

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

DYNAPASS IP HOLDINGS LLC,

Plaintiff

v.

EXPERIAN INFORMATION SERVICES,
INC.,

Defendant.

CIVIL ACTION NO. 2:23-cv-00066

ORIGINAL COMPLAINT FOR
PATENT INFRINGEMENT

JURY TRIAL DEMANDED

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Dynapass IP Holdings LLC (“Plaintiff”) files this original complaint against Experian Information Services, Inc., (“Defendant”) alleging, based on Plaintiff’s own knowledge as to itself and its own actions, and based on information and belief as to all other matters, as follows:

PARTIES

1. Plaintiff is a Delaware limited liability company, with its principal place of business at 16192 Coastal Highway, Lewes, Delaware 19958.

2. Defendant Experian Information Services, Inc. is an Ohio corporation with a principal place of business at 475 Anton Blvd., Costa Mesa, CA 92626. Defendant Experian Information Services, Inc. may be served c/o CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, TX 75201.

JURISDICTION AND VENUE

3. This is an action for infringement of a United States patent arising under 35 U.S.C. §§ 271, 281, and 284–85, among others. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 and § 1338(a).

4. Venue is proper in this district pursuant to 28 U.S.C. §§ 1400(b) and 1391(c).

5. Defendants are subject to this Court’s specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to Defendant’s presence and substantial business in this forum, including (i) at least a portion of the infringements alleged herein; and/or (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 Texas and in this district.

6. Specifically, Defendant intends to do and does business in Texas, directly or through intermediaries and offer its products and/or services to customers and potential customers located in Texas, including in this district.

7. Defendant maintains a regular and established place of business in this district, including at 701 Experian Parkway, Allen, TX 75013.

COUNT I

DIRECT INFRINGEMENT OF U.S. PATENT NO. 6,993,658

8. Plaintiff repeats and re-alleges the allegations in Paragraphs 1–7 as if fully set forth in their entirety.

9. On January 31, 2006, U.S. Patent No. 6,993,658 (the “’658 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Use of

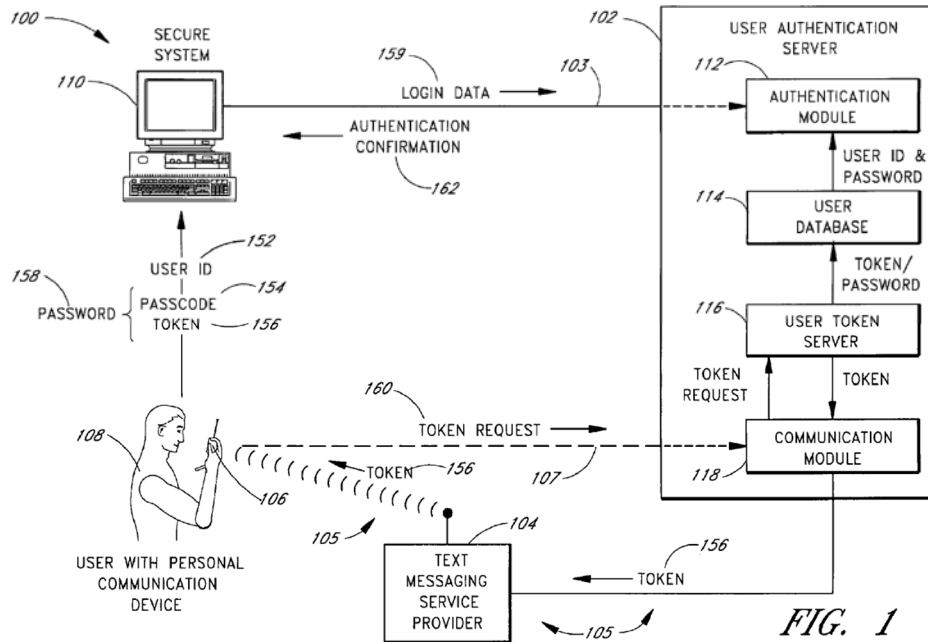
Personal Communication Devices for User Authentication.” A copy of the ’658 Patent is attached as Exhibit A.

10. Plaintiff is the owner of the ’658 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the ’658 Patent against infringers, and to collect damages for all relevant times.

11. The ’658 Patent describes systems for authenticating users to secure systems through user tokens that are supplied to personal communication devices such as mobile telephones and pagers.

12. The named inventors of the ’658 Patent recognized that secure systems at the time of the invention utilized a user ID and password pair to authenticate users. But those authentication methods suffered from several deficiencies including, but not limited to, inconvenience of frequent password changes and hard-to-remember passwords resulting in users writing down their passwords, which compromised security. The named inventors of the ’658 Patent also recognized that two-factor authentication can improve the security of the authentication mechanism, while also improving user convenience.

13. In two-factor authentication, access and authentication to a secure system are determined by (1) secret information known to the user, such as a passcode, and (2) information provided to the user through an object possessed by the user, such as a token. The named inventors of the ’658 Patent recognized that the user’s personal communication device could be used as the “object possessed by the user” to receive a token. This process is depicted, for example, in Figure 1 of the ’658 Patent, reproduced below:



14. The claims of the '658 Patent are not directed to an abstract idea. For example, claim 5 of the '658 Patent recites a user authentication system with a specific arrangement of devices and networking configuration. The claimed user authentication system authenticates users to a secure computer network. The authentication system includes a user database that associates the user's personal communication device with the user. That personal communication device communicates with the user authentication system over a cell phone network.

15. The claimed user authentication system also includes a control module that is configured to create new passwords based at least upon a token and a passcode. The token is not known to the user, whereas the passcode is known to the user. The control module associates the new password with the user. The token is transmitted to the user through the cell phone network.

16. The claimed user authentication system also includes an authentication module that receives the password from the user through a secure computer network. Claim 5 requires that the secure computer network is different from the cell phone network. Receipt of the password


activates access to the user's account. Access to the user account is deactivated after a predetermined amount of time.


17. Taken as a whole, the claimed inventions of the '658 Patent are not limited to well-understood, routine, or conventional activity. Rather, the claimed inventions include inventive components that improve upon the functioning and operation of user authentication systems. The '658 Patent also acknowledges other forms of two-factor authentication, such as the RSA SecurID product, such that the claims of the '658 Patent do not preempt the field.

18. The written description of the '658 Patent describes each of the limitations of the claims in technical detail, allowing a skilled artisan to understand the scope of the claims and how the non-conventional and non-generic combination of claim limitations is patently distinct from and improved upon what may have been considered conventional or generic in the art at the time of the invention.

19. Defendant has made, had made, used, imported, provided, supplied, distributed, sold, or offered for sale infringing products and/or systems, including, for example, but not limited to, the systems and applications Defendant uses to offer multifactor authentication services to its one-time password ("OTP") customers (the "Accused Instrumentalities").

20. The Accused Instrumentalities include, for example, but are not limited to, the systems and applications that provide two-factor authentication services to Defendant's OTP customers as described and depicted below:

[Solutions](#) [Industries](#) [Thought Leadership](#) [About Experian](#)

Client Sign In 



Multifactor authentication solutions

Effective, appropriate and low-friction multifactor authentication solutions

[Learn more >](#)

[Business](#) / [Solutions](#) / [Identity Solutions](#) / Multifactor Authentication  Share

One-time password authentication during remote transactions

Multifactor authentication services

Verify a consumer's identity during remote transactions

With the advent of newer and more adaptable communication technologies, remote transactions continue to increase. There is a need for more efficient ways to secure these transactions and prove the identity of an individual on the other end of a remote channel.

Multifactor authentication uses a combination of elements to verify a consumer's identity. It's based on the premise that an unauthorized person is unlikely to be able to supply the same proof elements as the true consumer to prove his or her identity. If one of the required components in an authentication transaction is missing or supplied incorrectly, the consumer's identity is not established with sufficient certainty to allow the requested transaction to proceed. This prevents potential fraud.

Two or more of the following credentials are used in multifactor authentication:



- **What the user knows** — Password, PIN, unique information.



- **What the user has** — Mobile phone, bankcard, token.

- **Who the user is** — Biometric verification such as fingerprint, eye iris, voice, typing speed.

Our multifactor authentication service uses a one-time password (what the user knows) delivered to the consumer's mobile phone or landline (what the user has) via a verified phone number. Through the one-time password (OTP) authentication process, businesses and government agencies can strengthen their authentication process in high-risk transactions, adhere to regulations or secure high-value consumer transactions quickly — with little to no additional impact on the consumer.

Our OTP offers organizations the option of having us create a unique alphanumeric code generated for each authentication transaction or providing us with a unique code delivered to a verified consumer phone via text or voicemail.

- How long has the consumer had the phone number?
- Is the number being forwarded?
- Is the number assigned to a prepaid phone?
- Has the number been ported?



Beyond message delivery

In addition to delivering a generic or customized alphanumeric password to the verified phone, Experian® provides other capabilities in our OTP offering:

- **Verification of phone to consumer** — Before attempting an OTP send, we independently verify that the phone number provided by the consumer can be linked to that consumer.
- **Phone attributes verification** — We validate other phone attributes, such as porting, forwarding, account tenure and contract type.
- **OTP included in final verification results** — Because our OTP service verifies consumer information, we can include the verification in the result delivered as part of the transaction.

21. The Accused Instrumentalities include, for example, but are not limited to, a computer processor and a user database that associates users (e.g., Defendant's OTP customers' users) with their personal communication device (e.g., mobile phone). Those personal communication devices are configured to communicate with the Accused Instrumentalities via a cell phone network.

22. The Accused Instrumentalities include, for example, but are not limited to, a control module that creates new passwords based at least upon a token and a passcode, wherein the token is not known to the user and the wherein the passcode is known to the user. The token includes, for example, but is not limited to, the access code provided by the Accused Instrumentalities.

23. The Accused Instrumentalities include, for example, but are not limited to, a communication module for transmitting the token to the personal communication device through the cell phone network, including, for example, but not limited to via the Short Message Service (SMS), which can also be referred to as “text” messaging as Defendant acknowledges:

Multifactor authentication services

Verify a consumer's identity during remote transactions

With the advent of newer and more adaptable communication technologies, remote transactions continue to increase. There is a need for more efficient ways to secure these transactions and prove the identity of an individual on the other end of a remote channel.

Multifactor authentication uses a combination of elements to verify a consumer's identity. It's based on the premise that an unauthorized person is unlikely to be able to supply the same proof elements as the true consumer to prove his or her identity. If one of the required components in an authentication transaction is missing or supplied incorrectly, the consumer's identity is not established with sufficient certainty to allow the requested transaction to proceed. This prevents potential fraud.

Two or more of the following credentials are used in multifactor authentication:



- **What the user knows** — Password, PIN, unique information.



- **What the user has** — Mobile phone, bankcard, token.

- **Who the user is** — Biometric verification such as fingerprint, eye iris, voice, typing speed.

Our multifactor authentication service uses a one-time password (what the user knows) delivered to the consumer's mobile phone or landline (what the user has) via a verified phone number. Through the one-time password (OTP) authentication process, businesses and government agencies can strengthen their authentication process in high-risk transactions, adhere to regulations or secure high-value consumer transactions quickly — with little to no additional impact on the consumer.

Our OTP offers organizations the option of having us create a unique alphanumeric code generated for each authentication transaction or providing us with a unique code delivered to a verified consumer phone via text or voicemail.

- How long has the consumer had the phone number?
- Is the number being forwarded?
- Is the number assigned to a prepaid phone?
- Has the number been ported?



Beyond message delivery

In addition to delivering a generic or customized alphanumeric password to the verified phone, Experian® provides other capabilities in our OTP offering:

- **Verification of phone to consumer** — Before attempting an OTP send, we independently verify that the phone number provided by the consumer can be linked to that consumer.
- **Phone attributes verification** — We validate other phone attributes, such as porting, forwarding, account tenure and contract type.
- **OTP included in final verification results** — Because our OTP service verifies consumer information, we can include the verification in the result delivered as part of the transaction.

24. The Accused Instrumentalities include, for example, but are not limited to, an authentication module that receives the user's password from the user, through a secure computer network (e.g., Defendant's multifactor authentication services). The secure computer network is different than the cell phone network. The authentication module activates access to the user's account in response to the password and deactivates the account within a predetermined amount

of time after activating the account, such that the user's account is then not accessible through any password via the secure computer network.

25. By making, having made, using, importing, providing, supplying, distributing, selling, or offering for sale the Accused Instrumentalities, Defendant has directly infringed (literally and/or under the doctrine of equivalents) at least Claim 5 of the '658 Patent. Defendant's infringement in this regard is ongoing.

26. Plaintiff has been damaged as a result of Defendant's infringing conduct as alleged above. Thus, Defendant is liable to Plaintiff in an amount that compensates it for such infringements, 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.

27. Plaintiff and/or its predecessors-in-interest have satisfied all statutory obligations required to collect pre-filing damages for the full period allowed by law for infringement of the '658 Patent.

JURY DEMAND

Plaintiff hereby requests a trial by jury on all issues so triable by right.

PRAYER FOR RELIEF

Plaintiff requests that the Court find in its favor and against Defendant, and that the Court grant Plaintiff the following relief:

a. Judgment that one or more claims of the '658 Patent have been infringed, either literally and/or under the doctrine of equivalents, by Defendant and/or all others acting in concert therewith;

b. Judgment that Defendant accounts for and pay to Plaintiff all damages to and costs incurred by Plaintiff because of Defendant's infringing activities and other conduct complained of herein;

c. Pre-judgment and post-judgment interest on the damages caused by Defendant's infringing activities and other conduct complained of herein;

d. That this Court declare this an exceptional case and award Plaintiff its reasonable attorneys' fees and costs in accordance with 35 U.S.C. § 285; and

e. All other and further relief as the Court may deem just and proper under the circumstances.

Dated: February 20, 2023

By: /s/ Fred I. Williams

Fred I. Williams

Texas State Bar No. 00794855

Michael Simons

Texas State Bar No. 24008042

WILLIAMS SIMONS & LANDIS PLLC

The Littlefield Building

601 Congress Ave., Suite 600

Austin, TX 78701

Tel: 512.543.1354

fwilliams@wsltrial.com

msimons@wsltrial.com

Todd E. Landis

Texas State Bar No. 24030226

WILLIAMS SIMONS & LANDIS PLLC

2633 McKinney Ave., Suite 130 #366

Dallas, TX 75204

Tel: 512.543.1357

tlandis@wsltrial.com

John Wittenzellner

Pennsylvania State Bar No. 308996

WILLIAMS SIMONS & LANDIS PLLC

1735 Market Street, Suite A #453

Philadelphia, PA 19103

Tel: 512.543.1373

johnw@wsltrial.com

Attorneys for Plaintiff Dynapass IP Holdings LLC