Coleman W. Watson, Esq. (SBN 266015)
coleman@watsonllp.com
WATSON LLP
601 S. Figueroa Street, Suite 4050
Los Angeles, CA 90017
Telephone: 213.228.3233
Facsimile: 213.330.4222

Attorneys for Plaintiff, Transaction Secure, LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

TRANSACTION SECURE, LLC, a foreign limited liability company, Plaintiff, vs. STRIPE, INC., a foreign corporation, Defendant.	Case No.: 5:19-cv-04052-EJD **AMENDED COMPLAINT FOR PATENT INFRINGEMENT** **DEMAND FOR INJUNCTIVE RELIEF** **DEMAND FOR JURY TRIAL**

Plaintiff, TRANSACTION SECURE, LLC, sues Defendant, STRIPE, INC., and alleges as follows:

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, STRIPE, INC., is a foreign corporation, organized under the laws of the State of Delaware, with its headquarters in San Francisco, California. 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 California.

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.

INTRADISTRICT ASSIGNMENT

7. Pursuant to Local Civil Rule 3-2(d), this action is properly assigned to the San Jose Division because the Court transferred this action to this Division from the San Francisco Division.

COUNT I

PATENT INFRINGEMENT

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

9. 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.

10. 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

11. 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 electronically by businesses in databases or on physical paper documents which can be viewed by many individuals within a business.

12. 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.

13. 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.

14. 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.

15. 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

16. Plaintiff is the assignee of the entire right, title, and interest in the '921 Patent, including the right to assert causes of action arising under the '921 Patent.

17. 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.

18. The '921 Patent provides a solution to this problem by both reducing the number of times that personal identity information is exposed on the Internet and generating unique alpha-numeric codes that are encrypted with specific personal identity information that must match authentication requests.

19. 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 entity to verify the person's identity.

20. 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.

21. Claim 1 represents an improvement in the art because a trusted entity independently authenticates a person's identity based on a series of information provided by a person to the trusted entity. This, in turn, eliminates the need for a transactional entity to independently authenticate a person's identity, which significantly reduces costs to the transactional entity. In fact, under the method claimed, a person does not provide his or her personal identity information to a

transactional entity. Because the method gives the transactional entity greater confidence in authentication without the need to actually expose personal identity information, the identity theft problem is reduced.

22. The '921 Patent further represents an improvement in computer technology because under the method claimed, authentication is achieved by a trusted entity and a transactional entity matching encrypted alpha-numeric codes that contain undecipherable information to the human eye, whereas in the prior art, authentication was achieved by only a person and a transactional entity (or many different transactional entities). The '921 Patent reduces the identity theft problem by relying solely on authentication between the trusted entity and transactional entity, both of whom are already in the business of handling and adequately protecting confidential information, unlike a person.

23. Overall, the claims of the '921 Patent do not merely gather, analyze, and output data, nor does the '921 Patent merely add an algorithm to old data to 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. Under the method claimed, the '921 Patent transforms personal identity information (SSN, birthdate, etc.) that is easily decipherable by providing a unique alpha-numeric code containing that same information that is undecipherable to the human eye, which mitigates the possibility of identity theft.

24. Thus, the risk of fraud is much lower under the '921 Patent because the unique alpha-numeric code has no value to an identity thief and a trusted entity will only authenticate such code if it is received by a transactional entity.

25. Identity theft is a problem uniquely suited to the Internet because it rarely requires "real world" evidence to confirm a person's identity, and the pure exchange of digital information allows identity thieves to capitalize on stealing

identities. Thus, technological advancements in digital information has made it the predominant form of communication, which has created a problem unique to digital information. The method claimed by the '921 Patent addresses this problem through a technological advancement over two-factor authentication by requiring a person to verify their personal identity information to a trusted entity, who then guards against identity theft by generating the unique alpha-numeric codes and then matching these codes only against transactional entities. The end result of this method is to ensure that persons are authenticated, not simply that devices are authenticated, which was the state of the art in two factor authentication.

26. 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://stripe.com/docs/connect/quickstart and https://stripe.com/docs/connect/express-accounts.

27. Defendant's website operates as the Accused Product.

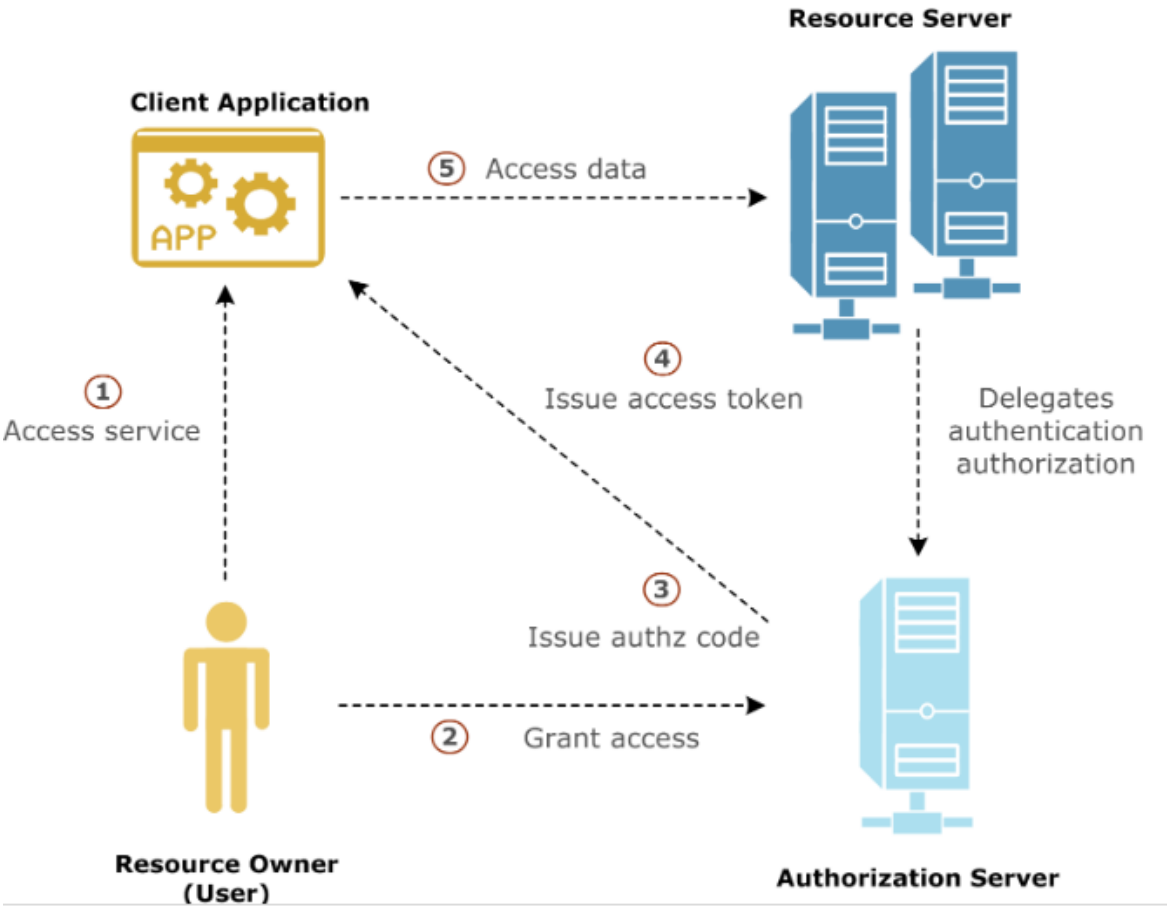
28. The Accused Product is a trusted entity, as claimed by Plaintiff, to authenticate account holders when such holders want to access a service from a resource server (i.e., a transactional entity), by using non-personal information for securing personal data:

> Using Express accounts is the easiest way for your platform to onboard users with Connect. When you use Express accounts, Stripe collects banking information from your users and handles identity verification, reducing the work that would otherwise be the responsibility of your platform. A live Express integration

The OAuth connection flow

An Express account connects to your platform using an OAuth flow:

1. Starting on your site, the user clicks a link that takes them to Stripe and includes your platform's `client_id`.
2. On Stripe's website, the user provides the necessary contact and payout information.
3. The user is redirected back to your site along with an authorization code.
4. Finally, your site makes a request to our OAuth token endpoint to complete the connection and fetch the user's new Stripe account ID.



Stripe provides a unique identifier for your platform called a `client_id`.

Stripe offers a standard OAuth 2.0 flow to connect to Stripe accounts. To complete the flow, you need a page that starts the connection process, and a page to which users are directed after connecting their accounts. The redirect page is the same as your `redirect_uri`.

OAuth also enables resource owners (end users) to authorize limited third-party access to their server resources without sharing their credentials.

29. 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://stripe.com/us/privacy.

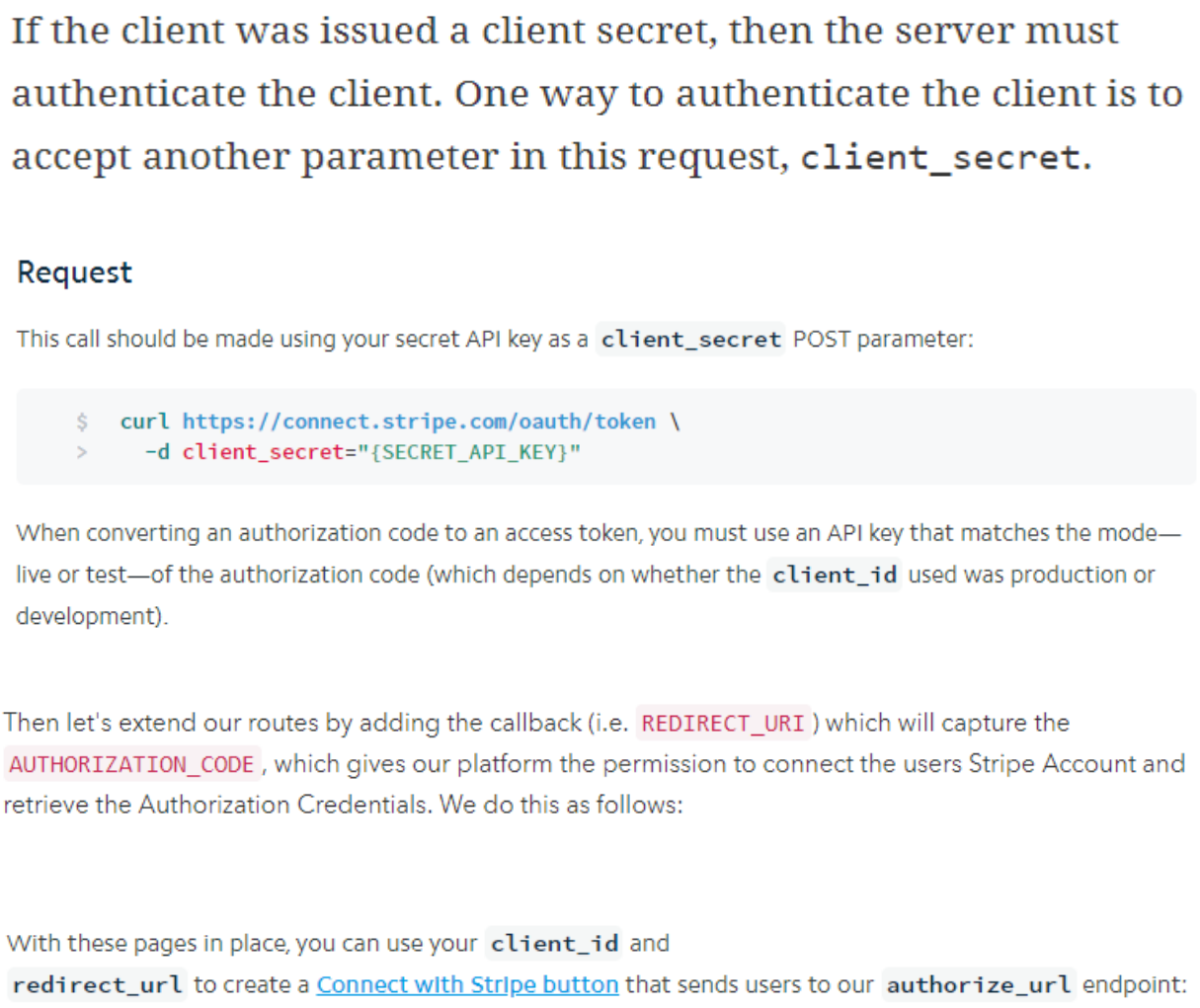
30. Defendant, in a secure repository, provides users with authorization login details (i.e., user identifier and password) that they are associated with, but the login details do not contain the personal details:

Before you can begin the flow, you'll need to register a client and create a user. Registration will give you a client ID an secret your application will use during the OAuth flow.

- Your `client_id`, a unique identifier for your platform, generated by Stripe

OAuth 2.0 is an open standard for authorization that enables client applications to access server resources on behalf of a specific *resource owner*. OAuth also enables resource owners (end users) to authorize limited third-party access to their server resources without sharing their credentials. For example, a Gmail user could allow LinkedIn or Flickr to have access to their list of contacts without sharing their Gmail user name and password.

31. The user then requests Defendant for resource access to a trusted entity computer system. The request includes the user identifier and the password. Defendant provides an authorization code to obtain an access token and ID token for accessing the services:



If the client was issued a client secret, then the server must authenticate the client. One way to authenticate the client is to accept another parameter in this request, `client_secret`.

Request

This call should be made using your secret API key as a `client_secret` POST parameter:

```
$ curl https://connect.stripe.com/oauth/token \
> -d client_secret="{SECRET_API_KEY}"
```

When converting an authorization code to an access token, you must use an API key that matches the mode—live or test—of the authorization code (which depends on whether the `client_id` used was production or development).

Then let's extend our routes by adding the callback (i.e. `REDIRECT_URI`) which will capture the `AUTHORIZATION_CODE`, which gives our platform the permission to connect the users Stripe Account and retrieve the Authorization Credentials. We do this as follows:

With these pages in place, you can use your `client_id` and `redirect_url` to create a Connect with Stripe button that sends users to our `authorize_url` endpoint:

32. Defendant provides a unique authorization code to the user in response of the request of the user, just as in the '921 Patent, which includes a user identified and access key, wherein the unique code is thereafter transmitted to a transactional entity to authenticate the user's identity without giving personal information to the transactional entity to mitigate against the risk of identity theft.

33. The unique authorization code is required to obtain an access token. This access token then used by the user for accessing the services.

34. In the Accused Product, the user identity is verified by the resource server by using the authorization code to allow the user to access the code:

35. Upon information and belief, Defendant has known of the existence of

the '921 Patent, and its acts of infringement have been willful and/or in disregard for the '921 Patent, without any reasonable basis for believing that it had a right to engage in the infringing conduct.

36. Defendant's acts of infringement of the '921 Patent have caused and will continue to cause Plaintiff damages for which Plaintiff is entitled to compensation pursuant to 35 U.S.C. § 284.

37. Defendant's acts of infringement of the '921 Patent have caused and will continue to cause Plaintiff immediate and irreparable harm unless such infringing activities are also enjoined by this court pursuant to 35 U.S.C. § 283. Plaintiff has no adequate remedy at law.

38. Upon information and belief, the '921 Patent, at all times material, was and is in compliance with 35 U.S.C. § 287.

WHEREFORE, Plaintiff, TRANSACTION SECURE, LLC, demands judgment against Defendant, STRIPE, INC., and respectfully seeks the entry of an order (i) adjudging that Defendant has infringed the '921 Patent, in violation of 35 U.S.C. § 271; (ii) granting an injunction enjoining Defendant, its employees, agents, officers, directors, attorneys, successors, affiliates, subsidiaries and assigns, and all of those in active concert and participation with any of the foregoing persons or entities from infringing the '921 Patent; (iii) ordering Defendant to account and pay damages adequate to compensate Plaintiff for Defendant's infringement of the '921 Patent, with pre-judgment and post-judgment interest and costs, pursuant to 35 U.S.C. § 284; (iv) ordering that the damages award be increased up to three times the actual amount assessed, pursuant to 35 U.S.C. § 284; (v) declaring this case exceptional and awarding Plaintiff its reasonable attorneys' fees, pursuant to 35 U.S.C. § 285; and, (vi) awarding such other and further relief as this court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, TRANSACTION SECURE, LLC, hereby demands a trial by jury of all issues so triable pursuant Fed. R. Civ. P. 38.

/s/ *Coleman Watson*
Coleman W. Watson, Esq.

DATED on September 30, 2019

Respectfully submitted,

WATSON LLP

/s/ Coleman Watson

Coleman W. Watson, Esq.
California Bar No. 266015
Florida Bar. No. 0087288
Georgia Bar No. 317133
New York Bar No. 4850004
coleman@watsonllp.com
docketing@watsonllp.com

WATSON LLP
601 S. Figueroa Street, Suite 4050
Los Angeles, CA 90017
Telephone: 213.228.3233
Facsimile: 213.330.4222

Attorneys for Plaintiff, Transaction Secure, LLC