UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF INDIANA

INDIANAPOLIS DIVISION

TRANSACTION SECURE, LLC, a foreign limited liability company,

Plaintiff,

vs.

FORMSTACK, LLC, a domestic limited liability company,

Defendant.

Case No.: 1:19-cv-3703

COMPLAINT FOR PATENT INFRINGEMENT

INJUNCTIVE RELIEF DEMANDED

JURY TRIAL DEMANDED

Plaintiff, TRANSACTION SECURE, LLC, sues Defendant, FORMSTACK, LLC, and alleges:

NATURE OF THE ACTION

1. This is an action for infringement of United States Patent No. 8,738,921 under the Patent Act, 35 U.S.C. § 271, *et seq.*, based on Defendant's unauthorized commercial manufacture, use, importation, offer for sale, and sale of infringing products and services in the United States.

PARTIES

2. Plaintiff, TRANSACTION SECURE, LLC, is a foreign limited liability company.

3. Defendant, FORMSTACK, LLC, is a domestic limited liability company, organized under the laws of the State of Indiana, with its headquarters in Indianapolis and/or Fishers, Indiana. Defendant uses, sells, and/or offers to sell products and/or services in interstate commerce that infringe the '921 Patent.

SUBJECT MATTER JURISDICTION

4. This court has original jurisdiction over the subject matter of this action, pursuant to 28 U.S.C. §§ 1331 and 1338(a), because this action involves a federal question relating to patents.

PERSONAL JURISDICTION

5. The court has general *in personam* jurisdiction over Defendant because Defendant resides and is found in the State of Indiana.

VENUE

6. Venue is proper in this court, pursuant to 28 U.S.C. § 1400(b), because Defendant has a regular and established place of business in this district and resides in this district.

COUNT I

PATENT INFRINGEMENT

7. Plaintiff repeats and re-alleges paragraphs 2 through 6 by reference, as if fully set forth herein.

8. On May 27, 2014, the United States Patent & Trademark Office (USPTO) duly and legally issued the '921 Patent, entitled "System and Method for Authenticating a Person's Identity Using a Trusted Entity." A true and authentic copy of the '921 Patent is attached hereto as **Exhibit "A"** and incorporated herein by reference.

9. The '921 Patent teaches both a system and method for protecting sensitive information from identity theft and claims an advancement over two-factor authentication, which is now the predominate form of digital authentication of sensitive information.

State of the Art

10. The identity theft problem exists largely because a person's name, SSN, and birthday are frequently used and given to others to verify the person's identity. Individuals use this information to get employment, apply for a credit card, obtain a mortgage, buy a mobile phone, get healthcare, and perform numerous other transactions. A person's SSN and birthday are usually stored by businesses electronically in databases or on physical paper documents which can be viewed by many individuals within a business.

11. Once a person supplies his/her SSN and birthday, they lose control of how that information will be used and who will view that information.

12. At times, business computer systems and databases get hacked into allowing the hacker access to the person's personal identity information. At other times, the SSN and

birthday are transmitted to businesses and others electronically via the Internet.

13. The Internet is an unsecured network, so information not properly encrypted can be viewed by others on the Internet. There are various ways an impersonator or identity thief can obtain a person's SSN or birthday. The thief can obtain this information by looking at business records, viewing unencrypted messages with this information, or other types of fraud.

14. Once a thief has someone’s SSN and birthday, the thief can use that information anytime during the lifetime of the person because of the permanence of SSN and birthday and its association with the person. The SSN and birthday have been reliable indicators of a person’s existence but their widespread use by both the person and identity theft impersonators has made them of little use in authenticating the identity of person using the information.

The Patent-In-Suit

15. Plaintiff is the assignee of the entire right, title, and interest in the ‘921 Patent at the USPTO, including the right to assert causes of action arising under the ‘921 Patent.

16. The system and method of the ‘921 Patent increase the efficiency of components that use software because of the benefits claimed by the ‘921 Patent, namely flexibility and a higher degree of certainty as to authenticating that a person is who he/she claims to be. The prior art is described as uncertain because under the prior art, a user’s assurance of authentication is limited to just confirming that certain devices are what they claim to be, not that certain persons are who they claim to be.

17. Through Claim 1, the ‘921 Patent claims:

> A method for authenticating a person’s identity to a transactional entity using a trusted entity with a secure repository of a person’s personal identity information, comprising: receiving personal identity information at a trusted entity computer system, the personal identity information being confidentially stored by the trusted entity computer system; in the secure repository, storing a user identifier and a password that are associated with, but do not contain, the personal identity information; at the trusted entity computer system, receiving a request from the person for a unique code, the request including the user identifier and the password, the person’s identity having been previously authenticated by the trusted entity computer system; providing the unique code to the person, the unique code comprising a person identifier and a key, wherein the unique code is thereafter transmitted to a transactional entity to identify the person without providing the personal identity information to the transactional entity; and the trusted entity computer system confirming the unique code to the transactional

18. Through Claim 24, the ‘921 Patent claims:

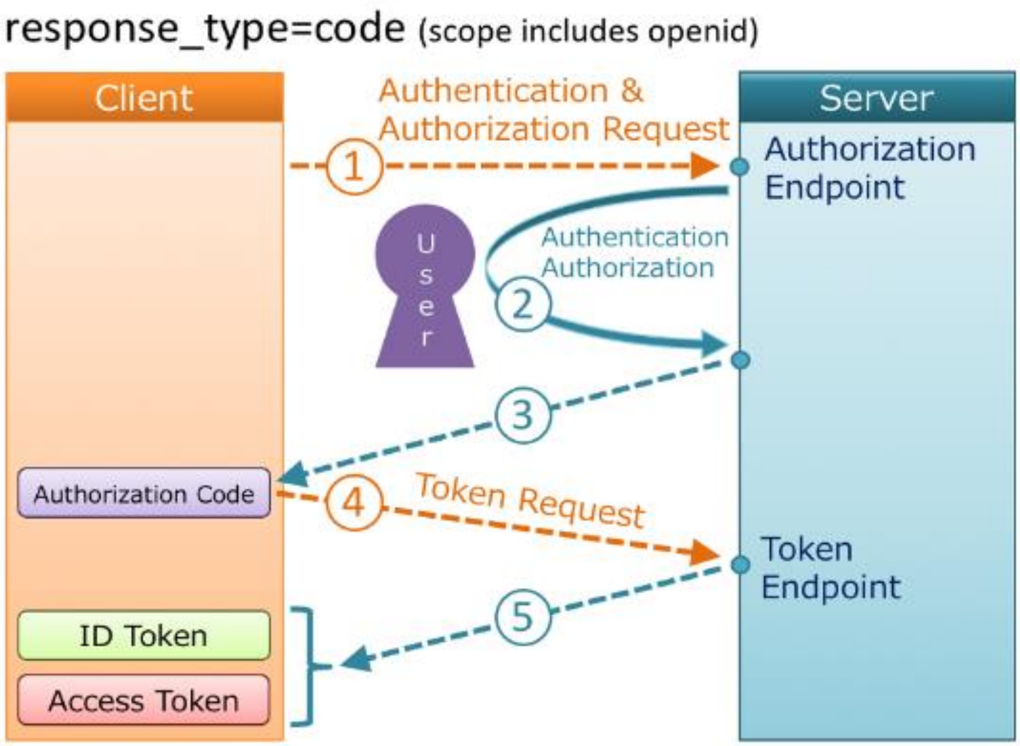
> A system for authenticating a person’s identity to a transactional entity using a trusted entity, comprising: a trusted entity which receives personal identity information from a person, the personal identity information being confidentially stored by the trusted entity; a user identifier associated with but not containing any of the personal identity information; a password associated with but not containing any of the personal identity information; a client module with a person input device for a person to enter the user identifier and the password, a person processing unit connected to the person input device to prompt the person for the user identifier and the password, and a person display unit connected to the person processing unit to display a the key associated with a person identifier to form a unique code to the person, the person’s identity having been previously authenticated by the trusted entity; a transactional processing module with an transactional input device for the transactional entity to enter the key, a transactional processing unit connected to the transactional input device to prompt the transactional entity for the key, and a transactional display unit connected to the transactional processing unit to display a message to the transactional entity authenticating the person's identity and to display a photograph of the person, whereby the photograph is a secondary verification to the unique code; and a trusted entity server with a trusted entity processing unit to process requests from the client module and the transactional processing module using a network, and a database accessible to the trusted entity processing unit to store the user identifier, the password, the unique code, and the person's personal identity information, including the photograph.

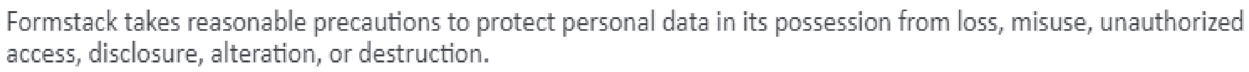
19. Overall, the claims of the ‘921 Patent do not merely gather, analyze, and output data. Indeed, the ‘921 Patent does not merely add an algorithm to old data and generate new data. Instead, the ‘921 Patent teaches a system and method that is not concerned with manipulation of data, but rather, an improvement in the state of the art no matter what the underlying data describes.

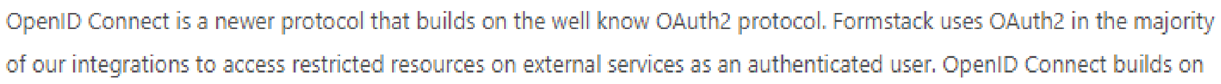
20. Defendant infringes at least Claim 1 of the ‘921 Patent through an authentication method it uses, along with a system for authenticating a person’s identity, which such method is disclosed at: https://medium.com/@darutk/diagrams-of-all-the-openid-connect-flows-6968e3990660.

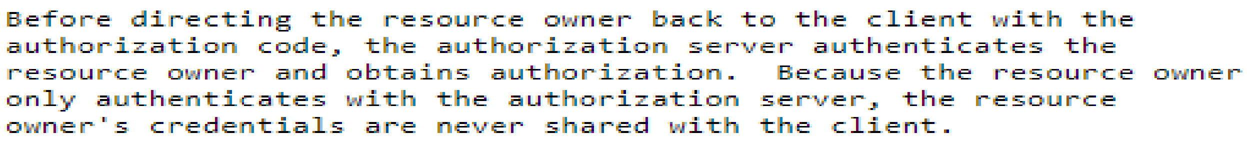
21. Defendant’s website operates as the Accused Product.

22. The Accused Product is a trusted entity, as claimed by Plaintiff, to authenticate account holders when such holders want to access a service from a resource server (i.e., a transactional entity), by using non-personal information for securing personal data:




Formstack takes reasonable precautions to protect personal data in its possession from loss, misuse, unauthorized access, disclosure, alteration, or destruction.


OpenID Connect is a newer protocol that builds on the well know OAuth2 protocol. Formstack uses OAuth2 in the majority of our integrations to access restricted resources on external services as an authenticated user. OpenID Connect builds on


```
Before directing the resource owner back to the client with the
authorization code, the authorization server authenticates the
resource owner and obtains authorization.  Because the resource owner
only authenticates with the authorization server, the resource
owner's credentials are never shared with the client.
```

23. The Accused Product receives personal information from users at a trusted entity computer system, such as their name, age, birthdate, email address, phone number etc. when users create an account. Defendant then confidentially stores this data for promoting safety and security, throgh a process explained at https://www.formstack.com/privacy.

24. Defendant, in a secure repository, provides users with authorization login details (i.e., user identifier and password) that they are associated with, but the login details do not contain the personal details:

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase®
Smarter legal research.