INTELLECTUAL PROPERTY OFFICE

BLO/180/09

29 June 2009

PATENTS ACT 1977

APPLICANT HSBC France

ISSUE Whether patent application number GB 0700698.4 complies with sections 1(1)(b) and 1(1)(d)

HEARING OFFICER B Micklewright

DECISION

1 This application results from the entry into the national phase in the UK of international application no. PCT/FR2005/001684, which was filed on 1 July 2005 claiming a priority of 2 July 2004 from an earlier French application. It was published under serial no. WO 2006/013258 on 9 February 2006 and reprinted under serial no. GB 2431268 on entry to the national phase.

2 Objections to lack of novelty and to exclusion under section 1(2) of the Patents Act 1977 ("the Act") had not been pursued, but the applicant was unable to persuade the examiner that the invention involves an inventive step as required by section 1(1)(b). In response to the offer of a hearing, the applicant has asked for the matter to be decided on the basis of the documents on the file of the application.

3 After I examined the documents on file, I asked the applicant for further submissions on several issues: the date of an internet citation, the common general knowledge of the person skilled in the art, and the relevance of the business method exclusion in the light of a new judgment, *AT&T Knowledge Ventures LP* [2009] EWCH 343 (Pat) which was issued on 3 March 2009. The applicant's attorney made submissions on these matters in a letter received on 29 April 2009.

The invention

4 The invention is a method of authenticating a user by a provider, typically a bank offering internet or telephone services. For many such services, it is customary for the provider to ask for complementary authorisation (such as date or place of birth) in addition to the identifier and password but this confers only a weak level of extra security.

5 In the latest amended form, claim 1 reads:

> "Method of remote authentication of a user by a provider, wherein communication between said provider and said user is effected electronically, including the following steps:
>
> a) transmission from said user to said provider of an identifier,
>
> b) determination by said provider of a processing rule applicable to a code, previously provided by the provider to the user, consisting of characters and available to said user and said provider, said rule being to extract a certain number of characters from said code,
>
> c) transmission from said provider to said user of said processing rule,
>
> d) determination by said user of at least one character of said code identifiable by its position in the code, said position being supplied by said processing rule to obtain first authentication data,
>
> e) transmission from said user to said provider of said first authentication data, and, independently of the steps b) to e),
>
> f) recovery by said provider of said code,
>
> g) processing of said code by said provider by means of said processing rule to obtain second authentication data, and, after reception of said first authentication data and determination of said second authentication data,
>
> h) comparison of said first authentication data and said second authentication data by said provider, wherein said processing rule is modified on each execution of the method.",

and claim 9 is to a use of this method for "the remote authentication of a user by a banking establishment or a trader offering goods or services over the internet".

6 The code can be provided on a card for the user, but in use only the result of processing the code in accordance with a provider-determined rule is transmitted to the provider – not the code itself. Therefore even if a third party recovers the result of the transmission he cannot determine the code. The processing rule is preferably modified at random after each execution of the method.

The law

Inventive step

7 Section 1(1)(b) of the Act requires an invention to involve an inventive step before a patent can be granted. According to section 3 this requirement is satisfied if the invention "is not obvious to a person skilled in the art, having regard to any matter which forms part of the state of the art by virtue of section 2(2) above (and disregarding section 2(3) above)". I do not need to quote sections 2(2) and (3) in full, but they have the effect that the prior art to be considered comprises all matter made available to the public, whether in the UK or elsewhere, by written or oral description, by use or in any other way, before the priority date of the invention (in this case 2 July 2004).

8 In *Windsurfing International Inc. v Tabur Marine (Great Britain) Ltd,* [1985] RPC 49, the Court of Appeal formulated a four-step approach for assessing whether an invention is obvious to a person skilled in the art. This approach was restated and elaborated upon by the Court of Appeal in *Pozzoli SPA v BDMO SA* [2007] EWCA Civ 588 where Jacob LJ reformulated the *Windsurfing* approach as follows:

> (1)(a) Identify the notional "person skilled in the art".
>
> (1)(b) Identify the common general knowledge of that person.
>
> (2) Identify the inventive concept of the claim in question or if that cannot be readily 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 claim as construed.
>
> (4) Viewed without any knowledge of the alleged invention as claimed, do those differences constitute steps that would have been obvious to the person skilled in the art or do they require any degree of invention?

9 In assessing whether the invention claimed in the application in suit involves an inventive step, I will therefore use this *Windsurfing/Pozzoli* approach.

Excluded subject matter

10 Section 1(1)(d) of the Act states that a patent may be granted only for an invention in respect of which the grant of a patent for it is not excluded by subsections (2) and (3) or section 4A. Section 1(2)(c) states that things which consist of "a scheme, rule or method for performing a mental act, playing a game or doing business, or a program for a computer" are not inventions for the purposes of the Act, but only to the extent that a patent or application for a patent relates to that thing as such.

11 There is a large amount of case law in relation to these provisions. The most recent judgments of the Court of Appeal on the matter are *Aerotel Ltd v Telco Holdings Ltd Ors Rev 1* [2007] RPC 7 and *Symbian Ltd's Application* [2009] RPC 1. In *Aerotel* the Court of Appeal reviewed all the previous case law and specified the following four-step test as a methodology of determining whether an invention was excluded from patentability under section 1(1)(d):

> (1) Properly construe the claim;
>
> (2) identify the actual contribution;
>
> (3) ask whether it falls solely within the excluded subject matter;
>
> (4) check whether the actual of alleged contribution is actually technical in nature.

12 In *Symbian* the Court of Appeal confirmed that the above test is intended to be equivalent to the prior case law test of "technical contribution". In the present case I will therefore use the *Aerotel* test and ensure in my consideration of steps (3) and (4) that I determine whether the invention makes a technical contribution.

Arguments and analysis

Inventive step

13 The examiner's objection rests on two disclosures:

D1: An article "Banking on Trust" by Laurika Bretherton from "Computing" on 20 February 2004 accessed at http://www.vnunet.com/computing/features/2072376/banking-trust. This is concerned generally with the need for financial institutions to win customer trust when introducing new electronic products. It includes one specific case study from Lloyds TSB briefly describing a solution to the problem of hackers using the bank's keystroke logging software to record what a user is typing on the keyboard; this avoids use of the keyboard altogether:

> "After a customer logs on to the site and fills in access details, a menu appears asking for a random set of numbers or letters from memorable data. The customer then uses the mouse to click on the characters in the box"

and is said to have been launched to customers without notification as a security measure.

D2: GB 2379525 A (Fujitsu Services Limited, published 12 March 2003). In this specification an authorisation computer receives the details of a proposed online transaction and sends a message to the customer's mobile phone asking the customer to confirm payment by supplying a specified, randomly selected, set of characters of a multi-character pass phrase. Preferably the pass phrase is at least 14 characters long and is a memorable phrase of personal significance to the customer, from which the customer is asked to supply three specified characters.

Date of the "Computing" internet disclosure

14 The "Computing" article is available on the internet and is dated 20 February 2004. The reliability of this date is disputed by the applicant. The article appears to have been published in "Computing" magazine (an industry-focused IT publication) but the examiner has not been able to locate a paper copy of the relevant issue. The only evidence before me of the date of publication of this article is therefore the date specified in the article at the above URL (and at http://www.computing.co.uk/computing/features/2072376/banking-trust, a sister website to vnunet). Neither web page has been archived on the site www.archive.org. Two issues therefore arise. Firstly, was this article actually made available to the public on 20 February 2004? Secondly, has it been altered since its initial publication?

15 The applicant's attorney highlighted that section 2 is one of those sections listed in section 130(7) as being framed so as to have, as nearly as practicable, the same effects in the UK as the corresponding provisions of the EPC. They then argued that, unless there is UK case law to the contrary or some other reason, I should follow the reasoning in the EPO's Technical Board of Appeal decision in *Konami Limited* T 1134/06 in relation to the reliability of dates of web pages.

16 In this EPO Decision the Technical Board of Appeal argues that a higher burden of proof than that applied to more traditional documents should be applied to internet documents. In particular they say that in determining whether an internet disclosure was made available to the public the same questions should be answered as with prior use or oral disclosure. At the EPO such issues and the questions of when the internet disclosure was made available to the public, what was made available and under which circumstances it was made available to the public, must be proved "beyond reasonable doubt" rather than on the "balance of probabilities". This Decision also includes a discussion on the reliability of a website and the impact this has on whether further evidence is needed to answer these questions. In particular paragraph 4.2 states:

> "In certain cases, where a web site belonging to a reputable or trusted publisher publishes online electronic versions of paper publications, content and date can be taken at face value and the need for supporting evidence dispensed with."

17 UK law has taken a rather different approach to the burden of proof required in establishing publication dates for documents and dates for cases of alleged prior use. This is summarised very clearly in paragraph 2.29.1 of the Manual of Patent Practice, which states:

> "2.29.1 In cases of alleged prior use, the required standard of proof is the balance of probabilities. Within this standard, the Patents County Court in *Kavanagh Balloons Pty Ltd v Cameron Balloons Ltd* [2004] RPC 5 held that a flexible degree of probability should be applied to evidence relating to prior use. The cogency of the evidence had to match the occasion and be proportionate to the subject matter. Because of the nature of the monopoly itself and question of public interest, no stricter standard should be applied. It was held that it was not necessary for an opponent to prove his case "up to the hilt" as had been required by the EPO Technical Board of Appeal in *Sekisui/shrinkable sheet* [1998] OJEPO 161 (T 472/92). The hearing officer in *Colley's Application* [1999] RPC 97 also distinguished from Sekisui by not requiring proof "up to the hilt", but followed this decision and *Demmeler Maschinenbau GmbH & Co KG* (T 908/95) in holding that mere assertion of prior use was insufficient: place, time and detail were essential."

18 It is therefore clear that UK practice has departed from EPO practice in relation to the burden of proof used in assessing cases of alleged prior use. As the EPO's approach to prior use forms the basis of the Technical Board of Appeal's

Decision in T1134/06, I do not consider that I am bound to follow the EPO's reasoning in this case. Rather it seems to me more appropriate, in line with UK cases in this general area such as *Kavanagh Balloons*, that the date and contents of internet disclosures be assessed on the balance of probabilities, just as it is for cases of alleged prior use or, for that matter, dating any other categories of prior disclosure. The applicant agreed that the correct standard of proof is the balance of probabilities but argued that *Kavanagh Balloons* describes how the balance of probabilities is not an absolute standard and that the nature of the issue may affect the kind and the cogency of the evidence necessary to bring the scale down on one side or the other. I accept this point as far as it goes and will take it account when reaching my decision but I note that although the judge in *Kavanagh Balloons* was prepared to assess the evidence relating to prior use on a flexible and proportionate basis, this had to be within the overall requirement of proof on the balance of probabilities, that is, whether the alleged prior use was more likely than not.

19 Other relevant guidance on this matter is found in paragraphs 18.09.2 and 18.09.3 of the Manual of Patent Practice which state:

> "18.09.2 As Mann J indicated in *Macrossan's Patent Application* [2006] EWHC 705 (Ch), any doubt should be resolved in the applicant's favour only if the doubt is substantial. This could arise if the examiner's assertions as to the common general knowledge have been challenged and expert evidence would be needed to establish the position, or if the date of a prior disclosure has been challenged and the examiner does not have access to material that would confirm the date. Certainly the examiner is not required to meet the criminal burden-of-proof standard in raising and pursuing an objection.
>
> 18.09.3 When assessing the relevance of an internet disclosure at the substantive examination stage, a document should be cited unless the examiner is certain that it falls outside the state of the art. If the applicant contests the publication date the examiner should decide the matter on the balance of the evidence available. Evidence from sources such as archive.org, while not conclusive, may provide justification for an examiner's view that there is little doubt as to the date of disclosure."

These paragraphs support my view that I should decide the matter of a contested date of an internet disclosure on the balance of the evidence available. Only if there is substantial doubt should I give the applicant any benefit of the doubt.

20 I now turn to the particular internet disclosure in question. The websites www.vnunet.com and www.computing.co.uk are operated by Incisive Media Ltd. They define themselves as a Business to Business (B2B) information provider serving the financial and business markets globally. Both these websites provide news and reviews in the IT sphere to their readers. Each article includes a date. Incisive Media also publish a number of magazines available in paper format,

some targeted at consumers (such as the well-known “Personal Computer World”) and also the magazine “Computing” targeted at IT professionals and well known in the industry, which has as its website www.computing.co.uk. The internet disclosure in question includes the following headnote:

> “Laurika Bretherton, Computing 20 Feb 2004”.

It would therefore seem that the article in question was published in the paper version of “Computing” magazine. The examiner has tried to obtain a paper copy of the relevant issue of the magazine but to date has not been able to. I do however consider it highly likely that this article did appear in a paper version of the “Computing” magazine on or around 20 February 2004.

21 Even if that were not the case, the websites above are highly reputable with a long history of publishing for both IT consumers and the IT industry. I consider that the dates they give to articles are reliable and that the content of the articles such as the disclosure in question is unlikely to be altered once published. I therefore conclude that on the balance of probabilities the internet disclosure in question was made available to the public on 20 February 2004. In fact, even if I was to follow the reasoning in T 1134/06, I would have concluded that the date of the internet article had been proved “up to the hilt” and could be taken at face value without the need for supporting evidence given the trusted and reliable nature of the websites in question and their links with paper publications.

Inventive step

22 Turning now to the matter of inventive step, I will use the *Windsurfing/Pozzoli* approach to determine whether the invention claimed in the application in suit involves an inventive step.

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

23 The examiner identified the person skilled in the art as an electronic engineer/ computer programmer skilled in user authentication processes. The applicant’s attorney has not contested this. This seems to me to be a reasonable identification of the person skilled in the art and I therefore accept the examiner’s identification.

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

24 Password authentication schemes where a user enters a password known both to themselves and to the service provider in order to obtain access to a service were very well known prior to the priority date of the application in suit and the person skilled in the art would definitely have been aware of them and known how to implement them as part of their common general knowledge at that date.

25 The person skilled in the art would also have had knowledge of the authentication of users of credit or debit cards at the priority date, both when used for purchasing items and for obtaining cash from automated teller machines (ATMs). In particular it would have been part of their common general knowledge that

when a user is first sent a credit or debit card they are also sent a PIN (Personal Identification Number) for use with that card. This is standard practice for PINs for credit cards.

26 Moreover the person skilled in the art would be aware that the PIN was normally sent separately to the card to reduce the security risks. Although the user may change the PIN, the original number is set by the provider. Similar systems were also used prior to the priority date of the invention in other applications, e.g. for accessing services on a cable TV network or for providing initial access to an IT system or service on a network. It was also common for a user to be sent both usernames and passwords (e.g. by email) in order to obtain access to a website or to other web services. These systems were also widely known to the public in general and in my view would have been part of the common general knowledge of the person skilled in the art at the priority date of the invention.

27 The applicant's attorney pointed out that I have not provided any evidence that these situations were indeed common general knowledge at the priority date. The applicant did not however disagree but rather went on to comment on why their invention was not obvious in the light of this alleged common general knowledge. In my view these situations would have been well known to the public in general at the priority date of the application in suit and would certainly have been part of the common general knowledge of the person skilled in the art at that date.

28 The examiner in one of his reports commented that if a password is provided by a provider to a user, the provider can ensure that the password is more secure than one a user may select. The examiner considered this an obvious advantage but the applicant disagreed. I agree with the examiner. Problems with users selecting weak passwords (e.g. ones that are easy to guess) have been known for as long as passwords have been in use and the person skilled in the art would, in my view, have been aware at the priority date of the application in suit that an obvious advantage to a user being supplied with a password not of their own choosing is that it can be made more secure, and would take this into account when designing an authentication system.

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

29 In his report of 4 December 2008 the examiner identified the inventive concept as the following:

> "The inventive concept of claim 1 relates to transmitting a rule relating to extracting a certain number of characters from a code (known to both a user and a 'provider', the code being provided by the 'provider') to a user, the user and provider determining at least one character of a code identified by a position in the code (the position being provided by the rule), the user transmitting the at least one character to the provider who then compares that at least one character identified by means of the processing rule to the at least one character which the provider identified by way of using at least one rule in relation to the code."

The attorney has identified the core features of the invention in similar terms, and I agree with the examiner's identification of the inventive concept subject to one clarification. The code is provided by the provider *prior* to a particular request by the user for authentication.

(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 claim as construed

30 Documents D1 and D2 each disclose all the features of the inventive concept of the application in suit except that of the provider previously providing the code rather than the user. D1 is silent on the provider of the code but does describe the code as "memorable data" which suggests that it is more likely that the user provides the code so that they can select a code memorable to themselves, although does not rule out the possibility of the provider providing the code. I would not however say that D1 implicitly discloses that the provider could provide the code. D2 clearly sets out that it is the customer who selects the pass phrase. This therefore constitutes a difference between the "state of the art" and the inventive concept of the independent claims of the application in suit.

31 The applicant disagreed with the assertion that D1 disclosed the determination by the provider of a processing rule instructing users to extract a certain number of characters and the associated steps of claim 1. Although these steps may not be explicitly set out in D1, they are clearly implied and therefore implicitly disclosed. These features do not therefore constitute a difference between the cited prior art and the inventive concept of claim 1.

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

32 Taking first the document D1, I have to decide whether it would be obvious to the person skilled in the art of user authentication processes to operate the system disclosed in D1 in a manner where the "memorable data" was a code provided by the provider. I note that the possibility of the provider providing the code initially and then the user being able to change the code falls within the scope of the claims of the application in suit. D1 is silent as to who provides the "memorable data". There are several possibilities. It could be provided by the user and communicated to the provider, by the provider and communicated to the user, or by a third party who communicates it both to the user and the provider or who handles the authentication process itself. The memorable data is clearly required to be memorable to the user. The most obvious solution would therefore be for the user to supply the memorable data, for example when initially registering with the online banking service.

33 In my view however a person skilled in the art of user authentication processes would be aware that often it is required to give a user initial access to a server to facilitate the setting up of, for example, an account with the service, just as is done for PINs for credit and debit cards, and also be aware that users are sometimes given passwords and other login information to obtain access to IT

systems and networks or to websites and web services (e.g. by email or by post). The applicant's attorney did not consider it obvious to use such approaches in the system of D1 but I disagree. This would be an obvious way of giving the user at least initial access to the system and the person skilled in the art would, taking into account their common general knowledge, think to implement or adapt the system of D1 in such a way. Moreover there are also obvious advantages to the provider providing the code, in particular so that they can ensure that the code is robust against security attacks. I therefore consider it obvious that the skilled person would also think to implement the system disclosed in D1 in a manner where, at least initially, the provider provides the data from which a random set of numbers or letters is requested.

34 Furthermore the entire purpose of the Lloyds TSB system disclosed in D1 is to avoid a situation where the user has to enter the pass phrase in its entirety into a computer in order to prevent keystroke logging attacks. The standard way of registering with the provider of an internet-based service in order to specify a pass phrase is via a form on a website and this would not prevent this problem. A number of possible solutions are available but in my view, given that the person skilled in the art would be aware of the provider providing PINs or other access codes to the user via, for example, the postal system and also aware that websites sometimes give users a password to obtain access to particular sites or services (e.g. by email), the person skilled in the art would think to apply such a technique to the system of D1, where it is the provider who provides the "memorable data", particularly given the obvious advantage that it enables the provider to ensure that the data is more robust against security attacks. This would be an obvious solution to the problem of preventing keystroke logging attacks. Thus this adds weight to my conclusion that the claimed invention is obvious in the light of the disclosure of D1.

35 Turning now to D2, this document relates to electronic payment authorisation system for authorising payments on an e-commerce website and uses text messages on a mobile telephone to transmit portions of a pass phrase. Unlike D1, it provides more specific details on the selection of the "secret pass phase", stating on page 4:

> "The registration process on the website then invites the customer to select a secret pass phrase, preferably at least 14 characters long. Selecting an appropriate pass phrase, which is in reality a long PIN, is an important part of the registration process. The user is guided to select a phrase of meaning only to them …"

In the payment process a text message is sent to the user's mobile telephone requesting three randomly selected characters of their pass phrase. The user selects these characters by replying to the text message.

36 Would there then be anything that would cause a person skilled in the art to adapt the system to one where the provider, at least initially, provides the pass phrase? The motivation for the invention disclosed in D2 is found on page 5 where it is stated:

> "It can be seen that the method described above ensures that only a portion of the pass phrase is transmitted during each individual transaction. Thus, even if the messages are intercepted, the pass phrase is not revealed, and messages cannot simply be replayed since a different random selection of characters will be requested for each transaction."

37 There is however a weak link in this system, namely that the pass phrase must be entered in full by the user during the registration process on the website. A person skilled in the art would in my view clearly see this weak point and would want to eliminate it if possible. That person would know of the system of sending PINs for credit cards to users by post, and would note that on page 4 of D2 the pass phrase is described as "in reality a long PIN". They would also be aware as part of their common general knowledge of other systems where the provider provides a password, such as to obtain access to an IT service or to a website or web service, and that this would have the obvious advantage that the provider could choose a password which is more robust against security attacks. It would therefore have been an obvious modification of the system of D2, instead of using a user-generated pass phrase which is memorable, to send to the user by post or by other means a long PIN for use with the system. The invention claimed in claim 1 therefore also lacks an inventive step over the disclosure of D2.

Other claims

38 There are 7 dependent claims in the latest form of the clams, all dependent on independent method claim 1, and also claim 9 which claims the use of the method of claim 1 to a particular class of services. The features of these claims are as follows:

Claim 2 The processing rule is determined at random.

Claim 3 The code is affixed to a carrier.

Claim 4 The code is imprinted on a credit type card.

Claim 5 The processing rule identifies a plurality of characters to be selected by supplying their positions in the code.

Claim 6 The extracted characters must be put into order according to the order of the position of each character.

Claim 7 The user also sends a password to the provider for preliminary authentication alongside transmission of the identifier.

Claim 8 The provider refuses further any new authentication attempt by the user after a particular number of failed attempts.

Claim 9 The method of claim 1 is used by a banking establishment or a trader offering goods or services over the internet.

39 The features of claims 2, 5, 6 and 9 are disclosed in the cited prior art. Claims 3,

4, 7 and 8 are standard features of authentication systems. Moreover claims 3 and 4 do not in my view add any technical features to claim 1. I therefore conclude that dependent claims 2-9 also lack an inventive step over the cited prior art.

Excluded subject matter

40 The examiner initially raised an objection that the claimed invention was excluded from patentability under sections 1(1)(d) and 1(2)(c) of the Act. He later however dropped the objection. Following the referral of the case to me for a Decision on the inventive step issue a new judgment was issued by the Patents Court, *AT&T Knowledge Ventures LP* [2009] EWHC 343 (Pat) (03 March 2009). In this judgment Lewison J considered two appeals from Decisions of the comptroller in relation to excluded subject matter. The latter, CVON Innovations Limited's application, covered in paragraphs 49-58 of the judgment, is particularly relevant to the present case. I therefore asked the applicant for any submissions they may have in relation to the relevance of this judgment to the patentability of the application in suit. In the light of this judgment I will consider in full whether the invention claimed in the application in suit is excluded from patentability under sections 1(1)(d) and 1(2)(c) of the Act, applying the *Aerotel* steps and considering whether there is a technical contribution.

1) Properly construe the claim

41 Construing the claims is in this case straightforward. In claim 1, remote authentication of a user by a provider is carried out by transmitting an identifier from the user to a provider. The provider then determines a processing rule which extracts a certain number of characters from a code previously provided by the provider to the user and transmits this rule to the user. The user then determines at least one character of the code by its position, the position being supplied by the processing rule, and transmits the resulting at least one character to the provider. The provider then applies the processing rule to the code and compares its result with that transmitted by the user. The processing rule is modified each time the method is executed.

2) Identify the actual contribution

42 In *Aerotel* it is made clear that identifying the contribution is best summed up by determining what the inventor has really added to human knowledge, and this involves looking at the substance and not the form of the claims.

43 There are two main features in claim 1. The first of these is that a code (i.e. a password or PIN) is generated by the provider previous to a particular request for authentication by the user. The second feature relates to a step whereby the provider transmits a rule to the user which extracts a certain number of characters from the code, the authentication of the user being dependent on whether the user correctly returns the extracted characters.

44 As I have found in relation to inventive step, the second of these features is disclosed in the cited prior art and thus is known, but is not known in combination

with the first feature (although I have found this combination to be obvious). To determine the actual contribution I need to assess the claimed invention as a whole and thus need to consider the interaction between the various features, known or otherwise. I have to decide whether the actual contribution relates to the first feature in isolation or to a combination of the two features.

45 I note that the second feature requires both the user and the provider to know the code, but is independent of who originally generated the code. The authentication process works in exactly the same way whether it is the user, the provider, or a third party who previously generated the code. In fact the first feature, namely the provider providing the code rather than the user, could be applied to other authentication systems that make use of passwords or PINs and is not tied to the particular system to which the second feature relates. The contribution cannot therefore in my view include both the feature of the provider providing the code and also the feature of the particular authentication method, whereby certain characters of the code are extracted by the user in dependence upon a code, such a method being disclosed in documents D1 and D2 discussed above. The applicant could have equally chosen another known authentication system to which to apply the first feature to. The two features do not in my view interact in such a way that they can be taken as a unitary whole to deliver a contribution.

46 I therefore conclude that the actual contribution relates to a method of authentication whereby a provider provides a code (such as a password or PIN) to the user for subsequent use in an authentication process.

3) Ask whether the identified contribution falls solely within the excluded subject matter

47 In determining whether the identified contribution falls solely within the excluded subject matter, Lewison J's judgment in *AT&T Knowledge Ventures LP, Re* [2009] EWHC 343 (Pat) (03 March 2009) is relevant.

48 CVON's invention related to a messaging system such as that used for transmitting text messages between mobile phones. The system modified messages sent from one terminal to another dependent upon the membership of the sender or recipient of a "group" which could be anything from a supermarket loyalty scheme to a sports club or an online community. A third party database server contained details of the members of the group in question. CVON's invention related to allowing a subscriber to prompt for updates by a using an ID and password rather than the third party.

49 The judge quoted and agreed with the comments made by the hearing officer in the following paragraph:

> "In my view, allowing a subscriber to prompt for updates to and authentication of his group membership records is not a technical matter, but a decision in relation to the business of running a message modification service. In particular, it is a business choice, made when deciding how to run the message modification service, that one should obtain some sort of confirmation that the subscriber is a member of the

> group claimed. Furthermore, it is a business choice to allow the authentication to be prompted by the subscriber – that is to say, it is a business decision about how the authentication should be carried out. Thus, for example, it is a choice made in respect of the business of running a message modification service to decide to ask the subscriber to provide log-in details or other data, which are used to verify membership of a particular on-line forum or other group. The way in which this data is then used to carry out the authentication involves the conventional use of websites and the internet. Thus the decision to use such an authentication step bestows no saving technical element upon the contribution as I have identified it.
>
> 48 It follows that there is nothing in these improvements which bring the claimed invention outside of the business method exclusion. The improvement that results is an improved business method – that is to say, a better way of using a conventional message modification system to modify the content of messages on the basis of subscribers' records."

The judge then stated "In other words the contribution is that the subscriber, rather than the third party, who initiates the authentification process".

50 There are certain similarities between CVON's invention and that of the application in suit. Both involve authentication of a user in an electronic communication, the context of the electronic communication typically being some kind of business activity (logging onto a website such as a banking website or sending a modified text message). Both relate to taking a decision on where a key aspect of the authentication process occurs. In CVON authentication is prompted by the subscriber rather than the third party. In the present case the code used for authentication is provided initially by the provider rather than by the user.

51 In the case of CVON both the hearing officer and the judge found this to be a business choice. The hearing officer said "It is a business decision about how the authentication should be carried out". Thus the excluded business method is not merely the high-level message sending but the actual implementation.

52 The applicant's attorney argues that the actual generation of the code by the service provider is in itself technical and not a business method. I disagree. In my view the decision on who generates the code is not a technical matter but rather is a business decision in relation to the business of running an electronic service such as a bank offering online services. When running such a service it is a business decision, made when deciding how users obtain access the service, that the provider specifies a code needed by the user to access the service rather than that code being specified by the user. It is a business choice about how the authentication is to be carried out. I note that once the code has been specified either by the user or the provider the subsequent authentication steps are identical whoever previously provided the code. Thus the decision that the provider specifies the code rather than the user is not a technical contribution. I conclude that the contribution relates entirely to a business method and that there is no technical contribution. The claimed invention is therefore excluded from

patentability under sections 1(1)(d) and 1(2)(c).

4) Check whether the actual or alleged contribution is actually technical in nature

53 In my analysis under step 3) above I have found that the actual contribution is not technical in nature.

Conclusion

54 I have found that the date of an internet citation is valid. I have then found that the claimed invention does not involve an inventive step and is excluded from patentability under section 1(1)(d) and 1(2)(c). I have inspected the application and can see no amendment which could result in a patentable claim. I therefore refuse the application.

Appeal

55 Under the Practice Direction to Part 52 of the Civil Procedure Rules, any appeal must be lodged within 28 days.

B MICKLEWRIGHT
Deputy Director acting for the Comptroller