Citation: Regions Asset Company (Re), 2025 CACP 4
Commissioner's Decision #1685
Décision du commissaire nº 1685
Date: 2025-03-14

TOPIC:	A11	New Matter
	J00	Meaning of Art
	J10	Computer Programs

SUJET:	A11	Nouvelle Matière
	J00	Signification de la technique
	J10	Programmes d'ordinateur

Application No. 2660638
Demande nº 2 660 638

IN THE CANADIAN PATENT OFFICE

DECISION OF THE COMMISSIONER OF PATENTS

Patent application number 2660638, having been rejected under subsection 199(1) of the *Patent Rules* (SOR/2019-251), has consequently been reviewed in accordance with paragraph 86(7)(c) of the *Patent Rules* (SOR/2019-251). The recommendation of the Patent Appeal Board and the decision of the Commissioner are to refuse the application.

Agent for the Applicant:

Norton Rose Fulbright Canada LLP
2500-1 Place Ville Marie,
Montreal, Quebec
H3B 1R1

INTRODUCTION

[1] This recommendation concerns the review of rejected patent application number 2,660,638, which is entitled “TRANSACTION SECURITY SYSTEM HAVING USER DEFINED SECURITY PARAMETERS” and is owned by Regions Asset Company. The Patent Appeal Board (the Board) reviewed the rejected application pursuant to paragraph 86(7)(c) of the *Patent Rules* (SOR/2019-251).

[2] As explained below, I recommend that the Commissioner of Patents refuse the application.

BACKGROUND

The application

[3] The present application was filed under the provisions of the Patent Cooperation Treaty and has an effective filing date in Canada of August 8, 2007. It was laid open to public inspection on February 21, 2008.

[4] The claimed subject-matter relates to a method for screening fraudulent transactions, comprising providing a security center having (1) a user security parameter system in communication with a user security parameter management system, the user security parameter management system having a user security parameter module and a graphical user interface; and (2) a secondary security system comprising a neural network for receiving an alert to learn a pattern of legitimate transactional behavior, comport with adjusted user security parameters in communication with a transaction processing system.

[5] The application has 22 claims on file that were received at the Patent Office on April 2, 2019.

Prosecution history

[6] On April 27, 2020, a Final Action was issued pursuant to subsection 86(5) of the *Patent Rules*. The Final Action indicated that the application is defective on the ground that all of the claims 1 to 22 on file at the time of Final Action encompass

non-patentable subject-matter and therefore do not comply with section 2 of the *Patent Act*.

[7] The response to the Final Action dated August 26, 2020 disagreed with the non-patentable subject-matter assessment.

[8] On August 26, 2021, the application was forwarded to the Patent Appeal Board for review under paragraph 86(7)(c) of the *Patent Rules* along with a Summary of Reasons explaining that the rejection is maintained as the arguments presented in response to the Final Action are not persuasive.

[9] In a letter dated September 20, 2021, the Patent Appeal Board forwarded a copy of the Summary of Reasons to the Applicant and requested that they confirm their continued interest in having the application reviewed.

[10] In a letter dated December 20, 2021, the Applicant confirmed their interest in having the review proceed.

[11] I was assigned to review the instant rejected application under paragraph 86(7)(c) of the *Patent Rules* and to make a recommendation to the Commissioner of Patents as to its disposition.

[12] In a Preliminary Review letter sent on October 8, 2024, I set out my preliminary analysis of the patentable subject-matter issue with respect to the claims on file. I was of the preliminary view that the claims on file are directed to non-patentable subject-matter.

[13] In the same letter, and according to subsection 86(9) of the *Patent Rules*, I also considered whether the amended specification on file contains new matter that cannot be reasonably inferred from the specification or drawings contained in the application on its filing date. I was of the preliminary view that the description on pages 4a, 4b and 4c and the claims on file encompass new matter and would not comply with section 38.2 of the *Patent Act*.

[14] The Preliminary Review letter also provided the Applicant with an opportunity to make both written and oral submissions.

[15] On December 6, 2024, the Applicant provided a written Response to the Preliminary Review letter and a set of proposed claims (proposed claims set).

[16] In letter dated December 16, 2024, I acknowledged an electronic communication from the Applicant dated December 13, 2024 wherein the Applicant ultimately declined to participate in an oral hearing.

THE ISSUES

[17] The first issue to be addressed by this review is whether the specification contains new matter that cannot be reasonably inferred from the specification or drawings contained in the application on its filing date.

[18] I also consider whether claims 1 to 22 of the instant application are defective as lacking patentable subject-matter and are therefore non-compliant with section 2 of the *Patent Act*. As it was the case in the Preliminary Review letter, it is my view that this also involves a question of compliance with subsection 27(8) of the *Patent Act*.

[19] After considering the claims on file, I reviewed the proposed claims set to determine if they would be considered a necessary amendment under subsection 86(11) of the *Patent Rules*.

PURPOSIVE CONSTRUCTION

Legal Principles and Office Practice

[20] In accordance with *Free World Trust v Électro Santé Inc*, 2000 SCC 66 [*Free World Trust*] and *Whirlpool Corp v Camco Inc*, 2000 SCC 67 [*Whirlpool*], purposive construction is performed from the point of view of the person skilled in the art (POSITA) in light of the relevant common general knowledge (CGK), considering the whole of the disclosure including the specification and drawings. In addition to interpreting the meaning of the terms of a claim, purposive construction distinguishes the essential elements of the claim from the non-essential elements. Whether or not an element is essential depends on the intent

expressed in or inferred from the claim, and on whether it would have been obvious to the skilled person that a variant has a material effect upon the way the invention works.

[21] "Patentable Subject-Matter under the *Patent Act*" (CIPO, November 2020) [*PN2020–04*] also discusses the application of these principles, pointing out that all elements set out in a claim are presumed essential unless it is established otherwise or such presumption is contrary to the claim language.

Analysis

The POSITA and the relevant CGK

[22] In the Preliminary Review letter on pages 4 to 11, I set out a preliminary analysis in respect of the purposive construction of the claims on file, including identification of the POSITA and the relevant CGK:

> Since both interpretation of term meaning and identification of the essential elements are done in light of the relevant CGK, one must first identify the POSITA to determine their CGK.
>
> *The POSITA and the relevant CGK*
>
> The Final Action on page 2 defines the POSITA as a person "having background in fraud-prevention systems, neural networks, and in computerized financial data processing systems".
>
> With regard to the CGK, the Final Action states the following on page 2:
>
> > This person's CGK would include neural network-based fraud-prevention systems that identify and block fraudulent transactions before they occur.
> >
> > This person's CGK would also include general-purpose hardware, such as computers, central processing units, memories, hard disk drives, floppy disk drives, optical disk drives, input/output interfaces, such as mice, keyboards, display monitors, audio-visual input

devices; communication devices, such as modems, transceivers, communication cards, satellite dishes, antennas, network adapters; mobile phones, personal digital assistants (PDA), including computing and networking capabilities and functioning as general purpose computers; networks, such as the Internet, the World Wide Web, WANs, LANs, analog or digital wired and wireless telephone networks, such as public switched telephone networks and integrated services digital networks; digital subscriber lines (xDSL), radio, television, cable, or satellite systems. See pages 8-10 of the description. This person's CGK would also include general-purpose software, such as operating systems (DOS, Windows 2000, Windows XP, Windows NT, OS/2, UNIX or Linux), application programs such as word processing programs, database programs, spreadsheet programs, graphics programs; client applications, such as an internet service provider client application, an e-mail client application or an instant messaging client application; and browser applications. See pages 8-11 of the description.

The hardware and the software platforms disclosed by the application are thus conventional and part of the CGK.

In the Response to the Final Action dated August 26, 2020, the Applicant did not contest or otherwise comment on the characterization of the POSITA and their CGK as identified above.

The Summary of Reasons on page 2 presented the same identification of the POSITA and their CGK found in the Final Action.

Having reviewed the specification as a whole, it is my preliminary view that the characterization of the POSITA and their CGK as identified in the Final Action is reasonable and I therefore adopt it for the purposes on this preliminary review.

[23] The Applicant did not contest or comment on the characterization of the POSITA and their CGK in the Response to the Preliminary Review letter. I therefore adopt

the above characterizations of the POSITA and their CGK for the purpose of my final analysis.

The claims on file

[24] There are 22 claims on file. I consider that independent claim 1 is representative of the subject-matter of independent claims 7, 10, 13 and 19:

> 1. A computer-implemented method for detecting fraudulent electronic transactions,
> comprising:
> providing a security center having:
> (1) a user security parameter system in communication with a user security parameter management system, the user security parameter management system having
> a user security parameter module and a graphical user interface; and
> (2) a secondary security system comprising a neural network for receiving an alert to learn a pattern of legitimate transactional behavior, comport with adjusted user security parameters, and in communication with a transaction processing system,
> establishing a user security parameter by the user security parameter module, the user security parameter specifying a level of settings for conducting financial transactions;
> adjusting the user security parameter by a processor for a predetermined period of time by specifying an action that the security center is to take when a pending transaction fails to comply with the pattern of legitimate transactional behavior;
> receiving a transaction by the transaction processing system via a computer network connecting the security center to a source of the transaction, the transaction characterized by a transaction parameter;
> applying the adjusted user security parameter by the transaction processing system;

evaluating the transaction by the user security parameter system by comparing the transaction parameter to the adjusted user security parameter;

analyzing the transaction parameter with the neural network designed to comport with the adjusted user security parameters;

making a decision by the user security parameter system as to whether the transaction complies with the adjusted user security parameter;

applying the adjusted user security parameter by the secondary security system;

making a decision by the secondary security system whether the pending transaction complies with the adjusted user security parameter;

authenticating the transaction by the secondary security system;

determining by the user security parameter system whether the transaction is fraudulent or non-fraudulent based on the comparison based on an analysis of the evaluated transaction parameter; and

providing a notice of fraudulent transaction by the processor to the user via the computer network connecting the security center to the user, based on the adjusted user security parameter.

[25] The computer-implemented method of independent claim 7 is directed to distinguishing between fraudulent and non-fraudulent transactions and introduces an additional step for capturing and storing the user security parameter.

[26] The computer-implemented method of independent claim 10 is directed to screening electronic transactions wherein the evaluation step is performed at the user security parameter module. Claim 10 also recites an additional step for capturing and storing the user security parameter and comprises a step to decide whether to process the pending transaction. Further, the nature of the notification is not limited to fraud detection but rather more generally aimed at the screening outcome.

[27] Independent claim 13 embodies a computer-implemented method for fraudulent electronic transaction security screening with similarities to claims 1, 7 and or 10 but is directed to a system comprising structural components instead of method

steps, including a transaction processing system, a user security parameter system, and a security center with defined modules.

[28] Independent claim 19 embodies a computer-implemented method for fraudulent electronic transaction security screening with similarities to claims 1, 7 and or 10 but is directed to a computer-readable storage device containing a set of instructions and structured routines for fraud screening instead of method steps.

[29] Dependent claims further specify an additional step of determining whether to process the transaction (claim 2), specify when the user security parameter is established (claim 3), specify the type of transaction (claims 4, 17 and 21), specify the nature of the user security parameter (claims 5, 8, 11, 14 and 20), specify an additional step of selecting a security parameter in which to allow transactions, to block transactions, or to send the notice to the user (claims 6, 9, and 12), specify the presence of an additional notification module (claim 15), specify that the graphical user interface is accessible through a computer network (claim 16), or specify that the security parameter is temporarily adjustable for preset periods of time (claims 18 and 22).

Essential elements

[30] In the Preliminary Review letter, I also expressed the preliminary view that all of the elements in the claims on file are essential. The Applicant did not contest or comment on the essentiality of the claimed elements and I therefore consider all of the elements of the claims to be essential for the purpose of my final analysis.

NEW MATTER

[31] In my view, and for the reasons set out below, the instant specification is an amended specification that comprises new matter that cannot be reasonably inferred from the specification or drawings contained in the application on its filing date and therefore does not comply with section 38.2 of the *Patent Act*.

Legal background

[32] Section 38.2 of the *Patent Act* sets forth the conditions under which amendments may be made to the specification and drawings of a patent application:

> Amendments to specifications and drawings
>
> 38.2 (1) Subject to subsections (2) to (3.1) and the regulations, the specification and drawings contained in an application for a patent in Canada may be amended before the patent is issued.
>
> Restriction
>
> (2) The specification and drawings contained in an application, other than a divisional application, may not be amended to add matter that cannot reasonably be inferred from the specification or drawings contained in the application on its filing date.

[33] The question as to whether matter added to the specification by amendment complies with section 38.2 of the *Patent Act* is considered from the point of view of the POSITA: see Re Uni-Charm Corp's Patent Application 2313707 (2013), CD 1353 (Pat App Bd & Pat Commr) at para 13.

[34] Therefore, assessing whether there is new matter requires a comparison of the pending specification with the originally filed specification and drawings and a determination as to whether the subject-matter of the amendments would have been reasonably inferable from the original specification or drawings by the POSITA.

Analysis

[35] As mentioned above, the instant application, including the original specification, was filed under the *Patent Cooperation Treaty* and has an effective filing date in Canada of August 8, 2007. The applicant submitted an amended description on February 23, 2015, notably new pages 4, 4a, 4b, 4c and 4d. I assess the

description and the claims on file for new matter based on the originally filed specification.

[36] In the Preliminary Review Letter on pages 11 to 12, I set out my preliminary analysis of the new matter issue regarding two limitations found in the independent claims on file that relate to the recited secondary security system defined as i) comprising a neural network for receiving an alert to learn a pattern of legitimate transactional behavior, and ii) that comports with adjusted user security parameters:

> In my preliminary view, the originally filed specification does not appear to explicitly or implicitly disclose the following limitations in the independent claims on file with regard to the recited secondary security system:
>
> - comprising a neural network for receiving an alert to learn a pattern of legitimate transactional behavior; and
> - comport with adjusted user security parameters;
>
> Further, in my preliminary view, the POSITA would not reasonably infer the above limitations in the independent claims on file from the originally filed specification. The originally filed specification discloses a secondary security system comprising a neural network which can learn patterns of legitimate transactional behavior but the originally filed specification does not disclose, teach or suggest neither that the neural network learning is initiated on the basis of a received alert nor that it comports with adjusted user security parameters.
>
> It is therefore my preliminary view that the description on pages 4a, 4b and 4c and the claims on file encompass new matter and would not comply with section 38.2 of the *Patent Act*.

[37] The Response to the Preliminary Review Letter submitted the following on pages 4 and 5 [emphasis in the original]:

The Applicant respectfully disagrees and submits that the originally filed specification supports these features. For example, the description as filed states:

> “In the area of electronic transactions, neural networks can learn patterns of legitimate behavior for consumers and business. Using this pattern of legitimate behavior, the neural network can then search and identify transactions that fall outside of this established behavioral pattern. The fraud-prevention system can use this information from the neural network to identify and block fraudulent transactions before they occur” (page 1, lines 26-30; emphasis added)

> “The fraud-prevention system can acquire this security parameter information from the user and can store it in a user security parameter database. The user may specify these user security parameters at the outset of acquiring a financial account for conducting transactions, or at any time thereafter. The fraud-prevention system can use these user security parameters to screen subsequent transactions. When transactions contain indicia outside of the user security parameters, the fraud-prevention system may either warn the user with a warning message and allow the transaction, or the fraud-prevention system may block the transaction with or without sending a warning message. The fraud-prevention system can block the transaction by signaling a neural network or a third party notification system, or, in certain embodiments, within the system itself**.** The fraud-prevention system allows transactions that comport with the user security parameters.” (see, for example, page 2, line 24, to page 3, line 2; emphasis added)

> “Security center 140 also includes a secondary security system 160. Secondary security system 160 may include a commercially available neural network, which can learn patterns of legitimate transactional behavior in order to filter out fraudulent transactions.” (page 14, lines 14-17; emphasis added)

> "Card security settings management module is in communication with an authentication system **330**, such as neural network having fraud detection rules. Settings database is in communication with card alert management system **340** that sends warnings or [alerts] to user when a pending transaction request has certain parameters that fail to meet the specified user security parameters. Settings database is also in communication with a debit card management system **350**." (page 15, lines 12-17; emphasis added)
>
> "User maintains his user security parameters in step **370**. These user security parameters are uploaded to security center in block **380**. Security system communicates with an authentication system, such as a neural network, which is operatively in communication with transaction processing system, in step **390**, in order to provide real time updates of information to the authentication system." (page 15, lines 21-26; emphasis added)
>
> "Customer alerts **430** in an alert management system is in communication with alert database **490**, which communicates with security center in block **380** in order to send warning messages or alerts to user. Secondary security systems such as neural networks may be in communication with alert database **490**, a third party alert **500**, or an additional third party alert **510**." (page 16, lines 3-7; emphasis added)

As indicated in section 16.05 of the MOPOP: "A claim is objected to for lack of support by the description if the terms used in the claim are not used in the description and cannot be clearly inferred from the description".

The Applicant submits that the terms used in the claims are used in the description as filed and can be clearly inferred therefrom. For at least these reasons, it is submitted that the above-mentioned claim features are fully supported by the description.

[38] It is my view that subsection 38.2(2) of the *Patent Act* (introduced above in the "Legal background" section) is the most relevant provision to the instant issue of

whether a prior amendment added matter that cannot reasonably be inferred from the specification or drawings contained in the application on its filing date.

[39] It is also my view that §20.01 of the *Manual of Patent Office Practice* (CIPO) [MOPOP], modified on October 2022, is the section of MOPOP that relates to the legislative restrictions of subsection 38.2(2) of the *Patent Act* regarding amendments to specifications and drawings:

> Under the *Patent Act*, the specification and drawings of an application may be amended, as long as the amendments, *inter alia*, do not contain new matter when compared to what was filed originally. Subsections 38.2(2) to 38.2(4) of the *Patent Act* and sections 155.6 and 155.7 of the *Patent Rules* provide limits on what matter can form part of an amendment, anything outside of which is considered new matter.

[40] On the other hand, section §16.05 of MOPOP that was cited by the Applicant in the Response to the Preliminary Letter relates to whether a claim is fully supported by the description as required by section 60 of the *Patent Rules*, an issue that was not raised in the Preliminary Review Letter:

> A claim must be fully supported by the description as required by section 60 of the *Patent Rules*. All the characteristics of the embodiment of the invention which are set forth in the claim must be fully set forth in the description (Section 60 of the *Patent Rules*). However, since any claims included in the application at the time of filing are part of the specification (see subsection 27(4) of the *Patent Act* and the definition of “description” in subsection 1(1) of the *Patent Rules*), any matter in the originally filed claims that was not included in the description as filed may be added to the description (except for divisional applications which have further requirements regarding new subject-matter see section 20.04 for more details).
>
> A claim is objected to for lack of support by the description if the terms used in the claim are not used in the description and cannot be clearly inferred

> from the description. Terms used in the claims and in the description must be used in the same sense.

[41] Now, I offer the following observations regarding the submission that the specific passages of the originally filed description cited above are examples that show that the originally filed specification supports the claimed features at issue.

[42] With regard to a neural network for receiving an alert to learn a pattern of legitimate transactional behavior, it is my view that any and all mentions of an alert or a warning message in the originally filed specification, including those quoted by the Applicant, were made in a context wherein the purpose of said alert or warning message is to provide notice to the user.

[43] Neither the passages cited by the Applicant, nor the rest of the originally filed specification, disclose, teach or suggest that an alert would initiate learning of a pattern of legitimate transactional behavior by a neural network. The originally filed description discusses the general learning capability of neural networks which can adapt to data and identify patterns. However, there is no explicit or implicit disclosure of alerts triggering the learning process within the context of the secondary security system.

[44] With regard to the rest of the specification, it is also my view that the originally filed claims do not recite, suggest or imply any alert triggering the learning of a neural network. The closest references to an alert are found in originally filed dependent claims 25, 32 and 39 that recite a “user notification module” or a “user notification routine” for sending a user a message, subject-matter that is aligned with the originally filed description discussed above but that does not relate to alerts triggering the learning process of a neural network.

[45] It is therefore my view that the POSITA would understand from the originally filed specification that the learning of a pattern of legitimate transactional behavior by a neural network occurs based on the data the system receives but not as a result of a specific alert.

[46] Turning now to a secondary security system comprising a neural network that “comports with adjusted user security parameters”. While the originally filed

specification teaches on pages 2 to 3 that the fraud-prevention system overall uses user-adjusted security parameters, said specification does not explicitly or implicitly suggest that embodiments comprising a secondary security system that includes a neural network would operate based on or adapt to adjusted parameters.

[47] A secondary security system is first introduced on page 12, lines 31 to 32 and further described on page 14, lines 14 to 17 of the originally filed description as possibly including “a commercially available neural network, which can learn patterns of legitimate transactional behavior in order to filter out fraudulent transactions”. The only other mention of a secondary security system comprising a neural network is found in a passage on page 16, lines 3 to 7 wherein it is disclosed that secondary security systems such as neural networks may be in communication with an alert database within an alert management system in order to send warning messages or alerts to a user.

[48] The originally filed claims do not recite or define a secondary security system. Dependent claims 4, 13, 20, 28, 35 and 41 refer to the concept of adjusted user security parameter. Dependent claims 9, 15, 17, 22, 29 (incorrectly numbered claim 39 in the originally filed claims), 36 and 42 refer to a neural network and recite the step of “further comprising analyzing the transaction parameter with a neural network”. Claims 1, 4 and 9 are representative and read as follows:

> 1. A method for screening fraudulent transactions, comprising:
> establishing a user security parameter based on a user instruction;
> receiving a transaction, the transaction characterized by a transaction parameter;
> comparing the transaction parameter to the user security parameter to evaluate the transaction.
>
> 4. The method of claim 1, further comprising temporarily adjusting the user security parameter for a predetermined period of time.
>
> 9. The method of claim 1, further comprising analyzing the transaction parameter with a neural network.

[49] It is my view that the POSITA would understand from the originally filed claims as a whole that the recited step of analyzing the transaction parameter with a neural network is performed in addition to and separate from a step of comparing the transaction parameter to the user security parameter, adjusted or not, to evaluate the transaction. It is also my view that the POSITA would not understand from the originally filed claims as a whole that the recited neural network comports with user security parameters, adjusted or not.

[50] On the basis of the foregoing, it is my view that the originally filed specification only discloses a secondary security system having a commercially available neural network that can learn patterns of legitimate transactional behavior in order to filter out fraudulent transactions or as part of an alert management system in order to send warning messages or alerts to users. Neither the passages cited by the Applicant, nor the rest of the originally filed specification, disclose, teach or suggest that said neural network is designed to comport with the adjusted user security parameters.

[51] In conclusion, it is my view that a “secondary security system comprising a neural network for receiving an alert to learn a pattern of legitimate transactional behavior and that comports with adjusted user security parameters” constitutes subject-matter that cannot be reasonably inferred from the specification or drawings contained in the application on its filing date and thus claims 1 to 22 on file and description pages 4a, 4b and 4c of the instant amended specification do not comply with section 38.2 of the *Patent Act*.

PATENTABLE SUBJECT-MATTER

[52] In my view, the actual invention defined by the claims on file is not directed to patentable subject-matter, for the reasons that follow.

Legal Principles and Office Practice

[53] Any patentable invention must fall within the definition set out in section 2 of the *Patent Act*, including falling within one of the categories defined therein:

> **invention** means any new and useful art, process, machine, manufacture or composition of matter, or any new and useful improvement in any art, process, machine, manufacture or composition of matter.

[54] Subsection 27(8) of the *Patent Act* also prescribes that:

> No patent shall be granted for any mere scientific principle or abstract theorem.

[55] *PN2020–04* describes the Patent Office's approach to determining if a claim is patentable subject-matter:

> To be both patentable subject-matter and not be prohibited under subsection 27(8) of the *Patent Act*, the subject-matter defined by a claim must be limited to or narrower than an actual invention that either has physical existence or manifests a discernible physical effect or change and that relates to the manual or productive arts, meaning those arts involving or concerned with applied and industrial sciences as distinguished in particular from the fine arts or works of art that are inventive only in an artistic or aesthetic sense.

[56] The determination of the actual invention is a relevant and necessary question in assessing patentable subject-matter (*Canada (Attorney General) v Amazon.com Inc*, 2011 FCA 328 at para 42 [*Amazon*]). As stated by the Federal Court of Appeal in *Canada (Attorney General) v Benjamin Moore & Co*, 2023 FCA 168 at para 68 [*Benjamin Moore*], this determination is in line with that Court's statement in *Schlumberger Canada Ltd v Commissioner of Patents*, [1982] 1 FC 845 (CA) at 847 [*Schlumberger*] that a patentable subject-matter assessment involves determining what, according to the application, has been discovered. The actual invention is identified in the context of the new discovery or knowledge and must ultimately satisfy the "physicality requirement" that is implicit in the definition of "invention" (*Amazon* at paras 65 and 66).

[57] There is a requirement for something with physical existence, or something that manifests a discernible effect or change. Nonetheless, the mere presence of a practical application does not meet this requirement (*Amazon* at paras 66 and

69). As *Amazon* (para 44) tells us, “a patent claim may be expressed in language that is deliberately or inadvertently deceptive” and that what appears on its face to be an “art” or “process” may in fact be a claim to an unpatentable mathematical formula. This was the situation in *Schlumberger*. In that case, the claims “were not saved by the fact that they contemplated the use of a physical tool, a computer, to give the novel mathematical formula a practical application” (*Amazon* at para 69)

[58] The patentable subject-matter concerns regarding the well-known use of a computer to process an algorithm, illustrated by *Schlumberger*, are expressed in the factors set out in *PN2020–04* that may be considered when reviewing computer-implemented inventions, namely:

- the mere fact that a computer is among the essential elements of the claimed invention does not necessarily mean that the claimed invention is patentable subject-matter;
- an algorithm itself is abstract, unpatentable subject-matter and prohibited by subsection 27(8) of the *Patent Act*;
- a computer programmed to merely process an abstract algorithm in a well-known manner without improving the functionality of the computer will not make it patentable subject-matter; and
- if processing an algorithm improves the functionality of the computer, then the computer and the algorithm would together form a single actual invention that would be patentable.

[59] The above factors and the general concerns around the well-known use of a computer to process new abstract algorithms can be seen to involve considerations of novelty or ingenuity. Canadian law does not prohibit considerations of the novelty or ingenuity of elements of a claim in considering patentable subject-matter and finds support in situations like that of *Schlumberger* where a known tool, a computer, is used to give an abstract mathematical formula a practical application (*Benjamin Moore* at paras 69–70, referring to *Amazon*). These considerations assist in the determination of the

discovery or new knowledge, the method of its application and the actual invention (*Benjamin Moore* at para 89) that is ultimately measured against the physicality requirement.

[60] As noted in *Benjamin Moore* at para 94 (and similarly expressed in *Amazon* at para 61), the physicality requirement will not likely be satisfied without something more than only a well-known instrument, such as a computer, being used to implement an abstract method. The factors set out above from *PN2020–04* assist in determining whether something more is present.

Analysis

[61] In the Preliminary Review letter on pages 10 to 13, I set out my preliminary analysis of the patentable subject-matter issue:

> The Final Action identified a patentable subject-matter defect with respect to the claims on file based on the Office Practice at the time, now superseded by *PN2020–04*. The supplemental analysis provided in the Summary of Reasons considered *PN2020–04* but was performed prior to *Benjamin Moore*. My preliminary analysis below takes into consideration both *PN2020–04* and *Benjamin Moore*.
>
> Although there is a need for something with physical existence, or that manifests a discernible effect or change (*Amazon* at paras 59, 61, 66 and 69; *Benjamin Moore* at paras 53, 61, 64, 89 and 94; see also *PN2020–04* at "Subject-matter"), not every mere involvement of a "practical application" is enough to fulfil the "physicality requirement" of the section 2 definition of invention (*Amazon* at paras 66–67 and 69; *Benjamin Moore* at paras 89 and 94; see also *PN2020–04* at "Computer-implemented inventions").
>
> One must first determine what is "put forward as novel" or "what new knowledge has been added to human wisdom" (*Shell Oil Co v Canada (Commissioner of Patents)*, [1982] 2 SCR 536 at 548; *Amazon* at paras 62–63; *Benjamin Moore* at paras 64, 69, 87, 89 and 94; *PN2020–04* at "Subject-matter"). The "actual invention" (*PN2020–04* at "Subject-matter") is

identified in the context of the “new knowledge” and must ultimately satisfy the “physicality requirement” that is implicit in the definition of “invention”. Thus it is necessary to determine whether the essential elements form a single actual invention that either has physical existence or manifests a discernible effect or change.

I first note that, in the context of the claims on file and the application as a whole, the contemplated neural network to be used for detecting fraudulent electronic transactions as per the claimed subject-matter is a CGK commercially available neural network (see description at page 14, lines 14-17) and that said neural network must *comport* with the set of rules established by the user security parameters. In other words, the subject-matter of the claims on file is primarily driven by the set of rules established by the user security parameters.

It is also my preliminary view that the POSITA would understand from the application as a whole that the subject-matter of the claims on file is intended to improve known methods for electronic transaction fraud-prevention methods that are using a neural network. This is aligned with the following passage of the description that highlights the shortcomings of CGK neural network in the field of electronic transactions found on pages 1-2 of the description and that are allegedly addressed by the disclosed invention:

> Neural networks can be a powerful tool for preventing electronic transactional fraud. However, the neural network is ineffective at preventing fraud during the period during which it is learning the legitimate pattern of behavior. Further, while the neural network can learn a legitimate pattern of behavior for a consumer or business, that pattern may not fully reflect the customer’s or business’ actual pattern of behavior. Still further, the neural network may prove slow in adapting to the changing behavioral patterns of consumers and businesses. It is therefore desirable to develop improved methods and systems for electronic transaction fraud-prevention.

Having regard to the independent claims on file, the actual invention in this case preliminarily appears to be directed to a computer-implemented set of abstract rules and algorithms for detecting fraudulent electronic transactions.

More specifically, established and adjustable user security parameters (e.g., geographic location, a monetary value range, a transaction mode, an account access parameter, a class of goods, or a class of services) are used together with a neural network that comports with said user security parameters to evaluate a given transaction in order to determine whether the transaction is fraudulent or non-fraudulent and, on the basis of said security parameters and outcome of the evaluation, allow the transaction, block the transaction, and/or send a notice to the user.

It is my preliminary view that the recited user security parameters are abstract rules established by the customer user (see page 15, lines 29-30 of the description) and that the neural network is, in the context of the instant application, a commonly known and commercially available software (see page 14, line 15 of the description) utilizing generic computer input/output. In the context of the claims on file, the user security parameters and the neural network are used within a series of recited abstract steps directed to data communication, data comparison, data analysis and/or data presentation.

It is also my preliminary view that both the user security parameters and the neural network as well as the recited abstract steps are implemented by generic computer elements and generic input/display means. This view is aligned with pages 8 to 11 of the instant description that describe the generic nature of the computer elements that may be used to implement the recited set of abstract rules, algorithms and method steps.

With regard to the alleged modifications to conventional neural networks in order to confer an ability to receive an alert to learn a pattern of legitimate transactional behavior; to comport with adjusted user security parameters; and to be in communication with a transaction processing system (see the

Response to the Final Action on page 2), I expressed my preliminary view above that a neural network for receiving an alert to learn a pattern of legitimate transactional behavior and that comports with adjusted user security parameters would constitute new matter that was not disclosed in, or would not have been reasonably inferred from, the original specification or drawings by the POSITA.

In any case, had I been of the view that the claims on file did not comprise new matter based on the originally filed specification, I would have been of the preliminary view that such modifications constitute additional and/or modified abstract rules for the neural network which do not alter the generic nature of the recited neural network.

Now, a computer cannot be used to give an unpatentable abstract idea a practical application satisfying the physicality requirement implicit in the definition of invention in section 2 of the *Patent Act* simply by programming the idea into the computer by means of an algorithm (*Amazon* at paras 61 to 63, 66 and 69; *Benjamin Moore* at paras 69 and 87). This was the situation in *Schlumberger* where the computer was merely acting in a well-known manner.

According to *PN2020–04*, “[i]f a computer is merely used in a well-known manner, the use of the computer will not be sufficient to render the disembodied idea, scientific principle or abstract theorem patentable subject-matter and outside the prohibition under subsection 27(8) of the *Patent Act.*”

In my preliminary view, and as mentioned above, there is no suggestion in the specification that the claimed computer-related elements represent anything other than generic computer components, including the neural network as a secondary security system. Similarly, in my preliminary view, there is no suggestion in the specification that the claimed computer-related steps performed by these elements represent anything other than well-known functions of generic computer components, or that the functioning of

the computer is improved by the recited abstract rules, algorithms or abstract method steps.

The Response to the Final Action on page 2 submits that the problem being addressed by this invention is to provide improved speed, because the conventional neural networks proved slow in adapting to the changing behavioral patterns of consumers and businesses during this learning phase. The improved speed is provided by bypassing the learning phase of conventional neural networks using the adjusted user security parameters.

It is my preliminary view that, insofar as the learning phase of conventional neural networks was a problem that is addressed by the presence of the recited user security parameters, it is a problem related to abstract algorithms that are slow in adapting during this learning phase and thus the learned pattern of behavior for a consumer or business may not fully reflect the customer's or business' actual legitimate pattern of behavior. The abstract rules in the form of adjusted user security parameters do not address or improve the inherent shortcomings of the conventional neural networks *per se* but rather act as the overriding set of parameters to determine whether a transaction is legitimate or not while the neural network is slowly adapting to the changing behavioral patterns of consumers and businesses.

Further, the data entry functionality, the processing functionality, the communication functionality or any other technical functionality of the recited computer-related elements are not enhanced of improved by the user security parameters. The computer-related elements are merely used in a well-known manner and are therefore not part of the single actual invention of the claims on file.

Therefore, it is my preliminary view that the subject-matter of the independent claims on file does not satisfy the physicality requirement as set out in *Amazon* and *PN2020–04* as the actual invention of these claims is a set of abstract rules, algorithms and abstract method steps that are implemented by generic computer elements in order to determine whether a

> given transaction is fraudulent or non-fraudulent and, in certain embodiments, to subsequently allow the transaction, block the transaction, and/or send a notice to the user.
>
> Furthermore, in my preliminary view, the additional limitations recited in the dependent claims do not add any features that would satisfy the physicality requirement and render the claims patentable.
>
> In light of the above, it is my preliminary view that claims 1 to 22 on file are directed to non-patentable subject-matter, falling outside the definition of invention in section 2 of the *Patent Act* and prohibited by subsection 27(8) of the *Patent Act*.

[62] The Response to the Preliminary Review letter, on pages 5 to 6, offers the following submissions and arguments:

- The problem is directed to the way in which neural networks functioned at the time of invention;
- The instant application does not merely contemplate the use of generic computer elements or of a generic neural network that is fed with a user security parameter for a predetermined amount of time. The inventor re-designed the neural network to bypass the conventional required learning period that a neural network needs in order to detect changes in a transaction pattern. This was achieved by providing the neural network with the ability to comport with adjusted user security parameters;
- The modifications do not merely constitute additional and/or abstract rules for the neural network but change the manner in which the neural network functions, resulting in an altered neural network. The altered neural network provides: (1) an ability to receive an alert to learn a pattern of legitimate transactional behavior; (2) comport with adjusted security parameters; and (3) be in communication with a transaction processing system;
- The claims effect an improvement in the technical field. The claimed methods are directed to training neural networks to detect fraudulent transactions. As stated in

paragraph [0005] of the specification, the claims provided improved methods and systems for electronic fraud-prevention that overcome the problems of preventing fraud during the period which the neural network is learning a legitimate pattern of behavior, the neural network learning a legitimate pattern of behavior with adjusted security parameters therefore improving the neural network's ability to adapt to the changing behavioral patterns of consumers and businesses;

- The claimed subject-matter enhances the functioning of the computer itself and improves the computer software's abilities to both learn and evaluate the data flow in transactional patterns. This is not merely abstract but allows a computer to function with improved speed and increased accuracy; and

- The claimed computer-related elements are not merely generic computer components, the claimed computer-related steps performed by these elements represent more than well-known functions of generic computer components, and the functioning of the computer is improved by the claimed method steps.

[63] These arguments have been carefully considered but are not persuasive for the following reasons.

[64] Central to most if not all the provided submissions is the argument that the inventor "re-designed" a generic and commercially available neural network to provide a modified neural network with an ability to receive an alert to learn a pattern of legitimate transactional behavior and comport with adjusted security parameters.

[65] I gave reasons above as to why it is my view that a "neural network for receiving an alert to learn a pattern of legitimate transactional behavior and that comports with adjusted user security parameters" would constitute new matter that was not disclosed in, or would not have been reasonably inferred from, the original specification or drawings by the POSITA.

[66] Further and independently of the above, it is my view that the POSITA would understand that a neural network within the context of the instant application is a computerized algorithm (see page 1, lines 15 to 22) and that the contemplated neural network is a conventional component in the context of a secondary

security system such as the one recited in the claims on file (see p. 14 of the description: “[s]econdary security system 160 may include a commercially available neural network”.

[67] Had I been of the view that the claims on file did not comprise new matter based on the originally-filed specification, I would have been of the view that the asserted modifications do not “re-design” the conventional neural network but rather apply additional and/or modified abstract rules for the conventional neural network.

[68] In that regard, it is my view that the POSITA would understand from the amended specification that these alleged modifications are external rule-based adjustments regarding when initiating the learning process (upon receiving an alert) and an additional abstract constraint (must comport with adjusted user security parameters).

[69] Further, the absence of any detail regarding the nature of the asserted modifications in the specification that allegedly “change the manner in which the neural network functions” does not suggest a re-design of the computerized algorithm at the core of the neural network learning and analytical functions *per se*.

[70] Although I do not generally disagree with the submission that the claimed subject-matter is directed to methods for electronic fraud-prevention that overcome the problems of preventing fraud during the period which the neural network is learning a legitimate pattern of transactional behavior, it is my view that the POSITA would understand that the specification is focused on a rule-based fraud prevention system that is using user security parameters and that said problems are addressed by applying abstract rules or steps to a conventional neural network.

[71] It is also submitted that the claimed subject-matter enhances the functioning of the computer itself and improves the computer software’s abilities to both learn and evaluate the data flow in transactional patterns. It is my view that while it is arguable that the recited abstract rules or abstract method steps provide

improved computerized methods for detecting fraudulent electronic transactions that are using a neural network, neither the abstract rules, the abstract steps nor the conventional network improve the generic computer elements that implement said methods or that support the abstract architecture of the neural network.

[72] In that regard, the specification teaches that the recited methods are implemented on generic computer elements (see pages 8 to 11) and there is no indication in the specification that the data entry functionality, the processing functionality, the communication functionality or any other technical functionality of the recited computer-related elements is actually improved by the recited abstract rules and steps.

[73] In other words, while the claimed computer-implemented methods may provide better fraud detection for users as they reflect the customer's or business' actual pattern of behavior, it does so via an abstract set of rules established by the user security parameters, not by improving the fundamental capabilities of the computing elements.

[74] In view of the foregoing, it remains my view that the subject-matter of the independent claims on file does not satisfy the physicality requirement as set out in *Amazon* and *PN2020–04* as the actual invention of these claims is a set of abstract rules and computerized algorithms for detecting fraudulent electronic transactions implemented by generic computer elements that execute a series of abstract rules directed to data communication, data comparison, data analysis and/or data presentation to determine whether a transaction is fraudulent or non-fraudulent.

[75] Relevant to the above conclusion is my view that neither the recited set of abstract rules nor the computerized algorithm, i.e., the neural network, improve the functioning of the recited computing device or any of its computer elements and thus together do not form a single actual invention.

[76] As for the dependent claims on file that further specify features as listed above at para [25], it is my view that the recited additional limitations do not add any

features not already addressed with regard to the independent claims or that would satisfy the physicality requirement and render the claims patentable.

[77] In conclusion, it is my view that claims 1 to 22 on file are directed to non-patentable subject-matter, falling outside the definition of invention in section 2 of the *Patent Act* and prohibited by subsection 27(8) of the *Patent Act*.

PROPOSED CLAIMS

[78] For the reasons that follow I do not consider that the proposed claims overcome the defects explained above with respect to section 38.2, section 2 and subsection 27(8) of the *Patent Act*.

[79] As mentioned in the “Prosecution history” section above, the Applicant submitted a set of claims comprising claims 1 to 19 with the Response to the Preliminary Review letter (proposed claims).

[80] Proposed independent claims 1, 6, 8, 10 and 15 are amended to recite “wherein the user security parameter is a geographic location, a monetary value range, a transaction mode, an account access parameter, a class of goods, or a class of services”.

[81] Proposed dependent claims 18 and 19 further recite “causing the transaction processing system to allow and complete the transaction when the transaction is determined to be non-fraudulent” and “causing the transaction processing system to deny and block the transaction when the transaction is determined to be fraudulent”.

[82] The proposed claims still encompass a neural network for receiving an alert to learn a pattern of legitimate transactional behavior and that comports with adjusted user security parameters. I therefore consider that the proposed claims encompass subject-matter that cannot be reasonably inferred from the specification or drawings contained in the application on its filing date for the same reasons expressed above with regard to the claims on file.

[83] With regard to the patentable subject-matter issue, I expressed my view above that established and adjustable user security parameters such as geographic location, a monetary value range, a transaction mode, an account access parameter, a class of goods, or a class of services are abstract rules established by the customer user. I also considered above the subject-matter of dependent claims 5, 8, 11, 14 and 20 on file that recite these same features now incorporated in the proposed independent claims. It is therefore my view that the proposed amendments found in proposed independent claims 1, 6, 8, 10 and 15 would not affect the analysis of patentable subject-matter set out for the claims on file above and that the provided reasons would equally apply.

[84] With regard to the features “causing the transaction processing system to allow and complete the transaction when the transaction is determined to be non-fraudulent” and “causing the transaction processing system to deny and block the transaction when the transaction is determined to be fraudulent” recited in proposed claims 18 and 19, it is my view that allowing or denying the transfer and manipulation of abstract information or data does not have physical existence or manifest a discernible physical effect or change as contemplated by *Amazon*.

[85] I therefore conclude that the proposed amendments do not comply with section 38.2 of the *Patent Act* and that the proposed claims are directed to non-patentable subject-matter, falling outside the definition of invention in section 2 of the *Patent Act* and prohibited by subsection 27(8) of the *Patent Act*.

[86] Since the proposed claims would not overcome the defects identified for the claims on file, they are not considered “necessary” amendments for compliance with the *Patent Act* and *Patent Rules* as required by subsection 86(11) of the *Patent Rules*.

RECOMMENDATION OF THE BOARD

[87] In view of the above, I recommend that the application be refused on the basis that:

- claims 1 to 22 on file and description pages 4a, 4b and 4c comprise subject-matter that cannot be reasonably inferred from the specification or drawings contained in the application on its filing date and thus the instant amended specification does not comply with section 38.2 of the Patent Act.
- claims 1 to 22 on file encompass subject-matter outside the definition of invention and do not comply with section 2 of the Patent Act; and
- claims 1 to 22 on file define subject-matter prohibited by subsection 27(8) of the *Patent Act*.

Marcel Brisebois

Member

DECISION OF THE COMMISSIONER

[88] I concur with the conclusions and recommendation of the Board that the application be refused on the basis that:

- claims 1 to 22 on file and description pages 4a, 4b and 4c comprise subject-matter that cannot be reasonably inferred from the specification or drawings contained in the application on its filing date and thus the instant amended specification does not comply with section 38.2 of the Patent Act.
- claims 1 to 22 on file encompass subject-matter outside the definition of invention and do not comply with section 2 of the Patent Act; and
- claims 1 to 22 on file define subject-matter prohibited by subsection 27(8) of the *Patent Act*.

[89] Therefore, in accordance with section 40 of the *Patent Act*, I refuse to grant a patent on this application. Under section 41 of the *Patent Act*, the Applicant has six months within which to appeal my decision to the Federal Court of Canada.

Konstantinos Georgaras

Commissioner of Patents
Dated at Gatineau, Quebec
this 14th day of March, 2025.