

**IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF TEXAS  
GALVESTON DIVISION**

Autoscribe Corporation

*Plaintiff,*

v.

Tsevo, LLC and  
GambleID, LLC

*Defendants.*

§  
§  
§  
§  
§  
§  
§  
§  
§  
§  
§  
§

Case No. \_\_\_\_\_

JURY TRIAL DEMANDED

**PLAINTIFF’S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT**

Plaintiff Autoscribe Corporation (“Autoscribe” or “Plaintiff”) hereby submits this Original Complaint for patent infringement against Defendants Tsevo, LLC (“Tsevo”) and GambleID, LLC (“GambleID”) (together, “Defendants”) 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. Tsevo is a Limited Liability Company organized under the laws of Texas, with its headquarters at 1121 Delano St. Suite 100 Houston, TX 77003.<sup>1</sup> Tsevo can be served through its registered agent: Corporation Service Company, 211 E. 7TH St. Suite 620, Austin, TX 78701.

3. GambleID is a Limited Liability Company organized under the laws of Nevada, with its headquarters at 1121 Delano St. Suite 100 Houston, TX 77003.<sup>2</sup> GambleID can be served

<sup>1</sup> <https://www.tsevo.com> (last visited March 10, 2024).

<sup>2</sup> <https://www.gambleid.com> (last visited March 10, 2024).

through its registered agent: Corporation Service Company, 112 North Curry Street, Carson City, NV 89703.

## 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, Defendants have 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, Defendants maintain their headquarters at 1121 Delano St. Suite 100 Houston, TX 77003, which is located in this district.

7. Additionally, Defendants have customers in the District, including, *e.g.*, Waterborne Energy and Genscape, Inc.<sup>3</sup>

8. The Court has personal jurisdiction over Defendants, in part, because Defendants have minimum contacts within the State of Texas; Defendants have purposefully availed themselves of the privileges of conducting business in the State of Texas; Defendants regularly conduct business within the State of Texas; and Autoscribe's causes of action arise directly from Defendants' business contacts and other activities in the State of Texas, including by virtue of

---

<sup>3</sup> <https://tsevo.com/Industry/EnergyOilGas> (last visited March 11, 2024); *see also* <https://pitchbook.com/profiles/company/61792-57> (last visited March 11, 2024) (stating that Waterborne Energy maintains its corporate office at 2323 South Shepherd Drive Suite 1010 Houston, TX 77019); <https://www.woodmac.com/products/short-term-analytics/power/> (last visited March 11, 2024) (stating that Genscape was acquired by Wood Mackenzie, which maintains an office at 5847 San Felipe St #1000, Houston, TX 77057).

Defendants' infringement in the State of Texas. More specifically, Defendants are subject to the Court's general jurisdiction, in part, due to their continuous and systematic contacts with the State of Texas, including because Tsevo is a Texas LLC and because Defendants share a principal place of business in the District. Further, Defendants are subject to the Court's specific jurisdiction, in part, because Defendants have committed patent infringement and/or has induced and/or contributed to acts of infringement by others 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 Defendants reside in the District and because Defendants have committed patent infringement and/or has induced and/or contributed to acts of infringement by others in the District and have a regular and established place of business in the District, as discussed above.

### **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. Autoscribe has complied with any marking requirements under 35 U.S.C. § 287 with regard to the Asserted Patent.

17. Defendant Tsevo is a financial technology company with a heavy presence in payments and compliance for several industries, including the “Fantasy, Social, & Regulated Gaming;” “Energy / Oil & Gas;” and “Fashion & Retail” industries. Through its payment products, Tsevo has processed hundreds of millions of transactions.<sup>4</sup>

18. Defendant GambleID is a financial technology company in the gambling industry,

---

<sup>4</sup> <https://www.tsevo.com> (last visited March 10, 2024).

offering “end-to-end payment solutions for gaming.”<sup>5</sup> Through its marketing, GambleID boasts of “33 million validated players,” including in the “Sports Book / Fantasy,” “Sweepstakes,” “E-Sports & Social,” “Skill-Based Gaming,” “Casino,” and “Horse Racing” industries.<sup>6</sup>

19. As discussed in greater detail below, Defendants provide and use processing solutions, including their “Smart Cashier” and “Token Vault” products, that are covered by the Asserted Patent.

20. Defendants compete directly against Autoscribe, including through their “Smart Cashier” and “Token Vault” products, causing Autoscribe to lose significant profits.

21. Accordingly, Defendants’ infringement, as described below, has injured, and continues to injure Autoscribe.

#### **IV. COUNT I: INFRINGEMENT OF THE ASSERTED PATENT**

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

23. Defendants have directly infringed and continue 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.

24. Defendants are 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.

25. Defendants have and continue 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.

---

<sup>5</sup> <https://www.gambleid.com> (last visited March 10, 2024).

<sup>6</sup> <https://www.gambleid.com/#about> (last visited March 10, 2024).

26. Defendants' infringing services include, for example, the services Defendants provide through their "Smart Cashier" and "Token Vault" products, as well as any other similar methods performed by Defendants (collectively, the "Infringing Methods").

27. 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.

28. Through their “Smart Cashier” and “Token Vault” products, Defendants perform 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 Defendants’ marketing for their Smart Cashier product:<sup>7</sup>

---

<sup>7</sup> <https://tsevo.com/Products/SmartCashier> (last visited March 10, 2024).

The image is a marketing graphic for 'SMART CASHIER™ • PAYMENT MANAGEMENT GATEWAY'. It features a light gray background with a thin teal line at the top left. The content is organized into six columns, each with a teal icon, a title, and a short paragraph. The icons are: a wallet for Credit & Debit Cards, a folder for Alternative Payments, a bank account for Bank & Merchant Accounts, a return arrow for Deposit & Payout Gateway, a shield with an 'x' for Anti-Fraud & Compliance, and a checkmark for PCI Compliance. The text in each column describes the service's capabilities in that area.

**SMART CASHIER™ • PAYMENT MANAGEMENT GATEWAY**

**Credit & Debit Cards**  
Start taking Visa, MasterCard, Discover, and American Express credit/debit cards on your site or app.

**Alternative Payments**  
We connected to more than just credit/debit cards, **Smart Cashier™** connects you PayPal, Dwolla, PayToo, Stripe, and more.

**Bank & Merchant Accounts**  
Bring your own merchant processing account for deposits and payouts or we can help you get set up with one of the many that we work with.

**Deposit & Payout Gateway**  
The integrated gateway checkout offers a beautiful & customizable managed payment flow that works great across desktop and mobile.

**Anti-Fraud & Compliance**  
Enhanced anti-fraud protection identifies high-risk transactions, stops fraudulent charges, and monitors suspicious customer behavior.

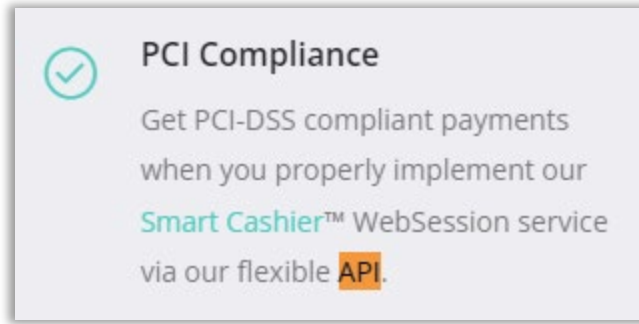
**PCI Compliance**  
Get PCI-DSS compliant payments when you properly implement our **Smart Cashier™** WebSession service via our flexible API.

29. Defendants provide, 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 excerpt from Defendants’ marketing for their Smart Cashier product:<sup>8</sup>

---

<sup>8</sup> *Id.*

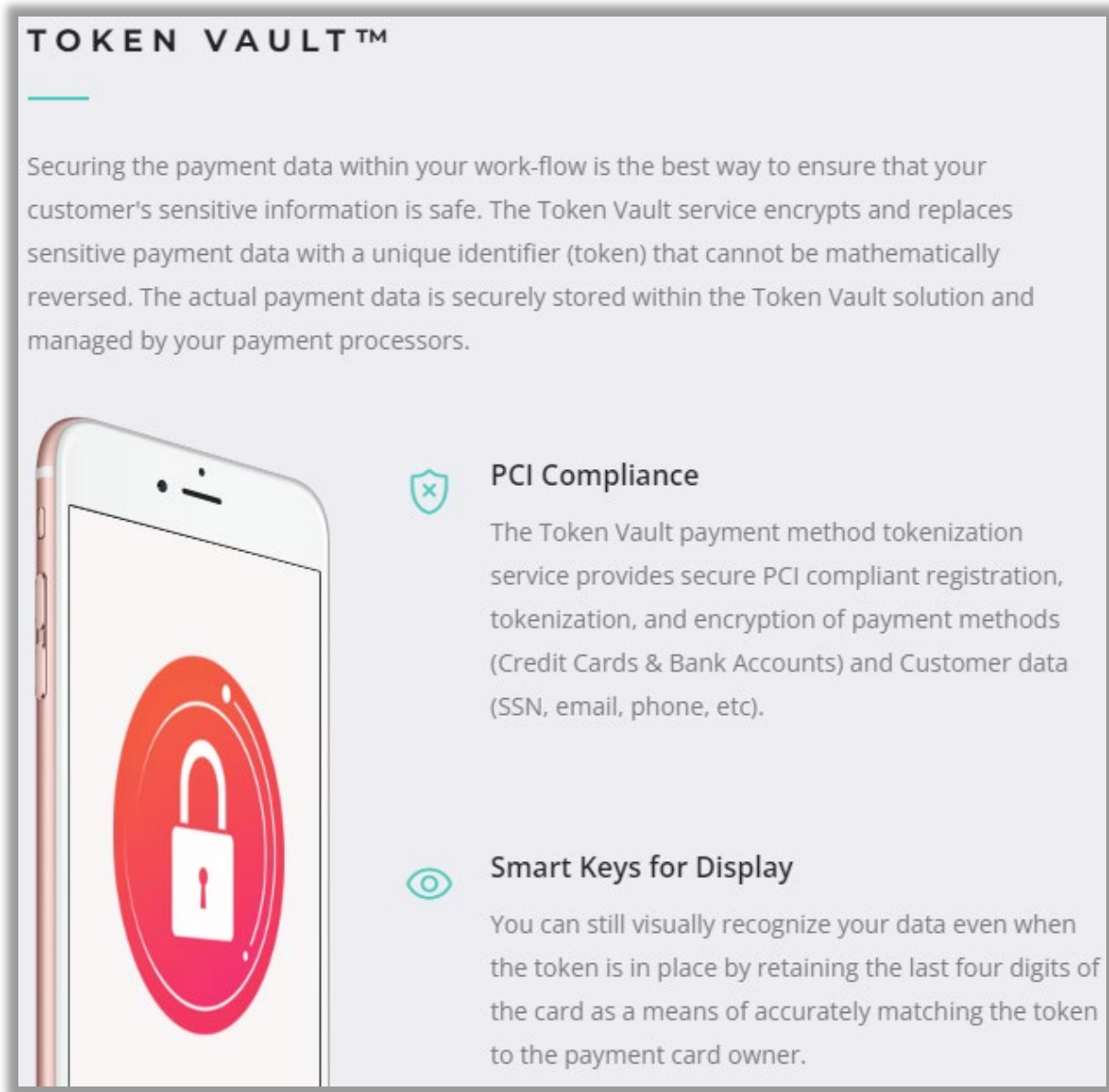




30. Defendants' API provides financial account registration and token retrieval functions that can be executed to process the payment transaction. This is shown by, *e.g.*, the following excerpt from Defendants' marketing for their Smart Cashier product:<sup>9</sup>


---

<sup>9</sup> *Id.*


The graphic features the title "TOKEN VAULT™" at the top left. Below it is a paragraph of text explaining the service. To the left of the text is an illustration of a smartphone with a red padlock icon on its screen. To the right of the smartphone are two bullet points, each with a teal icon: a shield with an 'x' for "PCI Compliance" and an eye for "Smart Keys for Display".

**TOKEN VAULT™**

Securing the payment data within your work-flow is the best way to ensure that your customer's sensitive information is safe. The Token Vault service encrypts and replaces sensitive payment data with a unique identifier (token) that cannot be mathematically reversed. The actual payment data is securely stored within the Token Vault solution and managed by your payment processors.

 **PCI Compliance**

The Token Vault payment method tokenization service provides secure PCI compliant registration, tokenization, and encryption of payment methods (Credit Cards & Bank Accounts) and Customer data (SSN, email, phone, etc).

 **Smart Keys for Display**

You can still visually recognize your data even when the token is in place by retaining the last four digits of the card as a means of accurately matching the token to the payment card owner.

31. Defendants' API provides access to the financial account registration and token retrieval functions to the merchant server. This is shown by, *e.g.*, the following excerpt from Defendants' documentation for marketing for their "GIDX" platform:<sup>10</sup>

---

<sup>10</sup> <https://www.tsevo.com/Docs/ApiReference> (last visited March 10, 2024).

### Accessing the GIDX Platform API

As part of your Merchant On-boarding process you will receive a security packet containing the end point URL, version number for your implementation, and the specific security credentials assigned to your account. The URL provided in this documentation may not be the one assigned to your account and may not result in valid connectivity.

In order to access the GIDX Platform environment you will need to obtain your security keys; you can find this set of keys within the "Integration" section of the GIDX Portal located at [GIDX Environment Portal](#).

32. Defendants' API 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 "MerchantCustomerID," "CustomerIpAddress," and "CashierPaymentAmount" parameters of the "CreateSession" method of the "WebCashier" folder of Defendants' documentation:<sup>11</sup>

---

<sup>11</sup> [https://www.tsevo.com/Docs/WebCashier#MethodRef\\_ID\\_CreateSession](https://www.tsevo.com/Docs/WebCashier#MethodRef_ID_CreateSession) (last visited March 10, 2024).

## WebCashier: CreateSession

This method should be called to create a new Cashier Web Session within the GIDX system for payments.

**Request Type:** HTTP POST: JSON Content Body  
**Parameters:** CreateSessionWebCashierRequest (*object*)  
**Return Value:** CreateSessionWebCashierResponse (*object*)

**Endpoint URL:** <https://api.gidx-service.in/v3.0/api/WebCashier/CreateSession>

**CreateSessionWebCashierRequest** ▾

---

Standardized Parameters	Standard Request <i>See the Standardized Paramaters above.</i>
MerchantCustomerID	String <b>Required</b> <span>ABC-123</span> <i>Your unique ID for this customer.</i>
CustomerIpAddress	String <b>Required</b> <span>66.249.76.138</span> <i>IP address for the current device (The Customers' Device – NOT your servers IP address) for this active session.</i>
CashierPaymentAmount	Object <span>CashierPaymentAmount Object</span> See Library <i>Optional - See object reference CashierPaymentAmount</i>

33. Defendants’ API authenticates the payee. This is shown by, e.g., the “ApiKey” and

“MerchantID” parameters of the “WebCashier” folder of Defendants’ documentation:<sup>12</sup>

## WebCashier: Request & Response Parameter Constants

The following parameters are used in every **WebCashier** Method Request and Responses. They are labeled within the methods below as Standardized Request Parameters and Standardized Response Parameters.

**Making a Request**  
Each API method has a corresponding Request object used to transport the request parameters as shown below.

**Using the Response**  
Each Response object returned from the method Request will contain properties you can use to determine the status of the methods service. Use the **IsSuccess** property along with the **ResponseCode** and **ResponseMessage** values to detect if the Request completed without a problem.

**Standardized Request Parameters** ▾

---

<b>ApiKey</b>	String	<b>Required</b>	<code>4QhgwWJxRlqVctrc75xHEQ</code>
	<i>Your assigned ApiKey, provided to you by the GIDX team.</i>		
<b>MerchantID</b>	String	<b>Required</b>	<code>VpGYLoXhSS+WgU9N415IJQ</code>
	<i>Your assigned Merchant ID, provided to you by the GIDX team.</i>		

34. Defendants’ API 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

<sup>12</sup> <https://www.tsevo.com/Docs/WebCashier> (last visited March 10, 2024).

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 “SessionURL” described under “Cashier Service” in the GIDX Platform documentation:<sup>13</sup>

**Cashier Service (Payment / Deposit)** ⓘ

14. Using the Web Session Cashier Service provides you with a hosted managed process for customer deposits, payouts, and payment method management.

This allows a merchant to control the functionality of the cashier and payment functionality through settings on the account rather than needing to write additional code for multiple use case scenarios.

15. The [CreateSession](#), located in the [WebCashier](#) Service, will return several values that are needed for initiating the Web Session process.

- [ReasonCodes](#): System codes containing Customer Identity, Device, and Location information - if available.
- [SessionURL](#): An encrypted, one time use, script-tag.
- And other values including the sessions expiration time and echoed MerchantSessionID for security purposes.

16. The merchant decrypts and embeds the [SessionURL](#) (one time use script-tag) into the HTML webpage displayed to the customer on their device.

NOTE: This HTML webpage should contain the required metatags and javascript outlined in the example located under the [Merchant Preparation](#) section.

- 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 displayed within the webpage provided by the merchant server. This is shown by, *e.g.*, the

---

<sup>13</sup> <https://www.tsevo.com/Docs/Integration> (last visited March 10, 2024).

description of the “direct connection” described under “Cashier Service” in the GIDX Platform documentation:<sup>14</sup>

16. The merchant decrypts and embeds the SessionURL (one time use script-tag) into the HTML webpage displayed to the customer on their device.  
  
NOTE: This HTML webpage should contain the required metatags and javascript outlined in the example located under the [Merchant Preparation](#) section.
17. Once embeded and viewed by the customer the script-tag will connect to the GIDX Service directly from the customers device; this direct connection will initiate the following process...
  - The customers device is authenticated using the encrypted token of the script-tag.
  - The GIDX Service detects and interprets the customers device attributes and analyzes the connection.
  - Based on these attributes and connection status the appropriate service interface is rendered as Bootstrap Formatted HTML and sent back to the customers device where it is then rendered into the interface and displayed based on the merchants settings.

*The HTML interface, that is rendered and embedded by the script-tag into the merchants page on the customers device, is completely customizable by the merchant using standard CSS, jQuery/JavaScript, or other client side scripting languages.*

- 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 “HTML interface” in the same excerpt shown above.
- 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

---

<sup>14</sup> *Id.*

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 documentation discussed in the previous paragraphs and by the “HTML webpage”:<sup>15</sup>

---

<sup>15</sup> *Id.*



16. The merchant decrypts and embeds the SessionURL (one time use script-tag) into the HTML webpage displayed to the customer on their device.

NOTE: This HTML webpage should contain the required metatags and javascript outlined in the example located under the [Merchant Preparation](#) section.

17. Once embedded and viewed by the customer the script-tag will connect to the GIDX Service directly from the customers device; this direct connection will initiate the following process...
  - The customers device is authenticated using the encrypted token of the script-tag.
  - The GIDX Service detects and interprets the customers device attributes and analyzes the connection.
  - Based on these attributes and connection status the appropriate service interface is rendered as Bootstrap Formatted HTML and sent back to the customers device where it is then rendered into the interface and displayed based on the merchants settings.

*The HTML interface, that is rendered and embedded by the script-tag into the merchants page on the customers device, is completely customizable by the merchant using standard CSS, jQuery/JavaScript, or other client side scripting languages.*

Based on the Merchant Cashier Service settings the embedded interface will present the customer the following screens/process.

- Select/provide the deposit amount.
- Select the payment method type - Credit Card, eCheck/ACH, PayPal, PayNearMe, etc.
- Register the Payment Method (if this is the customer first time to make a deposit, or they are making a deposit with a new payment method)
- Confirm the deposit amount and click finalize.
- - If the customer **HAS successfully verified** their identity already then the transaction is processed and completed.
  - If the customer **HAS NOT successfully verified** their identity then this deposit is held in a pending state and the customer is dynamically prompted to verify their identity using the WebReg Customer Verification service.

35. Defendants receive the sensitive financial account information provided by the payer via the secure socket layer connection. This is indicated by, *e.g.*, the excerpt shown above

and by the “Example Response” that Defendants provide for “Save PaymentMethod”:<sup>16</sup>

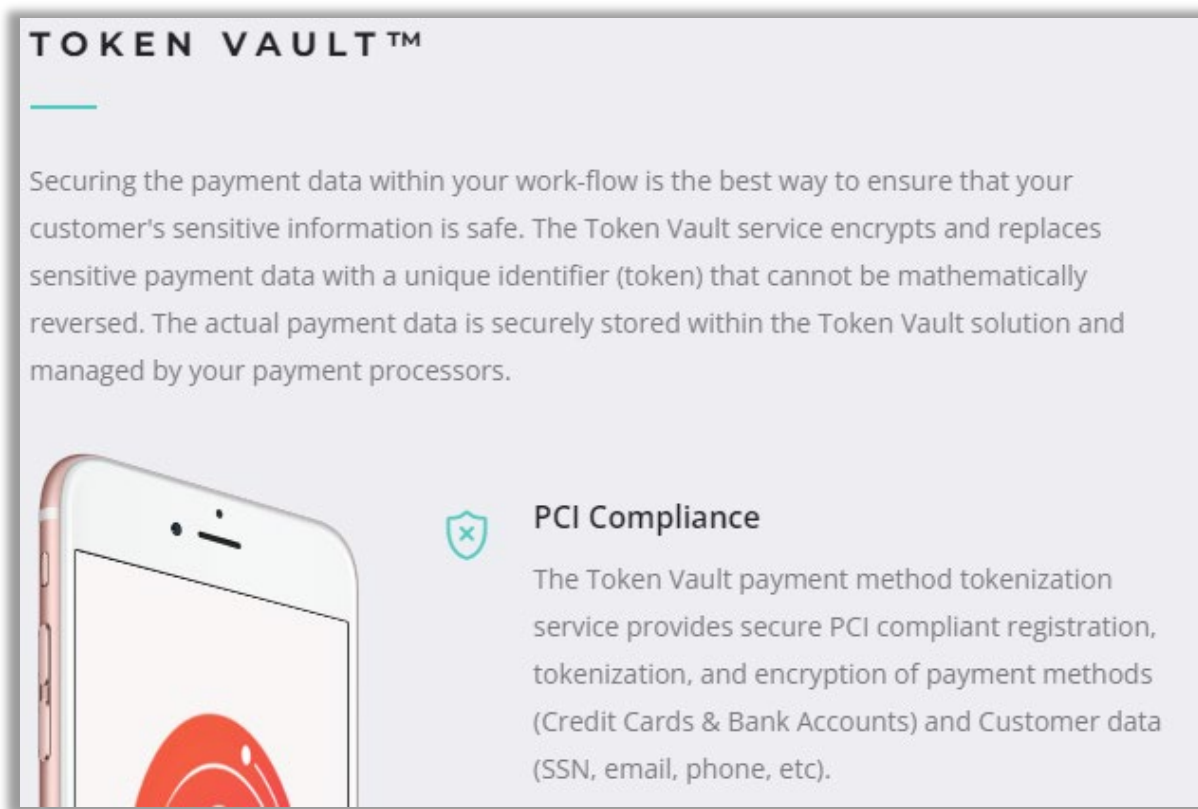
```
//Example Response
{
  "MerchantID": "fUHSaCnsmUKRto3PTPZC5w",
  "MerchantSessionID": "4qm2go9a6q6lk43voe1p44hbb7",
  "ResponseCode": 0,
  "ResponseMessage": "No error.",
  "PaymentMethod": {
    "Type": "CC",
    "Token": "6CADB8D0-6FAE-40DE-937E-03BA3EC9A7A5",
    "DisplayName": "Visa (...1111)",
    "NameOnAccount": "John Smith",
    "CardNumber": "xxxxxxxxxxxx1111",
    "ExpirationDate": "11/2024",
    "Network": "Visa",
    "AVSResult": "ExactMatch",
    "CVVResult": "Match",
    "BillingAddress": {
      "AddressLine1": "1234 Main St",
      "City": "Anytown",
      "StateCode": "TX",
      "PostalCode": "77002",
      "CountryCode": "US"
    }
  }
}
```

36. Defendants store the sensitive financial account information in a secure storage location and performs each software process required to maintain compliance with one or more information security standards. This is shown by, e.g., the following excerpt from Defendants’

---


<sup>16</sup> [https://www.tsevo.com/Docs/DirectCashier#MethodRef\\_ID\\_PaymentMethod\\_Save](https://www.tsevo.com/Docs/DirectCashier#MethodRef_ID_PaymentMethod_Save) (last visited March 10, 2024):

marketing for their Smart Cashier product:<sup>17</sup>



**TOKEN VAULT™**

Securing the payment data within your work-flow is the best way to ensure that your customer's sensitive information is safe. The Token Vault service encrypts and replaces sensitive payment data with a unique identifier (token) that cannot be mathematically reversed. The actual payment data is securely stored within the Token Vault solution and managed by your payment processors.

 **PCI Compliance**

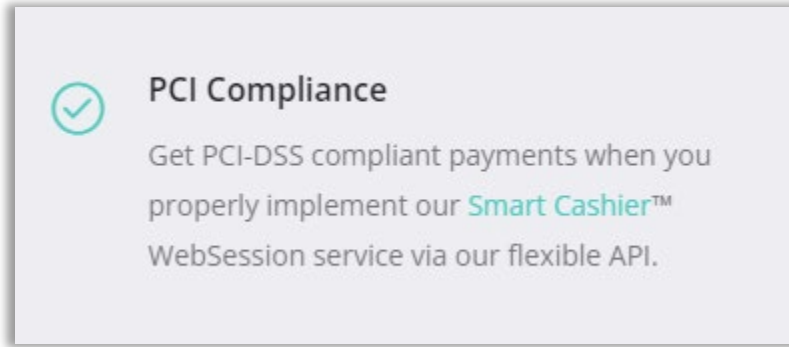
The Token Vault payment method tokenization service provides secure PCI compliant registration, tokenization, and encryption of payment methods (Credit Cards & Bank Accounts) and Customer data (SSN, email, phone, etc).

37. Defendants execute 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 excerpt above show “a non-sensitive electronic data token,” and the “PCI Compliance” excerpt in Defendants’ marketing

---

<sup>17</sup> *Id.*

materials shows that it processes a payment:<sup>18</sup>



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

39. Defendants have and continue 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: Genscape, Waterborne Energy, DraftDemons.com, and HogWildPoker.<sup>19</sup>

40. Defendants have and continue 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.

41. Defendants 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.

---

<sup>18</sup> <https://tsevo.com/Products/SmartCashier> (last visited March 10, 2024).

<sup>19</sup> <https://tsevo.com/Industry/EnergyOilGas> (last visited March 11, 2024); <https://tsevo.com/#Clients> (last visited March 11, 2024).

42. As discussed in Paragraphs 23–37, above, Defendants advertise the Infringing Methods, publish specifications and promotional literature encouraging customers to implement and incorporate the Infringing Methods into end user products, create and/or distribute user manuals for the Infringing Methods that provide instructions and/or encourage infringing use, and offer support and/or technical assistance to their customers that provide instructions on and/or encourage infringing use.

43. Defendants encourage and facilitate their customers to infringe the Asserted Patent by promoting the Infringing Methods, for example, providing documentation and stating in their documentation for the GIDX Platform that “This set of documents serves as the integration guide for implementing services of the GIDX Platform API within the operator’s environment. The following pages outline the GIDX Platform API access points, security, methods, and parameters. As always, please contact us at devteam@tsevo.com any time if further explanation is needed.”<sup>20</sup>

44. Defendants’ customers that incorporate the Infringing Methods into other products and services (*e.g.*, Genscape, Waterborne Energy, DraftDemons.com, and HogWildPoker) each directly infringe the Asserted Patent pursuant to Defendants’ instructions and advertisements.

45. Additionally, Defendants have and continue 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.

46. As discussed in Paragraphs 23–37, above, Defendants provide 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.

---

<sup>20</sup> <https://www.tsevo.com/Docs/ApiReference> (last visited March 10, 2024).

47. Defendants do 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.

48. Defendants' customers that incorporate the APIs and example code into other products and services (*e.g.*, Genscape, Waterborne Energy, DraftDemons.com, and HogWildPoker) each directly infringe the Asserted Patent.

#### **V. JURY DEMAND**

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

#### **VI. PRAYER FOR RELIEF**

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

- a) A declaration that Defendants have directly infringed one or more claims of the Asserted Patent, either literally or under the doctrine of equivalents;
- b) A declaration that Defendants have induced and/or contributed to infringement and/or are 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 Defendants' 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: March 18, 2024

Respectfully submitted,

/s/ Jason McManis

Jason McManis (attorney-in-charge)

Texas Bar No.: 24088032

S.D. Tex. No.: 3138185

Colin Phillips

Texas Bar No.: 24105937

S.D. Tex. No.: 3576569

Chun Deng

Texas Bar No.: 24133178

S.D. Tex. No.: 3860688

Angela Peterson

Texas Bar No.: 24137111

S.D. Tex. No.: 3862849

**AHMAD, ZAVITSANOS & MENSING, PLLC**

**1221 McKinney Street, Suite 2500**

Houston, Texas 77010

Tel.: (713) 655-1101

Facsimile: (713) 655-0062

jmcmanis@azalaw.com

cphillips@azalaw.com

cdeng@azalaw.com

apeterson@azalaw.com

*Attorneys for Autoscribe Corporation*