

**STARK, U.S. District Judge:**

On November 1, 2013, SecureBuy LLC (“SecureBuy” or “Plaintiff”) filed a declaratory judgment action against CardinalCommerce Corporation (“Cardinal” or “Defendant”) for non-infringement and invalidity under one or more of 35 U.S.C. §§ 101, 102, 103, and 112 of U.S. Patent Nos. 8,140,429 (the “429 Patent”), 7,051,002 (the “002 Patent”), and 7,693,783 (the “783 Patent”) (collectively, “the patents-in-suit”). (D.I. 1) On November 12, 2013, Cardinal filed an answer and counterclaims against SecureBuy. (D.I. 5) In its counterclaims, Cardinal alleges direct, indirect, and willful infringement of the patents-in-suit due to SecureBuy’s alleged making, using, selling, offering for sale, or importing of the SecureBuy 2.0 platform to perform authentication processing of a transaction. (*Id.*)

Pending before the Court is the issue of claim construction of various disputed terms of the patents-in-suit. The parties completed briefing on claim construction on May 15, 2014. (D.I. 104, 107, 136, 140) The parties also submitted technology tutorials (D.I. 102, 103) and Cardinal provided an expert report (D.I. 106). The Court held a *Markman* hearing on May 27, 2014. (*See* D.I. 179) Trial is scheduled to begin on August 4, 2014.

## **I. LEGAL STANDARDS**

“It is a bedrock principle of patent law that the claims of a patent define the invention to which the patentee is entitled the right to exclude.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (internal quotation marks omitted). Construing the claims of a patent presents a question of law. *See Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 977-78 (Fed. Cir. 1995), *aff’d*, 517 U.S. 370, 388-90 (1996). “[T]here is no magic formula or catechism for conducting claim construction.” *Phillips*, 415 F.3d at 1324. Instead, the court is free to attach

the appropriate weight to appropriate sources “in light of the statutes and policies that inform patent law.” *Id.*

“[T]he words of a claim are generally given their ordinary and customary meaning . . . [which is] the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application.” *Id.* at 1312-13 (internal citations and quotation marks omitted). “[T]he ordinary meaning of a claim term is its meaning to the ordinary artisan after reading the entire patent.” *Id.* at 1321 (internal quotation marks omitted). The patent specification “is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.” *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996).

While “the claims themselves provide substantial guidance as to the meaning of particular claim terms,” the context of the surrounding words of the claim also must be considered. *Phillips*, 415 F.3d at 1314. Furthermore, “[o]ther claims of the patent in question, both asserted and unasserted, can also be valuable sources of enlightenment . . . [b]ecause claim terms are normally used consistently throughout the patent . . . .” *Id.* (internal citation omitted).

It is likewise true that “[d]ifferences among claims can also be a useful guide . . . . For example, the presence of a dependent claim that adds a particular limitation gives rise to a presumption that the limitation in question is not present in the independent claim.” *Id.* at 1314-15 (internal citation omitted). This “presumption is especially strong when the limitation in dispute is the only meaningful difference between an independent and dependent claim, and one party is urging that the limitation in the dependent claim should be read into the independent claim.” *SunRace Roots Enter. Co., Ltd. v. SRAM Corp.*, 336 F.3d 1298, 1303 (Fed. Cir. 2003).

It is also possible that “the specification may reveal a special definition given to a claim term by the patentee that differs from the meaning it would otherwise possess. In such cases, the inventor’s lexicography governs.” *Phillips*, 415 F.3d at 1316. It bears emphasis that “[e]ven when the specification describes only a single embodiment, the claims of the patent will not be read restrictively unless the patentee has demonstrated a clear intention to limit the claim scope using words or expressions of manifest exclusion or restriction.” *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 906 (Fed. Cir. 2004) (internal quotation marks omitted), *aff’d*, 481 F.3d 1371 (Fed. Cir. 2007).

In addition to the specification, a court “should also consider the patent’s prosecution history, if it is in evidence.” *Markman*, 52 F.3d at 980. The prosecution history, which is “intrinsic evidence,” “consists of the complete record of the proceedings before the PTO [Patent and Trademark Office] and includes the prior art cited during the examination of the patent.” *Phillips*, 415 F.3d at 1317. “[T]he prosecution history can often inform the meaning of the claim language by demonstrating how the inventor understood the invention and whether the inventor limited the invention in the course of prosecution, making the claim scope narrower than it would otherwise be.” *Id.*

A court also may rely on “extrinsic evidence,” which “consists of all evidence external to the patent and prosecution history, including expert and inventor testimony, dictionaries, and learned treatises.” *Markman*, 52 F.3d at 980. For instance, technical dictionaries can assist the court in determining the meaning of a term to those of skill in the relevant art because such dictionaries “endeavor to collect the accepted meanings of terms used in various fields of science and technology.” *Phillips*, 415 F.3d at 1318. In addition, expert testimony can be useful “to

ensure that the court's understanding of the technical aspects of the patent is consistent with that of a person of ordinary skill in the art, or to establish that a particular term in the patent or the prior art has a particular meaning in the pertinent field." *Id.* Nonetheless, courts must not lose sight of the fact that "expert reports and testimony [are] generated at the time of and for the purpose of litigation and thus can suffer from bias that is not present in intrinsic evidence." *Id.* Overall, while extrinsic evidence "may be useful" to the court, it is "less reliable" than intrinsic evidence, and its consideration "is unlikely to result in a reliable interpretation of patent claim scope unless considered in the context of the intrinsic evidence." *Id.* at 1318-19.

Finally, "[t]he construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction." *Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1250 (Fed. Cir. 1998). It follows that "a claim interpretation that would exclude the inventor's device is rarely the correct interpretation." *Osram GmbH v. Int'l Trade Comm'n*, 505 F.3d 1351, 1358 (Fed. Cir. 2007).

## II. CONSTRUCTION OF DISPUTED TERMS

### 1. authentication program

Cardinal's Proposed Construction	SecureBuy's Proposed Construction
<p>This term requires no construction beyond its plain and ordinary meaning. To the extent, however, that the Court believes that such term requires additional explication, Cardinal proposes the following:</p> <p>“Program or initiative for verifying that a consumer is likely to be who he/she claims to be.”</p>	<p><b>Construction For ‘002 Patent:</b>            “A program or initiative employed by a payment processing network, <i>e.g.</i>, VbV, SecureCode, SPA, whereby the identity of an enrolled cardholder is actively authenticated by the bank or financial institution issuing the payment instrument.”</p> <p><b>Construction for ‘429 Patent:</b>            “A program or initiative employed by a payment processing network, <i>e.g.</i>, VbV, SecureCode, SPA, PayPal, <i>etc.</i> whereby the identity of an enrolled cardholder is actively authenticated by the bank or financial institution issuing the payment instrument or payment option.”</p>
<p><b>Court's Construction:</b> “Program or initiative for verifying that a consumer is likely to be who he/she claims to be.”</p>	

The parties agree that the authentication program is fundamentally a “program or initiative for verifying that a consumer is likely who he/she claims to be.” The parties disagree, however, as to whether the authentication done by the authentication program must (i) be employed by a payment processing network, (ii) be “active,” and (iii) be resolved by the bank or financial institution issuing the payment instrument. Plaintiff proposes adding all three of these limitations into the claim term, but none of them are supported by the intrinsic evidence.

In support of its position, Plaintiff cites to the ‘002 patent at 1:50-56 and 5:11-21, as well as identical passages in the ‘783 and ‘429 patents:

Accordingly, various credit card networks have implemented initiatives or programs aimed at safeguarding against

fraud. For example, Visa® and MasterCard® both support authentication initiatives whereby a cardholder is authenticated by the bank or financial institution issuing the card, i.e., the issuing bank.

...

The approach detailed in the present specification provides a secure, scalable and modular solution for merchants to participate in and support various payment authentication initiatives, such as, e.g., Visa's 3-D Secure Verified by Visa (VbV) and MasterCard's SecureCode and/or Secure Payment Application (SPA). It provides payment gateways, acquirers, merchant service providers (MSP) and independent sales organizations (ISO) an easy and effective way to provide their merchants with the means for cardholder authentication, as defined by various authenticating programs, e.g., VbV, SecureCode, SPA, etc.

('002 patent at 1:50-56, 5:11-21)

These passages describe a preferred embodiment of an authentication program that is employed by a payment processing system and is authenticated by a bank or financial institution. However, these passages do not clearly disclaim claim scope or provide an express definition of the "authentication program" term. Additionally, nothing in the patent specification requires that the authentication be "active." In fact, the intrinsic record never distinguishes between active and passive authentication. Nor does Plaintiff cite persuasive support in the specification for construing "authentication program" differently for the '002 and '429 patents.

The Court will adopt the broader, alternative construction proposed by Cardinal.

**2. authentication protocol**

<b>Cardinal's Proposed Construction</b>	<b>SecureBuy's Proposed Construction</b>
<p>“A prescribed set of rules, including those for formatting and routing messages, governing the transmission of messages over a communications network to verify that a consumer is likely who he/she claims to be.”</p>	<p>“Specific procedures or processing logic required/prescribed by the authentication program/initiative to actively authenticate the identity of the consumer/cardholder.”</p>
<p><b>Court's Construction:</b> “A prescribed set of rules, including those for formatting and routing messages, governing the transmission of messages over a communications network designed to verify that a consumer is who he/she claims to be.”</p>	

SecureBuy's primary concern with Cardinal's construction is that “a prescribed set of rules” cannot support different programs and different protocols, e.g., the protocols employed by Visa and MasterCard. However, SecureBuy offers no persuasive reason why there cannot be separate “prescribed set(s) of rules” for each of the various protocols.

Cardinal's construction requires that the prescribed set of rules be designed to verify that a consumer is who he/she claims to be, which both parties agree is a necessary part of the authenticating process. Additionally, Cardinal's construction requires that the prescribed set of rules include rules for “formatting and routing messages.” This limitation is supported by the specification. In particular, the specification teaches a:

means for obtaining an authentication determination for the transaction in accordance with the selected authentication protocol, including means for formatting messages and routing the formatted messages over the communications network in accordance with one or more mandates of the selected authentication protocol.

(‘429 patent at 3:65-4:4) SecureBuy improperly omits the “formatting and routing messages” limitation. SecureBuy would also inject an “actively authenticate” limitation which is not supported by the specification.



The Court will adopt Cardinal's construction.

**3. authentication determination**

<b>Cardinal's Proposed Construction</b>	<b>SecureBuy's Proposed Construction</b>
"An indication of whether a consumer has been authenticated."	"The response from the entity issuing the payment instrument or option being used as to as to whether the consumer has been authenticated."
<b>Court's Construction:</b>	"An indication of whether a consumer has been authenticated."

The dispute between the parties with respect to the "authentication determination" term is whether the entity determining the authenticity of the consumer must be the same entity that issues the payment instrument or option. SecureBuy argues yes, while Cardinal disagrees.

SecureBuy's position is not supported by the intrinsic evidence. As Cardinal notes, some claims expressly require that the "authentication determination" come from the issuing entity (*see, e.g.*, '002 patent claim 8 ("authentication determination made by the issuing entity")) while others do not (*see, e.g., id.*, claim 5 (claiming "obtaining an authentication determination for the commercial transaction in accordance with the selected authentication protocol, including formatting messages and routing the formatted messages over the communications network in accordance with one or more mandates of the selected authentication protocol," but not requiring that the "authentication determination" come from the issuing entity)). Hence, reading SecureBuy's proposed limitation into the "authentication determination" term would render certain claims redundant.

Accordingly, the Court will reject SecureBuy's construction and adopt Cardinal's proposal.

**4. connection layer**

<b>Cardinal’s Proposed Construction</b>	<b>SecureBuy’s Proposed Construction</b>
“A software layer interface used to communicate with external resources.”	“A generic software layer on the third party server that supports multiple types of connectors (including an HTTPS server, a direct connector, an easy connector, and an optional other connector) to connect to and receive payment information from the merchants and to send to the distribution layer.”
<b>Court’s Construction:</b> “A generic software layer for external entities to connect to and process a specific payment authentication transaction.”	

The parties raise several disputes with respect to the connection layer term. SecureBuy argues that a connection layer must (i) support multiple types of connectors including an HTTPS server, a direct connector, an easy connector, and an optional other connector, (ii) connect to and receive payment information from the merchants, and (iii) send information to the distribution layer. The Court agrees with Cardinal that none of these proposed limitations are required by the intrinsic record.

The specification of the ‘429 patent recites that:

The connectivity layer 210 provides a generic layer for external entities such as merchants to connect to and process a specific payment authentication transaction. The connectivity layer 210 supports the following connectors: an HTTPS server 212; a “direct connector” 214, as it is termed herein; and, an “easy connector” 216, as it is termed herein; and an optional “other connector” 218, as it is termed herein.

(‘429 patent at 7:39-45) Cardinal argues that the specification does not require that the connection layer be able to support all three listed connectors (an HTTPS server, a “direct connector,” and an “easy connector”). The Court agrees. Although the embodiment described

above includes all three listed connectors, Claim 2 of the '002 patent sets this requirement out in a dependent claim:

- 2. The system of claim 1, wherein the connection layer supports a plurality of connection means allowing for different types of connectivity with the merchant.

('002 patent at 12:45-47) Accepting SecureBuy's construction, which would require that the connection layer even in claim 1 support a plurality of connection means, would render claim 2 redundant. Hence, the Court will reject SecureBuy's proposed limitation.

SecureBuy next contends that the connection layer must communicate with the merchant. However, as the specification states, the connection layer need only enable communication with "external entities *such as* merchants" (emphasis added).

Accordingly, the Court will reject SecureBuy's proposed limitations but will add the well-supported limitation that the software layer enable external entities to connect to and process a specific payment authentication transaction.

**5. distribution layer**

<b>Cardinal's Proposed Construction</b>	<b>SecureBuy's Proposed Construction</b>
"A software layer for routing messages among other software layers within the system."	"A software layer configured to route messages from the connection layer to the correct one of a plurality of plug-in components in the plug-in layer listening for the messages."
<b>Court's Construction:</b> "A software layer for routing messages among other software layers within the system."	

Both parties agree that the distribution layer is a software layer that routes messages among other software layers. SecureBuy contends that the distribution layer specifically routes

messages from the connection layer to a plug-in component in the plug-in layer. However, Claim 1 of the '002 patent explicitly requires that the distribution layer route messages from the connection layer to a correct plug-in component in the plug-in layer:

a distribution layer residing between the connection layer and the plug-in layer, said distribution layer determining from the payment information received for each transaction which of the different authentication program is prescribed for the type of payment instrument identified in the payment information, and routing communications between the connection layer and selected plug-in components in the plug-in layer, wherein said payment information for each transaction is routed to the plug-in component responsible for administering the authentication program for the particular payment instrument used for that transaction.

('002 patent at 12:33-44) Thus, importing SecureBuy's proposed limitation would render much of the language in Claim 1 superfluous. Hence, the Court will reject SecureBuy's proposed limitation and adopt Cardinal's broader construction instead.

**6. plug-in layer**

<b>Cardinal's Proposed Construction</b>	<b>SecureBuy's Proposed Construction</b>
<p>"A software layer comprising various plug-in components."</p>	<p>"Software layer that contains a plurality of different, individual plug-in components that listen to the message distribution layer for a specific message type and are activated by the message distribution layer that sends messages to the specified plug-in component based upon the type of payment instrument being used for the transaction being processed."</p>
<p><b>Court's Construction:</b> "A software layer comprising various plug-in components."</p>	

Both parties agree that a plug-in layer is at least a software layer comprising or containing various plug-in components. SecureBuy contends that the various plug-in components must (i) be different, individual components, (ii) listen for a specific message, and (iii) be activated by

those messages.

SecureBuy finds support for these additional limitations in the following portion of the specification:

The plug-in layer 230 includes a plurality of individual authentication initiative plug-in components 232 that listen to the message distribution layer 220 for a specific message type.

(‘002 patent at 8:47-54) However, there is no basis for reading this description of an embodiment of the invention into a limitation of the plug-in layer claim term. As Cardinal correctly points out, the claims themselves provide functional language limiting the plug-in layer where such limitations were intended by the patentees:

a plug-in layer including a plurality of plug-in components, each plug-in component administering a different one of a plurality of authentication programs in accordance with the authentication programs in accordance with the authentication protocols prescribed to obtain an authentication determination for the transactions . . . .

(‘002 patent Claim 1 at 12:27-32) Reading the “different, individual components” limitation into the “plug-in layer” term would render much of Claim 1 redundant.

The Court will adopt Cardinal’s proposed construction.

7. “means for determining from the payment information received at the universal platform server, for each commercial transaction, which of the different authentication protocols is prescribed by the payment network for the type of payment instrument identified in the payment information” (‘002 patent)

“means for determining from the payment information received at the server which of the different authentication protocols is prescribed for the type of payment option identified in the payment information” (‘783 patent)

Cardinal’s Proposed Construction	SecureBuy’s Proposed Construction
<p><b><u>‘002 Patent</u></b>  <b>Function:</b>            Determining from the payment information received at the universal platform server, for each commercial transaction, which of the different authentication protocols is prescribed by the payment network for the type of payment instrument identified in the payment information.</p> <p><b>Structure:</b>            A general purpose computer, with a plug-in layer that includes a plurality of plug-in components each associated with an authentication protocol (e.g., VbV, SecureCode or SPA) corresponding to a type of payment instrument, programmed to:</p> <p>(1) determine the type of payment instrument from the payment information received (‘002 Patent, Col. 10:7-11); and</p> <p>(2) determine whether the payment instrument of step (1) is enrolled in an authentication program/initiative (‘002 Patent, Col. 10:12-37; Col. 10:54-67), each of which is associated with a particular authentication protocol (‘002 Patent, Col. 3:15-20; Col. 9:52-57).</p>	<p><b><u>‘002 Patent</u></b>            Indefinite.</p> <p>To the extent, however, that the Court believes that such term is amenable to construction, SecureBuy proposes the following construction:</p> <p><b>Function:</b>            Determining from the payment information received at the server which of the different authentication protocols is prescribed for the type of payment option identified in the payment information.</p> <p><b>Corresponding Structure:</b>            A general purpose computer programmed with an algorithm for determining the payment processing network to which a credit card belongs from the credit card number according to prior art methods.</p>

**'783 Patent**

**Function:**

Determining from the payment information received at the server which of the different authentication protocols is prescribed for the type of payment option identified in the payment information.

**Structure:**

A general purpose computer, with a plug-in layer that includes a plurality of plug-in components each associated with an authentication protocol (e.g., VbV, SecureCode or SPA) corresponding a type of payment instrument, programmed to:

- (1) determine the type of payment instrument from the payment information received ('783 Patent, Col. 10:7-11); and
- (2) determine whether the payment instrument of step 1 is enrolled in an authentication program/initiative ('783 Patent, Col. 10:12-37; Col. 10:54-67), each of which is associated with a particular authentication protocol ('783 Patent, Col. 9:50-55).

**'783 Patent**

**Indefinite**

To the extent, however, that the Court believes that such term is amenable to construction, SecureBuy proposes the following construction:

**Function:**

Determining from the payment information received at the server which of the different authentication protocols is prescribed for the type of payment option identified in the payment information.

**Structure:**

A general purpose computer programmed with an algorithm for determining the payment processing network to which a credit card belongs from the credit card number according to prior art methods.

**Court's Construction:**

**'002 Patent**

**Function:** Determining from the payment information received at the universal platform server, for each commercial transaction, which of the different authentication protocols is prescribed by the payment network for the type of payment instrument identified in the payment information.

**Structure:** A general purpose computer, with a plug-in layer that includes a plurality of plug-in components each associated with an authentication protocol (e.g., VbV, SecureCode or SPA) corresponding to a type of payment instrument, programmed to:

(1) determine the type of payment instrument from the payment information received ('002 Patent, Col. 10:7-11); and

(2) determine whether the payment instrument of step (1) is enrolled in an authentication program/initiative ('002 Patent, Col. 10:12-37; Col. 10:54-67), each of which is associated with a particular authentication protocol ('002 Patent, Col. 3:15-20; Col. 9:52-57).

**'783 Patent**

**Function:** Determining from the payment information received at the server, for each commercial transaction, which of the different authentication protocols is prescribed by the payment network for the type of payment instrument identified in the payment information.

**Structure:** A general purpose computer, with a plug-in layer that includes a plurality of plug-in components each associated with an authentication protocol (e.g., VbV, SecureCode or SPA) corresponding to a type of payment instrument, programmed to:

(1) determine the type of payment instrument from the payment information received ('783 Patent, Col. 10:7-11); and

(2) determine whether the payment instrument of step (1) is enrolled in an authentication program/initiative ('783 Patent, Col. 10:12-37; Col. 10:54-67), each of which is associated with a particular authentication protocol ('783 Patent, Col. 9:50-55).

The parties agree that this term should be construed pursuant to 35 U.S.C. § 112, ¶ 6.

The parties also agree as to the function of this means-plus-function term. The parties disagree



as to the corresponding structure for the recited functions.

A structure disclosed in the specification qualifies as corresponding structure if the specification or the prosecution history “clearly links or associates that structure to the function recited in the claim.” *B. Braun Med., Inc. v. Abbott Labs.*, 124 F.3d 1419, 1424 (Fed. Cir.1997). In addition to disclosing corresponding structure, the patent’s specification must provide “an adequate disclosure showing what is meant by that [claim] language. If an applicant fails to set forth an adequate disclosure, the applicant has in effect failed to particularly point out and distinctly claim the invention as required by the second paragraph of section 112.” *In re Donaldson Co.*, 16 F.3d 1189, 1195 (Fed. Cir. 1994) (en banc). Therefore, “a means-plus-function clause is indefinite if a person of ordinary skill in the art would be unable to recognize the structure in the specification and associate it with the corresponding function in the claim.” *Noah Sys., Inc. v. Intuit Inc.*, 675 F.3d 1302, 1311-12 (Fed. Cir. 2012).

The parties agree that for both patents, the determining means serves the function of determining from the payment information received at the server, for each commercial transaction, which of the different authentication protocols is prescribed by the payment network for the type of payment instrument or payment option identified in the payment information. To accomplish this function, the determining means must (i) determine the type of payment option identified in the payment information and (ii) determine which authentication protocol is prescribed by the payment network for that type of payment option. Cardinal’s proposed structure performs both of these functions and is supported by the specification.

The claim term is not indefinite, as its scope would be reasonably certain to one of ordinary skill in the art. *See Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124

(2014).

The specification discloses that:

Notably, the payment processing network to which a credit/debit card belongs can be determined from the card number as is known in the art.

Optionally, the MAPS 200 determines from the enrollment status of the particular payment instrument being used for the transaction. For example, the MAPS 200 may maintain a local cache or database of card numbers that identifies those payment instruments enrolled in for participation in various authentication programs and/or initiatives. If the particular payment instrument being used is not enrolled in a particular authentication program for the determined type of payment instrument, then the process may be ended at this point with the MAPS 200 returning a “not enrolled” message or data back to the thin-client 106 installed on the merchant’s server 100. Accordingly, the thin-client 106 passes this information to the payment processing function 104 to be bundled with the transaction data for submission of the completed transaction to the established underlying payment processing infrastructure.

(‘002 Patent at 10:7-37; ‘783 Patent at 10:9-39) The specification thus discloses how one of ordinary skill in the art may determine which payment option is identified in the payment information as well as whether the payment option is enrolled in an authentication program. Each authentication program is further associated with a particular authentication protocol, satisfying the requirement that the determining means determine “which of the different authentication protocols is prescribed by the payment network for the type of payment instrument identified in the payment information.” (See ‘002 patent at 9:52-57; ‘783 patent at 9:51-55) (teaching that “[t]he payment instrument [or method] may be either enrolled in or not enrolled in an authentication program conforming to one of a plurality of authentication protocols prescribed for the respective plurality of different types of payment instruments by payment networks

supporting the same”).

Because Cardinal’s proposed structure contains all of the steps necessary to perform the determining means, the Court will adopt that construction.

8. **means for selecting, in accordance with the determination of step (b), a particular authentication protocol from the plurality of different authentication protocols supported by the universal platform server (‘002 patent)**

**“means for selecting, in accordance with the determination made by the means for determining, a particular authentication protocol from the plurality of different authentication protocols supported by the server” (‘783 patent)**

Cardinal's Proposed Construction	SecureBuy's Proposed Construction
<p><b><u>'002 Patent</u></b>  <b>Function:</b> Selecting, in accordance with the determination of step (b), a particular authentication protocol from the plurality of different authentication protocols supported by the universal platform server.</p> <p><b>Structure:</b> A general purpose computer, with a plug-in layer that includes a plurality of plug-in components each associated with an authentication protocol (<i>e.g.</i>, VbV, SecureCode or SPA) corresponding to a type of payment instrument, programmed to:</p> <p>(1) in accordance with the determination of step (b), send a message to the plug-in component associated with the determined authentication protocol ('002 Patent, Col. 10:12-43; Col. 10:53-67).</p>	<p><b><u>'002 Patent</u></b>  Indefinite</p> <p>To the extent, however, that the Court believes that such term is amenable to construction, SecureBuy proposes the following construction:</p> <p><b>Function:</b> Selecting, in accordance with the determination of step (b), a particular authentication protocol from the plurality of different authentication protocols supported by the universal platform server.</p> <p><b>Structure:</b> The universal platform server; including a general purpose computer, with a message distribution layer programmed to route messages, and plug-in layer that includes a plurality of individual authentication initiative plug-in components each associated with a different authentication protocol (<i>e.g.</i>, VbV, SecureCode or SPA) corresponding to a type of payment instrument. The plug-in components are programmed to listen to a message distribution layer for a specific message type. The respective plug-in component is activated by the message distribution layer that sends messages to the specified plug-in component based upon the type of payment instrument being used for the transaction being processed.</p>

**'783 Patent**

**Function:**

Selecting, in accordance with the determination made by the means for determining, a particular authentication protocol from the plurality of different authentication protocols supported by the server.

**Structure:**

A general purpose computer, with a plug-in layer that includes a plurality of plug-in components each associated with an authentication protocol (*e.g.*, VbV, SecureCode or SPA) corresponding to a type of payment instrument, programmed to:  
(1) in accordance with the determination made by the means for determining, send a message to the plug-in component associated with the determined authentication protocol ('783 Patent, Col. 10:37-45).

**'783 Patent**

**Function:**

Selecting, in accordance with the determination made by the means for determining, a particular authentication protocol from the plurality of different authentication protocols supported by the server.

**Structure:**

A general purpose computer, with a message distribution layer programmed to route messages, and plug-in layer that includes a plurality of individual authentication initiative plug-in components each associated with a different authentication protocol (*e.g.*, VbV, SecureCode or SPA) corresponding to a type of payment instrument. The plug-in components are programmed to listen to a message distribution layer for a specific message type. The respective plug-in component is activated by the message distribution layer that sends messages to the specified plug-in component based upon the type of payment instrument being used for the transaction being processed.

**Court's Construction:**

**'002 Patent**

**Function:**

Selecting, in accordance with the determination of step (b), a particular authentication protocol from the plurality of different authentication protocols supported by the universal platform server.

**Structure:**

The universal platform server (see below); including a general purpose computer, with a message distribution layer programmed to route messages, and plug-in layer that includes a plurality of individual authentication initiative plug-in components each associated with a different authentication protocol (e.g., VbV, SecureCode or SPA) corresponding to a type of payment instrument. The plug-in components are programmed to listen to a message distribution layer for a specific message type. The respective plug-in component is activated by the message distribution layer that sends messages to the specified plug-in component based upon the type of payment instrument being used for the transaction being processed.

**'783 Patent**

**Function:**

Selecting, in accordance with the determination made by the means for determining, a particular authentication protocol from the plurality of different authentication protocols supported by the server.

**Structure:**

A general purpose computer, with a message distribution layer programmed to route messages, and plug-in layer that includes a plurality of individual authentication initiative plug-in components each associated with a different authentication protocol (e.g., VbV, SecureCode or SPA) corresponding to a type of payment instrument. The plug-in components are programmed to listen to a message distribution layer for a specific message type. The respective plug-in component is activated by the message distribution layer that sends messages to the specified plug-in component based upon the type of payment instrument being used for the transaction being processed.

The parties have two primary disputes with respect to the “means for selecting” term:

(i) is the distribution layer necessary structure for the recited function, and (ii) are the plug-in components programmed?

The Court agrees with SecureBuy that the distribution layer is essential structure. Both parties agree that the selecting means requires sending a message to the plug-in component that is

associated with the determined authentication protocol. According to the only embodiment disclosed in the specifications,

if the particular payment instrument being used is enrolled in an authentication program, then the payment information is passed to the message distribution layer 2520 that routes it to the proper plug-in component 232 in the plug-in layer 230.

(‘002 patent at 10:37-41; ‘783 patent at 37-41) Because a means-plus-function claim is limited to the structure disclosed within the specification, and because the only embodiment disclosed in the specifications requires that the payment information be passed to the plug-in component via the distribution layer, it follows that the distribution layer is a necessary element of the structure of the selecting means term.

The Court further agrees with SecureBuy that the plug-in components are programmed to listen to the message distribution layer for a specific message type. (‘002 patent at 8:46-49; ‘783 patent at 46-49) (“The plug-in layer 230 includes a plurality of individual authentication initiative plug-in components 232 that listen to the message distribution layer 220 for a specific message type.”) Because SecureBuy’s alternate construction is supported by the intrinsic record, the Court will adopt it. (The Court also does not find the term indefinite.)

9. Universal platform server

Cardinal’s Proposed Construction	SecureBuy’s Proposed Construction
<p>This term requires no construction beyond its plain and ordinary meaning. To the extent, however, that the Court believes that such term requires additional explication, CardinalCommerce proposes the following construction:</p> <p>“A server configured to support a plurality of merchants and a plurality of authentication protocols.”</p>	<p>Indefinite</p> <p>To the extent, however, that the Court believes that such term is amenable to construction, SecureBuy proposes the following construction:</p> <p>“A software suite consisting of the merchant authentication processing system (MAPS) and multiple ways for merchants to integrate with the MAPS, including a direct connection, easy connection and thin client.”</p>
<p><b>Court’s Construction:</b> “A server configured to support a plurality of merchants and a plurality of authentication protocols.”</p>	

“[A] patent is invalid for indefiniteness if its claims, read in light of the specification delineating the patent, and the prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention.” *Nautilus*, 134 S. Ct. at 2124. SecureBuy contends that the “universal platform server” term is indefinite. The Court disagrees.

The patent specification states that:

In accordance with a preferred embodiment, the present invention serves as a centralized merchant processing system for authenticated payments, allowing a merchant to securely and easily accommodate authentication of consumers and/or cardholders in accordance with a variety of authentication initiatives implemented by credit card networks, and to process electronic transactions through any payment network using a single platform.

(’002 patent at 4:46-53) In context, this “single platform” is the universal platform server. This server allows a merchant to securely and easily accommodate authentication of consumers and/or cardholders in accordance with a variety of authentication initiatives. This lends the platform its



“universal” nature.

Accordingly, a universal platform server is, as Cardinal contends, a server that is configured to support a plurality of merchants and a plurality of authentication protocols.<sup>1</sup>

**10. “payment option,” “payment instrument,” and “payment information”**

<b>Cardinal’s Proposed Construction</b>	<b>SecureBuy’s Proposed Construction</b>
<p><b><u>Payment option:</u></b> This term requires no construction beyond its plain and ordinary meaning.</p> <p><b><u>Payment instrument:</u></b> This term requires no construction beyond its plain and ordinary meaning.</p> <p><b><u>Payment information:</u></b> This term requires no construction beyond its plain and ordinary meaning.</p>	<p><b><u>Payment Option:</u></b> “A credit card, debit card or other method of payment such as PayPal, Bill Me Later®, Western Union®, and Secure eBill.”</p> <p><b><u>Payment instrument:</u></b> “Credit card or debit card.”</p> <p><b><u>Payment information:</u></b>  <b>Construction For ‘002 Patent:</b>            “Information that includes the identity of the particular payment instrument being used.”</p> <p><b>Construction For ‘783 and ‘429 Patents:</b>            “Information that includes the identity of the particular payment options being used.”</p>
<p><b>Court’s Construction:</b></p> <p><b><u>Payment Option:</u></b> “A credit card, debit card or other method of payment such as PayPal, Bill Me Later®, Western Union®, Secure eBill etc.”</p> <p><b><u>Payment instrument:</u></b> “A tangible method of payment including, e.g., credit card and debit card.”</p> <p><b><u>Payment information:</u></b></p> <p><b>Construction For ‘002 Patent:</b> “Information that includes the identity of the particular payment instrument being used.”</p> <p><b>Construction For ‘783 and ‘429 Patents:</b> “Information that includes the identity of the particular payment options being used.”</p>	

<sup>1</sup>One of ordinary skill in the art would not fail to be reasonably certain of this claim scope simply due to the specification’s failure to use the term “universal platform server.”

According to SecureBuy, “payment instrument” and “payment option” are different terms with distinct definitions. Payment instrument, SecureBuy contends, is a narrower term and refers only to credit and debit cards. Payment option, on the other hand, is a broader term and includes credit and debit cards along with other methods of payment such as PayPal, Bill Me Later, Western Union, and Secure eBill. The Court largely agrees with SecureBuy.

The term “payment instrument” only appears in the claims of the ‘429 and ‘002 patents. The term “payment option” appears in the claims of the ‘783 and ‘429 patents. The ‘002 patent defines “payment instrument(s).” (*See* ‘002 patent at 6:4-11) (“The checkout processing function 102 supports payment with a plurality of different types of payment instruments, e.g. credit and/or debit cards, belonging to different payment processing networks, e.g., Visa®, MasterCard®, etc.”). The key difference between the ‘002 patent and the ‘783 and ‘429 patents is that the latter patents broadened the disclosure to include payment methods not described in the ‘002 patent. The ‘783 and ‘429 patents used the term “payment options” to include the additional payment methods:

The checkout processing function 102 supports payment with a plurality of different types of payment instruments, e.g., credit and/or debit cards, belonging to different payment processing networks, e.g., Visa®, MasterCard®, etc. Alternatively, other payment options may include PayPal®, Bill Me Later®, Western Union, Secure eBill, etc. That is to say, the consumer/cardholder optionally selects the particular type of payment instrument or payment method being used for the commercial transaction from a plurality of supported payment types.

(‘783 patent at 5:64-6:7; ‘429 patent at 5:65-6:7) The varying specifications therefore support SecureBuy’s contention that “payment instrument” is a narrower term than “payment option.”

As SecureBuy’s proposal implies, the patentee used the term “instrument” to distinguish a tangible “instrument” from an intangible “method.” However, unlike SecureBuy’s proposal, the specifications provide lists of instruments and options that are exemplary, not exhaustive. Accordingly, the Court will adopt SecureBuy’s proposed constructions for all three “payment” terms but will modify them so that the listed examples are merely exemplary, not exhaustive.

11. “first party,” “second party,” “third party,” and “fourth party”

<b>Cardinal’s Proposed Construction</b>	<b>SecureBuy’s Proposed Construction</b>
<p><b><u>First party:</u></b> This term requires no construction beyond its plain and ordinary meaning.</p> <p><b><u>Second party:</u></b> This term requires no construction beyond its plain and ordinary meaning.</p> <p><b><u>Third party:</u></b> This term requires no construction beyond its plain and ordinary meaning.</p> <p><b><u>Fourth party:</u></b> This term requires no construction beyond its plain and ordinary meaning.</p>	<p><b><u>First party:</u></b> “The party accepting payment (the merchant).”</p> <p><b><u>Second party:</u></b> “The party providing payment (the consumer/buyer/cardholder).”</p> <p><b><u>Third party:</u></b> “A merchant authentication processing system containing connection, distribution and plug-in layers.”</p> <p><b><u>Fourth party:</u></b> “Issuing bank/entity.”</p>
<p><b>Court’s Construction:</b></p> <p><b><u>First party:</u></b> “A party that is different from the second party, third party, or fourth party.”</p> <p><b><u>Second party:</u></b> “A party that is different from the first party, third party, or fourth party.”</p> <p><b><u>Third party:</u></b> “A party that is different from the first party, second party, or fourth party.”</p> <p><b><u>Fourth party:</u></b> “A party that is different from the first party, second party, or third party.”</p>	

SecureBuy contends that the patent specifications particularly identify each of the first, second, third, and fourth parties. Cardinal disagrees and contends that the “party” terms simply distinguish one party from the others in the set, i.e., the “first party” is simply any party that is not the second, third, or fourth party. The Court agrees with Cardinal.

SecureBuy insists that the “first party” must be the merchant/party accepting payment. However, claims 2 and 7 of the ‘429 patent can be read such that the first party is the consumer and the second party is the merchant. (*See* ‘429 patent (Claim 2 requiring “providing the first party with one or more payment options, wherein each of the one or more payment options is associated with one of the plurality of authentication protocols”) (Claim 7 specifying “wherein the server of the third party receives the payment information from the first party via the second party”))

Similarly, SecureBuy proposes limiting “third party” to “a merchant authentication processing system containing connection, distribution and plug-in layers.” As SecureBuy notes, the term “third party” is never used in the patent specifications. The limitations proposed by SecureBuy are based on an exemplary embodiment but should not be read into the term.

Accordingly, the Court will construe the four “party” terms according to their plain and ordinary meaning, i.e., simply as parties that are different from each other.

12. **“Obtaining an authentication determination for the transaction in accordance with the selected protocol,” “obtaining an authentication determination from a fourth party in accordance with the authentication protocol,” “obtain an authentication determination in accordance with its associated authentication protocol.”**

Cardinal's Proposed Construction	SecureBuy's Proposed Construction
These terms require no construction beyond their plain and ordinary meaning.	"Carrying out those steps of the pertinent protocol necessary to get the authentication determination from the issuing entity/fourth party."
<b>Court's Construction:</b> "Carrying out those steps of the pertinent protocol necessary to get the authentication determination."	

The parties essentially dispute whether "obtaining" requires more than merely "receiving." The Court finds that it does. Receiving may be a passive act whereas obtaining requires the performance of some action. As the claims themselves note, obtaining the authentication determination must be done in accordance with, i.e., in a manner specified by, the authentication protocol. The Court agrees with SecureBuy that "obtaining . . . in accordance with the . . . protocol" requires "carrying out the steps of the pertinent protocol *necessary* to get that authentication determination" (emphasis added).

SecureBuy's proposed construction further requires that the authentication determination must come from the issuing entity/fourth party. For the reasons discussed with respect to the "authentication determination" term above, the Court disagrees.

13. **"means for obtaining an authentication determination for the commercial transaction in accordance with the selected authentication protocol, including formatting messages and routing the formatted messages over the communications network in accordance with one or more mandates of the selected authentication protocol" ('002 patent)**

**"means for obtaining an authentication determination for the commercial transaction in accordance with the selected authentication protocol, including formatting messages and routing the formatted messages" ('783 patent)**

Cardinal's Proposed Construction	SecureBuy's Proposed Construction
<p><b><u>'002 Patent</u></b>  <b>Function:</b>  Obtaining an authentication determination for the commercial transaction in accordance with the selected authentication protocol, including formatting messages and routing the formatted messages over the communications network in accordance with one or more mandates of the selected authentication protocol.</p> <p><b>Structure:</b>  A general purpose computer, with a plug-in layer that includes a plurality of plug-in components each associated with an authentication protocol (<i>e.g.</i>, VbV, SecureCode or SPA) corresponding to a type of payment instrument, programmed to:</p> <p>(1) format and route a message redirecting a cardholder to complete an authentication with an issuing entity as mandated by the selected authentication protocol ('002 Patent, Col. 11:1-6); and</p> <p>(2) receive a message pursuant to the selected authentication protocol containing an authentication determination in accordance with routing instructions provided as part of the message to the merchant ('002 Patent, Col. 11:6-12).</p>	<p><b><u>'002 Patent</u></b>  Indefinite</p> <p>To the extent, however, that the Court believes that such term is amenable to construction, SecureBuy proposes the following construction:</p> <p><b>Function:</b>  Obtaining an authentication determination for the commercial transaction in accordance with the selected authentication protocol, including formatting messages and routing the formatted messages over the communications network in accordance with one or more mandates of the selected authentication protocol.</p> <p><b>Structure:</b>  The consumer browser, authentication server, and a general purpose computer having with a plug-in layer that includes a plurality of plug-in components each associated with an authentication protocol (<i>e.g.</i>, VbV, SecureCode or SPA) corresponding to a type of payment instrument, programmed to format and route a message redirecting a cardholder browser to complete an authentication with an issuing entity server as mandated by the selected authentication protocol.</p>

**'783 Patent**

**Function:**

Obtaining an authentication determination for the transaction in accordance with the selected authentication protocol, including formatting and routing the formatted messages over the communications network in accordance with one or more mandates of the selected authentication protocol.

**Structure:**

A general purpose computer, with a plug-in layer that includes a plurality of plug-in components each associated with an authentication protocol (*e.g.*, VbV, SecureCode or SPA) corresponding to a type of payment instrument, programmed to:

- (1) format and route a message redirecting a cardholder to complete an authentication with an issuing entity as mandated by the selected authentication protocol ('783 Patent, Col. 10:66-Col.11:4); and
- (2) receive a message pursuant to the selected authentication protocol containing an authentication determination in accordance with routing instructions provided as part of the message to the merchant ('783 Patent, Col. 11:5-10).

**'783 Patent**

**Function:**

Obtaining an authentication determination for the transaction in accordance with the selected authentication protocol, including formatting and routing the formatted messages over the communications network in accordance with one or more mandates of the selected authentication protocol.

**Structure:**

The consumer browser, authentication server, and a general purpose computer having with a plug-in layer that includes a plurality of plug-in components each associated with an authentication protocol (*e.g.*, VbV, SecureCode or SPA) corresponding to a type of payment instrument, programmed to format and route a message redirecting a cardholder browser to complete an authentication with an issuing entity server as mandated by the selected authentication protocol.

**Court's Construction:**

**'002 Patent**

**Function:**

Obtaining an authentication determination for the commercial transaction in accordance with the selected authentication protocol, including formatting messages and routing the formatted messages over the communications network in accordance with one or more mandates of the selected authentication protocol.

**Structure:**

A general purpose computer, with a plug-in layer that includes a plurality of plug-in components each associated with an authentication protocol (e.g., VbV, SecureCode or SPA) corresponding to a type of payment instrument, programmed to:

- (1) format and route a message redirecting a cardholder to complete an authentication with an issuing entity as mandated by the selected authentication protocol ('002 Patent, Col. 11:1-6); and
- (2) receive a message pursuant to the selected authentication protocol containing an authentication determination in accordance with routing instructions provided as part of the message to the merchant ('002 Patent, Col. 11:6-12).

**'783 Patent**

**Function:**

Obtaining an authentication determination for the transaction in accordance with the selected authentication protocol, including formatting and routing the formatted messages over the communications network in accordance with one or more mandates of the selected authentication protocol.

**Structure:**

A general purpose computer, with a plug-in layer that includes a plurality of plug-in components each associated with an authentication protocol (e.g., VbV, SecureCode or SPA) corresponding to a type of payment instrument, programmed to:

- (1) format and route a message redirecting a cardholder to complete an authentication with an issuing entity as mandated by the selected authentication protocol ('783 Patent, Col. 10:66-Col.11:4); and
- (2) receive a message pursuant to the selected authentication protocol containing an authentication determination in accordance with routing instructions provided as part of the message to the merchant ('783 Patent, Col. 11:5-10).

The parties dispute whether the consumer browser and authentication server are part of



the structure necessary to perform the claimed function. Both parties seem to agree that MAPS executes the obtaining means. Thus, the only question is whether MAPS contains the consumer browser and authentication server. As Figure 3 of the specifications shows, the consumer browser and authentication server are not part of MAPS. This is further supported by the description in the specification:

For example, to accommodate a particular authentication initiative, a particular plug-in component 232 optionally formats and routes a messages to an issuing entity, e.g., an issuing bank having issued the particular payment instrument being used for the transaction, requesting that the issuing entity confirm the enrollment status of the particular payment instrument being used for the transaction. Upon obtaining a response to the enrollment request message from the issuing entity, the information may be returned to the merchant's server 100 in the same manner as if the MAPS 200 performed the enrollment check itself.

(‘002 patent at 56-67; ‘783 patent at 10:55-65) Accordingly, the Court will adopt Cardinal’s proposed constructions.

14. **“means for returning the obtained authentication over the communications network to a designated entity” (‘783 patent)**  
**“means for returning the obtained authentication determination to the first party’s server” (‘002 patent)**

<b>Cardinal's Proposed Construction</b>	<b>SecureBuy's Proposed Construction</b>
---	--

**'783 Patent**

**Function:**

Returning the obtained authentication determination over the communications network to a designated entity.

**Structure:**

A general purpose computer, with a plug-in layer that includes a plurality of plug-in components each associated with an authentication protocol (e.g., VbV, SecureCode or SPA) corresponding to a type of payment instrument, programmed to:

(1) verify that the obtained authentication determination was received from the issuing entity ('783 Patent, Col. 11:10-13); and

(2) sending the verified authentication determination to the designated entity ('783 Patent, Col. 10:49-51; Col. 1:13-17).

**'002 Patent**

**Function:**

Returning the obtained authentication determination to the first party's server

**Structure:**

A general purpose computer, with a plug-in layer that includes a plurality of plug-in components each associated with an authentication protocol (e.g., VbV, SecureCode or SPA) corresponding to a type of payment instrument, programmed to:

(1) verify that the obtained authentication determination was received from the issuing entity ('002 Patent, Col. 11:12-16); and

(2) send the verified authentication determination to the first party's server ('002 Patent, Col. 10:51-52).

**'783 Patent**

**Function:**

Returning the obtained authentication determination over the communications network to a designated entity.

**Structure:**

A general purpose computer, with a message distribution layer programmed to route messages, and plug-in layer that includes a plurality of individual authentication initiative plug-in components each associated with a different authentication protocol (e.g., VbV, SecureCode or SPA) corresponding to a type of payment instrument. The respective plug-in component activated by the selecting means is programmed to verify that the obtained authentication determination was received from the issuing entity and send the verified authentication determination to the merchants payment gateway.

**'002 Patent**

**Function:**

Returning the obtained authentication determination to the first party's server

**Structure:**

A general purpose computer, with a message distribution layer programmed to route messages, and plug-in layer that includes a plurality of individual authentication initiative plug-in components each associated with a different authentication protocol (e.g., VbV, SecureCode or SPA) corresponding to a type of payment instrument. The respective plug-in component activated by the selecting means is programmed to verify that the obtained authentication determination was received from the issuing entity and send the verified authentication determination to the merchants payment gateway.

## **Court's Construction**

### **'783 Patent**

**Function:** Returning the obtained authentication determination over the communications network to a designated entity

**Structure:** A general purpose computer, with a connection layer programmed to route messages, and plug-in layer that includes a plurality of individual authentication initiative plug-in components each associated with a different authentication protocol (*e.g.*, VbV, SecureCode or SPA) corresponding to a type of payment instrument. The respective plug-in component activated by the selecting means is programmed to verify that the obtained authentication determination was received from the issuing entity and send the verified authentication determination to the merchants payment gateway.

### **'002 Patent**

**Function:** Returning the obtained authentication determination to the first party's server

**Structure:** A general purpose computer, with a connection layer programmed to route messages, and plug-in layer that includes a plurality of individual authentication initiative plug-in components each associated with a different authentication protocol (*e.g.*, VbV, SecureCode or SPA) corresponding to a type of payment instrument. The respective plug-in component activated by the selecting means is programmed to verify that the obtained authentication determination was received from the issuing entity and send the verified authentication determination to the merchants payment gateway.

The parties have several disputes with respect to the “means for returning” term. First, the parties dispute whether the external connection layer is necessary structure to perform the function.<sup>2</sup> Second, the parties dispute whether it is necessary to limit the structure such that the plug-in component is programmed to verify that the obtained authentication determination was received.

---

<sup>2</sup> In its initial proposals, SecureBuy sought to have a “message distribution layer programmed to route messages” as part of the construction for this term. (D.I. 92 at 20, 33) However, from the claim construction briefing and Markman hearing, it appears that SecureBuy actually seeks a construction incorporating the “connection layer programmed to route messages.” (D.I. 140 at 7)

On the first issue, the Court finds that the connection layer is necessary structure. The Court has already found that a connection layer is “a generic software layer for external entities to connect to and process a specific payment authentication transaction.” The authentication determination is being returned by some external party, requiring a communication layer, making the communication layer a necessary part of the “means for returning” structure.

On the second issue, the Court agrees with SecureBuy that plug-in components need to be programmed to perform the disclosed algorithm. The specification states that:

Optionally, the plug-in component 232 verifies that the response to the second message was obtained from the issuing entity, e.g., by checking a digital signature incorporated with the response.

(’002 patent 11:12-15; ’783 patent at 11:10-13) Because the structure disclosed in the specification limits the “returning means” to this particular embodiment, the Court finds that the “returning means” term is so limited.

Accordingly, the Court adopts SecureBuy’s proposed construction.

**15. Plug-in/Plug-in component**

<b>Cardinal’s Proposed Construction</b>	<b>SecureBuy’s Proposed Construction</b>
<p><b>Construction:</b> This term requires no construction beyond its plain and ordinary meaning. To the extent, however, that the Court believes that such term requires additional explication, CardinalCommerce proposes the following construction:</p> <p>“A software component that is modular such that it is designed to be inserted into an existing software application.”</p>	<p>“Software component that executes the set procedures required for the respective, specified authentication protocol.”</p>
<p><b>Court’s Construction:</b> “A software component that is modular such that it is designed to be inserted into an existing software application.”</p>	

Both parties agree that the “plug-in”/“plug-in component” is a software module.

SecureBuy’s construction adds limitations such as “execut[ing] the set procedures required for the respective, specified authentication protocol” that are explicitly stated in the claims and would be redundant if incorporated into the “plug-in” terms’ construction. (*See, e.g.*, ‘002 patent Claim 1 (“each plug-in component administering a different one of a plurality of authentication programs in accordance with the authentication protocols prescribed . . . .”)). Accordingly, the Court will adopt Cardinal’s construction.

### **III. CONCLUSION**

The Court will construe the disputed claim terms of the patents-in-suit consistent with this Memorandum Opinion. An appropriate Order follows.

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

SECUREBUY, LLC, :  
 :  
 : Plaintiff, :  
 :  
 : v. : C.A. No. 13-1792-LPS  
 :  
 : CARDINALCOMMERCE CORPORATION, :  
 :  
 : Defendant. :  
 :

---

**ORDER**

At Wilmington, this **16th** day of **June, 2014**:

For the reasons set forth in the Memorandum Opinion issued this date,

IT IS HEREBY ORDERED that the disputed claim language of U.S. Patent Nos.

8,140,429 (the “429 Patent”), 7,051,002 (the “002 Patent”), and 7,693,783 (the “783 Patent”)

are construed as follows:

<b>Claim Term</b>	<b>Court’s Construction</b>
<b>authentication program</b>	Program or initiative for verifying that a consumer is likely to be who he/she claims to be.
<b>authentication protocol</b>	a prescribed set of rules, including those for formatting and routing messages, governing the transmission of messages over a communications network designed to verify that a consumer is who he/she claims to be.
<b>authentication determination</b>	An indication of whether a consumer has been authenticated.
<b>connection layer</b>	A generic software layer for external entities to connect to and process a specific payment authentication transaction.
<b>distribution layer</b>	A software layer for routing messages among other software layers within the system.
<b>plug-in layer</b>	A software layer comprising various plug-in components.

<p><b>means for determining from the payment information received at the universal platform server, for each commercial transaction, which of the different authentication protocols is prescribed by the payment network for the type of payment instrument identified in the payment information</b> ('002 Patent)</p>	<p><b>Function:</b> Determining from the payment information received at the universal platform server, for each commercial transaction, which of the different authentication protocols is prescribed by the payment network for the type of payment instrument identified in the payment information.</p> <p><b>Structure:</b> A general purpose computer, with a plug-in layer that includes a plurality of plug-in components each associated with an authentication protocol (e.g., VbV, SecureCode or SPA) corresponding to a type of payment instrument, programmed to:</p> <p>(1) determine the type of payment instrument from the payment information received ('002 Patent, Col. 10:7-11); and</p> <p>(2) determine whether the payment instrument of step (1) is enrolled in an authentication program/initiative ('002 Patent, Col. 10:12-37; Col. 10:54-67), each of which is associated with a particular authentication protocol ('002 Patent, Col. 3:15-20; Col. 9:52-57).</p>
<p><b>means for determining from the payment information received at the server which of the different authentication protocols is prescribed for the type of payment option identified in the payment information”</b> ('783 patent)</p>	<p><b>Function:</b> Determining from the payment information received at the server, for each commercial transaction, which of the different authentication protocols is prescribed by the payment network for the type of payment instrument identified in the payment information.</p> <p><b>Structure:</b> A general purpose computer, with a plug-in layer that includes a plurality of plug-in components each associated with an authentication protocol (e.g., VbV, SecureCode or SPA) corresponding to a type of payment instrument, programmed to:</p> <p>(1) determine the type of payment instrument from the payment information received ('783 Patent, Col. 10:7-11); and</p> <p>(2) determine whether the payment instrument of step (1) is enrolled in an authentication program/initiative ('783 Patent, Col. 10:12-37; Col. 10:54-67), each of which is associated with a particular authentication protocol ('783 Patent, Col. 9:50-55).</p>



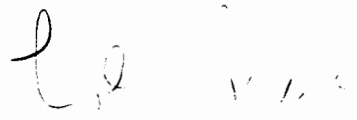
<p><b>means for selecting, in accordance with the determination of step (b), a particular authentication protocol from the plurality of different authentication protocols supported by the universal platform server ('002 patent)</b></p>	<p><b>Function:</b> Selecting, in accordance with the determination of step (b), a particular authentication protocol from the plurality of different authentication protocols supported by the universal platform server.</p> <p><b>Structure:</b> The universal platform server (see below); including a general purpose computer, with a message distribution layer programmed to route messages, and plug-in layer that includes a plurality of individual authentication initiative plug-in components each associated with a different authentication protocol (e.g., VbV, SecureCode or SPA) corresponding to a type of payment instrument. The plug-in components are programmed to listen to a message distribution layer for a specific message type. The respective plug-in component is activated by the message distribution layer that sends messages to the specified plug-in component based upon the type of payment instrument being used for the transaction being processed.</p>
<p><b>means for selecting, in accordance with the determination made by the means for determining, a particular authentication protocol from the plurality of different authentication protocols supported by the server" ('783 patent)</b></p>	<p><b>Function:</b> Selecting, in accordance with the determination made by the means for determining, a particular authentication protocol from the plurality of different authentication protocols supported by the server.</p> <p><b>Structure:</b> A general purpose computer, with a message distribution layer programmed to route messages, and plug-in layer that includes a plurality of individual authentication initiative plug-in components each associated with a different authentication protocol (e.g., VbV, SecureCode or SPA) corresponding to a type of payment instrument. The plug-in components are programmed to listen to a message distribution layer for a specific message type. The respective plug-in component is activated by the message distribution layer that sends messages to the specified plug-in component based upon the type of payment instrument being used for the transaction being processed.</p>
<p><b>Universal platform server</b></p>	<p>A server configured to support a plurality of merchants and a plurality of authentication protocols.</p>

<p><b>“payment option,” “payment instrument,” and “payment information”</b></p>	<p><b><u>Payment Option</u></b>: A credit card, debit card or other method of payment such as PayPal, Bill Me Later®, Western Union®, and Secure eBill etc.</p> <p><b><u>Payment instrument</u></b>: A tangible method of payment including, e.g., credit card or debit card.</p> <p><b><u>Payment information</u></b>:  <b>Construction For ‘002 Patent</b>:  Information that includes the identity of the particular payment instrument being used.</p> <p><b>Construction For ‘783 and ‘429 Patents</b>:  Information that includes the identity of the particular payment options being used.</p>
<p><b>“first party,” “second party,” “third party,” and “fourth party”</b></p>	<p><b><u>First party</u></b>: A party that is different from the second party, third party, or fourth party.</p> <p><b><u>Second party</u></b>: A party that is different from the first party, third party, or fourth party.</p> <p><b><u>Third party</u></b>: A party that is different from the first party, second party, or fourth party.</p> <p><b><u>Fourth party</u></b>: A party that is different from the first party, second party, or third party.</p>

<p><b>“Obtaining an authentication determination for the transaction in accordance with the selected protocol,” “obtaining an authentication determination from a fourth party in accordance with the authentication protocol,” “obtain an authentication determination in accordance with its associated authentication protocol.”</b></p>	<p>Carrying out those steps of the pertinent protocol necessary to get the authentication determination.</p>
<p><b>means for obtaining an authentication determination for the commercial transaction in accordance with the selected authentication protocol, including formatting messages and routing the formatted messages over the communications network in accordance with one or more mandates of the selected authentication protocol (‘002 patent)</b></p>	<p><b>Function:</b> Obtaining an authentication determination for the commercial transaction in accordance with the selected authentication protocol, including formatting messages and routing the formatted messages over the communications network in accordance with one or more mandates of the selected authentication protocol.</p> <p><b>Structure:</b> A general purpose computer, with a plug-in layer that includes a plurality of plug-in components each associated with an authentication protocol (<i>e.g.</i>, VbV, SecureCode or SPA) corresponding to a type of payment instrument, programmed to: (1) format and route a message redirecting a cardholder to complete an authentication with an issuing entity as mandated by the selected authentication protocol (‘002 Patent, Col. 11:1-6); and (2) receive a message pursuant to the selected authentication protocol containing an authentication determination in accordance with routing instructions provided as part of the message to the merchant (‘002 Patent, Col. 11:6-12).</p>

<p><b>means for obtaining an authentication determination for the commercial transaction in accordance with the selected authentication protocol, including formatting messages and routing the formatted messages ('783 patent)</b></p>	<p><b>Function:</b> Obtaining an authentication determination for the transaction in accordance with the selected authentication protocol, including formatting and routing the formatted messages over the communications network in accordance with one or more mandates of the selected authentication protocol.</p> <p><b>Structure:</b> A general purpose computer, with a plug-in layer that includes a plurality of plug-in components each associated with an authentication protocol (e.g., VbV, SecureCode or SPA) corresponding to a type of payment instrument, programmed to: (1) format and route a message redirecting a cardholder to complete an authentication with an issuing entity as mandated by the selected authentication protocol ('783 Patent, Col. 10:66-Col.11:4); and (2) receive a message pursuant to the selected authentication protocol containing an authentication determination in accordance with routing instructions provided as part of the message to the merchant ('783 Patent, Col. 11:5-10).</p>
<p><b>means for returning the obtained authentication determination to the first party's server ('002 patent)</b></p>	<p><b>Function:</b> Returning the obtained authentication determination to the first party's server</p> <p><b>Structure:</b> A general purpose computer, with a connection layer programmed to route messages, and plug-in layer that includes a plurality of individual authentication initiative plug-in components each associated with a different authentication protocol (e.g., VbV, SecureCode or SPA) corresponding to a type of payment instrument. The respective plug-in component activated by the selecting means is programmed to verify that the obtained authentication determination was received from the issuing entity and send the verified authentication determination to the merchants payment gateway.</p>

<p><b>means for returning the obtained authentication over the communications network to a designated entity ('783 patent)</b></p>	<p><b>Function:</b> Returning the obtained authentication determination over the communications network to a designated entity</p> <p><b>Structure:</b> A general purpose computer, with a connection layer programmed to route messages, and plug-in layer that includes a plurality of individual authentication initiative plug-in components each associated with a different authentication protocol (<i>e.g.</i>, VbV, SecureCode or SPA) corresponding to a type of payment instrument. The respective plug-in component activated by the selecting means is programmed to verify that the obtained authentication determination was received from the issuing entity and send the verified authentication determination to the merchants payment gateway.</p>
<p><b>Plug-in/Plug-in component</b></p>	<p>A software component that is modular such that it is designed to be inserted into an existing software application.</p>



UNITED STATES DISTRICT JUDGE