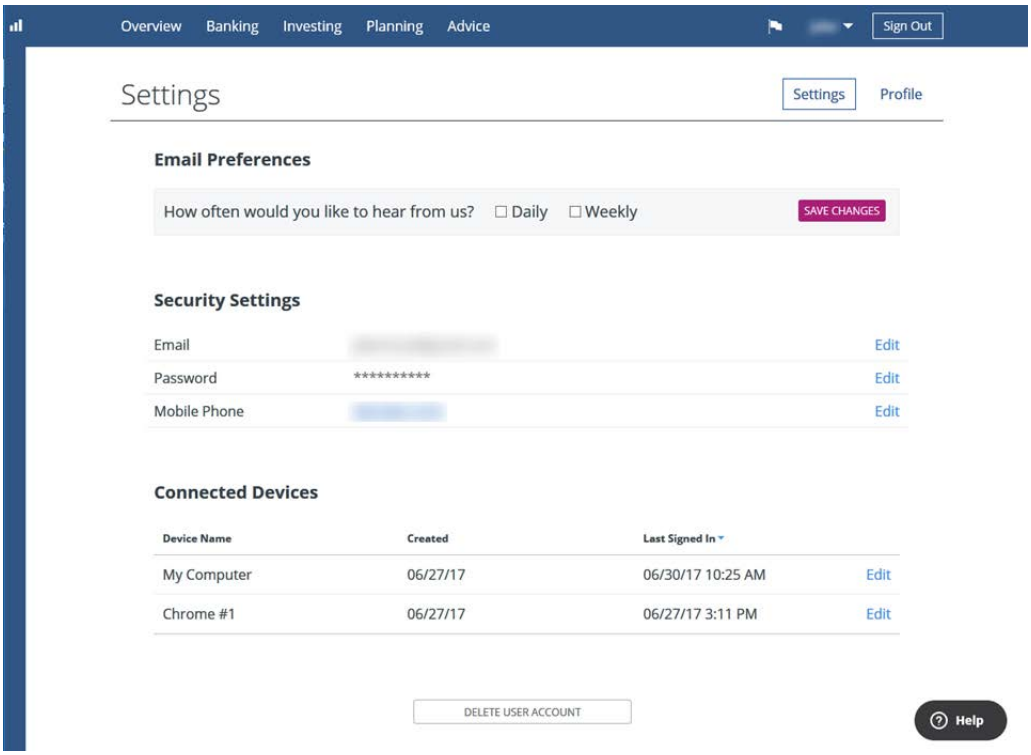
19. More specifically and upon information and belief, Defendant provides a two-factor authentication service for its users.



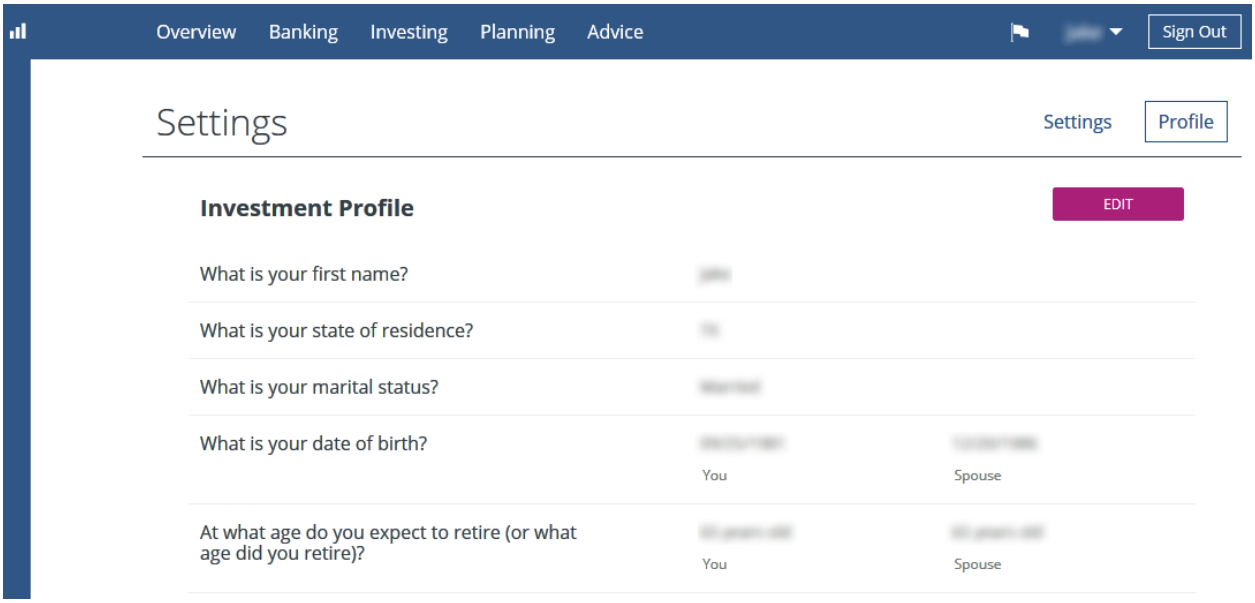
Id. Defendant's two-factor authentication must run on one or more computer systems (e.g., a server with authentication functionality). Defendant stores user-authentication policies specified by the user.



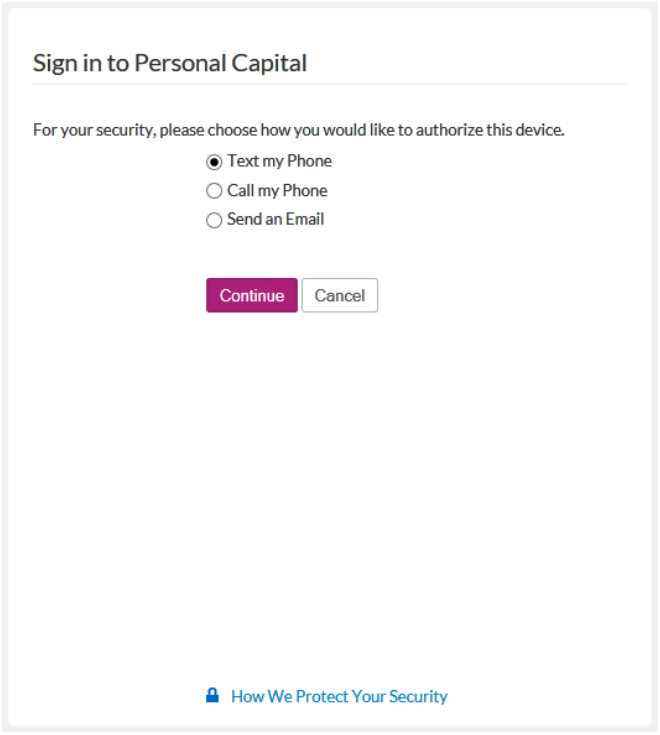
https://home.personalcapital.com/page/login/goHome.



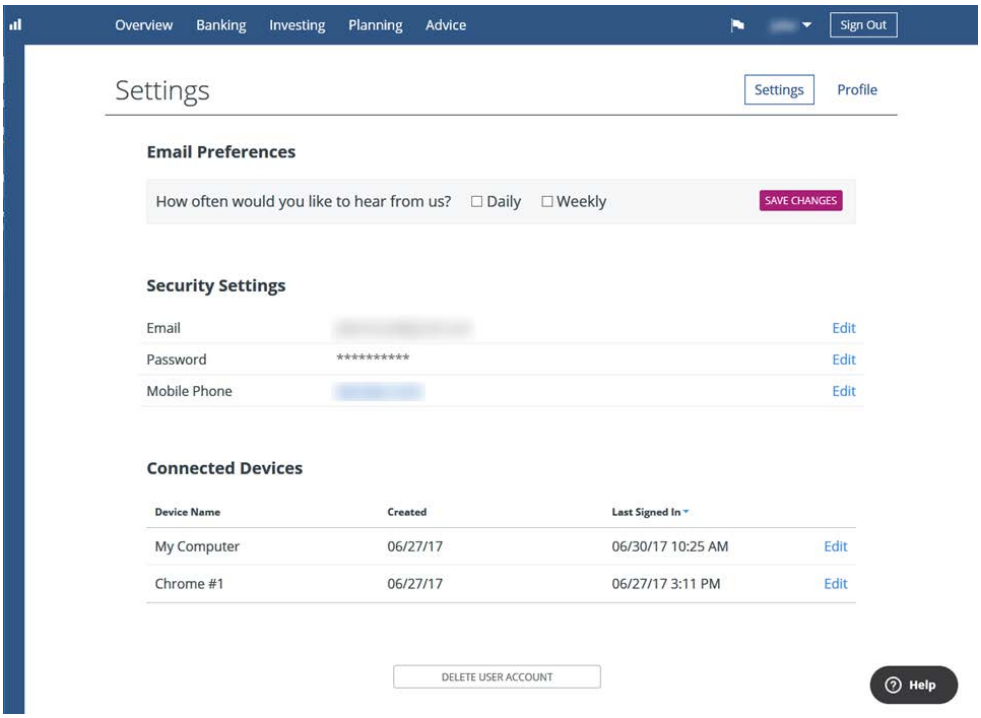
https://home.personalcapital.com/page/login/app#/settings.



https://home.personalcapital.com/page/login/app#/settings/profile. Defendant's two-factor authentication includes account interface routines where a user can specify, modify, add and delete a user-authentication policy.

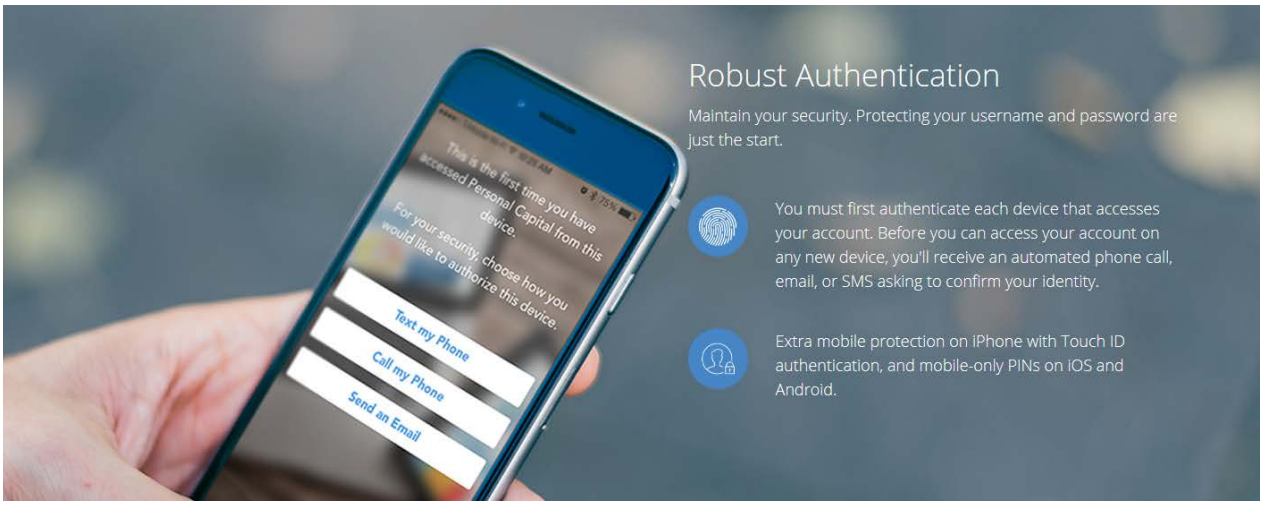


https://home.personalcapital.com/page/login/goHome.

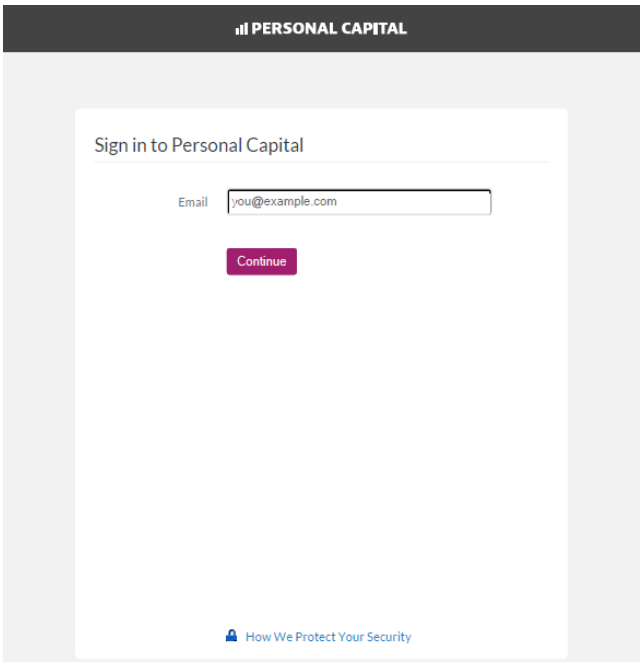


https://home.personalcapital.com/page/login/app#/settings. Defendant implements an authentication interface (e.g., API, network-protocol based interface, and/or function call

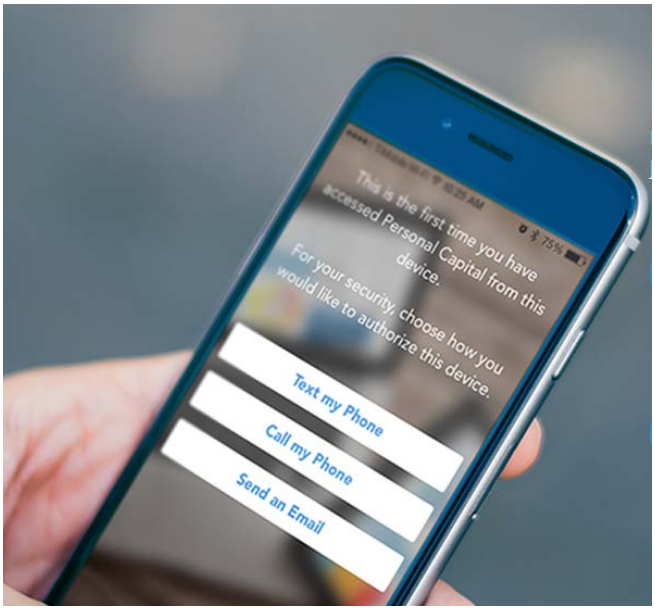
interface) by which, following initiation of a transaction by the user (e.g., a login attempt), the authentication-service client (Defendant's website) submits an authentication request to Defendant's authentication service.



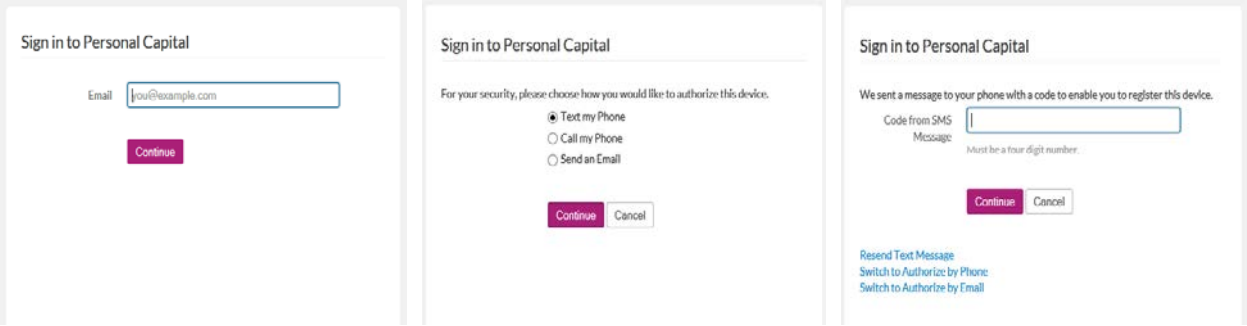
https://www.personalcapital.com/financial-software/security. A user inputs the "Email" and "Password" into Defendant's website and the information is submitted through the first communications medium (e.g., Internet via a browser) or through a second communications medium (e.g., Personal Capital mobile application running on a tablet, smartphone or computer).



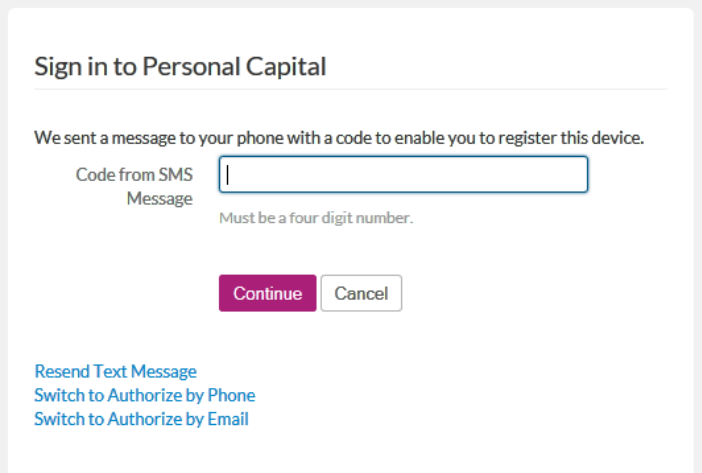
https://home.personalcapital.com/page/login/goHome.



https://www.personalcapital.com/financial-software/security. Defendant's authentication routines employ variable-factor authentication whereby a user provides secret information (e.g., a username, password or the one-time code generated by Defendant's authentication service) and demonstrates control of a tangible object (e.g., the user's smartphone) as specified by the stored user authentication policies.



https://home.personalcapital.com/page/login/goHome. The user communicates with Defendant's authentication service by receiving the security code via text message (SMS), voice call or email, all of which are a different communications media from the first and second communications media.



https://home.personalcapital.com/page/login/goHome. A user can communicate with Defendant's authentication service through a different device than the one used to initiate the transaction with the authentication service client. For example, a user may first attempt to login to Defendant's website using a computer, but then receive the SMS, voice call or email with the one-time code using a smartphone.

20. SAIP is entitled to recover from Defendant the damages sustained by SAIP as a result of Defendant's infringement of the '213 patent in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

JURY DEMAND

SAIP hereby demands a trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, SAIP requests that this Court enter judgment against Defendant as follows:

A. An adjudication that Defendant has infringed the '213 patent;

B. An award of damages to be paid by Defendant adequate to compensate SAIP for Defendant's past infringement of the '213 patent and any continuing or future infringement

through the date such judgment is entered, including interest, costs, expenses and an accounting of all infringing acts including, but not limited to, those acts not presented at trial;

C. A declaration that this case is exceptional under 35 U.S.C. § 285, and an award of Tangelo's reasonable attorneys' fees; and

D. An award to SAIP of such further relief at law or in equity as the Court deems just and proper.

Dated: July 13, 2017

STAMOULIS & WEINBLATT LLC

/s/ Richard C. Weinblatt

Stamatios Stamoulis #4606
Richard C. Weinblatt #5080
Two Fox Point Centre
6 Denny Road, Suite 307
Wilmington, DE 19809
Telephone: (302) 999-1540
Facsimile: (302) 762-1688
stamoulis@swdelaw.com
weinblatt@swdelaw.com

Attorneys for Plaintiff
Smart Authentication IP, LLC