Citation: Fédération des Caisses Desjardins du Québec (Re), 2020 CACP 1
Commissioner’s Decision #1521
Décision du Commissaire #1521
Date: 2020-03-10

TOPIC:	J-00	Meaning of Art
	O-00	Obviousness
SUJET:	J-00	Signification de la technique
	O-00	Évidence

Application No. : 2,855,740

Demande nº 2 855 740

IN THE CANADIAN PATENT OFFICE

DECISION OF THE COMMISSIONER OF PATENTS

Patent application number 2,855,740, having been rejected under subsection 30(3) of the *Patent Rules* (SOR/96-423) as they read immediately before October 30, 2019, has consequently been reviewed in accordance with paragraph 199(3)(c) of the *Patent Rules* (SOR/2019-251). The recommendation of the Board and the decision of the Commissioner are to refuse the application.

Agent for the Applicant:

NORTON ROSE FULBRIGHT CANADA LLP
1 Place Ville Marie, Suite 2500
Montréal, Quebec H3B 1R1

INTRODUCTION

[1] This recommendation concerns the review of rejected Canadian patent application number 2,855,740 which is entitled "METHOD IN AN NON WEB-BASED APPLICATION OF A MOBILE DEVICE FOR TRANSFERRING FUNDS TO A SAVINGS ACCOUNT" and is owned by FÉDÉRATION DES CAISSES DESJARDINS DU QUÉBEC (the Applicant).

[2] A review of the rejected application has been conducted by the Patent Appeal Board (the Board) pursuant to paragraph 199(3)(c) of the *Patent Rules* (SOR/2019-251) (the *Patent Rules*). As explained in more detail below, our recommendation to the Commissioner of Patents is to refuse the application.

BACKGROUND

The application

[3] The application, with claimed priority date of April 8, 2014, was filed in Canada on July 3, 2014, and was laid open to public inspection on September 12, 2014.

[4] The application relates to banking transactions with mobile devices. More specifically, the instant application is directed to a simplified method of authenticating a user for performing banking transactions via a non web-based application on a mobile device.

Prosecution history

[5] On June 5, 2017, a Final Action (FA) was issued pursuant to subsection 30(4) of the *Patent Rules* (SOR/96-423) as they read immediately before October 30, 2019 (the former *Rules*), in which the application was rejected on the basis of non-statutory subject-matter and obviousness. The FA stated that claims 1 to 37, dated October 18, 2016 (the claims on file), did not comply with section 2 of the *Patent Act*, and that the claims on file would have been obvious thus did not comply with section 28.3 of the *Patent Act*.

[6] On September 5, 2017, a response to the FA (R-FA) was filed by the Applicant. In the R-FA, the Applicant argued that the claims on file complied with section 2 of the *Patent Act* and were not obvious. Additionally, the Applicant stated that claim 1 was amended. However, no amendment was submitted in the R-FA.

[7] Since the Examiner maintained the position that the application did not comply with

section 2 and section 28.3 of the *Patent Act* after considering the R-FA, the application was forwarded to the Board on November 8, 2017, along with a Summary of Reasons (SOR), explaining the Examiner's rationale for the objection.

[8] The SOR was forwarded to the Applicant on November 10, 2017. In a response dated February 12, 2018, the Applicant indicated its continued interest in the application being reviewed by the Board.

[9] The present panel (the Panel) was formed to review the instant application under paragraph 30(6)(c) of the former *Rules* (now paragraph 199(3)(c) of the *Patent Rules*).

[10] In a preliminary review letter dated October 10, 2019 (PR letter), the Panel presented its preliminary analysis and rationale as to why the subject-matter of the claims on file complied with section 2 of the *Patent Act*, and why the claims on file would have been obvious and did not comply with section 28.3 of the *Patent Act*. The PR letter also offered the Applicant the opportunities to make written submissions and to attend a hearing.

[11] In a letter dated October 29, 2019, the Applicant requested an oral hearing.

[12] In a response to the PR letter (R-PR) dated November 7, 2019, the Applicant contended that the claims on file would not have been obvious. Additionally, the Applicant submitted a proposed set of claims (the first set of proposed claims) for consideration.

[13] An oral hearing was held before the Panel on November 21, 2019 (the hearing).

[14] On November 27, 2019, the Applicant submitted a further response including a new set of proposed claims 1 to 111 (the second set of proposed claims) in an effort to overcome the obviousness objection, and argued in favour of non-obviousness of the claims.

ISSUES

[15] There are two issues to be considered in this review:

- Whether the claims on file define statutory subject-matter falling within the definition of invention in section 2 of the *Patent Act*; and
- Whether the claims on file would not have been obvious to a person skilled in the art, thus comply with section 28.3 of the *Patent Act*.

[16] In this review, we will first address the subject-matter issue. Second, we will consider the obviousness issue. Finally, we will consider the two sets of proposed claims.

LEGAL PRINCIPLES AND OFFICE PRACTICE

Purposive construction

[17] In accordance with *Free World Trust v Électro Santé Inc*, 2000 SCC 66, essential elements are identified through a purposive construction of the claims done by considering the whole of the disclosure, including the specification and drawings (see also *Whirlpool v Camco*, 2000 SCC 67 at paragraphs 49(f) and (g) and 52). In accordance with the *Manual of Patent Office Practice* (CIPO) at §12.02, revised June 2015 [*MOPOP*], the first step of purposive claim construction is to identify the skilled person and his or her relevant common general knowledge (CGK). The next step is to identify the problem addressed by the inventors and the solution put forth in the application. Essential elements can then be identified as those required to achieve the disclosed solution as claimed.

Statutory subject-matter

[18] The definition of invention is set out in section 2 of the *Patent Act:*

> "[I]nvention" 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.

[19] Following the Federal Court of Appeal decision in *Canada (AG) v Amazon.com*, 2011 FCA 328 [*Amazon*], the Office released an examination memo "Examination Practice Respecting Computer-Implemented Inventions", PN2013-03 (CIPO, March 2013) [*PN2013–03*] that clarified the Office's approach to determining if a computer-related invention is statutory subject-matter.

[20] As indicated in *PN2013-03*, section 2 of the *Patent Act* provides the definition of invention and must be read in conjunction with subsection 27(8) of the *Patent Act*, which excludes mere scientific principles and abstract theorems. Disembodied inventions (e.g. mere ideas, schemes, plans or sets of rules, etc.) are not included within the meaning of section 2 of the *Patent Act*. Where a computer is found to be an essential element of a construed claim, or if the claim is directed to a technical solution to a technical problem, the claimed subject-matter will generally be statutory. On the other hand, if it is determined that the essential

elements of a construed claim are limited to only matter excluded from the definition of invention, and does not define "something with physical existence, or something that manifests a discernable effect or change" (*Amazon*, paragraph 66), the claim is not compliant with section 2 of the *Patent Act*, and consequently, not patentable.

Obviousness

[21] The *Patent Act* requires that the subject-matter of a claim not be obvious. Section 28.3 of the *Patent Act* reads as follows:

> The subject-matter defined by a claim in an application for a patent in Canada must be subject-matter that would not have been obvious on the claim date to a person skilled in the art or science to which it pertains, having regard to
>
> (a) information disclosed more than one year before the filing date by the applicant, or by a person who obtained knowledge, directly or indirectly, from the applicant in such a manner that the information became available to the public in Canada or elsewhere; and
>
> (b) information disclosed before the claim date by a person not mentioned in paragraph (a) in such a manner that the information became available to the public in Canada or elsewhere.

[22] In *Apotex Inc v Sanofi-Synthelabo Canada Inc*, 2008 SCC 61, at paragraph 67, the Supreme Court of Canada stated that it is useful in an obviousness inquiry to follow the following four-step approach:

> (1)(a) Identify the notional "person skilled in the art";
>
> (1)(b) Identify the relevant common general knowledge of that person;
>
> (2) Identify the inventive concept of the claim in question or if that cannot readily be done, construe it;
>
> (3) Identify what, if any, differences exist between the matter cited as forming part of the "state of the art" and the inventive concept of the claim or the claim as construed;
>
> (4) Viewed without any knowledge of the alleged invention as claimed, do those differences constitute steps which would have been obvious to the person skilled in the art or do they require any degree of invention?

ANALYSIS

Purposive construction

[23] There are 37 claims on file, including independent claims 1, 18, 19, and 37, and dependent claims 2 to 17 and 20 to 36. In our view, claims 1, 18, 19, and 37 are representative of the

claims on file:

> 1. A method in a non web-based application of a mobile device for transferring funds from a user to a savings account of the user, the method comprising:
>
> persistently storing an identifier token at the mobile device, the identifier token being associated to the user;
>
> when funds are to be transferred:
>
> sending the identifier token from the persistent storing at the mobile device to a server system as an automatic response to the non web-based application being opened in the mobile device to transfer funds to the savings account,
>
> automatically receiving, from the server system and as a response to sending the identifier token, and displaying at the mobile device information identifying a balance of at least one source account of the user, and an editable amount of funds to be transferred to the savings account of the user, along with an indication of a single action to be performed to transfer the funds to the savings account of the user, and
>
> sending from the mobile device to the server system a request for fund transfer of the editable amount along with the identifier token in response to the single action being performed.
>
> 18. A computer program product comprising a computer readable memory storing computer executable instruction thereon that when executed by a mobile device with processor perform the method steps of any one of claims 1 to 17.
>
> 19. A method for transferring funds to a savings account of a user by a transaction server based on a request from a non web-based application of a mobile device operated by the user, the method comprising:
>
> upon validation of a user identity via a mobile device, sending an identifier token uniquely identified to the user for persistent storage at the mobile device;
>
> when funds are to be transferred:
>
> receiving a communication from the mobile device with the identifier token from persistent storage,
>
> automatically obtaining, from at least one account server, a balance of at least one source account of the user, and automatically sending to the mobile device the balance of the at least one source account and an editable amount of funds to be transferred to a savings account of the user, for display,
>
> receiving from the mobile device a request for fund transfer of the editable amount along with the identifier token in response to a single action transfer being performed at the mobile device, recognizing the identifier token, and
>
> sending to the account server the request for fund transfer of the editable amount to the savings account of the user.

> 37. A computer program product comprising a computer readable memory storing computer executable instruction thereon that when executed by a computer perform the method steps of any one of claims 19 to 36.

The person skilled in the art

[24] In the PR letter (page 5), we adopted the identification of the person skilled in the art used in the FA:

> The person skilled in the art is considered to be an individual or a team comprising one or more computer scientists, banking specialists and IT professionals who have relevant education and experience in designing, programming and implementing non web-based applications of mobile devices for transferring funds.

[25] The Applicant did not dispute this characterization in the R-PR or in the submissions after the hearing and we adopt it in this review.

The common general knowledge

[26] In the PR letter (page 5), we adopted the identification of the CGK as stated in the FA (page 4):

> • Mobile application development for banking institutions;
>
> • Utilizing communication and security protocols to setup or authenticate account users access; and
>
> • General database knowledge such as querying, updating, storing and retrieving data.

[27] The Applicant did not dispute this identification in the R-PR or in the submissions after the hearing and we adopt it in this review.

[28] Additionally, the PR letter (page 6) identified the following knowledge as CGK of the skilled person:

> • Authenticating a user using a client identifier for performing financial transactions (see “Background of the Art” of the instant application, which makes reference to Canadian patent CA2246933C), including:
>
> > ◦ using a persistently stored client identifier on a client device to authenticate a client in a server system to perform transactions,
> >
> > ◦ performing a single action regarding a transaction after transactional information is displayed on the client device, and

  - ◦ in response to the single action being performed, sending to the server system a transaction request along with the client identifier.

- • Design, implementation, operation, and maintenance of:
  - ◦ online banking systems including server systems and mobile client devices, and
  - ◦ computer networks that utilize internetworking technologies and protocols;
- • Displaying financial account information received from a server system on a client computer device;
- • Utilizing session tokens to increase security during online financial transactions; and
- • Knowledge of traditional client access mechanisms for online banking, including login to a financial account with a password or PIN.

[29] In the R-PR (page 2) and during the hearing, the Applicant contended that "[p]atent '933, which pertaining to online purchases, is unrelated to banks or financial institutions", and in support, cited paragraph [0003] of the application, which states that "… methods and systems such as those of Canadian Patent No. 2,246,933 allow transactions that do not involve bank accounts, and thus do not have to deal with the highly regulated security and sensitivity required by banking transactions."

[30] We agree that Canadian patent 2,246,933 does not directly involve bank accounts. However, in our view, CGK in relation to the instant application should not be limited to only online banking-related transactions. Instead, any knowledge related to online financial transactions may be relevant. Furthermore, the "BACKGOUND OF THE ART" of the application indicates that the contents of Canadian patent 2,246,933 are related common knowledge. Although this patent does not specifically mention "banking" or "financial institution", it is directed to online shopping for goods and services. In our view, online shopping and online banking are two sub-disciplines of online financial transactions, which share similar security concerns and usability improvement issues.

[31] In the R-PR (page 3) and during the hearing, the Applicant stated that documents D1 to D4, which were cited by the Examiner during the prosecution of the instant application, "illustrate the CGK":

- • D1: US 2010/0125514 A1 May 20, 2010 Blackhurst et al.
- • D2: US 2011/0086616 A1 Aprils 14, 2011 Brand et al.
- • D3: EP 2 367 150 A2 September 21, 2011 Levchin et al.
- • D4: US 2014/0032400 A1 January 30, 2014 Cornforth et al.

[32] The R-PR (page 4) further contended that:

> D1-D4 fall within the state of the art described in the Background of the Art section of the present application, paragraph [0004]
>
> …
>
> None of the prior art references discuss a simplification. In fact, the expression "simplification" is absent altogether from D1-D4.
>
> Stated differently, the CGK is that the primary criterion in computer-implemented authentication process in online financial transactions is security, resulting in multiple steps performed by users.

[33] We agree that documents D1 to D4 collectively reflect aspects of the CGK. However, it is our view that the contents of D1 to D4 cannot be used to limit the scope of the CGK. As explained earlier, the single action financial transaction process as illustrated by Canadian patent 2,246,933, is also considered to be CGK.

[34] In the R-PR (page 3), the Applicant further stated that it reserves the right to debate the definition of the CGK as indicated in the PR letter. We have not received further submission regarding this statement.

[35] In view of above, we use the following identification of the CGK for this review in addition to the CGK as identified in the FA:

> • Authenticating a user using a client identifier for performing <u>online shopping transactions for goods and services</u> (see "Background of the Art" of the instant application, which makes reference to Canadian patent CA2246933C), including:
>
> ◦ using a persistently stored client identifier on a client device to authenticate a client in a server system to perform transactions,
>
> ◦ performing a single action regarding a transaction after transactional information is displayed on the client device, and
>
> ◦ in response to the single action being performed, sending to the server system a transaction request along with the client identifier.
>
> • Design, implementation, operation, and maintenance of:
>
> ◦ online banking systems including server systems and mobile client devices, and
>
> ◦ computer networks that utilize internetworking technologies and protocols;
>
> • Displaying financial account information received from a server system on a client computer device;
>
> • Utilizing session tokens to increase security during online financial transactions; and
>
> • Knowledge of traditional client access mechanisms for online banking, including login to a financial account with a password or PIN (Emphasis added).

Problem and solution

[36] The PR letter (pages 7 to 8) identified the problem and solution based on paragraphs [0002] to [0005] of the instant application, after considering the application as a whole as well as relevant CGK of the skilled person:

> Having considered the above cited paragraphs in the context of the entire specification, we are of the preliminary view that the problem to be solved as seen by the POSITA [person skilled in the art] with their CGK is a need to simplify the computer-implemented authentication process in online financial transactions while maintaining the required level of security.
>
> Based on the same paragraphs and considering the specification as a whole, in our preliminary view, we consider that the proposed solution is a computer-implemented method of performing a single action fund transfer via a non web-based application on a computer device, wherein a simplified authentication procedure is utilized to authenticate a user to access a financial account. The authentication procedure employs a locally stored identity token to facilitate automatic authentication with a server over a computer network.

[37] Regarding the problem, in the R-PR (pages 4 to 5) and during the hearing, the Applicant contended that the identified problem above "has overlooked one claim aspect, namely that the transactions are savings transactions":

> Any consumer is flooded with buying opportunities, whereby the act of putting funds away is in constant competition with impulsive buying behavior. As a telling example, electronic commerce has substantially simplified online purchasing, with online advertising being ubiquitous, and aggressively display on popular applications for mobile devices. Impulse purchasing is a well-documented consumer behavior, as is impulse savings. Online purchasing rarely involves live personnel, whereby online purchases may be achieved in a matter of seconds.
>
> Therefore, as part of the background, the present disclosure expresses that
>
> > *"A common trait is that many improvements in transactional systems and methods are related to expenses. The simplification of online transactions has been designed to facilitate purchases, which caters to the compulsive buyer.* (emphasis added)*"* - present application paragraph [0003]
>
> The present disclosure puts this behavior in contrast to the complexity of financial transactions:
>
> > *"Financial transactions with banks remain somewhat complex, for security reasons. For example, for fraud protection, such transactions are known to be more complex and require more steps, and cannot readily be simplified. A user must often inevitably login, spending precious time entering a password, etc."* - present application paragraph [0004]
>
> As a consequence, the present disclosure identifies the problem in the following terms:

> *"It is therefore an aim of the present disclosure to provide a method for performing savings transactions that overcome issues related to the prior art.* (emphasis added)*"* - present application, paragraph [0005]
>
> The present application expresses the problem of a need for speed when effecting fund transfers, even more so when considering the impulsive behavior at play in a savings transaction, i.e., of the type done when a user transfers funds to his/her own other accounts.
>
> Thus, with respect, the PAB has overlooked the problem of compulsive behavior versus savings transaction. (Emphasis in the original)

[38] Having considered the Applicant's arguments, we note that the only reference to compulsive or impulsive behavior in the specification of the instant application is in paragraph [0003], as recited above, which describes compulsive behavior of buyers of goods and services. There is no mention or indication in the specification regarding "impulse savings", or a "need for speed when effecting fund transfers". Instead, the specification states that the application is directed to "overcome[ing] issues related to the prior art" (paragraph [0005]), which are identified in paragraph [0003] and [0004] as "security and sensitivity required by banking transactions" and over-complex banking transaction processes due to security reasons.

[39] In view of above, based on the specification and the submission of the Applicant we are of the view that the problem is directed to "online banking transactions", which is a sub-discipline of "online financial transactions".

[40] In the R-PR (page 6) and the hearing, the Applicant further argues that the use of a mobile device is essential to the claimed solution, contending that there are specific security concerns regarding online banking using mobile devices. We agree that mobile devices are more susceptible to be lost or stolen than conventional desktop computers, and thus they entail further authentication challenges than conventional desktop computers.

[41] Therefore, we change our identification of the problem to "a need to simplify the computer-implemented authentication process in online banking transactions using mobile devices while maintaining the required level of security" (emphasis added).

[42] Regarding the solution, in the R-PR (page 5) and the hearing, the Applicant contended that the identified solution in the PR letter "ignores the concept of savings", and "the claimed subject-matter pertains to an application that aims at simplifying a savings transaction, to capitalize on impulsive behavior to increase one's savings account, such as a mortgage payment account, a credit line, etc." As explained above, we do not consider that the

specification as a whole provide support to the problem of “impulsive behavior to increase one’s saving account”. Instead, it pertains to the problem of authenticating complex online banking transactions due to security requirements.

[43] After considering the specification as a whole with the CGK of the skilled person, we also agree that the mobile device is part of the solution. The application addresses a specific solution using a mobile device containing a non web-based application to perform a secure authentication method. Therefore, the mobile phone containing the non web-based application is considered to be an essential part of the solution.

[44] Consequently, we change our identification of the solution to “a computer-implemented method of performing a single action fund transfer during online banking transactions via a non web-based application on a mobile device, wherein a simplified authentication procedure is utilized to authenticate a user to access a financial account. The authentication procedure employs a locally stored identity token to facilitate automatic authentication with a server over a computer network” (emphasis added).

The essential elements

[45] The PR letter (page 9) identified the essential elements:

> • persistently storing an identifier token at the computer device, the identifier token being associated to a user;
>
> • when funds are to be transferred:
>
> > - the computer device sending the identifier token to a server as an automatic response to the non web-based application being opened in the computer device,
> >
> > - the server automatically authenticating the user using the received identifier token,
> >
> > - the computer device receiving fund transfer information from the server,
> >
> > - a single action being performed on the computer device, indicating a transaction to be performed, and
> >
> > - the computer device sending a fund transfer request to the server in response to the single action being performed, along with the identifier token.

[46] In the R-PR (page 6), and during the hearing, the Applicant contended that the use of the mobile device, “single-action transfer to a user’s own account”, and “savings account”, are essential elements of the claims.

[47] Regarding the mobile device, as explained in Problem and Solution section, we agree that

this element is essential to the claimed subject-matter.

[48] Regarding the features of "single-action transfer to a user's own account" and "savings account", since "impulsive saving" is not considered to be part of the identified problem, it follows that the ownership or the type of the account to receive funds are not part of the identified solution. The problem that the instant application sets out to solve concerns the security and complexity of online banking transactions in general (see paragraphs [0003] and [0004]), not of just those relating to saving actions, nor of difficulties concerning ownerships of accounts during online banking operations. The instant application is directed to a simplified fund transfer banking transaction while maintaining certain level of security. The relevant transactions may involve a savings account, but may also involve other account types, and/or other banking operations with similar complexity and security requirements. Therefore, although we consider the single action fund transfer procedure essential, the type and the ownership of the account that receives the transferred fund are not considered to be essential.

[49] In view of above, we consider that the essential elements of the independent claims 1, 18, 19, and 37 are (differences from the PR letter identification are highlighted):

> • persistently storing an identifier token at a <u>mobile device</u>, the identifier token being associated to a user;
>
> • when funds are to be transferred <u>during an online banking transaction</u>:
>
> > - the <u>mobile device</u> sending the identifier token to a server as an automatic response to the non web-based application being opened in the <u>mobile device</u>,
> >
> > - the server automatically authenticating the user using the received identifier token,
> >
> > - the <u>mobile device</u> receiving fund transfer information from the server,
> >
> > - a single action being performed on the <u>mobile device</u>, indicating a transaction to be performed, and
> >
> > - the <u>mobile device</u> sending a fund transfer request to the server in response to the single action being performed, along with the identifier token.

[50] Dependent claims 2 to 17 and 20 to 36 are directly or indirectly dependent upon claims 1 and 19, respectively. Hence these claims share the same set of essential elements as identified above.

<u>Subject-matter</u>

[51] As we stated in the PR letter (pages 9 to 10), the claims 1 to 37 on file are directed to a

computer-implemented authentication method, wherein a locally stored digital token on a mobile device is transmitted to a server by a non web-based application for authenticating a user automatically. Since the essential elements include the use of physical hardware and technical elements, such as a mobile device and a server, and therefore define "something with physical existence, or something that manifests a discernable effect or change" (*Amazon*, para. 66), the claimed subject-matter is within the categories of invention as defined in section 2 of the *Patent Act*.

[52] In summary, we consider that the claims on file define statutory subject-matter and thus comply with section 2 of the *Patent Act*.

Obviousness

(1)(a) Identify the notional "person skilled in the art"

[53] The person skilled in the art has been identified above at paragraph [24].

(1)(b) Identify the relevant common general knowledge of that person

[54] The relevant CGK of the skilled person has been identified above at paragraph [26] and [35].

(2) Identify the inventive concept of the claim in question or if that cannot readily be done, construe it

[55] In the PR letter, the Panel considered the essential elements of the claims on file to be representative of the inventive concept of the claims.

[56] In the R-PR, the Applicant did not directly dispute this identification of the inventive concept. Accordingly, in view of the essential elements set out in paragraph [49], the inventive concept of the independent claims includes:

- persistently storing an identifier token at a mobile device, the identifier token being associated to a user;
- when funds are to be transferred during an online banking transaction:
  - the mobile device sending the identifier token to a server as an automatic response to the non web-based application being opened in the mobile device,
  - the server automatically authenticating the user using the received identifier token,

> - the mobile device receiving fund transfer information from the server,
>
> - a single action being performed on the mobile device, indicating a transaction to be performed, and
>
> - the mobile device sending a fund transfer request to the server in response to the single action being performed, along with the identifier token.

[57] Further features of dependent claims 2 to 17 and 20 to 36 will be considered in step (4).

(3) Identify what if any differences exist between the matter cited as forming part of the "state of the art" and the inventive concept of the claim or the claim as construed

[58] The PR letter (pages 10 to 11) identified the differences between the inventive concept of the independent claims and the state of the art:

> In the FA, the following documents were cited as relevant
>
> • D2: US 2011/0086616 A1 April 14, 2011 Brand et al.
>
> • D4: US 2014/0032400 A1 January 30, 2014 Cornforth et al.
>
> In addition, the following document arose during our preliminary review and we consider it to be relevant:
>
> • D5: US 8,280,351 B1 October 2, 2012 Ahmed et al.
>
> In our preliminary view, D5 is the most relevant prior art document. Documents D2 and D4 will not be considered further during this review.
>
> D5 discloses a method of automatically authenticating a mobile device to verify a user account, in response to start-up of a software application in the mobile device. More specifically, D5 discloses:
>
> • persistently storing an identifier token at a computer device, the identifier token being associated to a user (col. 3, lines 32 to 62);
>
> • when an user account is to be authenticated:
>
> > - the computer device sending the identifier token to a server as an automatic response to the non web-based application being opened in the computer device (col. 6, lines 26 to 38),
> >
> > - the server automatically authenticating the user using the received identifier token (col. 6, line 45, to col. 7, line 17), and
> >
> > - the server starting to communicate with the application once the authentication process is completed (col. 7, lines 13 to 17).
>
> In our preliminary view, the differences between D5 and the inventive concept of the independent claims of the instant application are that D5 does not disclose or teach:

> (i) A single action being performed on the computer device, indicating a transaction is to be performed; and
>
> (ii) The computer device sending a fund transfer request to the server in response to the single action being performed, along with the identifier token.

[59] In the R-PR (page 7), the Applicant contended that:

> D5 is unrelated to financial transactions altogether. Indeed, there is a complete absence of the expressions "fund", "finance*", "bank", "money", "savings" in D5.
>
> In this regard, case law is preponderant in dismissing D5 as relevant prior art.
>
> As per *Wenzel Downhole Tools Ltd. v. National-Oilwell Canada Ltd.* (2011), 98 C.P.R. (4th) 155 at para. 160 (F.C.), affd 108 C.P.R. (4th) 247 (C.A.):
>
> > *"there must be some reason, supported by evidence, which would justify a person skilled in the art- and not just experts prompted by counsel -to look beyond the field at issue".*
>
> Paragraph [0001] of the present application describes the technical field in the following terms: "*relates to banking transactions with mobile devices and, more particularly, to savings transactions*". D5 is outside the field at issue,
>
> As per *Laboratoires Servier v. Apotex Inc.* (2008) 70 C.P.R. (4th) 347 (F.C.), affd 75 C.P.R. (4th) 443(C.A.):
>
> > *"Obviousness is considered with reference to the prior art that a skilled person would look to in order to solve the problem addressed by the patent. This is ordinarily referred to as the general common knowledge."*
>
> The skilled person would not have come across D5 in a search for pertinent references. D5 pertains to a different correlation used in a different industry, in an unrelated use. D5 provides no guidance on financial transactions. Moreover, the teachings of D5 do not fall within the CGK described in the Review and commented above.

[60] Having considered the Applicant's arguments and the application as a whole, in view of the CGK of the skilled person, we disagree. We first note that the title of D5 ("AUTOMATIC DEVICE AUTHENTICATION AND ACCOUNT IDENTIFICATION WITHOUT USER INPUT WHEN APPLICATION IS STARTED ON MOBILE STATION") is directly related to the subject-matter of the instant application. Further, the Background of D5 (col. 1 and 2) states:

> A common practice is to challenge users for a user login identifier (ID) and a password. However, this approach is not optimal in the context of mobile station applications. The flowchart of FIG. 6 represents an outline of the events that usually take place during the start of a typical mobile application that mimics traditional web paradigm, with User ID/Password challenge.

> ...
>
> However, if a match was not found, at step p8, the user is redirected to the login page. The cycle may repeat/continue until a valid ID-password combination is submitted.
>
> This method may work fine in the traditional web paradigm where the user accesses an application using a personal computer (PC), but it poses a huge security risk and significant user inconvenience when applied to mobile devices.
>
> …
>
> User experience also presents concerns. Many mobile devices today do not have a full keyboard or data entry pad. Typing accurately on a mobile device having a limited keypad is not an easy task, for many average users. Entering data against the User ID/Password challenge may be difficult and frustrating. The requirement for user inputs for authentication therefore significantly impacts the user experience. Mobile users always prefer systems that require minimum user inputs or keystrokes.
>
> For at least the reasons outlined above, mobile applications need a transparent device authentication and user account identification mechanism that requires little or no user input [Emphases added].

[61] From the above, D5 is directed to solving the need of a simpler user account authentication process on a mobile device, without requiring a user to input login credentials, while maintaining desired level of security. This problem is analogous to the identified problems, only without mentioning that the account access is used for banking transactions relating to a bank account. We also note that that the account authentication method disclosed by D5 can be used for accounting and billing purposes (col. 10, lines 4 to 22). In our view, the skilled person, when facing the need of a simpler account authentication process on a mobile device, using a non-web based application, would have found D5 in a reasonable and diligent search. The skilled person would recognize that the generic authentication method disclosed by D5 may be used in many scenarios that require simpler but secure account authentication in a mobile device, including banking transactions or other account operations, such as those for accounting and billing purposes. Therefore, not mentioning the specific application of banking transactions is insufficient reason to dismiss D5. The field of mobile account authentication for facilitating financial transactions and account operations related to accounting and billing include both the instant application and D5.

[62] In the R-PR, the Applicant did not directly argue against the identification of the differences as identified in the PR letter. We adopt these differences in this review.

(4) Viewed without any knowledge of the alleged invention as claimed, do those differences constitute steps which would have been obvious to the person skilled in the art or do they require any degree of invention?

[63] Regarding the Panel analysis of the differences, the Applicant contended that:

> In item (5) of determining obviousness, the PAB states:
>
> > *"It is our preliminary view that these differences would have been obvious having regard to the CGK. Referring to our identification of the CGK above, performing a single action financial transaction utilizing a client identifier on a client mobile device is part of the CGK. It would therefore have been obvious to apply the simplified authentication method of 05 to well-known single action financial transactions that use similar client identifiers or tokens, thereby arriving at the inventive concept of the independent claims."* Review, page 12, lines 1-6
>
> With respect, the Applicant disagrees. D1-D4 do not teach *"well-known single action financial transactions"*, teaching instead transactions with numerous data entry. None of D1-D3 focus on the essential element of a savings account.
>
> Still in item (5), the PAB concludes:
>
> > *"Hence, in our preliminary view, it would have been obvious to a skilled person, facing the problem of how to perform fund transfers in a secure way without needing the use of conventional login with a password, to apply the simplified account authentication procedure of D5 to the CGK method of performing a single action financial transaction on a client device using a client identifier to communicate with a server system, to perform fund transfers as described by the inventive concept of the independent claims."* - Review, page 12, lines 27-32
>
> As a consequence of the mischaracterization of the problem and solution, the PAB does not discuss "savings account" in its conclusion.

[64] Although D1 to D4 do not disclose the single action financial transaction process, as explained above and as recited in the BACKGOURND OF THE ART section of the instant application, the content of Canadian patent 2,246,933, including its disclosure of the single action online shopping process is considered to be relevant CGK. Although the single action transaction process is disclosed for online shopping, which is considered a sub-discipline of online financial transactions, it would have been obvious for the skilled person to apply the single action process to another sub-discipline of online financial transactions, i.e. online banking. The basic operation of the single action financial transaction utilizing a persistently-stored identifier token remain similar in both cases, and is not dependent upon the data content (e.g., type of transaction, account type, etc.) of the single action order or request that is sent with the identifier token.

[65] With respect to the contended "essential element of a saving account", we explained above that the type of the account to receive funds is not considered to be an essential element of the claimed subject-matter. Furthermore, fund transferring, including fund transferring to savings accounts, is a well-known type of financial transaction. The instant application is directed to how to simplify known banking transaction authentication procedures while maintaining desired level of security. Therefore, the type of the banking transaction performed (e.g. transferring to a savings account) does not change the authentication process, and thus would not have required any inventive ingenuity.

[66] In view of above, as explained in the PR letter, it would have been obvious for a skilled person, facing the problem of how to perform fund transfers securely without user input of login credentials during authentication, to apply the simplified account authentication procedure of D5 and the CGK method of performing a single action transaction on a mobile device, in performing fund transfers as described by the inventive concept of the independent claims.

[67] Therefore, the independent claims 1, 18, 19, and 37 would have been obvious to a skilled person based on the disclosure of D5 in light of the CGK.

[68] The PR letter (page 13) also provided our rationale as to why the dependent claims would have been obvious:

> Dependent claims 2 to 17 and 20 to 36 share the same set of the inventive concept elements as claims 1, 18, 19, and 37. Additionally, they recite further features.
>
> Claims 2 to 4, 12, 20 to 23, and 31 recite performing login with a combination of the following parameters: a card number, a password, a personal answer, a user-selected image or phase. These well-known features of a conventional login procedure are considered to be part of the CGK.
>
> Claims 5 to 9 and 24 to 28 further recite utilizing a session token to create or modify a user configuration, which may include parameters such as selection of a source account, a value of money to be transferred, a selection of a type of project, and a goal value. It is known as part of the CGK that online financial transactions often utilize session tokens to increase transactional security. It is also a known practice that each transaction session may involve different configurational or operational parameters. Therefore, it would have been straightforward to combine the usage of a session token and the configuration of session-specific parameters. In this regard, we are of the preliminary view that the features recited in claims 5 to 9 and 24 to 28 are directed to obvious implementation choices and do not have inventive ingenuity.

> Claims 10, 11, 13 to 17, 29, 30, and 32 to 36 recite features that are either part of the CGK or obvious implementation choices.

[69] The Applicant did not dispute this analysis and we adopt it here. In summary, we are of the view that the features disclosed by these dependent claims, whether being considered alone or in combination with other claimed features, would have been obvious to the skilled person.

<u>The proposed claims</u>

[70] Since claims 38 to 74 of the second set of proposed claims, which is also the latest set of proposed claims, recite the same subject-matter as claims 1 to 37 of the first set of proposed claims, the first set of proposed claims will not be considered separately in this review.

[71] The second set of proposed claims were submitted as a voluntary amendment following the hearing to further define the claimed subject-matter. These claims recite additional features, as explained by the Applicant's letter (page 1) dated November 27, 2019:

> Claims 1-37 are as on file at the Final Office Action.
>
> Claims 38-74 are similar to claims 1-37. Claim 38 has the additional limitation
>
>> "whereby sending the identifier token, automatically receiving the balance and the indication of the single action, and sending the request for fund transfer occur to cause a fund transfer without entering a password."
>
> Claim 56 has the additional limitation
>
>> "whereby automatically obtaining the balance, automatically sending the balance, receiving the request for fund transfer, and sending the request for fund transfer cause a fund transfer without verification of a password"
>
> Claims 75-111 are similar to claims 1-37.
>
> Claim 75 has the additional limitation
>
>> "wherein sending the identifier token, and sending the request for fund transfer occur to cause a fund transfer without entering a password involves data of identity-less nature"
>
> Claim 93 has the additional limitation
>
>> "wherein receiving the request for fund transfer involves data of identity-less nature"

Subject-matter

[72] Since the amendments were submitted to overcome the obviousness objection, with only changes to define further details of the claimed authentication process, the additional features in the second set of proposed claims would not change our identifications of the skilled person, CGK, and problem/solution. Without deciding whether further essential elements are added to the claimed subject-matter, the essential elements as identified in paragraph [49] are still valid. In this case, the mobile device and the server remain being considered as essential physical elements of the claimed subject-matter. Therefore, the second set of proposed claims 1 to 111 would comply with section 2 of the *Patent Act*, for the same reasons stated above in our analysis.

Obviousness

Claims 1 to 37

[73] Since these claims are the same as the claims on file, we are of the view that these claims would have been obvious for the same reasons above.

Claims 38 to 74

[74] These claims recite the additional feature of performing the method steps during the fund transfer procedure without verification of a password. D5 discloses performing account authentication using a non web-based application on a mobile without requiring any user input at the mobile device, including verification of a password (col. 3, lines 3 to 11). After the authentication is completed successfully, there is no need to perform any further authentication during subsequent account operations. Therefore, in our view, this feature, when taken alone or combined with other features of the claimed subject-matter, would have been obvious to the skilled person, who possesses his/her CGK and is aware of the teachings of D5.

Claims 75 to 111

[75] These claims recite the additional features of “causing a fund transfer without entering a password involves data of identity-less nature” and “receiving the request for fund transfer involves data of identity-less nature”.

[76] The expression “involves data of identity-less nature” requires reference to the

specification to understand the meaning of this expression. There are two places in the specification regarding the “identity-less data”:

> [0040] The sequence of steps 150 may be repeated for subsequent transfers or the application may be closed as per 160. It is observed that the steps 151, and 153-155 involve identity-less data exchanged between the mobile device 20 and the application server 30. Stated differently, when the mobile device 20 is not in a configuration mode - the configuration mode being the sequences118, 119, 120, 130 and 131 - the mobile device 20 communicates with the server system using the pre-authorization granted by the identifier token. In exchange, the server system provides data to the mobile device 20 that cannot lead to an identification of the user A, no bank account numbers, no card numbers, no user name, i.e., identity-less data. On the other hand, as the configuration mode (i.e., creating or modifying the user configuration) allows access to identity data for the user A, additional safety steps are performed, as set forth above, to obtain a session token.
>
> …
>
> [0066] Further transfers may be performed, to projects different than the ones involved in the previous transfers, as shown by a return arrow. Otherwise, the transaction ends at 260. It is observed that the steps 251, 253 to 257 - those outside user configuration creation/changes - involve identity-less data exchanged between the mobile device 20 and the application server 30, which identity-less data does not provide confidential information enabling an identification of the user A. This is allowed by pre-authorization of identity-less data exchange based on the presence of the identifier token [Emphases added].

[77] Accordingly, the skilled person would understand that identity-less data exchanges between the mobile device and the server system may only occur when the mobile device is not in a configuration mode, and for subsequent account operations after the account authentication is completed. Therefore, the identity-less data as claimed refers to transaction-related data exchanged during subsequent financial transactions after the authentication is performed.

[78] During subsequent fund transfer actions, the identifier token is always sent together with the fund transfer request, as claimed. However, the specification does not disclose the content of the identifier token, nor provide any information regarding whether the identifier token is considered to be “identity-less data”. Instead, the claims recite that the identifier token is “associated to the user” (claim 1) or “uniquely identified to the user” (claim 19).

[79] In D5, after the pre-authentication is performed, there is also no need to transmit identity-related data for subsequent account actions. In fact, one of the problems D5 tries to solve is to prevent spoofing of login credentials and user identify data (col. 2), by not requiring input of a User ID and a password. Moreover, the identifier token used by D5, such as the Mobile Equipment Identifier or Electronic Serial Number, can only be used to identify a

specific mobile device, not a specific user, which also falls in the meaning of “identity-less data” as understood from paragraph 40 of the instant application.

[80] Further, the fund transfer request data as claimed also includes data other than the identity token data, e.g., an editable amount. Clearly, the editable amount is “identity-less data”, which cannot be lead to the identification of a user. In this case, the feature of fund transfer request data “involve[ing] data of identity-less nature”, such as the editable amount, does not add any additional limitation to the scope of the claimed subject-matter.

[81] Therefore, it is our view that the additional features of claims 75 to 111 would have been obvious to the skilled person with his/her CGK and in view of the teachings of D5. These features, when considered alone or in combination with other features of the claimed subject-matter, would have been obvious to the skilled person.

Conclusion on proposed claims

[82] In view of above, we are of the view that the latest set of proposed claims can not form “necessary” amendment pursuant to subsection 86(11) of the *Patent Rules*, since proposed claims 1 to 37 would have been obvious and do not comply with section 28.3 of the *Patent Act* for the same reasons explained above for the claims on file, and that proposed claims 38 to 111 would have been obvious and do not comply with section 28.3 of the *Patent Act* because the additional features, when combined with other claimed features, would have been obvious to the skilled person.

CONCLUSIONS

[83] We have determined that:

- Claims 1 to 37 on file define statutory subject-matter and comply with section 2 of the *Patent Act*;

- Claims 1 to 37 on file would have been obvious and therefore non-compliant with section 28.3 of the *Patent Act*; and

- The latest set of proposed claims 1 to 111 would have been obvious to the skilled person. Therefore, the introduction of these claims does not constitute “necessary” amendment pursuant to subsection 86(11) of the *Patent Rules*.

RECOMMENDATION OF THE BOARD

[84] In view of the above, the Panel recommends that the application be refused on the grounds that claims 1 to 37 on file would have been obvious and therefore non-compliant with section 28.3 of the *Patent Act*.

[85] Further, the proposed claims do not overcome the obviousness defect and therefore the introduction of these claims does not constitute “necessary” amendments pursuant to subsection 86(11) of the *Patent Rules*.

Liang Ji	Stephen MacNeil	Andrew Strong
Member	Member	Member

DECISION OF THE COMMISSIONER

[86] I concur with the findings of the Board and its recommendation that the application should be refused because the claims on file would have been obvious and thus do not comply with section 28.3 of the *Patent Act*.

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

Johanne Bélisle
Commissioner of Patents

Dated at Gatineau, Quebec,

This 10th day of March 2020