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.
13/294,134	11/10/2011	Murgesh Navar	TE2-015	6154

138557 7590 06/30/2020

Polsinelli LLP - TE2
3 Embarcadero Center
Suite 2400
San Francisco, CA 94111

EXAMINER
CHOO, JOHANN Y

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
06/30/2020	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):

sfpatent@polsinelli.com
uspt@polsinelli.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte MURGESH NAVAR and GEORGE MCMULLEN

Appeal 2020-000801
Application 13/294,134
Technology Center 3600

Before RICHARD M. LEBOVITZ, RACHEL H. TOWNSEND, and JAMIE T. WISZ, *Administrative Patent Judges*.

LEBOVITZ, *Administrative Patent Judge*.

DECISION ON APPEAL

The Examiner rejected the claims under 35 U.S.C. § 103 as obvious, and under 35 U.S.C. § 101 as reciting patent ineligible subject matter. Pursuant to 35 U.S.C. § 134(a), Appellant[1] appeals from the Examiner's decision to reject the claims. We have jurisdiction under 35 U.S.C. § 6(b).

We REVERSE.

---

[1] We use the word "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42. Appellant identifies the real party in interest as Blazer and Flip Flops, Inc. DBA The Experience Engine. Appeal Br. 3.

STATEMENT OF THE CASE

The claims stand rejected[2] by the Examiner as follows:

1. Claims 1, 2, 8, 9, 15, 16, 20, and 25–29 under pre-AIA 35 U.S.C. § 103(a) as obvious in view of Tieken (US 2011/0161233 A1, published Jun. 30, 2011) ("Tieken"), Fukaya (US 2006/0280297 A1, published Dec. 14, 2006) ("Fukaya"), and Youn et al. (US 2007/0230704 A1, published Oct. 4, 2007) ("Youn"). Non-final Act. 8.

2. Claims 3 and 10 under pre-AIA 35 U.S.C. § 103(a) as obvious in view of Tieken, Fukaya, Youn, and Blackhurst et al. (US 2011/0191160 A1, published Aug. 4, 2011) ("Blackhurst"). Non-final Act. 16.

3. Claims 4 and 11 under pre-AIA 35 U.S.C. § 103(a) as obvious in view of Tieken, Fukaya, Youn, and Flitcroft et al. (US 2003/0028481 A1, published Feb. 6, 2003) ("Flitcroft"). Non-final Act. 17.

4. Claims 5, 12 and 30 under pre-AIA 35 U.S.C. § 103(a) as obvious in view of Tieken, Fukaya, Youn, Flitcroft, and Hoerenz (US 2004/0267611 A1, published Dec. 30, 2004) ("Hoerenz"). Non-final Act. 18.

5. Claims 6 and 13 under pre-AIA 35 U.S.C. § 103(a) as obvious in view of Tieken, Fukaya, Youn, Flitcroft, Hoerenz, and Harris et al. (US 2006/0200480 A1, published Sep. 7, 2006 A1) ("Harris"). Non-final Act. 19.

6. Claims 17 and 18 under pre-AIA 35 U.S.C. § 103(a) as obvious in view of Tieken, Fukaya, Youn, and Bickerstaff et al. (US 2009/0036095 A1, published Feb. 5, 2009) ("Bickerstaff"). Non-final Act. 20.

[2] Non-final Office Action (Oct. 2, 2018) ("Non-final Act.").

7. Claim 19 under pre-AIA 35 U.S.C. § 103(a) as obvious in view of Tieken, Fukaya, Youn, Bickerstaff, and Zandonadi (US 2008/0257952 A1, published Oct. 23, 2008) ("Zandonadi"). Non-final Act. 22.

8. Claims 1–6, 8–13, 15–20, and 25–30 under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter. Non-final Act. 4.

Claim 1 is representative and reproduced below. The claim has been annotated with bracketed numbers and letters for reference to the limitations in the claim.

> 1. A method of encryption for recurring mobile transactions, the method comprising:
>
> [1] receiving a request for a mobile transaction transmitted from a mobile device over a communication network and received at a gateway server, wherein the request includes a user key that is not maintained at the mobile device and sensitive data;
>
> [2] executing instructions stored in memory of the gateway server, wherein execution of instructions by a processor of the gateway server:
>
> [2a] generates an encryption key based on a server key stored at the gateway server and the received user key, wherein the received user key is not maintained at the gateway server,
>
> [2b] encrypts the sensitive date in the request using the generated encryption key, and
>
> [2c] transmits the encrypted sensitive data over the communication network from the gateway server to the mobile device;
>
> [3] receiving a subsequent request for a different mobile transaction from the mobile device, the subsequent request including the user key that continues not to be maintained at the mobile device and the encrypted sensitive data; and
>
> [4] executing further instructions stored in the memory of the gateway server, wherein execution of the further instructions by the processor of the gateway server:

> [4a] generates a decryption key based on the user key received in the subsequent request and the stored server key, wherein the user key received in the subsequent request is not maintained at the gateway server
>
> [4b] decrypts the encrypted sensitive data using the generated decryption key, and
>
> [4c] transmits the decrypted sensitive data to a payment processor for processing.

CLAIM 1

There are two principal computer platforms in claim 1, a "gateway server" and a "mobile device." A gateway server is a server or other type of computing device which can communicate with a mobile device and a point-of-sale terminal. Spec. ¶¶ 18, 21, 22. The mobile devices can be "mobile phones, smartphones, personal digital assistants (PDAs), handheld computing device, portable computing devices *(e.g.,* laptop, netbook, tablets), or any other type of computing device capable of communicating over communication network." Spec. ¶ 20.

In step [1] of claim 1, the gateway server receives a request from the mobile device for a "mobile transaction" that includes a "user key" and "sensitive data. The "user key" can be a "PIN code." Spec. ¶ 9; Fig. 14 (showing a 4 digit PIN). The "sensitive data" is not defined in the Specification, but we understand it in the context of the Specification to include financial account information, such as a credit card number or bank account identifier. Spec. ¶¶ 5, 10. The "mobile transaction" can be a credit card purchase. Spec. ¶¶ 4, 10. The user key is not maintained at the mobile device. Thus, in step [1], the user enters a PIN number ("user key") and credit card information ("sensitive data") to make a purchase ("mobile transaction") and the information is sent to the gateway server.

In step [2a], an "encryption key" is generated at the gateway server based on a "server key" stored at the gateway server and the "user key" which is not maintained at the server. The "encryption key" is used to encrypt the sensitive data (step [2b]) which is then sent back to the mobile device (step [2c]). The mobile device therefore has the encrypted sensitive data (such as an encrypted credit card number).

A subsequent request for a different financial mobile transaction (e.g., to make a second credit card purchase) is made to the gateway server in step [3], where the request includes the user key (e.g., the PIN number) and the encrypted sensitive data (e.g., encrypted credit card number) generated in step [2]. Thus, the user does not have to send the unencrypted sensitive data again, but rather has an encrypted form to send to server.

In the last step of the claim, the gateway server generates a "decryption key" based on the "user key" and the "server key" (step [4a]). The gateway server decrypts the encrypted sensitive data (e.g., the credit card number) (step [4b]), and sends it to a payment processor for processing (step [4c]).

REJECTIONS BASED ON TIEKEN, FUKAYA, AND YOUN

The Examiner found that Tieken describes a method of encrypting "recurring" mobile transactions. The Examiner found that Tieken describes the same steps of claim 1, but not generating an encryption key at the gateway server using a "user key" and "server key" as in step [2a] of claim 1. Non-Final Act. 10. To meet this deficiency, the Examiner cited Fukaya which the Examiner found discloses combining a user key and a server key "to form a new keys used to encrypt information which is then sent back to

the user device." *Id.* at 10. The Examiner reasoned it would have been obvious to one of ordinary skill at the time of the invention to use Fukaya's "two-part key combination to encrypt information" in Tieken's method "to ensure that the encryption on each key is unique to the users requesting the encryption of their information and sending the result to the requesting party." *Id.*

The Examiner also stated that Tieken does not teach that the user key is not maintained at the mobile device or the gateway server as required by steps [1] and [2a] of the claim. Non-Final Act. 10–11. However, the Examiner found that Youn teaches a user key that is not maintained at either location. *Id.* at 11. The Examiner found it obvious to apply Youn's teachings to Tieken and Fukyama "to increase the amount of security by having the user input the user key at each transaction." *Id.*

Appellant contends that the Examiner's reliance on Tieken's "tokens" to teach the encryption steps of claim 1 is improper because the tokens are not the same as encrypted information. Appeal Br. 14. Rather, Appellant argues that tokens identify and replace a financial account number, but the token is not encrypting the account information ("sensitive data") as required by the claim. *Id.* at 14–15. Appellant also argues that Fukaya describes the *exchange* of encryption keys between devices, contrary to what is claimed, and does not describe a "user key" which is not stored on either the mobile device or the gateway server. *Id.* at 15.

We agree with Appellant that the Examiner did not establish prima facie obviousness of claim 1. We begin with Tieken by discussing an embodiment shown in Figure 3. Figure 3 of Tieken is reproduced below:

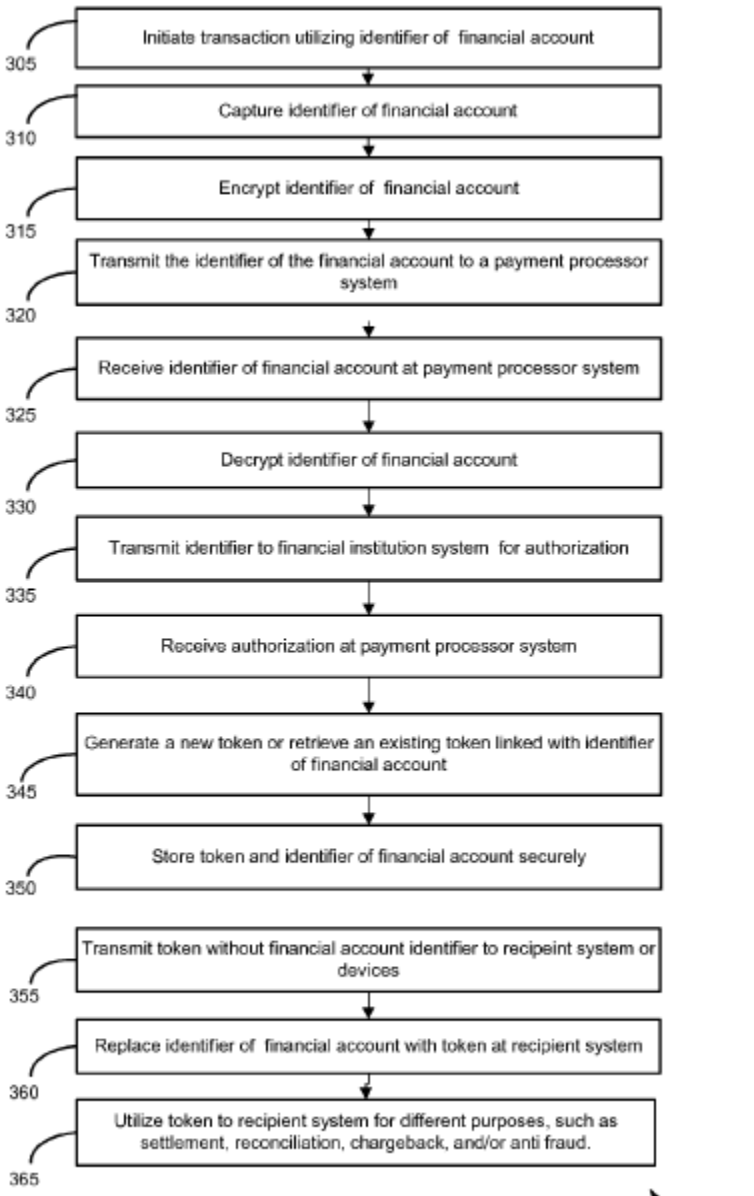

FIG. 3

Figure 3 is a block diagram showing the steps of an embodiment described in Tieken. Tieken ¶ 54. In step 315, the identifier of the financial account is encrypted. Tieken ¶ 56. Thus, this step is similar to step [2] of the claim, but Tieken does not use a "user key" (such as a PIN number) as part of the encryption process to generate an encryption key and encrypt the account information as in step [2a] and [2b] of claim 1. Rather, Tieken

receives the encryption key from another source, such as the payment processor. Tieken ¶ 56.

In claim 1, the encrypted data is sent back to the mobile device (step [2c]). This step, as indicated by Appellant, does not take place in Tieken. As shown in Figure 3 and explained by Tieken, after the financial account information is decrypted in step 330 and sent to the payment processor in step 335, a token is created in step 345. The token is stored in step 350, and transmitted back to a device in step 355. Tieken ¶¶ 8, 59. The token is sent back to the device, but the token does not contain encrypted data. While the token is used to protect the financial account information (Tieken ¶ 60), it is not used in subsequent mobile transactions as it is in step [3] of clam 1. To the contrary, Tieken states that tokens cannot be used to initiate a financial transaction. Tieken ¶¶ 10, 20. Tieken explains what the tokens are used for:

> The merchant or service provider may receive the transaction authorization. It may then delete the identifier of the financial account and all other sensitive data associated with the financial account, even if it is encrypted, and retain the token in its place. The merchant or service provider may store the token for numerous purposes, including, but not limited to, settlement, reconciliation, and chargebacks. The tokens along with other related transaction data may be used also for analytics and anti-fraud measures. If the tokens are intercepted or stolen, they may have no value to the thief, since they may not be used to initiate a financial transaction.

Tieken ¶ 10.

> The token may not be used to initiate a new transaction, such as a new purchase. However, the token may be utilized for other purposes, such as transaction refunds, transaction settlements, and transaction adjustments, merely by way of example. Furthermore, a merchant may utilize the token associate[d] with a customer's purchases [to] provide analytics regarding customer

> purchases. It may also be used for anti-fraud purposes, merely by way of example.

Tieken ¶ 20.

Therefore, while Tieken describes encrypting the financial data in step [2a], the encrypted data is not sent back to the mobile device as required by step [2c] and it is not used to provide payment information for a second and subsequent financial mobile transaction as in step [3] of the claim. *See* Appeal Br. 15. Figure 4 of Tieken shows another embodiment, but it also uses tokens in the same way as in Figure 3 and is deficient for the same reason.

The Examiner responded to Appellant's argument regarding the difference between how tokens are used in Tieken and the encrypted data in the claim by directing attention to paragraphs 7, 27, and 35 of Tieken. Ans. 6. However, these paragraphs describe the general use of encryption keys, but do not disclose sending the encrypted data back to the mobile device as in step [2c] of claim 1. The Examiner also referred to paragraphs 8, 28, 40, and 67 of Tieken. Non-Final Act. 9. These paragraphs refer to a token, which as explained above, is not the same as the encrypted data of step [2c] and [3]. The Examiner also stated that Appellant erroneously "mapped" the tokens to the encryption key (Ans. 5–6), but the Examiner referenced the tokens and the tokens are sent back to the device in Tieken.

The Examiner cited Fukaya for teaching combining a user key and server key as in step [2a] of the claim. Non-Final Act. 10. The Examiner also found Fukaya describes steps [2c] of the claim in sending the encrypted data back to the mobile device, citing paragraphs 93 and 100 of Fukaya. *Id.*

Paragraphs 93 and 100 of Fukaya describe preparing an encryption key Kab based on a key of the user sent to the server and a key of the server.

Fukaya further describes sending the encrypted data *and* server key back to the device. Fukaya ¶ 100. The data is then sent back to the server with the user key. *Id.* This step is done for authentication purposes. *Id.* Thus, as discussed by Appellant (Appeal Br. 16), this two-way exchange of encryption keys is very different from the claim, where no encryption keys are exchanged. The Examiner did not explain why it would have been obvious to send the encrypted data back to the mobile device, instead of using tokens as described by Tieken, and how this would have reasonably suggested re-using the encrypted data to initiate a subsequent mobile transaction as in step [3] of claim 1, when Tieken expressly teaches that tokens are not to be used for this purpose (Tieken ¶¶ 10, 20).

Youn describes a "user-secret" which corresponds to the "user key" of claim 1. Youn ¶¶ 8, 18. In Youn's process, the server encrypts the user secret and server key. Youn ¶ 28. When the user wants the server to decrypt data stored on its behalf, it requests encrypted information, decrypts it, and sends the server key back to the server. *Id.* Thus, while this step uses a user key in combination with a server key as in step [2a] of the claim, it does not use these two keys to generate an encryption key as also required by the step. In view of the deficiencies in Tieken and Fukaya as described above, even if there were a reason to use a user-secret instead of an encryption key as in Fukaya, one of skill in the art would still not have arrived at the claimed invention. Nonetheless, the Examiner's reasoning to modify Fukaya by using a "user-secret" is inconsistent with Fukaya which uses two encryption keys in a two way exchange. The Examiner did not explain why it would have been obvious to have not used two encryption keys, when Fukaya's method is based on that teaching.

For the foregoing reasons, the rejection of claim 1, and dependent claims 2, 8, 9, and 20–25, is reversed.

Independent claims 15, 16, and 20 have substantially the same limitations as claim 1 and is reversed for the same reason as claim 1.

Obviousness rejections 2–7 of dependent claims 3–6, 10–13, 17–19, and 30 are reversed, as well, because the Examiner did not establish that the additional publications cited in the rejections make up for the deficiencies in Tieken, Fukaya, and Young described above.

REJECTION BASED ON 101

Principles of Law

Under 35 U.S.C. § 101, an invention is patent-eligible if it claims a "new and useful process, machine, manufacture, or composition of matter." However, not every discovery is eligible for patent protection. *Diamond v. Diehr*, 450 U.S. 175, 185 (1981). "Excluded from such patent protection are laws of nature, natural phenomena, and abstract ideas." *Id.* The Supreme Court articulated a two-step analysis to determine whether a claim falls within an excluded category of invention. *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S.Ct. 2347 (2014); *Mayo Collaborative Servs. v. Prometheus Labs, Inc.*, 566 U.S. 66, 75–77 (2012).

In the first step, it is determined whether the claims at issue recited one of those patent-ineligible concepts. *Alice*, 134 S.Ct. at 2355. If it is determined that the claims recite an ineligible concept, then the second step of the two-part analysis is applied in which it is asked "[w]hat else is there in the claims before us?" *Id.* The Court explained that this step involves

> a search for an 'inventive concept' — *i.e.*, an element or combination of elements that is 'sufficient to ensure that the

> patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.'

Alice, 134 S.Ct. at 2355 (citing from *Mayo*, 566 U.S. at 75–77).

Alice, relying on the analysis in *Mayo* of a claim directed to a law of nature, stated that in the second part of the analysis, "the elements of each claim both individually and 'as an ordered combination'" must be considered "to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." *Alice*, 134 S.Ct. at 2355.

The PTO published guidance on the application of 35 U.S.C. § 101. USPTO's January 7, 2019 Memorandum, *2019 Revised Patent Subject Matter Eligibility Guidance,* 84 Fed. Reg. 50, 51–57 (2019) ("Eligibility Guidance"). This guidance provides additional direction on how to implement the two-part analysis of *Mayo* and *Alice*.

Step 2A, Prong One, of the 2019 Guidance, looks at the specific limitations in the claim to determine whether the claim recites a judicial exception to patent eligibility. In Step 2A, Prong Two, the claims are examined to identify whether there are additional elements in the claims that integrate the exception into a practical application, namely, is there a "meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the judicial exception." 84 Fed. Reg. 54 (2. Prong Two).

If the claim recites a judicial exception that is not integrated into a practical application, then as in the *Mayo/Alice* framework, Step 2B of the Eligibility Guidance instructs us to determine whether there is a claimed "inventive concept" to ensure that the claims define an invention that is significantly more than the ineligible concept, itself. 84 Fed. Reg. 56.

With these guiding principles in mind, we proceed to determine whether the claimed subject matter in this appeal is eligible for patent protection under 35 U.S.C. § 101.

Discussion

Claim 1 is directed to a "method." Following the first step of the *Mayo/Alice* analysis, we find that the "method" claim is also a "process," and therefore falls into one of the broad statutory categories of patent-eligible subject matter under 35 U.S.C. § 101. We thus proceed to Step 2A, Prong One, of the Eligibility Guidance.

Step 2A, Prong One

In Step 2A, Prong One, of the Eligibility Guidance, the specific limitations in the claim are examined to determine whether the claim recites a judicial exception to patent eligibility, namely whether the claim recites an abstract idea, law of nature, or natural phenomenon.

The Non-final Action was mailed Oct. 2, 2018, before the publication of the Eligibility Guidance. The Examiner stated that "the claims are directed to the abstract idea of protecting and processing financial data for a transaction with the use of processing information through a clearinghouse and a mathematical procedure for converting a data representation to another." Non-final Act. 5. In the Answer, mailed after the publication of the Eligibility Guidance, the Examiner stated that the "claims are directed to facilitating future transactions, i.e. managing human activity, and seems to merely utilize encryption as a general environment applied to the managing of human activity." Ans. 3. The Examiner also characterized the "user key"

and "server key" as "merely forms of data that are not used in any other way that would qualify them as any particular type of data, but instead act as mere generic data." Ans. 4. The Examiner also states that "the generation of keys does not seem to be the intended purpose of the claims." *Id.*

We do not agree with the Examiner's dismissal of the encryption steps as "mere generic data" and not the "intended purpose of the claims." Ans. 4. The encryption is used to encrypt the specific sensitive data and therefore is not "mere generic data" as found by the Examiner. The encryption and decryption steps are specific steps in the claim, and thus the Examiner's statement about them not being the intended purpose of the claim is not a basis to ignore them.

We agree with the Examiner's finding, however, that the claim is directed to "managing human activity," a category of abstract idea listed in the Eligibility Guidance. Specifically, the claim receives a request in step [1] for a mobile transaction, which can be a purchase using a credit card. After carrying out several steps of encryption and decryption, the decrypted sensitive data, which can be a credit card number, is transmitted in step [4c] to a payment process for processing. The claim therefore recites steps of "sales activities" (a "mobile transaction," "payment processor for processing" which is listed in the Eligibility Guidance the abstract idea of "[c]ertain methods of organizing human activity"). Eligibility Guidance, 84 Fed. Reg. 52. *See also* note 13 listing "the concept of 'local processing of payments for remotely purchase goods'" as falling within the category of "certain methods of managing human activity. *Id.*

Appellant states that "[h]uman activity cannot be encrypted." Reply Br. 2. Appellant further argues that the claims are not directed to organizing human activity, but only arise in digital transactions. *Id.* at 3.

The claim, as acknowledged by Appellant, recites steps in which purchase transactions are conducted. Reply Br. 3 ("Human-conducted purchase transactions conducted in person . . . are not, however, capable of encryption or capable of being encrypted by an encryption key"). The Eligibility Guidance lists sales and payment processing as managing human activity, which are reasonably understood to include the type of mobile purchase transaction recited in claim 1. Eligibility Guidance, 84 Fed. Reg. 52. Thus, we do not find Appellant's argument persuasive.

In sum, for the foregoing reasons, we find that claim 1 recites an abstract idea. Accordingly, we proceed to Step 2A, Prong Two, of the Eligibility Guidance.

Step 2A, Prong Two

Prong Two of Step 2A under the 2019 Eligibility Guidance asks whether there are additional elements that integrate the exception into a practical application. As in the *Mayo/Alice* framework, we must look at the claim elements individually and "as an ordered combination" to determine whether the additional elements integrate the recited abstract idea into a practical application. The Eligibility Guidance explains that "[a] claim that integrates a judicial exception into a practical application will apply, rely on, or use the judicial exception in a manner that places a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the judicial exception." Eligibility Guidance, 84 Fed. Reg. 54. Integration into a practical application is evaluated by

identifying whether there are additional elements individually, and in combination, which go beyond the judicial exception. Eligibility Guidance, 84 Fed. Reg. 54–55.

The PEG Update explains that "first the specification should be evaluated to determine if the disclosure provides sufficient details such that one of ordinary skill in the art would recognize the claimed invention as providing an improvement." Update to Subject Matter Eligibility 12.[3]

We begin with the Specification. The Specification explains that in prior art systems, "records were compromised from servers and applications when hackers attack centralized database." Spec. ¶ 7. The Specification further explains that although "[m]any merchants have implemented data encryption systems to protect stored credit card data," these encryption systems are still vulnerable, because "storage of the credit card data exposes the merchant and incentivizes hackers with the prospect of access to tens of thousands of stored credit card records." *Id.* To address this problem, the Specification describes using both a server key stored at the server and a "user-selected key," such as a PIN number, to generate an encryption key at a gateway sever to encrypt the credit card number. Spec. ¶ 9. "The server subsequently discards the user key, which is also not stored on the mobile device." *Id.* The server sends the encrypted credit card back to the mobile device. Spec. ¶ 10. "The encrypted credit card cannot be decrypted [at the gateway server] without the user entering the user key again to verify their identity and order" in addition to the gateway server employing the server

[3] Available at https://www.uspto.gov/sites/default/files/documents/peg_oct_2019_update.pdf (last accessed Jun. 9, 2020) ("PEG Update").

key. Spec. ¶¶ 9–10. Therefore, subsequent orders from the mobile device can be accomplished using the encrypted credit card and the user key without having to transmit the actual card number and with the security that the credit card information can only be decrypted in conjunction with a user key that is not stored on the device and which must be entered by the user to verify the order. Spec. ¶ 10. "Once the credit card information is securely stored on the mobile device, it enables the customer to order repeatedly from the same merchant or place one-off orders from different merchants without having to re-enter the credit card information." Spec. ¶ 36. The Specification explains how using credit card information encrypted with a user key in recurring purchases protects the credit card information from attackers. Spec. ¶ 41.

Claim 1, consistent with the Specification, generates an encryption key based on both the server key stored at the gateway server and the received user key at the gateway server (step [2a]) but does not store this user key on the mobile device or the gateway server. The sensitive data (e.g., credit card information) is encrypted at the server using the encryption key (step [2b]) and the encrypted data is sent back to the mobile device (step [2c]). In subsequent transactions, the user employs the encrypted data and user key (steps [2c],[3], which can only be decrypted by the gateway server using the stored server key and the user key which user key is not maintained at either location for attackers to gain access.

As explained by Appellant, the claims avoid the "failings" in the prior art by providing "for individualized encryption/decryption keys that are generated by combining a server key stored only at the gateway server with

a user key *(e.g.,* a PIN) that is never maintained . . . by any device." Appeal Br. 10. Appellant further states:

> Rather than relying on prior art requirements of repeated user registration and (insecure) credit card storage at the server, the claimed individualized encryption/decryption system incorporates a user-specific element . . . sent from but never maintained at the mobile device that is combined with a server key that is stored at the server only, thereby providing users with the opportunity to purchase products securely without actually having to register with the specific merchant's system or risk the merchant system storing their sensitive data.

Id.

The Examiner replies to Appellant's argument:

> None of these supposed improvements align with applicant's supposed "improvement upon conventional encryption", furthermore none of the supposed improvements are reliant upon any form of encryption. Therefore it is apparent that the encryption of the claims merely act as a generic encryption environment added to the claims without meaningfully adding to the abstract idea of managing human activity by facilitating future transactions. It is further noted that allowing purchases without registration with each individual merchant, is what occurs in everyday purchase transactions with both normal account identifiers and encrypted identifier/tokens. Therefore, even if appellant's assertion that "user key" and "server key" data is to be taken as specific data were to be accepted, such a designation would do little to materially contribute the alleged improvements.

Ans. 4.

As explained above, the claimed improvements are in using a user key in combination with a server key to encrypt sensitive data, where the user key is not maintained on the mobile device or the gateway server, and then sending the encrypted data back to the mobile device where it may be used to carry out additional purchases. The Examiner did not establish that these

steps recited in the claim are a "generic encryption environment" that do not serve as a material improvement to the method of accomplishing "recurring mobile transactions." The steps asserted to embody the improvement to the payment system are not abstract ideas, themselves, but constitute additional elements which provide a technological improvement to electronic payment transactions by making them more secure and providing merchant verification. Accordingly, we conclude that the judicial exception recited in claim 1 is integrated into a practical application and therefore the claim is patent eligible under 35 U.S.C. § 101. The rejection of claim 2–6, 8–13, 15–20, and 25–30 is reversed for the same reasons.

CONCLUSION

In summary:

Claims Rejected	35 U.S.C. §	Reference(s)/Basis	Affirmed	Reversed
1, 2, 8, 9, 15, 16, 20, 25–29	103	Tieken, Fukaya, Youn		1, 2, 8, 9, 15, 16, 20, 25–29
3, 10	103	Tieken, Fukaya, Youn, Blackhurst		3, 10
4, 11	103	Tieken, Fukaya, Youn, Flitcroft		4, 11
5, 12, 30	103	Tieken, Fukaya, Youn, Flitcroft, Hoerenz		5, 12, 30
6, 13	103	Tieken, Fukaya, Youn, Flitcroft, Hoerenz, Harris		6, 13
17, 18	103	Tieken, Fukaya, Youn, Bickerstaff		17, 18
19	103	Tieken, Fukaya, Youn, Bickerstaff, and Zandonadi		19

1–6, 8-13, 15–20, 25–30	101			1–6, 8–13, 15–20, 25–30
Overall Outcome				1–6, 8–13, 15–20, and 25–30

REVERSED