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

Autoscribe Corporation	§	
	§	
***Plaintiff*,**	§	
	§	
v.	§	**Civil Action No. _____**
	§	
Repay Holdings Corporation and Repay Holdings, LLC	§	**JURY TRIAL DEMANDED**
	§	
	§	
***Defendant*.**	§	
	§	

PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Autoscribe Corporation ("Autoscribe" or "Plaintiff") hereby submits this Original Complaint for patent infringement against Defendants Repay Holdings Corporation and Repay Holdings, LLC (together, "REPAY" or "Defendant") and alleges, based on its own personal knowledge with respect to its own actions and based upon information and belief with respect to all others' actions, as follows:

I. THE PARTIES

1. Autoscribe is a Corporation organized under the laws of the state of Maryland with its principal place of business at 12276 San Jose Blvd, Suite 624, Jacksonville, FL 32223.

2. Repay Holdings Corporation is a corporation organized under the laws of Delaware, with its headquarters at 3 West Paces Ferry Road Suite 200 Atlanta, GA 30305, and with a regular and established place of business at 5830 Crescent Drive, Suite 100, The Colony, TX 75056. Repay Holdings Corporation can be served through its registered agent: The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE, 19801.

3. Repay Holdings, LLC is a limited liability company organized under the laws of

Delaware, with its headquarters at 3 West Paces Ferry Road Suite 200 Atlanta, Georgia 30305, and with a regular and established place of business at 5830 Crescent Drive, Suite 100, The Colony, TX 75056. Repay Holdings, LLC can be served through its registered agent: The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE, 19801.

II. JURISDICTION AND VENUE

4. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a) because this action arises under the patent laws of the United States, 35 U.S.C. § 1 *et seq.*, including 35 U.S.C. § 271.

5. As discussed in greater detail below, Defendant has committed acts of patent infringement and/or has induced and/or contributed to acts of patent infringement by others in this judicial district, the State of Texas, and elsewhere in the United States, by making, using, offering for sale, selling, or importing various products or services that infringe Autoscribe's Asserted Patent (defined below).

6. As mentioned above, Defendant has a regular and established place of business in the District at 5830 Crescent Drive, Suite 100, The Colony, TX 75056. This location is one of Defendant's "principal facilities," and at 14,100 square feet, it is Defendant's largest facility.[1] This location is a physical place located in the District, and it is held out as a regular and established place of business of Defendant, including by signage indicating that it operates out of the building. Defendant is currently advertising several job postings at this location, including postings for a "Sr. Software Engineer" (the responsibilities of which include "[b]uilding and enhancing our core API, user interfaces, and backend processing systems" and "Developing and

[1] https://www.sec.gov/ix?doc=/Archives/edgar/data/1720592/000095017023005561/rpay-20221231.htm#item_2_properties (last visited July 26, 2023).

deploying to cloud-based technology") and a "Product Owner" (the responsibilities of which include "[d]efining and refining, with an Architect, the payment processing services serving all REPAY's merchants" and "[b]uilding a library of payment services with mature API definition").[2]

7. Additionally, Defendant has customers in the District, including, *e.g.*, Daimler Truck Financial Services USA LLC.[3]

8. The Court has personal jurisdiction over Defendant, in part, because Defendant has minimum contacts within the State of Texas; Defendant has purposefully availed itself of the privileges of conducting business in the State of Texas; Defendant regularly conducts business within the State of Texas; and Plaintiffs' causes of action arise directly from Defendant's business contacts and other activities in the State of Texas, including by virtue of Defendant's infringement in the State of Texas. More specifically, Defendant is subject to the Court's general jurisdiction, in part, due to its continuous and systematic contacts with the State of Texas. Further, Defendant is subject to the Court's specific jurisdiction, in part, because Defendant has committed patent infringement and/or has induced and/or contributed to acts of infringement by others in the State of Texas and because Defendant has a place of business in the State of Texas such that assertion of personal jurisdiction is reasonable and fair.

9. Venue is proper in this judicial District under 28 U.S.C. § 1400(b) because Defendant has committed patent infringement and/or has induced and/or contributed to acts of infringement by others in the District and has a regular and established place of business in the District, as discussed above.

---

[2] https://repay.wd1.myworkdayjobs.com/REPAYCareers (last visited July 26, 2023).
[3] https://dtf.repay.io/ebpp/#/ (last visited July 26, 2023).

III. BACKGROUND

10. Fraud in credit card and other financial transactions is a major problem, particularly in the online marketplace. Considerable resources are devoted to securing credit card and other account information provided to online merchants by payers. A single breach of security incident can compromise millions of credit card accounts, and such breaches are reported on a regular basis. As such, customers' financial data are sensitive in nature and are subject to strict regulations. Companies that fail to adequately protect customers' credit card data may face significant legal and regulatory consequences.

11. Autoscribe is a leading financial services company and payment processor, currently processing more than $2 billion in transactions annually and servicing thousands of financial institutions and corporate billers across the nation. As part of its mission, Autoscribe has invested significant resources and capital into developing new technologies to facilitate transactions and assist billers in meeting their compliance needs while minimizing costs and complexity.

12. Autoscribe has protected these technologies with a robust and growing patent portfolio.

13. On April 4, 2023, the United States Patent and Trademark Office ("USPTO") duly and legally issued United States Patent No. 11,620,621 ("the '621 Patent" or "the Asserted Patent"), titled "Enrolling a payer by a merchant server operated by or for the benefit of a payee and processing a payment from the payer by a secure server." The Asserted Patent is valid and enforceable.

14. The Asserted Patent is directed to "systems and methods for obtaining and using account information to process financial payments."

15. Autoscribe is the original applicant and the sole and exclusive owner of all rights,

title, and interest in the Asserted Patent, including the sole and exclusive right to prosecute this action, to enforce the Asserted Patent against infringers, to collect damages for past, present and future infringement of the Asserted Patent, and to seek injunctive relief as appropriate under the law.

16. Plaintiff has complied with any marking requirements under 35 U.S.C. § 287 with regard to the Asserted Patent.

17. Defendant is a financial technology company that mainly provides payment processing services and solutions. In 2022, it processed approximately $25.7 billion of card payments and generated approximately $280 million in annual revenues. Most of the revenues are derived from volume-based payment processing fees and other related fixed per transaction fees.

18. As discussed in greater detail below, Defendant provides processing solutions, including its "Payment API," that are covered by the Asserted Patent.

19. Defendant competes directly against Autoscribe, including through its "Payment API," causing Autoscribe to lose significant profits.

20. Accordingly, Defendant's infringement, as described below, has injured, and continues to injure Autoscribe.

IV. COUNT I: INFRINGEMENT OF THE ASSERTED PATENT

21. Autoscribe incorporates each of the allegations of paragraphs 1–20 above.

22. Defendant has directly infringed and continues to directly infringe the Asserted Patent by, for example, making, using, offering to sell, selling, and/or importing into the United States, without authority, products or services that practice one or more claims of the Asserted Patent.

23. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell

or import any products or services that embody the inventions of the Asserted Patent in the United States.

24. Defendant has and continues to directly infringe one or more claims of the Asserted Patent, including, for example, claim 1, either literally or under the doctrine of equivalents, by performing every step of the claimed method in violation of 35 U.S.C. § 271.

25. Defendant's infringing services include, for example, the services Defendant provides through its "Payment API," as well as any other similar methods performed by Defendant (collectively, the "Infringing Methods").

26. For example, Representative Claim 1 of the Asserted Patent claims:

> A method of processing a payment transaction from a payer to a payee, the method being performed by one or more secure servers, the method comprising:
>
> > providing, by the one or more secure servers to a merchant server providing a webpage to a payer computing system used by the payer, an application programming interface (API) that:
> >
> > provides financial account registration and token retrieval functions that can be executed to process the payment transaction;
> >
> > provides access to the financial account registration and token retrieval functions to the merchant server;
> >
> > receives, from the merchant server via the API, at least one data element associated with the payer and a payment amount from the payer to the payee;
> >
> > authenticates the payee; and
> >
> > executes the financial account registration function, upon initiation by the merchant server, by:
> >
> > > generating a uniform resource locator (URL), for establishing a secure socket layer connection via the internet between the secure server and the payer computing system, the URL comprising either:
> > >
> > > > a dynamic URL generated by the secure server for the payer and the payee; or a static URL and a hypertext

transport protocol (HTTP) parameter used by the secure server to identify the payer and the payee;

establishing the secure socket layer connection, in response to an HTTP request received from the merchant server for the generated URL, between the secure server and the payer computing system within a window or frame that is displayed within the webpage provided by the merchant server;

outputting instructions to the payer computing system, in response to the HTTP request for the generated URL, to render a financial account registration request form, within the window or frame that is displayed within the webpage provided by the merchant server, that provides functionality for the payer to provide sensitive financial account information associated with a financial account; and

outputting instructions to the payer computing system, in response to the HTTP request for the generated URL, to encrypt the sensitive financial account information provided by the payer and transmit the encrypted financial account information to the secure server via the secure socket layer connection;

receiving the sensitive financial account information provided by the payer via the secure socket layer connection;

storing the sensitive financial account information in a secure storage location and performing each software process required to maintain compliance with one or more information security standards;

executing a token retrieval function, upon initiation by the merchant server via the API, by:

providing a non-sensitive electronic data token representing the sensitive financial account information to the merchant server without providing the sensitive financial account information to the merchant server and without providing the non-sensitive electronic data token to the payer; and

processing the payment transaction using the sensitive financial account information by generating and transmitting an electronic request requesting the payment amount from the financial account, obtaining the payment amount, and forwarding at least a portion of the payment amount to the payee.

27. Through its Payment API, Defendant performs a method of processing a payment transaction from a payer to a payee, the method being performed by one or more secure servers

and meeting every element of Claim 1. The figure below is an excerpt from Defendant's documentation providing an overview of the purpose of the Payment API:[4]

Alliance Financing

This collection was created for {{Merchant Name}} to connect to REPAY's Platform for channels like SMS, IVR, Mobile and other external payments and payment management.

REPAY API

This collection contains the API requests that allow for interaction with the REPAY API which can be used for iFrame, payment level api to populate our reporting, channels like SMS, IVR, Mobile etc.

Payment API

The REPAY API is a full collection of endpoints that supports everything from provisioning users to making payments.

This folder will contain calls for unteracting with the service in the most ideal way to make payments both via token and sending full card data so that any application can send payment data via API completly OR by using our hosted checkout forms via iframe or other embedded solutions or redirects.

28. Defendant provides, by the one or more secure servers to a merchant server providing a webpage to a payer computing system used by the payer, an application programming interface (API). This is shown by, *e.g.*, the following excerpts from Defendant's documentation for its Payment API:[5]

[4] https://www.postman.com/repay-api-nation/workspace/repay-api-nation-s-public-workspace/documentation/9781366-91da388b-d862-4980-a2ba-2aca6d0420cb (last visited July 26, 2023).
[5] *Id.*

REPAY API

This collection contains the API requests that allow for interaction with the REPAY API which can be used for iFrame, payment level api to populate our reporting, channels like SMS, IVR, Mobile etc.

Payment API

The REPAY API is a full collection of endpoints that supports everything from provisioning users to making payments.

This folder will contain calls for unteracting with the service in the most ideal way to make payments both via token and sending full card data so that any application can send payment data via API completly OR by using our hosted checkout forms via iframe or other embedded solutions or redirects.

29. It provides financial account registration and token retrieval functions that can be executed to process the payment transaction. This is shown by, *e.g.*, the functions described in the "Card Payment" folder of the "Hosted Payments" section of the Payment API documentation:[6]

Card Payment

This folder contains the calls necessary to request a one time use url to send a user to for entering full card data on our hosted page to make AND make a payment vs just storing it with a 0.00 auth (previous call)

[6] *Id.* at "Hosted Payments" / "Card Payment" (last visited July 26, 2023).

POST **3rd -- Card Remit Webhook** Open Request→

"Your URL"

This is the information that will be passed back to the Webhook when a Card is stored within the Card Vault. The payment_method field will identify that the information stored is a Card-related or ACH.

You can wait for this event to be sent OR you can make the next request to lookup tokens by account on demand.

`stored_payment_id` = token from Retrieve vault tokens.

30. It provides access to the financial account registration and token retrieval functions to the merchant server. This is shown by, *e.g.*, the "calls" described in the "Card Payment" folder of the "Hosted Payments" section of the Payment API documentation:[7]

Card Payment

This folder contains the calls necessary to request a one time use url to send a user to for entering full card data on our hosted page to make AND make a payment vs just storing it with a 0.00 auth (previous call)

31. It receives, from the merchant server via the API, at least one data element associated with the payer and a payment amount from the payer to the payee. This is shown by, *e.g.*, the "amount" and "customer_id" in the "Get One-Time Use URL" portion of the "Card Payment" folder of the Payment API documentation:[8]

---

[7] https://www.postman.com/repay-api-nation/workspace/repay-api-nation-s-public-workspace/documentation/9781366-91da388b-d862-4980-a2ba-2aca6d0420cb (last visited July 26, 2023).

[8] *Id.* at "Hosted Payments" / "Card Payment" (last visited July 26, 2023).

POST 2nd -- Get One-Time Use URL Open Request→

https://{{subdomain}}.repay.io/checkout/merchant/api/v1/checkout-forms/{{checkout-form.id-card}}/paytoken

This endpoint returns a URL that may be used once and will remain active for a period of time to either embed in a host application or the user is redirected to this URL, provides the requite information to store payment info and then can be loaded automatically back to the host application via a callback URL or can be allowed to exit the process once paymnt is completed.

Field Name	Description	Example Data	Required or Optional
amount	Payment Amount	100.25	Required
customer_id	Contains the unique customer identification number	1023, 01-321	Required
transaction_type	Designates the transaction call type	auth, sale, scheduled_sale	Required
Source	Identity of the call to Repay.io	YourInstitutionName	Required

32. It authenticates the payee. This is shown by, *e.g.*, the "Authorization" request header in the "Card Payment" folder of the Payment API documentation:[9]

[9] *Id.*

POST 2nd -- Get One-Time Use URL Open Request→

https://{{subdomain}}.repay.io/checkout/merchant/api/v1/checkout-forms/{{checkout-form.id-card}}/paytoken

This endpoint returns a URL that may be used once and will remain active for a period of time to either embed in a host application or the user is redirected to this URL, provides the requite information to store payment info and then can be loaded automatically back to the host application via a callback URL or can be allowed to exit the process once paymnt is completed.

Field Name	Description	Example Data	Required or Optional
amount	Payment Amount	100.25	Required
customer_id	Contains the unique customer identification number	1023, 01-321	Required
transaction_type	Designates the transaction call type	auth, sale, scheduled_sale	Required
Source	Identity of the call to Repay.io	YourInstitutionName	Required

Request Headers

Authorization	apptoken {{apptoken}}
Content-Type	application/json

33. It executes the financial account registration function, upon initiation by the merchant server, by:

a. (i) Generating a uniform resource locator (URL), for establishing a secure socket layer connection via the internet between the secure server and the payer computing system, the URL comprising either: a dynamic URL generated by the secure server for the payer and the payee; or a static URL and a hypertext transport protocol (HTTP) parameter used by the secure server to identify the payer and the payee. This is shown by, *e.g.*, the "one-time use URL" described in

the "Card Payment" folder of the Payment API documentation:[10]

POST 2nd -- Get One-Time Use URL Open Request→

https://{{subdomain}}.repay.io/checkout/merchant/api/v1/checkout-forms/{{checkout-form.id-card}}/paytoken

This endpoint returns a URL that may be used once and will remain active for a period of time to either embed in a host application or the user is redirected to this URL, provides the requite information to store payment info and then can be loaded automatically back to the host application via a callback URL or can be allowed to exit the process once paymnt is completed.

Field Name	Description	Example Data	Required or Optional
amount	Payment Amount	100.25	Required
customer_id	Contains the unique customer identification number	1023, 01-321	Required
transaction_type	Designates the transaction call type	auth, sale, scheduled_sale	Required
Source	Identity of the call to Repay.io	YourInstitutionName	Required

Response

Body Headers (10) 200 OK

json


```
{
    "url": "https://{{subdomain}}.repay.io/checkout/#/checkout-form/51a32dd5-207b-4405-9477-f48de90562d3/eyJjdXN0b21lcl9pZCI6ICIxMjM0NTYiLCAicGF5dG9rZW4iOiAiN2piVkdoSU0yQ25LbkdWcE5UeDFYVmhXSnlGSndTWmQ5UTJuc0w2N0xrdms1WFVfa20uRFUtZ2pRLkxBRVpUQUdwQTFOVWx5UUY4ZGI5MnJPeGdqbyIsICJ0cmFuc2FjdGlvbl90eXBlIjogImF1dGgiLCAiYW1vdW50IjogIjAuMDAifQ==" }
```


b. (ii) Establishing the secure socket layer connection, in response to an HTTP request received from the merchant server for the generated URL, between the secure server and the payer computing system within a window or frame that is

[10] *Id.*

displayed within the webpage provided by the merchant server. This is shown by, *e.g.*, the description of the "one-time use URL" in the "Card Payment" folder of the Payment API documentation:[11]

POST 2nd -- Get One-Time Use URL Open Request→

https://{{subdomain}}.repay.io/checkout/merchant/api/v1/checkout-forms/{{checkout-form.id-card}}/paytoken

This endpoint returns a URL that may be used once and will remain active for a period of time to either embed in a host application or the user is redirected to this URL, provides the requite information to store payment info and then can be loaded automatically back to the host application via a callback URL or can be allowed to exit the process once paymnt is completed.

Field Name	Description	Example Data	Required or Optional
amount	Payment Amount	100.25	Required
customer_id	Contains the unique customer identification number	1023, 01-321	Required
transaction_type	Designates the transaction call type	auth, sale, scheduled_sale	Required
Source	Identity of the call to Repay.io	YourInstitutionName	Required

c. (iii) Outputting instructions to the payer computing system, in response to the HTTP request for the generated URL, to render a financial account registration request form, within the window or frame that is displayed within the webpage provided by the merchant server, that provides functionality for the payer to provide sensitive financial account information associated with a financial account. This is shown by, *e.g.*, the description of the purpose of the "Card

[11] *Id.*

Payment" folder and the description of the "Checkout Form":[12]

Card Payment

This folder contains the calls necessary to request a one time use url to send a user to for entering full card data on our hosted page to make AND make a payment vs just storing it with a 0.00 auth (previous call)

POST 1st -- Get Checkout Form ID Open Request→

https://{{subdomain}}.repay.io/checkout/merchant/api/v1/checkout

Getting the proper checkout form

When making any payment to REPAY one of the most important items to account for is how the payment, payment method, and customer will all be segemented for the merchant. There may be minimal routing of transacitons for a merchant or several scenarios that require REPAY's rule engine to be used.

To accomodate all merchants it is a *best* preactice to dynamically check REPAY for the proper checkout form to use for each transaction. At a minimum that means passing some data point to this endpoint.

The body of this request is an example that would allow us to return unique checkout forms based on the payment method type and Source of a transaciton; for exmaple we might require cvv for a Source of "customer portal"; where for "merchant portal" we do not (though it is best to aways require cvv).

Additionally as an example we might allow a Source of "merchant portal" to edit the amount of a payment on the REPAY form where this value is read only if the Source of "customer portal" is set (each Source will return a different id)

d. (iv) And outputting instructions to the payer computing system, in response to the HTTP request for the generated URL, to encrypt the sensitive financial account information provided by the payer and transmit the encrypted financial account information to the secure server via the secure socket layer connection. This is shown by, *e.g.*, the same portions of the Payment API documentation discussed in the previous paragraph

[12] https://www.postman.com/repay-api-nation/workspace/repay-api-nation-s-public-workspace/documentation/9781366-91da388b-d862-4980-a2ba-2aca6d0420cb (last visited July 26, 2023); *Id.* at "Hosted Payments" / "Card Payment" (last visited July 26, 2023).

and by the "one-time use URL":[13]

```
{
    "url": "https://{{subdomain}}.repay.io/checkout/#/checkout-form/51a32dd5-207b-4405-9477-f48de90562d3/eyJj
}
```

34. Defendant receives the sensitive financial account information provided by the payer via the secure socket layer connection. This is shown by, *e.g.*, the same portions of the Payment API documentation discussed in the previous paragraph and by the description of the "Get One-Time Use URL" portion of the "Card Payment" folder of the Payment API documentation:[14]

POST 2nd -- Get One-Time Use URL Open Request→

https://{{subdomain}}.repay.io/checkout/merchant/api/v1/checkout-forms/{{checkout-form.id-card}}/paytoken

This endpoint returns a URL that may be used once and will remain active for a period of time to either embed in a host application or the user is redirected to this URL, provides the requite information to store payment info and then can be loaded automatically back to the host application via a callback URL or can be allowed to exit the process once paymnt is completed.

Field Name	Description	Example Data	Required or Optional
amount	Payment Amount	100.25	Required
customer_id	Contains the unique customer identification number	1023, 01-321	Required
transaction_type	Designates the transaction call type	auth, sale, scheduled_sale	Required
Source	Identity of the call to Repay.io	YourInstitutionName	Required

35. Defendant stores the sensitive financial account information in a secure storage

[13] *Id.*
[14] *Id.*

location and performs each software process required to maintain compliance with one or more information security standards. This is shown by, *e.g.*, the description of "Hosted Payments" in the Payment API documentation:[15]

Hosted Payments

This folder contains requests that ultimately return a one-time use URL that users can be directed to in-line or can be embedded in an application but allows REPAY to capture the payment details and lower the PCI scope of the connecting application.

If it is determined users should be directed to the URL, a callback URL can be set and auto-loaded so the user is returned to the parent application.

Finally webhook samples are present with instructions on when in the processes they can be reeived and if customized will be updated samples of the customized data.

36. Defendant executes a token retrieval function, upon initiation by the merchant server via the API, by: providing a non-sensitive electronic data token representing the sensitive financial account information to the merchant server without providing the sensitive financial account information to the merchant server and without providing the non-sensitive electronic data token to the payer; and processing the payment transaction using the sensitive financial account information by generating and transmitting an electronic request requesting the payment amount from the financial account, obtaining the payment amount, and forwarding at least a portion of the payment amount to the payee. For example, the "tokens" described in the Payment API documentation show "a non-sensitive electronic data token," and the "Card Payment" folder in the documentation shows that it processes a payment:[16]

---

[15] https://www.postman.com/repay-api-nation/workspace/repay-api-nation-s-public-workspace/documentation/9781366-91da388b-d862-4980-a2ba-2aca6d0420cb (last visited July 26, 2023).
[16] *Id*.

POST **3rd -- Card Remit Webhook** Open Request→

"Your URL"

This is the information that will be passed back to the Webhook when a Card is stored within the Card Vault. The payment_method field will identify that the information stored is a Card-related or ACH.

You can wait for this event to be sent OR you can make the next request to lookup tokens by account on demand.

`stored_payment_id` = token from Retrieve vault tokens.

GET **OR Retrieve Vault Tokens** Open Request→

https://{{subdomain}}.repay.io/checkout/merchant/api/v1/customers/{{customer_id}}/vault-tokens

This endpoint allows you pass in the customer_id that was used when storing a payment method and return the tokens and associated token details.

Card Payment

This folder contains the calls necessary to request a one time use url to send a user to for entering full card data on our hosted page to make AND make a payment vs just storing it with a 0.00 auth (previous call)

37. Defendant had actual knowledge of the Asserted Patent and the infringement of the same no later than the date of this Complaint.

38. Defendant has and continues to indirectly infringe one or more claims of the Asserted Patent by inducing and/or contributing to direct infringement of the Asserted Patent by customers, importers, sellers, resellers, and users of the Infringing Methods. The direct infringers include, for example, at least the following: Daimler Truck Financial Services USA LLC,[17] First

[17] https://dtf.repay.io/ebpp/#/ (last visited July 26, 2023).

Tower Corp. (A/K/A Tower Loan),[18] Coastal Finance Company Inc.[19], and Adonis Auto Group Houston, LLC.[20]

39. Defendant has and continues to induce others to directly infringe, either literally or under the doctrine of equivalents, by, among other things, making, using, offering to sell, selling and/or importing into the United States, without authority, products or services that practice one or more claims of the Asserted Patent.

40. Defendant induced the infringement by others with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others infringe the Asserted Patent, but while at best, remaining willfully blind to the infringement.

41. As discussed in Paragraphs 21-36, above, Defendant advertises the Infringing Methods, publishes specifications and promotional literature encouraging customers to implement and incorporate the Infringing Methods into end user products, creates and/or distributes user manuals for the Infringing Methods that provide instructions and/or encourage infringing use, and offers support and/or technical assistances to its customers that provide instructions on and/or encourage infringing use.

42. Defendant encourages and facilitates its customers to infringe the Asserted Patent by promoting the Infringing Methods, for example, providing documentation and stating in its documentation for the Payment API that "This collection was created for {{Merchant Name}} to connect to REPAY's Platform for channels like SMS, IVR, Mobile and other external payments

[18] https://towerloan.repay.io/ebpp/#/ (last visited July 26, 2023).
[19] https://coastalfinanceco.repay.io/ebpp/#/ (last visited July 26, 2023).
[20] https://adonisautogroup.repay.io/ebpp/#/ (last visited July 26, 2023).

and payment management"[21] (where "{{Merchant Name }}" is intended to be replaced with the name of the specific customer).

43. Defendant's customers that incorporate the Infringing Methods into other products and services (*e.g.*, Daimler Truck Financial Services USA LLC, Tower Loan, Coastal Finance Company Inc., and Adonis Auto Group Houston, LLC) each directly infringe the Asserted Patent pursuant to Defendant's instructions and advertisements.

44. Additionally, Defendant has and continues to contribute to the direct infringement of others, either literally or under the doctrine of equivalents, by, among other things, offering to sell or selling within the within the United States, components of a patented device or an apparatus for use in practicing the claimed method, constituting a material part of the invention.

45. As discussed in Paragraphs 21-36, above, Defendant provides APIs and example code for the Infringing Methods that constitute a component of a patented device or an apparatus for use in practicing the claimed method.

46. Defendant does this knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial noninfringing use.

47. Defendant's customers that incorporate the APIs and example code into other products and services (*e.g.*, Daimler Truck Financial Services USA LLC, Tower Loan, Coastal Finance Company Inc., and Adonis Auto Group Houston, LLC) each directly infringe the Asserted Patent.

V. JURY DEMAND

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

---

[21] https://www.postman.com/repay-api-nation/workspace/repay-api-nation-s-public-workspace/documentation/9781366-91da388b-d862-4980-a2ba-2aca6d0420cb (last visited July 26, 2023).

VI. PRAYER FOR RELIEF

WHEREFORE, Autoscribe requests entry of judgment in its favor and against Defendant as follows:

a) A declaration that Defendant has directly infringed one or more claims of the Asserted Patent, either literally or under the doctrine of equivalents;

b) A declaration that Defendant has induced and/or contributed to infringement and/or is inducing and/or contributing to infringement of one or more claims of the Asserted Patent, either literally or under the doctrine of equivalents;

c) An award of damages pursuant to 35 U.S.C. § 284 adequate to compensate Autoscribe for Defendant's infringement of the Asserted Patent in an amount according to proof at trial (together with prejudgment and post-judgment interest), but no less than a reasonable royalty;

d) An award of costs and expenses pursuant to 35 U.S.C. § 284 or as otherwise permitted by law; and

e) Such other and further relief, whether legal, equitable, or otherwise, to which Autoscribe may be entitled or which this Court may order.

Dated: July 27, 2023

Respectfully submitted,

/s/ Colin Phillips

Colin Phillips
State Bar No.: 24105937
Jason McManis
State Bar No.: 24088032
Chun Deng
State Bar No.: 24133178
AHMAD, ZAVITSANOS & MENSING, PLLC
1221 McKinney Street, Suite 2500
Houston, Texas 77010
(713) 655-1101
cphillips@azalaw.com
jmcmanis@azalaw.com
cdeng@azalaw.com

Andrea L. Fair
State Bar No.: 24078488
WARD, SMITH, & HILL, PLLC
1507 Bill Owens Parkway
Longview, Texas 75604
(903) 757-6400
(903) 757-2323 (fax)
andrea@wsfirm.com

Attorneys for Autoscribe Corporation