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.
14/060,518	10/22/2013	Terence Spies	ID-40 Cont.	6230

146568 7590 07/02/2020

MICRO FOCUS LLC
500 Westover Drive
#12603
Sanford, NC 27330

EXAMINER
KIM, STEVEN S

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
07/02/2020	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):

software.ip.mail@microfocus.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte TERENCE SPIES and MATTHEW J. PAUKER

Appeal 2020-000585
Application 14/060,518
Technology Center 3600

Before JAMES A. WORTH, KENNETH G. SCHOPFER, and BRADLEY B. BAYAT, *Administrative Patent Judges*.

BAYAT, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellant[1] appeals under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 21, 23–28, 30–35, and 37–40, which are all the claims pending in the application. We have jurisdiction under 35 U.S.C. § 6(b).

We REVERSE.

---

[1] We use the term "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42(a). Appellant identifies the real party in interest as "EntIT Software LLC." Appeal Br. 1.

CLAIMED SUBJECT MATTER

Appellant's disclosure is directed to "purchase transaction systems that use payment card information and, more particularly, to systems in which cryptographic techniques are used to secure sensitive payment card information." Spec. 1, ll. 10–13.

Claims 21, 28, and 35 are the independent claims on appeal. Claim 21, reproduced below with added bracketed notations and emphasis, is illustrative of the claimed subject matter. *See* Appeal Br., Claims App.

21. A computer-implemented method comprising:

[(a)] receiving, by a transaction processing gateway, plural encrypted data from a plurality of terminals for respective transactions, the plural encrypted data derived by the plurality of terminals by *encrypting respective plural data using a plurality of respective encryption algorithms, each encryption algorithm of the plurality of respective encryption algorithms producing respective encrypted data using a different encryption algorithm format*;

[(b)] *identifying, by the transaction processing gateway, each of the different encryption algorithm formats used in encrypting the plural data*;

[(c)] decrypting, by the transaction processing gateway, the plural encrypted data *using a plurality of respective decryption algorithms that respectively correspond to the different encryption algorithm formats*, the decrypting of the plural encrypted data producing respective plural decrypted data;

[(d)] based on the plural decrypted data, authorizing or declining to authorize the respective transactions wherein the transactions are at respective terminals of the plurality of terminals; and

[(e)] encrypting, by the transaction processing gateway, *the plural decrypted data that has been decrypted using the plurality of decryption algorithms using a single encryption algorithm*.

REFERENCES

The prior art relied upon by the Examiner is:

Name	Reference	Date
Takagaki et al. ("Takagaki")	US 2004/0136533 A1	July 15, 2004
Oder, II et al. ("Oder")	US 7,891,563 B2	Feb. 22, 2011

REJECTIONS

Claims 21, 23–28, 30–35, and 37–40 are rejected under 35 U.S.C. § 101 as directed to a judicial exception without significantly more.

Claims 21, 23–28, 30–35, and 37–40 are rejected under 35 U.S.C. § 103(a) as unpatentable over Oder and Takagaki.

OPINION

Rejection under 35 U.S.C. § 101

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." 35 U.S.C. § 101. The Supreme Court, however, has long interpreted § 101 to include an implicit exception: "[l]aws of nature, natural phenomena, and abstract ideas" are not patentable. *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 216 (2014).

The Supreme Court, in *Alice*, reiterated the two-step framework previously set forth in *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 566 U.S. 66 (2012), "for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts." *Alice Corp.*, 573 U.S. at 217. The first step in that analysis is to "determine whether the claims at issue are directed to one of those patent-ineligible concepts." *Id.* If the claims are not directed to a patent-ineligible concept, e.g., an abstract idea, the inquiry ends. Otherwise, the inquiry proceeds to the second step where the elements

of the claims are considered "individually and 'as an ordered combination'" to determine whether there are additional elements that "'transform the nature of the claim' into a patent-eligible application." *Id.* (quoting *Mayo*, 566 U.S. at 78, 79). This is "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.'" *Id.* at 217–18 (alteration in original) (citation omitted).

The U.S. Patent and Trademark Office ("USPTO") published revised guidance for use by USPTO personnel in evaluating subject matter eligibility under 35 U.S.C. § 101. 2019 REVISED PATENT SUBJECT MATTER ELIGIBILITY GUIDANCE, 84 Fed. Reg. 50, 57 (Jan. 7, 2019) (the "2019 Revised Guidance"). That guidance revised the USPTO's examination procedure with respect to the first step of the *Alice* framework by (1) "[p]roviding groupings of subject matter that [are] considered an abstract idea"; and (2) "clarifying that a claim is not 'directed to' a judicial exception if the judicial exception is integrated into a practical application of that exception." *Id.* at 50. The 2019 Revised Guidance, by its terms, applies to all applications, and to all patents resulting from applications, filed before, on, or after January 7, 2019. *Id.*

In rejecting the pending claims under 35 U.S.C. § 101, and under the first step of the *Alice* framework and the 2019 Revised Guidance, the Examiner determined that the claims are directed to the abstract idea of "receiving transaction data, authorizing/declining transaction(s), and securing of the transaction data." Final Act. 5; *see also* Ans. 4. According

to the Examiner, this represents "Certain Methods of Organizing Human Activity." *Id.*

We have reviewed the eligibility of the pending claims under the *Alice* framework and in view of the 2019 Revised Guidance, and we are persuaded that the Examiner erred in concluding that the pending claims are directed to a judicial exception without significantly more.

Statutory Categories under § 101

To determine subject matter eligibility under 35 U.S.C. § 101, the Examiner must first determine if the claims fall into one of the four statutory categories of invention: processes, machines, manufactures, or composition of matter. *See* MPEP § 2106.03. Here, the Examiner makes conflicting statements about whether the claims fall into a statutory category. *See* Final Act. 4–5. The Examiner appears to find the claims do not fall into a statutory category because they are directed to an abstract idea (*id.*); however, the inquiries as to a statutory category (Step 1 of the Subject Matter Eligibility Test Flowchart, MPEP 2016(III)) and a judicial exception (Step 2A) are separate steps. Appellant argues, and we agree, that "independent claim 21 is directed to a process, independent claim 28 is directed to a machine, and independent claim 35 is directed to an article of manufacture. Thus, all claims are directed to respective statutory categories under § 101." Appeal Br. 7. We now turn to the two step *Alice* framework.

Step One of the Alice Framework (*2019 Revised Guidance*, *Step 2A*)
Step 2A, Prong One

The first step in the *Alice* framework is to determine whether the claims at issue are "directed to" a patent-ineligible concept, e.g., an abstract idea. *Alice Corp.*, 573 U.S. at 217. This first step, as set forth in the 2019

Revised Guidance (i.e., Step 2A), is a two-prong test; in Step 2A, Prong 1, we look to whether the claim recites a judicial exception, e.g., one of the following three groupings of abstract ideas: (1) mathematical concepts; (2) certain methods of organizing human activity, e.g., fundamental economic principles or practices, commercial or legal interactions; and (3) mental processes. 2019 Revised Guidance, 84 Fed. Reg. at 54. If so, we next consider whether the claim includes additional elements, beyond the judicial exception, that "integrate the [judicial] exception into a practical application," i.e., that apply, rely on, or use the judicial exception in a manner that imposes a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the judicial exception ("Step 2A, Prong 2"). *Id.* at 54–55. Only if the claim (1) recites a judicial exception and (2) does not integrate that exception into a practical application do we conclude that the claim is "directed to" the judicial exception, e.g., an abstract idea.

The Federal Circuit has explained that "the 'directed to' inquiry applies a stage-one filter to claims, considered in light of the specification, based on whether 'their character as a whole is directed to excluded subject matter.'" *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335 (Fed. Cir. 2016) (quoting *Internet Patents Corp. v. Active Network, Inc.*, 790 F.3d 1343, 1346 (Fed. Cir. 2015)). It asks whether the focus of the claims is on a specific improvement in relevant technology or on a process that itself qualifies as an "abstract idea" for which computers are invoked merely as a tool. *See id.* at 1335–36.

Here, we find the claims recite a judicial exception; however, the claims further integrate that exception into a practical application, and thus,

we agree with Appellant that the claims are not "directed to" the judicial exception of an abstract idea.

The Specification is entitled "PURCHASE TRANSACTION SYSTEM WITH ENCRYPTED PAYMENT CARD DATA," and states, in the background section, "when a customer makes a purchase at a store with a payment card such as a credit card or debit card, point-of-sale ["POS"] equipment in the store is used to acquire payment card data from the customer's card." Spec. 1, ll. 16–19. The POS equipment transfers this data to a purchase transaction computer that "check[s] the customer's account balance and other information to determine whether the customer is authorized to make a purchase and may debit the customer's account accordingly." *Id.* at 2, ll. 8–11. The Specification states that, "[i]f care is not taken to secure sensitive payment card data, it is possible that an attacker may obtain unauthorized access to the payment card data." Spec. 2, ll. 17–19. To prevent such unauthorized access, the Specification states "[i]t would therefore be desirable to be able to provide improved techniques for securing sensitive payment card information in payment card data processing systems." *Id.* at 3, ll. 3–5.

To that end, the Specification discloses a payment transaction system including a POS terminal that sends payment card data to a processor gateway, which performs transaction authentication and transaction clearance. Spec. 5, ll. 6–9. The gateway, in turn, sends payment card data to a card brand portal or other equipment associated with a credit card company and its affiliates for additional processing. *Id.* at 5, ll. 9–11. The Specification discloses that, if the payment data is not encrypted, the transmission of the data from the POS terminal equipment to the gateway

"in unencrypted form presents a potential avenue for attack by an attacker." *Id.* at 10, ll. 9–14. To prevent unauthorized access to the credit card information, the POS terminal is provided with an encryption engine, which "encrypt[s] sensitive information such as payment card information before this information is transmitted to [the] purchase transaction processing gateway." *Id.* at 10, ll. 15–23.

The Specification discloses "different point of sale terminals in [the system] may use different cryptographic algorithms in securing payment card information. With this type of arrangement, encryption algorithm identification information may be used to identify which encryption algorithm was used in encrypting different payment card data items." Spec. 21, ll. 4–10. The Specification provides an example encryption algorithm implemented by each POS terminal encryption engine, such as an algorithm with the inputs: "(1) plaintext payment card information, (2) a randomizing input (tweak), and (3) an encryption key." *Id.* at 17, l. 26–18, l. 3. "The encryption algorithm may produce ciphertext (i.e., an encrypted version of the plaintext payment card information) as a corresponding output" (*id.* at 18, ll. 3–6) and "may append an associated algorithm identifier to the resulting ciphertext" (*id.* at 21, l. 27–22, l. 1).

According to the Specification, the gateway then "receive[s] encrypted data in multiple formats (e.g., from multiple corresponding point of sale terminals)" (*id.* at 21, ll. 17–19) and, using the algorithm identifier, the gateway identifies the corresponding decryption algorithm and decrypts the data (*id.* at 22, ll. 6–9). Once the payment data is decrypted, the gateway uses the data to authorize the transaction and clear payment. *Id.* at 19, ll. 9–12. After the data is decrypted, "[i]t may be desirable to secure data [in a

database at the gateway] by re-encrypting the decrypted payment card information prior to storage in [the] database." *Id.* at ll. 13–15. The Specification discloses that, "[w]ith this type of arrangement, the payment card data will be secure, even if an attacker gains access to the contents of [the] database." *Id.* at ll. 15–17. "The re-encrypted payment card information may be encrypted using a cryptographic algorithm that is different than the algorithm that is used in encrypting and decrypting the payment card information conveyed between [the POS terminal and gateway]." *Id.* at ll. 23–28. The gateway may perform re-encryption of the payment data "with an encryption engine that uses a common key (or set of keys) to encrypt data, regardless of which point of sale terminal originated the payment card data. By using a single key (or set of keys), [the gateway] may simplify the process of encrypting and decrypting data stored in [the] database." *Id.* at 20, ll. 1–6.

Consistent with this disclosure, claim 21 recites a computer-implemented method, comprising: (a) receiving, by a transaction processing gateway, plural encrypted data from a plurality of terminals for respective transactions, the plural encrypted data derived by the plurality of terminals by encrypting respective plural data using a plurality of respective encryption algorithms, each encryption algorithm of the plurality of respective encryption algorithms producing respective encrypted data using a different encryption algorithm format; (b) identifying, by the transaction processing gateway, each of the different encryption algorithm formats used in encrypting the plural data; (c) decrypting, by the transaction processing gateway, the plural encrypted data using a plurality of respective decryption algorithms that respectively correspond to the different encryption algorithm

formats, the decrypting of the plural encrypted data producing respective plural decrypted data; (d) based on the plural decrypted data, authorizing or declining to authorize the respective transactions wherein the transactions are at respective terminals of the plurality of terminals; and (e) encrypting, by the transaction processing gateway, the plural decrypted data that has been decrypted using the plurality of decryption algorithms using a single encryption algorithm. *See* claim 21 *supra.*

Under the broadest reasonable interpretation, steps (a), (c), and (d) recite a method for a secure payment transaction by (a) receiving encrypted payment data from a plurality of transaction terminals; (c) decrypting the data; and (d) authorizing or declining to authorize respective transactions based on the data. For example, the method starts by a POS terminal acquiring a customer's payment data when the customer makes a purchase. *See* Spec. 1, ll. 16–19. At step (a), the POS terminal encrypts the data and sends it to a gateway for processing. *See id.* at 19, ll. 1–3. At steps (c) and (d), the gateway decrypts the data and authorizes or declines the transaction. *See id.* at ll. 4–12. These limitations recite a commercial interaction for secure sales transactions, which is a method of organizing human activity under the Revised Guidance and, therefore, is an abstract idea. *See* 2019 Revised Guidance, 84 Fed. Reg. at 52 (Certain methods of organizing human activity, which include fundamental economic practices and commercial interactions involving sales activities). Similar concepts have been held as abstract, including secure payment transactions (*see Innovation Scis., LLC v. Amazon.com, Inc.,* 778 F. App'x 859, 863 (Fed. Cir. 2019) (securely processing a credit card transaction with a payment server is an abstract idea)) and data encryption (*see Personalized Media Commc'ns, LLC*

v. Amazon.Com, Inc., 161 F. Supp. 3d 325, 333–34 (D. Del. 2015), *aff'd sub nom. Personalized Media Commc'ns, L.L.C. v. Amazon.com Inc.*, 671 F. App'x 777 (Fed. Cir. 2016) (using cryptography to encrypt and decrypt data is an abstract idea)).

Accordingly, we conclude those recitations of steps (a), (c), and (d) (without emphasis in claim 1), under the broadest reasonable interpretation, recite an abstract idea.

Step 2A, Prong Two

Having concluded that claim 1 recites a judicial exception, i.e. an abstract idea (Step 2A, Prong 1), we next consider whether the claim recites additional elements that integrate the judicial exception into a practical application (Step 2A, Prong 2). 2019 Revised Guidance, 84 Fed. Reg. at 51. When a claim recites a judicial exception and fails to integrate the exception into a practical application, the claim is "directed to" the judicial exception. *Id.* A claim may integrate the judicial exception when, for example, it reflects an improvement to technology or a technical field. *Id.* at 55.

Under Step 2A, Prong 2 of the 2019 Revised Guidance, the Examiner determines the claims are not integrated into a practical application, because they merely represent instructions to implement the abstract idea on generic computer components. Final Act. 6; Ans. 4–5. The Examiner reasons "the concepts of cryptography at [a] high level [of] generality is an abstract idea and not necessarily rooted in computer technology," because cryptography was used to protect information even before the advent of computers. Ans. 5.

Appellant contends the Examiner did not consider the ordered combination of the elements of the claims, as required by *McRO, Inc. v.*

Bandai Namco Games Am. Inc. Appeal Br. 8–10 (citing *McRO*, 837 F.3d 1299, 1313 (Fed. Cir. 2016)). Appellant argues "[b]y boiling the language of claim 21 down to a 'financial transaction in securing of sensitive payment information,' or that merely encrypting or decrypting data constitutes an abstract idea, the Examiner has in effect disregarded the actual specific ordered combination of elements recited in claim 21." *Id.* at 10. Appellant further contends "the claimed solution that is necessarily rooted in computer technology overcomes a problem specifically arising in the realm of computer technology, namely the technology of protecting data using encryption according to multiple different encryption algorithms as part of transaction processing." *Id.* at 14–15 (citing *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1255 (Fed. Cir. 2014). Appellant argues "[a] person of ordinary skill in the art would recognize that the authorizing or declining of transactions based on the foregoing of elements would lead to more secure transaction processing, thereby leading to an improvement in the relevant technology of transaction." *Id.* at 12. Finally, Appellant states that "the use of the 'single encryption algorithm' to encrypt the plural decrypted data that has been decrypted using the plurality of decryption algorithms can serve several useful purposes." *Id.*

We are persuaded that the claims recite additional elements integrating the judicial exception into a practical application that reflects an improvement to technology. The additional elements recited in claim 21 *supra* are *italicized*. These additional elements are the POS terminals "encrypting respective plural data using a plurality of respective encryption algorithms, each encryption algorithm of the plurality of respective encryption algorithms producing respective encrypted data using a different

encryption algorithm format," "identifying, by the transaction processing gateway, each of the different encryption algorithm formats used in encrypting the plural data," and the transaction processing gateway re-encrypting "the plural decrypted data that has been decrypted using the plurality of decryption algorithms using a single encryption algorithm."

We agree with Appellant that, in view of these additional claim elements, "[a] person of ordinary skill in the art would recognize that the authorizing or declining of transactions based on the foregoing elements would lead to more secure transaction processing, thereby leading to an improvement in the relevant technology of transaction." Appeal Br. 12. As discussed above, each POS terminal is provided with an encryption engine, which "encrypt[s] sensitive information such as payment card information before this information is transmitted to [the] purchase transaction processing gateway" to prevent unauthorized access to the credit card information. *See* Spec. at 10, ll. 15–23. Further, each POS terminal uses a different algorithm generated by random input that has particular encryption algorithm identification information, i.e., "each encryption algorithm of the plurality of respective encryption algorithms producing respective encrypted data using a different encryption algorithm format." *See id.* at 18, 11. 1–6; 21, ll. 4–10). Using the algorithm identifier, the gateway identifies the corresponding decryption algorithm and decrypts the data, i.e., "identifying, by the transaction processing gateway, each of the different encryption algorithm formats used in encrypting the plural data." *See id.* at 22, ll. 6–9. The gateway then uses a single encryption algorithm to simplify the process of encrypting and decrypting data stored in the database, i.e., the gateway re-encrypting "the plural decrypted data that has been decrypted using the

plurality of decryption algorithms using a single encryption algorithm." *See id. at* 20, ll. 4–7. The resulting method provides "improved techniques for securing sensitive payment card information in payment card data processing systems." *See id*. at 3, ll. 3–5.

Accordingly, we agree with Appellant that claim 21 improves the relevant technology (i.e., secure payment transaction systems) and is not directed to a result or effect that itself is the abstract idea and merely invoke generic processes and machinery. *See McRO*, 837 F.3d at 1314–16. In other words, the claim limitations provide a technical improvement in the functionality of secure payment transaction systems. *See* MPEP § 2106.05(a) ("Improvements to the Functioning of a Computer or To Any Other Technology or Technical Field").

Because we find that claim 21 recites additional elements that integrate the abstract idea into a practical application, we do not agree with the Examiner that claim 21 is "directed to" an abstract idea. Accordingly, we do not sustain the Examiner's rejection of claim 21 under 35 U.S.C. § 101. For the same reasons, we also do not sustain the Examiner's rejection of claims 23–27, which depend from claim 21.

Independent claims 28 and 35 include language substantially similar to the language of independent claim 21. Therefore, we do not sustain the Examiner's rejection of claims 28 and 35, as well as claims 30–34 and 37–40, which depend therefrom, for the same reasons set forth above with respect to claim 21.

Rejection under 35 U.S.C. § 103(a)

Independent Claims 21, 28, and 35

In rejecting claim 21, the Examiner finds Oder teaches sending plural encrypted data from a plurality of POS terminals to a gateway server, but Oder does not teach encrypting and decrypting the respective plural data based on "a plurality of respective encryption algorithms," where each algorithm uses "a different encryption algorithm format." Final Act. 8 (citing Oder col. 5, ll. 10–14; col. 9, ll. 24–40); *see also* Ans. 6–7. The Examiner finds Takagaki teaches the concept of using a plurality of respective encryption algorithms to produce encrypted data with different encryption algorithm formats. Final Act. 9 (citing Takagaki ¶¶ 109, 174, 188, 322 and 332); *see also* Ans. 6–7. In combining the teachings of Oder and Takagaki, the Examiner states that "it would have been obvious to one of ordinary skill in the art of data security to substitute one known encryption/decryption technique [in Takagaki] for another [in Oder] for protecting data between terminal(s) and a remote server," using no more than "ordinary creativity" to make the substitution. *Id.* at 7.

Appellant contends the combination of Oder and Takagaki does not teach "encrypting, by the transaction processing gateway, *the plural decrypted data that has been decrypted using the plurality of decryption algorithms* using a single encryption algorithm." Appeal Br. 16–19 (emphasis added). Appellant argues Oder teaches re-encrypting payment data at the gateway, but is silent regarding using multiple encryption algorithms and multiple decryption algorithms. *Id.* at 17, 19 (citing Oder, col. 6, l. 25). Appellant further argues that, although Takagaki refers to multiple encryption schemes, Takagaki teaches a particular encryption

algorithm has to be agreed upon between the sender and receiver, meaning a sender and recipient must use the same encryption algorithm. *Id.* at 17–18 (citing Takagaki ¶¶ 109, 174). Thus, Appellant contends the combination of Oder and Takagaki does not teach "the concept of first decrypting data using a plurality of decryption algorithms to produce plural decrypted data, followed by encrypting such plural encrypted data that has been decrypted using the plurality of decryption algorithms using a single encryption algorithm." *Id.* at 17.

We agree with Appellant that the Examiner erred in the rejection of claim 21. The Examiner relies on Takagaki to teach encrypting and decrypting the respective plural data based on "a plurality of respective encryption algorithms," where each algorithm uses "a different encryption algorithm format." Final Act. 8–9. However, as Appellant points out (Appeal Br. 17–18), Takagaki teaches a particular encryption algorithm has to be agreed upon between the sender and receiver, meaning there is only one encryption algorithm format being used at a time. *See* Takagaki ¶¶ 19, 109. Takagaki is directed to encrypting broadcast video data, and uses different levels of encryption strength to prevent CPU overload and loss of video. *Id.* ¶ 16–18. Figure 6 of Takagaki depicts an overview of possible algorithms: "algorithm a" has strong encryption but high CPU utilization; "algorithm c" has low CPU utilization but weaker encryption. Thus, Takagaki teaches different algorithms are possible, such as a strong encryption/high CPU algorithm and a weak encryption/low CPU algorithm, *but only one algorithm* is used for transmission at a time. *See* Takagaki, Fig. 6 and Fig. 16 (plural algorithms, selecting one to use). In other words, we find no teaching in Takagaki that the video receiver is receiving "plural

encrypted data from a plurality of terminals" and "identifying each of the different encryption algorithm formats." Rather, the algorithm format in Takagaki is negotiated and determined beforehand for a single transmission. Takagaki ¶ 109. Thus, we agree with Appellant that the combination of Oder and Takagaki does not teach a plurality of respective encryption and decryption algorithms for the plural encrypted data that is received at the transaction processing gateway, as required by claim 21.

Accordingly, Appellant has persuaded us of error in the Examiner's rejection of independent claims 21, 28, and 35 under 35 U.S.C. § 103(a). As such, we do not sustain the rejection.

Dependent Claims

Claims 23–27, 30–34, and 37–40 depend from independent claims 21, 28, and 35, respectively. The rejections of claims 23–27, 30–34, and 37–40 suffer from the same deficiency described above in the rejections of the independent claims. Accordingly, we do not sustain the Examiner's rejection of dependent claims 23–27, 30–34, and 37–40 under 35 U.S.C. § 103(a).

CONCLUSION

The rejection of claims 21, 23–28, 30–35, and 37–40 under 35 U.S.C. § 101 is reversed.

The rejection of claims 21, 23–28, 30–35, and 37–40 under 35 U.S.C. § 103 is reversed.

In summary:

Claims Rejected	35 U.S.C. §	Reference(s)/Basis	Affirmed	Reversed
21, 23–28, 30–35, 37–40	101	Eligibility		21, 23–28, 30–35, 37–40
21, 23–28, 30–35, 37–40	103(a)	Oder, Takagaki		21, 23–28, 30–35, 37–40
Overall Outcome				**21, 23–28, 30–35, 37–40**

REVERSED