UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/320,535	06/30/2014	Richard Lee Slater	37202/557001; 137707US	8163

57956 7590 08/24/2020

FBFK/Intuit
Robert Lord
3200 Southwest Freeway, Suite 3200
HOUSTON, TX 77027

EXAMINER
FENSTERMACHER, JASON B

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
08/24/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@fbfk.law
jhathaway@fbfk.law
rlord@fbfk.law

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte RICHARD LEE SLATER,
RANDAL GEYER, and MUGUR STEFANESCU

Appeal 2020-002313
Application 14/320,535
Technology Center 3600

Before JAMES P. CALVE, NINA L. MEDLOCK, and
BRADLEY B. BAYAT, *Administrative Patent Judges*.

CALVE, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Pursuant to 35 U.S.C. § 134(a), Appellant[1] appeals from the decision of the Examiner to reject claims 1, 3, 4, 9, 11, 12, 17, 19, 20, and 26–28, which are all the pending claims.[2] Appeal Br. 4. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.

---

[1] "Appellant" refers to "applicant" as defined in 37 C.F.R. § 1.42. Appellant identifies Intuit Inc. as the real party in interest. Appeal Br. 4.

[2] Claims 2, 5–8, 10, 13–16, 18, and 21–25 have been cancelled. *See* Appeal Br. 28–32 (Claims App.), filed Oct. 10, 2019. A Reply Under 37 C.F.R. § 1.116 was filed on July 18, 2019, to cancel claims 4, 12, and 20, but the amendment was not entered. *See* Adv. Action, mailed July 31, 2019.

CLAIMED SUBJECT MATTER

Claims 1, 9, and 17 are independent. Claim 1 is reproduced below.

1. A method comprising:
generating, at a token service operating in a payment card industry data security standard (PCI-DSS) system and in response to receiving a card data tokenize request from a point of sale (POS) system, a card data token,
wherein the card data tokenize request includes card data received from a card reader, and
wherein the card data token is a sequence of characters representing the card data and matching the format of the card data;
transmitting, by the token service, the card data token to the POS system;
thereafter receiving, by a payment service operating in the PCI-DSS system and from the POS system, a payment request comprising both sale data and the card data token, wherein the payment request is received via a gateway, and wherein the sale data includes a transaction amount, a tax amount, and an itemized list of items purchased;
generating, by the payment service, the detokenize and erase request comprising the card data token;
sending, by the payment service, the detokenize and erase request to the token service;
detokenizing, by the token service, card data from the card data token;
transmitting, by the token service, the card data;
receiving, by the payment service, the card data;
generating, by the payment service, a payment process request comprising the sale data and the card data;
sending, by the payment service, the payment process request to a payment authorization service;

receiving, at the payment service, a payment response from the payment authorization service in response to the sending the payment process request; and

sending, by the payment service, the payment response to the POS system.

Appeal Br. 27–28 (Claims App.).[3]

REJECTIONS

Claims 1, 3, 4, 9, 11, 12, 17, 19, 20, and 26–28 are rejected under 35 U.S.C. § 112(b) as being indefinite.

Claims 1, 3, 4, 9, 11, 12, 17, 19, 20, and 26–28 are rejected under 35 U.S.C. § 101 as being directed to a judicial exception without significantly more.

ANALYSIS

Indefiniteness of Claims 1, 3, 4, 9, 11, 12, 17, 19, 20, and 26–28

The Examiner determines that the limitations "generating, at a token service operating in a payment card industry data security standard (PCI-DSS) system and in response to receiving a card data tokenize request from a point of sale (POS) system, a card data token" and "thereafter receiving, by a payment service operating in the PCI-DSS system . . . , a payment request" in claim 1 make the claim indefinite because it is unclear what operating in a PCI-DSS system means, and what requirements are considered a PCI-DSS system. Final Act. 5–6. The Examiner finds that the Specification does not identify any particular requirements for operating in a PCI-DSS system or for generating a token in such a system at a token service so the scope of the invention is unclear. *Id.*; Ans. 6–9.

[3] Refers to the revised Claims Appendix that was filed on October 10, 2019, as do all other citations to the Claims Appendix in this decision.

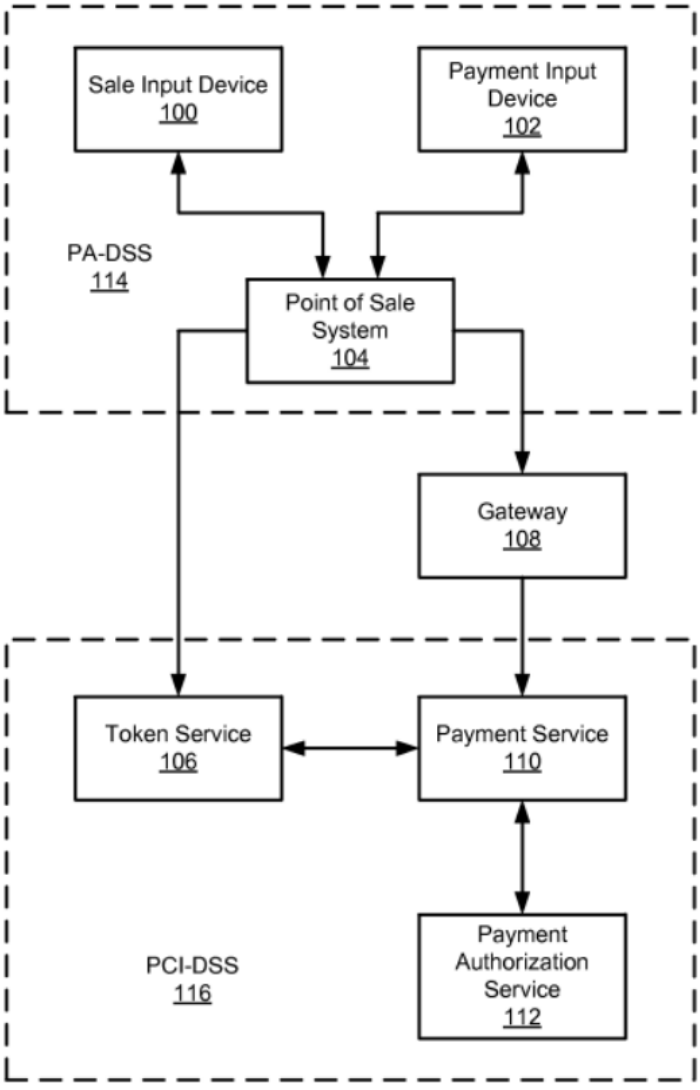
Appellant responds that the limitations "plainly recite a token service operating in the PCI-DSS and a payment service operating in the PCI-DSS" and therefore "the claims plainly limit the operating characteristics of the token service and the payment service to be constrained by the rules of the PCI-DSS." Appeal Br. 11–12 ("Thus, the plain meaning shows that certain components must operate according to the PCI-DSS standard."). Appellant also contends that the PCI-DSS standards are easily accessible, explicitly defined, and widely used in the art so that a skilled artisan would consider application of the PCI-DSS to a system to be determinate in scope. *Id.* at 12. Appellant asserts that "the PCI-DSS is used by millions of organizations, and must be very well known in the art" so the Examiner cannot assert "it is unknown what particular requirements are needed in order to be considered a PCI-DSS." *Id.* at 12–13; *see* Reply Br. 4–5.

Principles of Law

"The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention." 35 U.S.C. § 112(b). The language of "particularly" and "distinctly" requires claim terms to be clear rather than ambiguous, vague, or indefinite. *In re Packard*, 751 F.3d 1307, 1313 (Fed. Cir. 2014). Thus, "[a] claim is indefinite when it contains words or phrases whose meaning is unclear." *Id.* at 1309–10 (quoting MPEP § 2173.05(e)); *id.* at 1314 (affirming finding of indefiniteness under the MPEP standard). The USPTO rejects claims based on the perspective of a person of ordinary skill in view of the written description and prosecution history. *Id.* at 1312. This determination is a question of law. *Id.* at 1311. However, "[b]readth is not indefiniteness." *In re Gardner*, 427 F.2d 786, 788 (CCPA 1970).

Claim 1 recites a card data token is generated at a token service that operates in compliance with a payment card industry data security standard, i.e., a PCI-DSS, system. Also, a payment request is received by a payment service that operates in compliance with the PCI-DSS. The services are part of a system that operates in accordance with the PCI-DSS.

The Specification states that "[t]he token service (106), the payment service (108), and the payment authorization service (110) are governed by the PCI-DSS (116)." Spec. ¶ 15. Figure 1 of Appellant's disclosure is reproduced below to illustrate this configuration.



Appellant's Figure 1 above illustrates a system that includes token service 106, payment service 108, and payment authorization service 110 governed by the PCI-DSS 116. *Id.* ¶ 15. The fact that each service is governed by the PCI-DSS is illustrated by placing the token service 106, the payment service 108, and the payment authorization service 110 within a dashed-line box labelled PCI-DSS 116 to indicate that the services operate in compliance with, and are governed by, the PCI-DSS. *See id.*

"The gateway (108) is out of the scope of both the PA-DSS (114) and the PCI-DSS (116)." *Id.* Figure 1 illustrates this aspect with gateway 108 outside the areas/devices governed by PA-DSS 114 and PCI-DSS 116.

"[I]t is appropriate to look at industry standards and definitions to interpret disputed claim terms." *Advanced Fiber Techs. (AFT) Trust v. J & L Fiber Servs., Inc.*, 674 F.3d 1365, 1380 n.4 (Fed. Cir. 2012). Furthermore, as our reviewing court recently advised:

> We have previously found claims indefinite where the claim requires a specific measurement or calculation, more than one measurement method may be used and no guidance has been provided. *See Teva*, 789 F.3d at 1345; *Honeywell Int'l, Inc. v. ITC*, 341 F.3d 1332, 1339–40 (Fed. Cir. 2003). *Teva* is representative in this instance. In *Teva*, we determined that where the claim included a specific measurement of a "molecular weight" of a claimed copolymer and the specification did not indicate which of three measurement methods used in the industry was used (Mp, Mw, or Mn), the claim was indefinite. *Teva*, 789 F.3d at 1345. Because it was unclear which measurement to use for the claimed molecular weight and those different measurements would yield different results, the claim "failed to inform with *reasonable certainty* those skilled in the art about the scope of the invention." *Id.*

Pacific Coast Bldg. Prods., Inc. v. CertainTeed Gypsum, Inc., Appeal 2019-1524, 2020 WL 3526401, at *4 (Fed. Cir. June 30, 2020).

Here, claim 1 requires a token service and payment service operating in compliance with the PCI-DSS to generate a card data token and payment request, respectively. Appeal Br. 27 (Claims App.).[4] Claim 1 even recites that "the card data token is a sequence of characters representing the card data and matching the format of the card data." Appeal Br. 27 (Claims App.). Thus, claim 1 recites a specific format for the tokenized card data.

The Specification states that "the PCI-DSS (116) is a set of security requirements for payment processing systems that store, processes, [*sic*] or transmit card data." Spec. ¶ 22. Appellant asserts that these requirements are known and publicly-accessible at the PCI Security Standards Council website at https://www.pcisecuritystandards.org/. Appeal Br. 12. Appellant reproduces an excerpt from section 2.1.1 regarding Tokenization Guidelines. Reply Br. 12–13. Section 2.1.1 states that "[t]oken generation describes the process or method of creating a token. Common forms of token generation include *but are not limited to*: A mathematically reversible cryptographic function . . .[,] A one-way non-reversible cryptographic function . . .[, and] Assignment through an index function, sequence number or a randomly generated number (not mathematically derived from the PAN)." *See id.* at 12 (emphasis added). In light of the understanding in the art of the PCI-DSS and the Specification, a skilled artisan would understand that a token service operating in a PCI-DSS system can generate card token data in many ways that include, but are not limited, to cryptographic techniques and index functions. However, claim 1 recites a particular tokenization that generates a card data token as a sequence of characters that match the card data format.

[4] Independent claims 9 and 17 include similar limitations. *See* Appeal Br. 28–30 (Claims App.).

The Specification describes the claimed tokenization step as "[t]he token service (106) may further include functionality to provide a card data token keyed to the card data." Spec. ¶ 18. "[T]he card data token may be a sequence of characters matching the format of the card data." *Id.* ¶ 34.

No other features are recited for the card data token generated at a token service. No encryption is required. *See* Ans. 7. The Specification states that "[t]hose skilled in the art will appreciate that the card data does not need to be encrypted to be tokenized." Spec. ¶ 24.

The claimed tokenization step is consistent with section 2.1.1 which states card data can be tokenized by "[c]ommon forms of token generation" in addition to the examples of a mathematically reversible cryptographic function, a one-way, non-reversible cryptographic function, and assignment through an index function. Reply Br. 12–13. Thus, the claimed card data token format of a sequence of characters is consistent with the PCI-DSS and, in any event, is recited expressly and plainly in claim 1.

Claim 1 also recites "receiving, by a payment service operating in the PCI-DSS system and from the POS system, a payment request comprising both sale data and the card data token." Appeal Br. 27 (Claims App.). The scope of a payment service receiving a payment request is clear. The step includes receiving a payment request comprising sale data and the card data token. No other steps or features are recited or applicable.

Accordingly, we determine that the meaning of claim 1 is clear. The Examiner has not explained sufficiently why the scope of claim 1 (and independent claims 9 and 17) is not clear in light of the plain meaning of the claim language interpreted in light of the Specification and PCI-DSS.

Thus, we do not sustain this rejection of the claims.

Patent Eligibility of Claims 1, 3, 4, 9, 11, 12, 17, 19, 20, and 26–28

Appellant argues the claims as a group. Appeal Br. 14 ("The claims stand or fall with claim 1."). We select claim 1 as representative. *See* 37 C.F.R. § 41.37(c)(1)(iv).

Examiner's Determination

The Examiner determines that claim 1 recites certain methods of organizing human activity as a fundamental economic practice of protecting consumer information during a transaction and/or a commercial or legal transaction between the point of sale, token service, and payment service. Final Act. 8. The Examiner also determines that the steps recited in claim 1 manage an interaction between various payment entities to process payments for a customer and point of sale. *Id.* The Examiner further determines that reciting the concept in a particular environment of a PCI-DSS does not move the claims beyond an abstract idea when the steps are performed on generic computer components of a token service, a payment service, and the generic components do not integrate the abstract idea into a practical application. *Id.* at 8–9. The Examiner determines that the token service and payment service are recited at a high level of generality that amounts to instructions to apply the judicial exception using a generic computer system or service. *Id.* at 9.

The Examiner also determines that claim 1 lacks additional elements that amount to significantly more than the judicial exception because using a token service and a payment service to implement the abstract idea simply applies the exception using generic computer components, systems, and/or services that cannot provide an inventive concept. *Id.* at 10. The Examiner determines that the ordered combination adds nothing that is not already present when the steps are considered separately. *Id.*

Appellant's Contentions

Appellant argues that generating a card data token in a PCI-DSS system recites a specific instruction to a computer in an electronic payment system and therefore is not a method of organizing human activity, a mental process, or a mathematical formula. Appeal Br. 16. Appellant also argues that steps of generating, sending, and receiving the payment process request and payment response are specific acts performed by specific aspects of the PCI-DSS and, thus, relate to the use of an electronic payment system. *Id.* Appellant further asserts that the steps do not fall within certain methods of organizing human behavior because humans do not tokenize and detokenize data as claimed. *Id.* at 17. Appellant contends that humans do not organize human behavior by "generating . . . in response to receiving a card data tokenize request from a point of sale (POS) system, a card data token." *Id.* ("A POS system (e.g., a card reader) is clearly a device, and transmitting data to the device is not organizing human behavior.").

Appellant asserts that "[t]he *claimed* invention uses *limited life tokens* to be used within the PCI-DSS system to address the technical challenges of access control and data protection of electronic payment data in a network" so "the claims manifestly integrate any recited judicial exception . . . into a practical application of altering the secure processing of the electronic payment in a network." *Id.* at 18. Appellant argues that all of the features identified by the Examiner as a judicial exception under [Step 2A,] Prong One [of the USPTO's § 101 guidance] are practical applications of computer technology to enable electronic payments in an improved manner in the context of PCI-DSS. *Id.* Appellant also asserts that the claims recite an inventive concept because they are not obvious over the prior art. *Id.* at 19.

Principles of Law

Section 101 of the Patent Act states:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

35 U.S.C. § 101. This provision contains an implicit exception: "Laws of nature, natural phenomena, and abstract ideas are not patentable." *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 216 (2014).

To distinguish patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications, we first determine whether the claims are directed to a patent-ineligible concept. *Id.* at 217. If they are, we consider the elements of each claim, individually and "as an ordered combination," to determine if additional elements "'transform the nature of the claim' into a patent-eligible application" as an "inventive concept" sufficient to ensure the claims in practice amount to significantly more than a patent on the ineligible concept itself. *See id.* at 217–18.

The USPTO has issued guidance about this framework. 2019 Revised Patent Subject Matter Eligibility Guidance, 84 Fed. Reg. 50 (Jan. 7, 2019) ("Revised Guidance"). Under the Revised Guidance, to determine whether a claim is "directed to" an abstract idea, we evaluate whether the claim recites: (1) any judicial exceptions, including certain groupings of abstract ideas listed in the Revised Guidance (i.e., mathematical concepts, certain methods of organizing human activities such as a fundamental economic practice, or mental processes); and (2) additional elements that integrate the judicial exception into a practical application (*see* MPEP §§ 2106.05(a)–(c), (e)–(h) (9th ed. rev. 08.2017 Jan. 2018) ("MPEP")). *Id.* at 52–55.

Only if a claim (1) recites a judicial exception and also (2) does not integrate that exception into a practical application, do we then consider whether the claim (3) adds a specific limitation beyond the judicial exception that is not "well-understood, routine, conventional" in the field (*see* MPEP § 2106.05(d)) or (4) simply appends well-understood, routine, conventional activities previously known to the industry, specified at a high level of generality, to the judicial exception. *Id.* at 56.

Step 1: Is Claim 1 Within a Statutory Category?

Appellant argues the independent claims as a group. Appeal Br. 14–26. We select claim 1 as representative. *See* 37 C.F.R. § 41.37(c)(1)(iv).

Claim 1 recites a "method" which is a statutory category of 35 U.S.C. § 101, namely, a process. Final Act. 7. Thus, we next consider whether claim 1 as a whole recites a judicial exception.

Step 2A, Prong One: Does Claim 1 Recite a Judicial Exception?

We agree with the Examiner that claim 1 recites an abstract idea. The Revised Guidance enumerates this judicial exception as certain methods of organizing human activity—fundamental economic practices or commercial interactions and sales activities. Revised Guidance, 84 Fed. Reg. at 52.

The Specification at least implies that payment transaction processing is a fundamental economic practice. The Background states that "[w]hen processing payment transactions, payment data must be properly handled and protected throughout its life cycle from the point of sale system through all hosted applications." Spec. ¶ 1. "This is generally accomplished through a layered approach to security that meets well-defined access control and data protection (*e.g.*, encryption, tokenization, hashing) requirements." *Id.* Thus, payment transaction processing is widely known and used in the art.

Appellant recognizes that generating card data tokens and payment processing steps are part of electronic payment systems. Appellant argues that "generating a card data token is, in the context of the PCI-DSS system, manifestly a specific instruction to a computer in an electronic payment system environment." Appeal Br. 16. In addition, "generating, sending, and receiving the payment process request and the payment response are all specific acts performed by specific aspects of the PCI-DSS, and thus manifestly relate[] to the use of an electronic payment system." *Id.*

The steps of claim 1 recite aspects of the judicial exception. *See* Final Act. 7–8. These steps include "generating, at a token service . . . a card data token," "transmitting . . . the card data token to the POS system," "receiving, by a payment service . . . a payment request comprising both sale data and the card data token," "generating, by the payment service, the detokenize and erase request," "sending, by the payment service, the detokenize and erase request to the token service," "detokenizing, by the token service, card data from the card data token," "transmitting . . . the card data," "receiving . . . the card data," "generating, by payment service, a payment process request comprising the sale data and the card data," "sending, by the payment service, the payment process request to a payment authorization service," "receiving, at the payment service a payment response from the payment authorization service . . .," and "sending, by the payment service, the payment response to the POS system." Appeal Br. 27–28 (Claims App.).

The Specification indicates PCI-DSS is "a set of security requirements for payment processing systems that store, process[], or transmit card data." *Id.* ¶ 22. The Specification at least implies that payment processing systems are known in the art for processing card data and are governed by PCI-DSS.

Furthermore, Appellant does not dispute that the claimed method recites a fundamental economic practice relating to payment processing steps. Instead, Appellant argues that claim 1 is not a method of organizing human behavior because "humans do not tokenize and detokenize data, as claimed." Appeal Br. 17. Appellant asserts that "[t]he *claimed* invention uses *limited life tokens* to be used within the PCI-DSS system to address the technical challenges of access control and data protection of electronic payment data in a network." *Id.* at 18.

As the Federal Circuit held in an analogous situation involving a card transaction at a POS device, "[t]he idea that a customer may pay for items ordered from a remote seller at a third-party's local establishment is the type of fundamental business practice that, when implemented using generic computer technology, is not patent-eligible." *Inventor Holdings LLC v. Bed Bath & Beyond, Inc.*, 876 F.3d 1372, 1378 (Fed. Cir. 2017). Furthermore, in *Inventor Holdings*, the fundamental economic practice recited in the claims involved an "order code" that a remote seller generated and a buyer entered at a POS terminal in a local retail store to pay for an order. *Id.* at 1375. The claimed order code thus operated as a token to protect the credit card data of consumers because "[m]any consumers . . . do not feel secure in providing their credit card number to a 'stranger' over the telephone." *Id.*

In *Inventor Holdings*, "the invention cover[ed] purchasing goods from a remote seller by placing an order, receiving an order code, entering the order code at a POS terminal, and paying for the order in person." *Id.* Here, claim 1 recites similar steps that generate a card data token that is received at a POS system and sent to a payment service so card data is protected during portions of the payment processing. *See* Spec. ¶¶ 1, 14, 28, 34.

Just as the "card data token" and "token service" in claim 1 protect card data (*see id.* ¶¶ 1, 14, 18, 33), the order code in *Inventor Holdings* was alleged by the patentee to be "a unique solution to protect a person from having his or her credit card information stolen when making a remote purchase." *Inventor Holdings*, 876 F.3d at 1376. Nonetheless, the court determined that use of the order code in the payment process of *Inventor Holding* recited a fundamental economic practice. *Id.* at 1378; *see also* Revised Guidance, 84 Fed. Reg. at 52 & n.13 (citing *Inventor Holdings* and other similar cases that recite fundamental economic practices).

Essentially, the "token service" acts as a third party intermediary to facilitate the payment transaction by protecting the confidentiality of card data while also guaranteeing the reliability of the tokenized card data relative to the actual card data stored at the token service. The use of a third party intermediary to provide intermediated settlement services is a fundamental economic practice. *See Alice*, 573 U.S. at 219 ("On their face, the claims before us are drawn to the concept of intermediated settlement, *i.e.,* the use of a third party to mitigate settlement risk. Like the risk hedging in *Bilski*, the concept of intermediated settlement is 'a fundamental economic practice long prevalent in our system of commerce."). The method in *Alice* involved a method of exchanging financial obligations between two parties using a third-party intermediary to mitigate settlement risk by creating and updating "shadow" records that reflected the value of each party's actual accounts held at "exchange institutions" so only parties with sufficient resources can complete a transaction. *Id.* Here, the "token service" is an intermediary that protects/stores card data while ensuring that the correct card data is linked to the tokenized data and provided for final payment processing.

In an analogous situation, using a third party to provide a transaction performance guaranty service for an online commercial transaction recited an abstract idea involving the creation of a contractual relationship that is of ancient lineage. *See buySAFE, Inc. v. Google, Inc.*, 765 F.3d 1350, 1354–55 (Fed. Cir. 2014). The claims recited a method in which a party to an online commercial transaction requested a transaction performance guaranty for the transaction in which a safe transaction service provider underwrote the first party to provide the transaction performance guaranty service to facilitate the online transaction. *Id.* at 1351–52. Here, a POS system requests a card data token from a token service to facilitate a commercial transaction and the token service sends a card data token to the POS system. A payment service sends a detokenize and erase request to the token service and receives back detokenized card data used to complete the payment transaction. *See* Appeal Br. 27–28 (Claims App.). The token service essentially guarantees that the tokenized card data corresponds to the card data used in the transaction.

Protecting a cardholder's card data through tokenization is similar to other fundamental economic practices such as anonymous loan shopping. *Mortg. Grader, Inc. v. First Choice Loan Servs. Inc.*, 811 F.3d 1314, 1318, 1324 (Fed. Cir. 2016). In *Mortgage Grader,* the method recited the concept of "anonymous loan shopping" by collecting information to generate a credit grading so "the borrower is anonymous to the lender until the borrower has been informed of the cost of the loan based on the borrower's credit grading, and the borrower then chooses to expose its identity to a lender." *Id.* at 1324 (adopting district court's holding that the claims recited an abstract idea); *id.* at 1326 (holding the use of a generic computer to implement a "fundamental economic practice" cannot make the claims patent eligible).

Similarly, using a bank card as a token has been held to be patent ineligible. *See Smart Sys. Innovations LLC v. Chicago Transit Auth.*, 873 F.3d 1364, 1372 (Fed. Cir. 2017) ("The Asserted Claims of the '816 patent involve acquiring identification data from a bankcard and funding a transit ride from one of multiple balances associated with that bankcard."). The court held that the formation of a financial transaction in a particular field of mass transit and collection of data related to the transactions without reciting a new type of bankcard, turnstile, or database that improved any technological processes was patent ineligible. *Id.*; *see also CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1370 (Fed. Cir. 2011) (holding that using the Internet to verify credit-card transactions did not make claims to verifying the credit card transaction patent-eligible); *Bozeman Fin. LLC v. Fed. Reserve Bank of Atlanta*, 955 F.3d 971, 976 (Fed. Cir. 2020) (holding that the prevention of fraud in financial transactions is a fundamental economic principle or practice).

As these decisions illustrate, merely generating a card data token and generating, sending ,and receiving a payment process request and payment response as recited in claim 1 does not take the claim out of the realm of a fundamental economic practice when recited at a high level of generality as in claim 1. Therefore, we do not agree with Appellant's arguments that such steps make claim 1 non-abstract. *See* Appeal Br. 16.

The claims in *Inventor Holdings* recited the step of "generating a code and a purchase price for said remote order" and "transmitting said code and said purchase price to the customer." *Inventor Holdings*, 876 F.3d at 1374. A seller generated an "order code" and a buyer entered the code at a POS terminal to pay for an order without using his or her credit card. *Id.* at 1375.

Steps of generating, sending, receiving, and even storing data when recited at a high level of generality as in claim 1 do not take the claim out of the abstract realm. In *Accenture*, the court held a claim to generating tasks based on rules to be completed upon the occurrence of an event was an abstract idea. *Accenture Global Servs., GmbH v. Guidewire Software*, 728 F.3d 1336, 1344 (Fed. Cir. 2013). The claim limitations recited a database of tasks, a means to allow a client access to those tasks, and a set of rules that are applied to a task on a given event. *Id.* at 1345. Here, claim 1 recites tasks to be completed as part of an electronic payment transaction in which a card data token is generated and transmitted with sales data and card data is stored at a token service. Even if the tasks are based on rules of a PCI-DSS system, such broadly recited rules, without more, do not take claim 1 out of the abstract idea realm as illustrated by *Accenture's* holding.

Here, the steps of generating a card data token, sending and receiving the card data token and detokenized card data among elements of the system and storing card data and tokens recite a fundamental economic practice and a method of organizing human activity for commercial sales activities. The performance of these steps in an electrical payment system does not take the steps out of the abstract realm as illustrated by *Inventor Holdings* where the order code was generated and used to perform a sales transaction over an electronic payment network. *Inventor Holdings*, 876 F.3d at 1374–75, 1378.

The claimed tokenization recites "the card data token is a sequence of characters representing the card data and matching the format of the card data." Appeal Br. 27 (Claims App.). This step can be performed as a mental process. Ans. 10–11; *see Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1354 (Fed. Cir. 2016).

The Examiner determines that generating a card data token as claimed merely involves substituting a sensitive data element with a non-sensitive equivalent. Ans. 11. The Examiner finds that tokenizing data is a common practice in the financial and medical industries where a financial form replaces a user's full credit card number with a token (e.g., XXX-XXX-XXX-1234) or a medical form replaces a social security number (e.g., XXX-XX-1234). *Id.* at 11–12.

The Examiner also determines that the tokenization step, as claimed, can be performed as a mental process. *See id.* at 10–11 (finding that "the tokenization process could be as simple as replacing all numbers with X's, or replacing all ones with the letter A, all twos with the letter B, all threes with the letter C, etc., which is well within the capability of most humans."); *see also CyberSource Corp.*, 654 F.3d at 1372 (holding that the step of "obtaining information about other transactions that have utilized an Internet address that is identified with the [ ] credit card transaction" "can be performed by a human who simply reads records of Internet credit card transactions from a preexisting database."); *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat'l Ass'n*, 776 F.3d 1343, 1347 (Fed. Cir. 2014) (holding that humans always have performed the steps of collecting data, recognizing certain data in the set, and storing recognized data, e.g., by banks reviewing checks, recognizing relevant data of the amount, account number, and account holder identify, and storing the data in their records).

Accordingly, we determine that claim 1 recites the abstract idea of certain methods of organizing human activity of a fundamental economic practice involving commercial sales activities identified above.

Step 2A, Prong Two: Integration into a Practical Application

We next consider whether claim 1 recites any additional elements that integrate the abstract idea into a practical application. Revised Guidance, 84 Fed. Reg. at 54 (Revised Step 2A, Prong Two). We determine claim 1 lacks additional elements that improve a computer or other technology. The additional elements do not implement the abstract idea in conjunction with a particular machine or manufacture that is integral to the claim. They do not transform or reduce a particular article to a different state or thing. They do not apply the abstract idea in a meaningful way beyond merely linking it to a particular technological environment. *See* Revised Guidance, 84 Fed. Reg. at 55 and MPEP sections cited therein.

Appellant contends that claim 1 recites a technological solution to a technical challenge of providing access control and data protection in the PCI-DSS system, and this solution integrates any recited judicial exception into a practical application of altering the secure processing of the electronic payment. In particular, Appellant asserts that "[t]he *claimed* invention uses *limited life tokens* to be used within the PCI-DSS system to address the technical challenges of access control and data protection of electronic payment data in a network." Appeal Br. 18.

The Specification indicates that some embodiments process payments using limited life tokens to delete card swipe data post-authorization. Spec. ¶ 14. When the token service receives a card data tokenize request from a POS system, the request may include a time to life (TTL) value. *Id.* ¶ 33. The TTL value indicates the maximum amount of time the token service should store the card data before deleting it. *Id.* Thus, the token is erased at the end of the TTL value time even if an explicit erase operation fails. *Id.*

Appellant's argument is not commensurate with the scope of claim 1 and therefore cannot support an integration of the judicial exception. *See ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 769–70 (Fed. Cir. 2019) ("Even if ChargePoint's specification had provided, for example, a technical explanation of how to enable communication over a network for device interaction (which, as discussed above, it did not), the claim language here would not require those details. Instead, the broad claim language would cover any mechanism for implementing network communication on a charging station."); *Ericsson Inc. v. TCL Commc'ns Tech. Holdings Ltd.*, 955 F.3d 1317, 1325 (Fed. Cir. 2020) ("[T]he specification may be helpful in illuminating what a claim is directed to [but it] must always yield to the claim language when identifying the 'true focus of a claim.'") (citation omitted); *Synopsys, Inc. v. Mentor Graphics Corp.*, 839 F.3d 1138, 1149 (Fed. Cir. 2016) ("The § 101 inquiry must focus on the language of the Asserted Claims themselves."); *Digitech Image Techs., LLC v. Elec. for Imaging, Inc.*, 758 F.3d 1344, 1351 (Fed. Cir. 2014) ("Contrary to Digitech's argument, nothing in the claim language expressly ties the method to an image processor. The claim generically recites a process of combining two data sets into a device profile."); *Accenture*, 728 F.3d at 1345 ("[T]he important inquiry for a § 101 analysis is to look to the claim.").

As the court held in *Accenture*, "the complexity of the implementing software or the level of detail in the specification does not transform a claim reciting only an abstract concept into a patent-eligible system or method." *Accenture*, 728 F.3d at 1345. The specification contained detailed software implementation guidelines, but the claims only recited general software components arranged to implement the abstract concept on a computer. *Id.*

Here, claim 1 does not recite a "limited life token" or tokenizing card data to generate a limited life token that includes a time to life (TTL) value. Nor does claim 1 recite a step of erasing card data stored at a token service based on a TTL value. Therefore, the *claimed* invention does not recite or use a limited life token or TTL value within the PCI-DSS system. Instead, the claimed method merely recites the judicial exception identified above.

"It has been clear since *Alice* that a claimed invention's use of the ineligible concept to which it is directed cannot supply the inventive concept that renders the invention 'significantly more' than that ineligible concept." *BSG Tech LLC v. BuySeasons, Inc.*, 899 F.3d 1281, 1290 (Fed. Cir. 2018); *id.* at 1291 ("As a matter of law, narrowing or reformulating an abstract idea does not add 'significantly more' to it."); *RecogniCorp, LLC v. Nintendo Co.*, 855 F.3d 1322, 1327 (Fed. Cir. 2017) ("Adding one abstract idea (math) to another abstract idea (encoding and decoding) does not render the claim non-abstract."); *Synopsys*, 839 F.3d at 1151 ("But, a claim for a *new* abstract idea is still an abstract idea."); *Versata Dev. Grp., Inc. v. SAP Am., Inc.*, 793 F.3d 1306, 1335 (Fed. Cir. 2015) (holding claims that improved an abstract idea but did not recite the supposed computer improvements were not patent eligible); Revised Guidance, 84 Fed. Reg. at 55 n.24 (additional elements refer to claim features, limitations, and/or steps that are recited in a claim beyond the identified judicial exception).

Generating a card data token is recited as an abstract idea identified above. *See Braemar Mfg., LLC v. The ScottCare Corp.*, Appeal No. 2019-2263, 2020 WL 3564687, at *4 (Fed. Cir. July 1, 2020) (determining a "measure of merit" of a cardiac condition by executing a mathematical formula or selecting a value from a lookup table recites a mental process).

So too, receiving a payment request comprising both sale data and the card data token is recited as an abstract idea identified above. *See Digitech Image*, 758 F.3d at 1351 (holding a claim that generically recites a process of combining two data sets into a device profile was not patent eligible).

Because the features are part of the abstract idea, they cannot integrate that idea into a practical application. The token service, payment service, and payment authorization service are recited as generic components that perform generic functions of sending and receiving data. Thus, they do not implement the judicial exception on a particular machine that is integral to claim 1. The Specification's description of these components makes clear that they are generic components that do not improve the functioning of a computer or other technology. In some embodiments, token service 106 is a combination of hardware and software with functionality to receive card data and securely store it as tokenized card data. Spec. ¶ 18. The payment service 110 is a combination of hardware or software with functionality to receive a payment request and process the payment by communicating with the token service and payment authorization server 112. *Id.* ¶ 20. The POS system 104 is a combination of hardware and software with functionality to process payments for a business or individual. *Id.* ¶ 16.

"[N]ot every claim that recites concrete, tangible components escapes the reach of the abstract-idea inquiry." *See In re TLI Commc'ns LLC Patent Litig.*, 823 F.3d 607, 611 (Fed. Cir. 2016); *see also Alice*, 573 U.S. at 225–26 (an instruction to apply an abstract idea an unspecified generic computer is not enough to transform an abstract idea into a patent-eligible invention); *Mortg. Grader*, 823 F.3d at 1324–25 (holding claims reciting an "interface," "network," and a "database" are nonetheless directed to an abstract idea).

We recognize that "[s]oftware can make non-abstract improvements to computer technology just as hardware improvements can, and sometimes the improvements can be accomplished through either route." *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335 (Fed. Cir. 2016); *see* Appeal Br. 24. However, in this regard, "to be directed to a patent-eligible improvement to computer functionality, the claims must be directed to an improvement to the functionality of the computer or network platform itself." *Customedia Techs., LLC v. Dish Network Corp.*, 951 F.3d 1359, 1365 (Fed. Cir. 2020) (citing *Enfish*, 822 F.3d at 1336–39).

Here, claim 1 does not recite any steps or rules of a PCI-DSS system or other feature that improve computers or other technological process. As the court held for a claim to the use of credit card tokens to make purchases on a transit system in *Smart Systems*:

> Again, the claims recite the collection of financial data from third parties, the storing of that financial data, linking proffered credit cards to the financial data, and allowing access to a transit system based on the financial data. The claims are not directed to a combined order of specific rules that improve any technological process, but rather invoke computers in the collection and arrangement of data. Claims with such character do not escape the abstract idea exception under *Alice* step one.

Smart Sys., 873 F.3d at 1372–73; *see also Mortg. Grader*, 811 F.3d at 1325 ("Nothing in the asserted claims 'purport[s] to improve the functioning of the computer itself' or 'effect an improvement in any other technology or technical field.' . . . . Nor do the claims solve a problem unique to the Internet.") (citations omitted).

Appellant also argues that holdings in *Thales Visionix* and *Amdocs* illustrate why claim 1 here is patent eligible. *See* Appeal Br. 20–23.

In *Thales*, the claim recited a system for tracking the motion of an object relative to a moving reference frame. *Thales Visionix Inc. v. United States*, 850 F.3d 1343, 1345 (Fed. Cir. 2017). The claim recited "a first inertial sensor mounted on the tracked object," "a second inertial sensor mounted on the moving reference frame," and "an element adapted to receive signals from said first and second inertial sensors and configured to determine an orientation of the object relative to the moving reference frame based on the signals received from the first and second inertial sensors." *Id.*

The court held that the claims were directed to systems and methods that use inertial sensors in a non-conventional manner to reduce errors in measuring the relative position and orientation of a moving object on a moving reference frame. *Id.* at 1348–49. The patent specification described this use of the sensors as mitigating errors by eliminating calculations of inertia relative to the earth to allow the system to work with any type of moving platform. *Id.* at 1348.

Here, claim 1 does not claim sensors or sensor arrangements. Nor does claim 1 recite an unconventional arrangement of a token service, POS system, and payment service. Instead, these components perform generic functions of processing payments without any indication in the Specification that they are arranged or function in a way that improves technology beyond generating and transmitting tokenized card data at a high level of generality. Nor does claim 1 purport to improve the security of card data through the arrangement of these components or reduce transmission or payment errors. The claimed method simply transmits and receives card data and sales data and processes a detokenize and erase request for the card data stored at the token service.

In *Amdocs*, the claims recited using accounting information correlated to a first network accounting record to enhance the first network accounting record based on a distributed architecture that applied a number of field enhancements in a distributed fashion that represented a critical advance over the prior art by solving a technological problem of massive record flows that previously required massive databases. *Amdocs (Isr.) Ltd. v. Openet Telecom, Inc.*, 841 F.3d 1288, 1300–01 (Fed. Cir. 2016). The claimed distributed enhancement was a critical advance because it enabled load distribution so granular data can reside in the peripheries of the system close to information sources and reduce congestion on the network but still allow data to be accessible. *Id.* at 1300. Generic network devices worked together in a *distributed manner* so the first accounting record is correlated with accounting information from a second source to enhance the first network accounting record. *Id.* at 1299–1300. The claimed enhancing required the generic components to operate in an unconventional manner to improve computer functionality. *Id.* at 1300–01.

Here, claim 1 recites generic components arranged in no particular way to perform generic functions of sending, receiving, and storing payment processing data without improving computers or networks. A token service is the sole repository for tokenized card data. It sends tokenized card data to the POS system upon request and sends detokenized card data to a payment service upon receiving a detokenize and erase request. Tokenized card data is not correlated across the system or between two records as in *Amdocs*. No distributed computing function or time of life token is claimed either.

Accordingly, we determine that claim 1 lacks any additional elements sufficient to integrate the abstract idea into a practical application.

Step 2B: Does Claim 1 Include an Inventive Concept?

We next consider if claim 1 recites additional elements, individually, or as an ordered combination, that provide an inventive concept. *Alice*, 573 U.S. at 217–18. The second step of the *Alice* test is satisfied when the claim limitations involve more than the performance of well-understood, routine, and conventional activities previously known to the industry. *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1367 (Fed. Cir. 2018); *see* Revised Guidance, 84 Fed. Reg. 56 (explaining that the second step of the *Alice* analysis considers whether a claim adds a limitation beyond a judicial exception that is not "well-understood, routine, conventional" in the field).

Individually, the additional elements recited in claim 1, i.e., the generic token service, POS system, payment service, and payment authorization service, and the card data token generation process are generic computer components that perform generic functions of generating, sending, and receiving data at a high level of generality. *See buySAFE*, 765 F.3d at 1355 ("That a computer receives and sends the information over a network—with no further specification—is not even arguably inventive.").

As an ordered combination, these elements provide no more than when they are considered individually. *Alice*, 573 U.S. at 225. They are used as tools to implement the judicial exception. *See SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1169–70 (Fed. Cir. 2018) (claimed databases and processors did not improve computers but used available computers and functions as tools to execute the claimed process); *Inventor Holdings*, 876 F.3d at 1378 (considering the steps of representative claims as an "ordered combination" reveals they "amount to 'nothing significantly more' than an instruction to apply [an] abstract idea" using generic computer technology).

"The 'novelty' of any element or steps in a process, or even of the process itself, is of no relevance in determining whether the subject matter of a claim falls within the § 101 categories of possibly patentable subject matter." *Diamond v. Diehr*, 450 U.S. 175, 188–89, (1981). Even if the steps are groundbreaking, innovative, or brilliant, that is not enough for eligibility. *See Ass'n for Molecular Pathology v. Myriad Genetics, Inc.*, 569 U.S. 576, 591 (2013); *accord SAP Am.*, 898 F.3d at 1163 ("No matter how much of an advance in the finance field the claims recite, the advance lies entirely in the realm of abstract ideas, with no plausibly alleged innovation in the non-abstract application realm. An advance of that nature is ineligible for patenting."). "An abstract idea can generally be described at different levels of abstraction." *Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229, 1240 (Fed. Cir. 2016); *see also Western Express Bancshares v. Green Dot Corp.*, Appeal No. 2020-1079, 2020 WL 3967855, *3 (Fed. Cir. July 14, 2020) ("But the absence of the exact invention in the prior art does not prove the existence of an inventive concept."). Thus, the lack of a prior art rejection of the claims is not determinative of an inventive concept. *See* Appeal Br. 19.

As the court held in *Smart Systems*:

> The District Court held that the Asserted Claims lack an inventive concept because they recite general computer and technological components "like 'processor,' 'hash identifier,' 'identifying token,' and 'writeable memory,' the technical details of which are not described." . . . As a result, the District Court held that "[i]nvoking various computer hardware elements, which save time by carrying out a validation function on site rather than remotely, does not change the fact that in substance, the claims are still directed to nothing more than running a bankcard sale—that is, the performance of an abstract business practice." . . . We agree.

Smart Sys., 873 F.3d at 1374; *see also Alice*, 573 U.S. at 225 ("The same is true with respect to the use of a computer to obtain data, adjust account balances, and issue automated instructions; all of these computer functions are 'well-understood, routine, conventional activit[ies]' previously known in the industry.") (citation omitted).

Accordingly, we determine that claim 1 lacks an inventive concept sufficient to transform the abstract idea into patent eligible subject matter. Thus, we sustain the rejection of claims 1, 3, 4, 9, 11, 12, 17, 19, 20, and 26–28 as directed to a judicial exception under 35 U.S.C. § 101.

CONCLUSION

In summary:

Claims Rejected	35 U.S.C. §	Reference(s)/ Basis	Affirmed	Reversed
1, 3, 4, 9, 11, 12, 17, 19, 20, 26–28	101	Eligibility	1, 3, 4, 9, 11, 12, 17, 19, 20, 26–28	
1, 3, 4, 9, 11, 12, 17, 19, 20, 26–28	112(b)	Indefiniteness		1, 3, 4, 9, 11, 12, 17, 19, 20, 26–28
Overall Outcome			1, 3, 4, 9, 11, 12, 17, 19, 20, 26–28	

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED