Neutral Citation Number: [2024] EWCA Civ 606

Case No: CA-2024-000006

IN THE COURT OF APPEAL (CIVIL DIVISION)
ON APPEAL FROM THE HIGH COURT OF JUSTICE, BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES, INTELLECTUAL PROPERTY LIST (ChD), PATENTS COURT
Mrs Justice Bacon
[2023] EWHC 2361 (Pat)

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 4 June 2024

Before :

LORD JUSTICE SINGH
LORD JUSTICE ARNOLD
and
LORD JUSTICE NUGEE

- -

Between :

SYCURIO LIMITED	**Claimant/ Appellant**
- and -	
(1) PCI-PAL PLC **(2) PCI-PAL (UK) LIMITED**	**Defendants/ Respondents**

- -
- -

Michael Silverleaf KC and Kyra Nezami (instructed by **Michelmores LLP**) for the **Appellant**
Richard Davis KC, Edward Cronan and Laura Adde (instructed by **Shepherd & Wedderburn LLP**) for the **Respondents**

Hearing date : 21 May 2024

- -

Approved Judgment

This judgment was handed down remotely at 10.30am on 4 June 2024 by circulation to the parties or their representatives by e-mail and by release to the National Archives.

.....

Lord Justice Arnold:

Introduction

1. This is an appeal from an order made by Bacon J on 18 December 2023 revoking United Kingdom Patent No. 2 473 376 ("the Patent") for the reasons given in her judgment dated 25 September 2023 [2023] EWHC 2361 (Pat). The Patent is entitled "Signal detection and blocking for voice processing equipment". It discloses and claims apparatus for, and a method of, reducing fraud by call centre agents and others, by blocking dual-tone multi-frequency (DTMF) tones entered by a caller from being transmitted to the agent when the caller is using their telephone keypad to provide sensitive information required for a transaction, such as their payment card details. The invention has the advantage that voice communication between the caller and the agent is not interrupted. There is no challenge to the earliest claimed priority date of the Patent, which is 9 May 2008.

2. The judge held that, on the proper construction of claim 9 of the Patent, claim 9 was invalid since the claimed invention was obvious over each of two items of prior art referred to as Van Volkenburgh and Shaffer. It was and remains common ground that, if claim 9 is invalid, none of the other claims are independently valid. The judge also held that, even if claim 9 was valid, the Defendants ("PCI-PAL") had not infringed it. The Claimant ("Sycurio"), which is the proprietor of the Patent, appealed with permission granted by myself on five grounds. Ground 1 was that the judge had wrongly construed claim 9, and therefore had approached her assessment of obviousness on an erroneous basis. Sycurio did not challenge the judge's assessment if she had correctly construed claim 9. Sycurio's other grounds were directed to the issue of infringement. Having heard argument on ground 1, the Court announced that the appeal on that ground would be dismissed for reasons to be given later. That made it unnecessary to hear argument on the other grounds. This judgment sets out my reasons for reaching that conclusion.

Applicable legal principles

3. There was no dispute before either the judge or this Court as to the principles applicable to the construction of patent claims. It is therefore sufficient for the purposes of this appeal to set out the following well-established propositions. First, the claim must be interpreted through the eyes of the person, or team of persons, skilled in the art to whom the patent is addressed. Secondly, it must be interpreted taking into account the skilled person's or team's common general knowledge. Thirdly, the claim must be interpreted in the light of the description and drawings in the patent, that is to say, in context. Fourthly, the claim must be interpreted purposively, that is to say, having regard to the inventor's purpose as disclosed by the specification. Fifthly, the specification may disclose more than is claimed. Sixthly, where the language of the claim has a clear meaning, it is normally not legitimate either to extend or to cut down that meaning by reference to the description.

4. It follows from these principles that, as Sir Christopher Floyd recently said, with the agreement of Nugee LJ and myself, in *Philip Morris Products SA v Nicoventures Trading Ltd* [2022] EWCA Civ 1638, [2023] ECC 13 at [46]:

> "Whilst it is conceivable that a claim will fail to cover something described as an embodiment of the invention, the skilled person is likely to arrive at an understanding which does not have that result if the language is reasonably capable of bearing the wider meaning. The exclusionary language relied on to achieve the result of excluding from the claim something described as an embodiment of the invention would normally have to be clear."

The skilled team

5. The judge found that the Patent was addressed to a skilled team consisting of a person with expertise in telephony technology and a person with expertise in payments processing and the handling of payment information. There is no challenge by Sycurio to that finding.

Common general knowledge

6. At the end of the trial the parties agreed a statement of the skilled team's common general knowledge assuming that the team was composed as the judge found. The judge set out a summary at [42]-[68] which I reproduce below in slightly abbreviated form.

Call centre telephony systems

7. Prior to the priority date of the Patent, call centres used private telephone systems called private branch exchanges (PBXs), which comprised telephone lines (trunks) connected to the public switched telephone network (PSTN), and extensions to each telephone handset used by a call centre agent. During the 1980s, analogue PBX systems were replaced by digital PBXs, and by the priority date digital PBXs accounted for 90% of the market. The remaining systems used the Voice over Internet Protocol (VoIP) technology explained below, which businesses were starting to use by the priority date.

8. Both analogue and digital PBX systems used the traditional circuit switched network. By contrast, the more recent VoIP technology used (and continues to use) packet switched networks. The differences between these are discussed further below.

DTMF technology

9. DTMF technology is legacy technology which was widely used in the UK by the late 1970s. A DTMF tone is an audible sound created when two pure frequencies (one high, and one low) are combined. Each button on a telephone keypad generates a different DTMF tone when pressed, and DTMF tones can therefore be used to input information via telephone instead of providing information verbally.

10. At the priority date DTMF tones were commonly used by call centres to provide information (including payment information) to Interactive Voice Response (IVR) systems. An IVR system is an automated system with which a caller can interact on a telephone call through either voice or with DTMF tones, a typical use being in an automated welcome menu (e.g. press "1" for "sales", "2" for "accounts", etc). IVR

systems can play announcements and prompt callers to enter each piece of information, and can read information back to customers (such as a customer's credit card number) and ask them to confirm it. At the end of an interaction with an IVR, the system may transfer the caller to an appropriate member of staff (automatically or by asking the caller to press a button) or end the call.

11. At the priority date, it was common for call centre technology (including DTMF functionality and IVR systems) to be based on telephony cards which were inserted into computers, and which could manage multiple calls at a time. Because the telephony card fitted into a standard computer expansion slot, the manufacturer only needed to develop the hardware and software for the specific functions of the card; everything else could be written by the user on the computer as standard software code or configuration. Typical functionality on telephony cards included a "silent monitor" function whereby a supervisor or trainer could listen in on an agent's call for training or quality-control purposes, and a "whisper mode" whereby the supervisor could listen in to the call and speak to the agent, unheard by the caller.

12. Telephony card functionality also included DTMF blocking functionality (sometimes referred to as DTMF "clamping"), enabling DTMF tones to be blocked from one person on the call, such that the DTMF tones would not be heard by that person but the rest of the conversation would be heard. This functionality could be configured using the telephony card software. For example, when an agent pressed a DTMF button to transfer a customer to another agent, DTMF blocking could be used to prevent the customer from hearing the DTMF tone. DTMF blocking could be done in any direction (e.g. agent to caller or caller to agent), although there was no common general knowledge application at the priority date which required DTMF blocking in the caller to agent direction.

Card payment processing

13. Card payments are divided into two general categories: card present, or face-to-face payments, and card not present, or remote payments. The present case is concerned with remote payments, and specifically card payments processed over the telephone in a call centre environment.

14. There are four key parties to a credit or debit card payment transaction: (i) the cardholder, namely the customer who is paying by card; (ii) the merchant, namely the vendor that sells to the customer, and which accepts credit or debit card payments for the goods or services; (iii) the card acquirer, who acquires transactions from merchants and processes them; and (iv) the card issuer, which is the financial institution that has issued the credit or debit card to the cardholder on behalf of a particular card payment network (such as Visa or Mastercard).

15. Three steps are required to complete a card transaction:

    i) Validation involves checking that the card details provided by the customer are valid, e.g. checking that the correct number of digits have been entered. This is done by the merchant.

    ii) Authorisation is the process by which the card issuer decides whether to authorise the payment transaction. The authorisation request originates from

the seller, and is sent to the card acquirer and then on to the card issuer. The card issuer validates the card details and conducts fraud checking and credit checking to make the authorisation decision.

iii) Completion/settlement of the transaction follows an approved authorisation by the card issuer. It is only at this point that money changes hands. Settlement is handled by the card payment scheme which calculates the financial obligations between all participants in the system. After receiving an authorisation response, a transaction is completed by providing the customer with a receipt, and entering the details of the transaction on the settlement file. Those transaction details include the last four digits of the long card number (referred to as the Primary Account Number, or PAN), the transaction ID, and card expiry date, but not the card verification code. The remaining transaction data are then deleted from the system.

Security of payment systems

16. Originally, remote transactions were conducted with a customer reading their card details over the telephone to a merchant staff member or call centre agent. By the priority date, card details could also be entered by a customer using their telephone keypad to generate DTMF tones as described above. Both approaches had significant security problems, and at the priority date payment card fraud for remote transactions was a well-known problem in the payment card industry. One of the major vulnerabilities was the possibility of call centre agents gathering personal and customer data from their conversation with the customer, either by writing customers' card details down where these were provided verbally, or by recording DTMF tones and decoding them later.

17. The Payment Card Industry Data Security Standard (PCI DSS) is an international set of minimum data security standards to be followed by merchants and acquirers who handle payment card data, its purpose being to limit the compromise of payment systems, to ensure cardholder data are handled securely, and to protect those data from theft and fraudulent misuse. It was developed cooperatively by the international card networks, including Visa and Mastercard.

18. PCI DSS v1.1 was the applicable version of the standard at the priority date. It included the following requirements:

i) Requirement 3.2: "Do not store sensitive authentication data subsequent to authorisation (even if encrypted)".

ii) Requirement 3.3: "Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed)".

iii) Requirement 3.4: "Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches: [various encryption techniques]".

iv) Requirement 4.1: "Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet

> protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks".

19. Most of the requirements relate to securing data within the call centre, while the others are concerned with protecting the perimeter of that environment. The standard approach taken for PCI DSS compliance prior to 2008 was to protect the cardholder data environment. The preface to PCI DSS v1.1 described the scope of the PCI DSS security requirements by reference to the cardholder data environment as follows:

> "These security requirements apply to all 'system components'. System components are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment."

Techniques available for addressing fraud and the PCI DSS requirements

20. At the priority date, the most common method of payment processing over the telephone was via a conversation with the agent in which the caller simply read out their payment card details. The second most common approach, also in widespread use, was via an IVR with a payment line.

21. The widespread use of call recording in call centres presented a particular challenge for both of these approaches. The UK Financial Services Authority (FSA), the predecessor to the Financial Conduct Authority, had since the early 2000s required the whole telephone conversation relating to certain financial transactions to be recorded. This conflicted with (among other things) PCI DSS requirement 3.2. The FSA therefore agreed that card payment data could be excluded from the call recordings.

22. Two techniques were well known for mitigating fraud within a call centre and complying with the PCI DSS requirements (in particular requirement 3.2) whilst meeting the general FSA requirement for the recording of calls.

23. The primary solution available at the priority date was "pause and resume". Where call recording was being used in a call centre, the call recording would be paused manually by an agent or by an automated process prior to the caller reading out their card details. The call recording would then be resumed after the card details had been provided, thereby avoiding the capture of card details on the call recording files.

24. The second commonly used solution was "mid-call transfer", where the call was transferred from the call centre agent to an IVR, such that the agent was no longer on the call. The IVR system would then prompt the caller to enter their payment card details using DTMF. Once the transaction was completed, the call could be passed back to the agent. This solution resulted in normal voice communication between the caller and the agent being interrupted. Some implementations could, however, provide feedback to the agent showing progress on the IVR system. One perceived

disadvantage of mid-call transfer was that cardholders sometimes struggled to enter data and gave up.

VoIP and SIP

25. Both analogue and digital telephone calls in a circuit switched network require a physical connection (i.e. a circuit) to be established from one caller to another. The PSTN contains many switches (telephone exchanges) connected by communication links (trunks) to the public network, such that when a call is made, the system finds a route from the caller through multiple switches and trunks to establish a circuit with the callee.

26. In the 1970s data networks were established which communicated data via the Internet Protocol (IP), i.e. the early internet. In order to achieve high reliability and communication speeds, data were not sent via a single circuit, but were split into individual packets, with each packet sent across the network in the most efficient way. Different packets could therefore be sent by different routes. These IP based networks are called packet switched networks. By the early 2000s, telecommunications providers began to move to a packet switched approach. Businesses also started changing their circuit switched PBXs to packet switched PBXs, and moving their voice calls onto the IP network. When voice data are sent via a packet switched network, this is referred to as VoIP. The existence of VoIP technology was common general knowledge at the priority date.

27. Data communication on the internet (including VoIP calling) is controlled by a number of different protocols operating at different "layers" of the network stack. These layers consist of an application layer, where network applications reside; a transport layer, which transports application-layer data between two end points of an application; the network layer, which is responsible for moving network-layer packets from one end device to another, and which runs using the IP; a link layer which supports transmission and reception of data packets across links connecting routers or end-devices, using for example WiFi; and a physical layer which moves individual bits across the transmission medium of the link, using for example copper wire, coaxial cables, fibre optics, or 4G and WiFi radio channels.

28. The protocol used for a particular type of communication depends on the type of data being sent. One relevant protocol is the Session Initial Protocol (SIP), first defined in 2002. SIP is an application-layer protocol which is used to set up, end or otherwise manage a VoIP call between two or more parties.

<u>The specification</u>

29. The specification is not a well-drafted document. It is turgid, repetitive and diffuse. Navigation through the document is not assisted by the fact that, while it contains some sections that are differentiated by headings, in other places new sections start without being signposted by a heading. The specification also contains a considerable number of typographical errors, some of which are more obvious than others. Examples of obvious typographical errors are references to "dial-tone multi-frequency" (as well as to "dual-tone multi-frequency") and a number of references to Figure 5 when it is clear that Figure 6 is intended. An example of less obvious typographical errors is the first sentence of the "Overview" section discussed below.

The specification also contains some disconcerting inconsistencies in phraseology. For example, the first three paragraphs refer to "call centres", but the fourth and fifth paragraphs refer to "call switching centres". It is common ground that the meaning of these expressions is the same, however.

30. The judge set out a very succinct summary of the disclosure at [69]-[83]. In the light of the arguments on the appeal, I must set it out at rather greater length.

31. The specification begins, under the heading "**Telephone system**", at page 1 lines 2-8:

> "The present invention relates to a telephone call processing system and method, and in particular to an apparatus to enable a caller to perform a transaction, facilitated by a call centre, with a third party without having to disclose sensitive information to the call centre.
>
> Also described is a system for the secure communication of information and a method of operating the same. The system and method described finds particular use in the communication of information, such as personal and/or financial information, between a user and a call centre or the like."

32. The specification then describes at page 1 line 9 to page 2 line 25 the increasing use of call centres to provide services to the public, including enabling payment for goods or services by telephone using a payment card, and the problem of fraud by call centre agents described above.

33. At page 2 line 27 to page 3 line 8 are consistory clauses corresponding to claims 1 and 9. At page 3 lines 9-19 there is what appears at first blush to be a third consistory clause. On closer inspection, however, it can be seen that this paragraph begins with the words "Also provided is" and that it does not precisely match any of the claims, although it resembles claim 60.

34. The specification then states at page 3 lines 20-32:

> "Hence a telephone call processor with such a capability can be switched between a first 'normal' mode, wherein it is essentially transparent to the entities connected via the first and second telephone interfaces, and a second 'safe' mode, wherein potentially sensitive data sent by the first entity connected via the first, optionally telephone, interface is prevented from reaching the second entity connected via the second, optionally telephone, interface, whilst voice communication between the two entities remains unaffected. This can afford the advantage that the first entity may have a transaction facilitated by the second entity without having to disclose sensitive data to the second entity and whilst continuing a voice conversation with the second entity. This can provide security for the first entity combined with voice feedback to both entities, without exposing sensitive data to risk of compromise at the call centre.

> Preferably, the data signals comprise audio tones. More preferably, the data signals comprise DTMF (dial-tone multi-frequency) audio tones."

35. It is common ground that the words "such a capability" refer back at least to the two consistory clauses. Counsel for Sycurio submitted that those words did not necessarily embrace the apparatus described in the preceding, "also provided", paragraph, but the two paragraphs appear to be perfectly consistent with each other.

36. From page 3 line 31 to page 5 line 32 the specification sets out a series of implementation options, some introduced by the word "preferably" and others identified by phrases such as "may be adapted" and "may comprise". This section introduces the concept of a "masked" data signal as follows at page 4 lines 3-10:

> "Preferably, the call processor is further adapted, when in the second mode, to transmit to the second, optionally telephone, interface, in response to a data signal received at the first or second interface, a masked data signal unrelated to that received at the first or second, optionally telephone, interface.
>
> This is referred to as a 'masked' signal in that it is not possible to infer the original signal from it, the advantage being in that feedback is thereby provided to the second entity as to the fact of data being received from the first entity without making the second entity privy to the content of the data received."

It also introduces the possibility that the call processor may comprise "a telephony module (e.g. a telephony card)" (page 4 line 45).

37. At page 5 lines 33-40 there is a paragraph which states that "There is also provided" a method corresponding to the apparatus described at page 3 lines 9-19.

38. At page 5 line 41 the specification states: "Some further aspects will now be described". This is followed by nine sections, each with its own heading and each of which begins with the words "Also provided is":

i) "**Further secure mode**" (page 5 line 42 to page 6 line 22);

ii) "**Voice/Biometric verification**" (page 6 lines 23-37);

iii) "**Voice feedback generation**" (page 6 line 38 to page 7 line 3);

iv) "**Resilience**" (page 7 lines 4-20);

v) "**System Integration**" (page 7 lines 21-39);

vi) "**Controlling interaction with a third party**" (page 7 line 40 to page 8 line 16);

vii) "**Hosted Payment Gateway**" (page 8 lines 18-37);

viii) "**Modularisation**" (page 8 line 38 to page 9 line 12); and

ix) "**Other Aspects**" (page 9 line 13 to page 11 line 4).

39. The "**System Integration**" section reads as follows:

> "Also provided is a telephone call processor for handling sensitive information during a telephone call, the call processor comprising a first telephone interface, a second telephone interface, and a data interface, the call processor being adapted: to receive signals at the first telephone interface and to selectively transmit the signals received at the first telephone interface to the second telephone interface wherein the received signals include signals representing sensitive information, and wherein the signals representing sensitive information are blocked from transmission via the second interface; to process the received signals representing the sensitive information to generate data representing the sensitive information; and to transmit the generated data via the data interface.
>
> The data interface may be a secure interface (e.g. comprising a secure socket layer SSL socket) for communication of data in an encrypted form. The data may be encrypted such that the encrypted data is only capable of decryption by a certified computer device. The data may be encrypted such that the encrypted data is only capable of decryption by a certified computer device on which a specific certificate (e.g. an SSL certificate) is installed. The certificate may be generated by a source other than a standard certification authority. The data interface may be an interface for communication of data to a web page. The transmission of the generated data via the data interface may comprise transmission to a computer device."

40. The "**Hosted Payment Gateway**" section reads as follows:

> "Also provided is a telephone call processor for processing telephone calls, the call processor comprising a first telephone interface and a second telephone interface, the call processor being adapted: to receive signals at the first telephone interface and to selectively transmit the signals received at the first telephone interface to the second telephone interface wherein the received signals include signals representing information relating to a transaction, and wherein the signals representing information relating to the transaction are blocked from transmission via the second interface; to generate a verification request based on the transaction information; to transmit the verification request to a verification entity; and to receive a message from the verification entity to identify verification success or failure.
>
> The signals representing information relating to the transaction may represent purchaser information (e.g. credit card details, bank account details or the like). The call processor may be

> adapted to receive signals at the second interface which may represent further information relating to the transaction and may be adapted to generate the verification request based on the further transaction information. The signals representing further information relating to the transaction may represent vendor information (e.g. order/purchase/call reference number, merchant ID, required payment value or the like). The call processor may be adapted to generate signals representing a verification message based on the message received from the verification entity, and may be adapted to transmit the verification message to the second and/or first interface accordingly. The signals representing the verification message may comprise voice (or data) signals."

41. From page 11 line 5 to page 17 line 9 the specification describes various advantages of, and options for implementing, "the system and method described". This section begins at page 11 lines 5-7:

> "The system and method described may allow a user to conduct a transaction with a call centre involving the transmission of sensitive data, such as personal information, financial information and the like, with a significantly increased level of security."

42. At page 11 lines 21-25 the specification explains:

> "In the present specification, the term 'switch' is used to refer to any device or installation that may be called by a user to make a transaction over the telephone and includes any facility, such as a call centre or other institution where an agent or operator is active to collect information from the user that is sensitive and requiring secure transmission and handling."

43. At page 13 lines 17-36 the specification describes two alternatives as follows:

> "In the system described, a processor is provided in the system. The processor may [be] of any suitable form to process call signal data and suitable processors, in particular digital signal processors are well known in the art. The processor is employed to process the call signal data received from the user, in particular the transactional information, such that it is in a form that is not ordinarily readable by the agent or operator at the switch, but may still be processed in order to complete the transaction. The processing applied to the transactional information, in particular DTMF data, may be any required form. For example, the processing is at its simplest to identify that the telephone communication from the user contains transactional information, identify the transactional information and block its transmission to the switch. The thus blocked transactional data may be handled in a variety of ways, as described hereinafter.

> Alternatively, the processor may convert the format of the transactional information signal to one that may be processed by the switch or other recipient, but that is not ordinarily readable by an agent or operator at the switch or the other recipient. For example, the processor may convert an audible signal of the transactional information, such as a DTMF signal, into a data signal that is inaudible to the agent or operator at the switch and cannot be recorded by conventional means used to record telephone calls and transactions. Alternatively, the processor may alter or otherwise mask the audible tones, such that they are rendered meaningless to the agent or operator and cannot be used to generate the transactional information originally input by the user."

44. The same two alternatives are described in reverse order at page 14 lines 28-46 and following:

> "In one preferred embodiment, the processor identifies the transactional information received by the system from the user and converts this transactional information into a format that is not readily readable by the agent or operator at the switch, thereby ensuring the security of the transactional information and preventing it from being easily copied and used inappropriately. The format of the converted transactional information is one that may be processed by an appropriate device at the switch, such as a processor. The system then transmits the converted transactional information to the switch, preferably accompanied by call identifying data, such as a URN, where the transactional information is processed by the switch, but without being directly accessible by or readable by the agent or operator. A copy of the data transmitted to the switch may also be stored in the storage means local to the system, if desired.
>
> In an alternative, preferred arrangement, the system identifies and removes the transactional information from the call signal data received from the user and prevents its transmission to the switch, as described hereinbefore. The transactional information is then transmitted to a third party for further processing. The third party may be any third party or third party installation that is required to complete the transaction being conducted by the user. For example, in the case of a financial transaction, the third party installation may [be] that of a credit card company or bank, where credit card information and the like are processed, for example to complete payment for goods or services. …"

45. Between these two passages the specification introduces at page 14 line 4 the concept of a "uniform resource name (URN)" as part of the data identifying a call.

46. At page 17 lines 9-10 the specification states: "The invention will now be described, purely by way of example, with reference to the accompanying drawings". It then lists and describes 21 figures (although Figure 18 is erroneously referred to as "Figure 19"). Figure 1 is described both in the text (at page 17 line 12) and in the figure itself as illustrating the prior art. This is not true of any of the other figures. Figures 12 to 14(c) are described at page 17 lines 29-32 as follows:

> "Figure 12 shows another embodiment of the system, wherein an additional 30 verification stage is used;
>
> Figure 13 shows the call processor in operation as a hosted gateway;
>
> Figures 14(a) to 14(c) show different arrangements for different integration options".

47. Figure 2 is reproduced below.

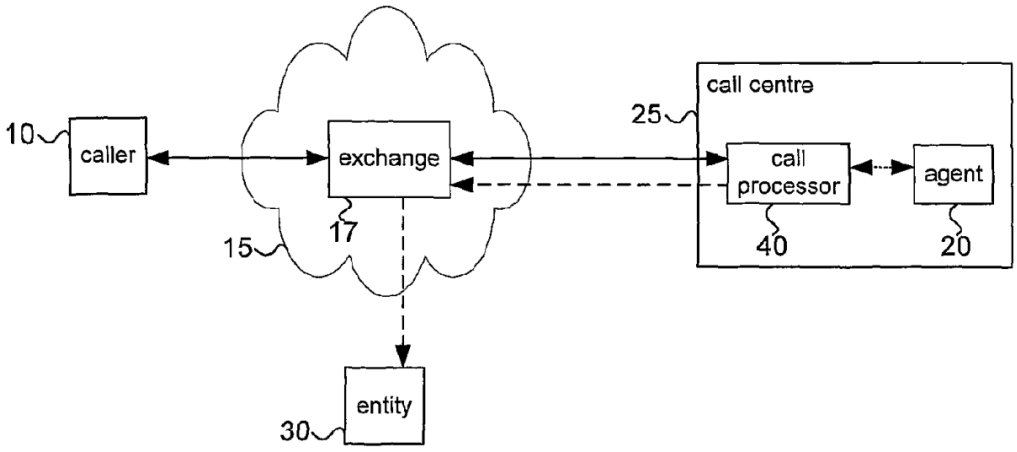

Figure 2

48. Figure 2 is described at page 18 lines 12-35 as follows:

> "Figure 2 shows a telephone call processing system, wherein a caller 10 communicates via a telephone network 15 (comprising one or more telephone exchanges 17) with an agent 20 in a call centre 25. The telephone call from the caller 10 to the agent 20 is 15 routed via a telephone call processor 40, located in the call centre 25. Call processor 40 is an intermediary for all such calls between caller 10 and agent 20 and is arranged such that the agent 20 has no means by which to circumvent the call processor 40 and interact with the caller 10 directly. As will be described below, call processor 40 acts to modify characteristics of the telephone call or signal from the caller 10 to the agent 20 and to route data to the entity 30 such that sensitive information from the caller 10 is barred from reaching the agent 20 whilst allowing agent 20 to assist caller 10 in facilitating the interaction with entity 30.

> As will be appreciated by those skilled in the art, the modification of the call characteristics is ideally done only during those times when sensitive data is being transmitted by the caller 10.
>
> In this embodiment, call processor 40 is located in the call centre 25; alternative embodiments may be envisaged by those skilled in the art. For example, call processor 40 may be located at a site within the telephone network 15 external to the call centre 25, and exchange 17 configured such that calls from the caller 10 to the call centre 25 are routed via call processor 40. By such means, call processing could be offered by [a] service provider as a service to the call centre 25. In a further alternative, call processor 40 is located at the location of the caller 10, as a part of or in addition to the telephony equipment of caller 10. Thus it can be seen that the call processor 40 could be placed at any point along the telephony network between caller 10 and agent 20, and also be made compatible with any traditional telephony network, including SIP (Session Initiation Protocol) and VoIP (Voice over IP) telephone systems."

49. Figure 3(a) is a schematic diagram showing components of the call processor. They include two telephone interfaces and a data interface. The text states at page 18 lines 41-42 that the call processor may be implemented as a standard PC with a telephony card. Figure 3(b) is a schematic diagram showing a modularised call processor. The text explains at page 19 lines 8-11 that the call processor essentially comprises three main modules, a telephony card 50, a telephony processing module (TPM) 52 and a data processing module (DPM) 54. It goes on to explain at page 19 lines 26-27 and page 19 line 46 to page 20 line 1 that the TPM can communicate with the telephony card, and the TPM and the DPM can communicate with each other, over a standard IP network interface. It then says at page 20 lines 4-10 that in the implementation described by reference to Figure 3(b), the telephony card, TPM and DPM are all in a single unit, but that other implementations are described later. It also says at page 20 lines 11-16 that, where the call processor is provided in "agent premises such as the call centre 25 (e.g. as described in Figure 2)" the TPM, DPM and/or telephony card may be provided as part of an application server at the premises which may be configured to handle other transaction-related applications.

50. Figure 4 shows the system operating in "normal" mode and Figure 5 shows the system operating in "safe" mode. So far as the latter is concerned, the specification states at page 20 lines 29-35:

> "The tones received by the agent 20 are modified such that the agent is only aware of the number of DTMF tones input by the caller 10 (thereby to allow feedback regarding input progress to the agent 20), but is unable to determine their identity i.e. which specific DTMF tones were sent. In the present embodiment this modification comprises masking the DTMF tones received from the caller 10 with a single frequency tone which is relayed to the agent for each DTMF tone input by the

> caller 10. Alternatively, each DTMF tone received from the caller 10 may be masked by a random tone."

51. Figure 6 is a schematic diagram showing the operating sequence of the telephone call processing system. This is described step by step at page 20 line 43 to page 25 line 41. Steps 1 to 10 are in "normal mode". At step 11 the agent manually, or agent software automatically, sets the call processor to "safe" mode for DTMF acquisition and forwards payment information to the call processor. The specification states at page 22 lines 13-15 that, "[a]s those skilled in the art will appreciate, a wide variety of methods of placing the call processor 40 into 'safe' mode will assist in compatibility with existing call centre systems". It goes on at page 22 line 22 to page 23 line 22:

> "Those skilled in the art will be able to contemplate a number of alternative scenarios regarding acquisition, processing and forwarding of the payment information to enable maximum compatibility with existing systems. For example:
>
> - Call processor 40 collects all or part of the card number from the caller 10 and passes this information to the agent's system or database A directly, bypassing the agent 20. The remainder of the card details can then be collected by the agent 20 by the usual method.
>
> - Call processor 40 is passed the amount to collect and the card type (e.g. Mastercard, Visa etc) by the agent application via CTI. The card number may be passed by DTMF tones from the caller 10 to the call processor 40, which then contacts the bank or other financial institution and verifies the payment via a secure external connection. The call processor 40 then indicates to the caller 10 and the agent 20 that the payment has been completed successfully, and also sends information back to the agent's system about the transaction (e.g. by means of a transaction URN). This method ensures that the card details never pass beyond the call processor 40 and the financial institute's systems.
>
> - Call processor 40 requests from the caller 10 the card number, type and password /PIN number. These are then transmitted securely to the appropriate financial institution for verification, the outcome being indicated to the caller 10 and agent 20 by means of speech recordings.
>
> Exemplary embodiments in which card details are passed to the agent's system or database without the[m] being divulged to the agent are described later with reference, in particular, to Figures 14(a) to 15.
>
> Exemplary embodiments in which sensitive information such as card details are passed by the call processor for verification by a third party entity, without being sent to the agent or the

> agent's system are described in more detail later with reference, in particular, to Figure 12."

52. The specification immediately goes on to say at page 23 lines 24-27 (italics in the original):

> "*once the call processor 40 enters DTMF acquisition/'safe' mode, DTMF tones from the caller 10 are blocked by the call processor 40 and prevented from reaching the agent 20 (or even the call centre switch). Normal voice communication however proceeds uninterrupted.*"

53. Later in the description of Figure 6, the specification explains at page 25 lines 7-21 that "verification" is "an optional step" in which a transaction is authorised by a third party verifying entity such as a bank, which may be done in accordance with a known standard such as Verified by Visa or MasterCard SecureCode.

54. Figures 7 to 10 show flow diagrams for the operation of certain aspects of the call processor. Figure 11 shows "an alternative arrangement of the elements of the telephone call processing system, wherein the call processor 40 is located outside the call centre" (page 27 lines 17-18).

55. Figure 12 is reproduced below.

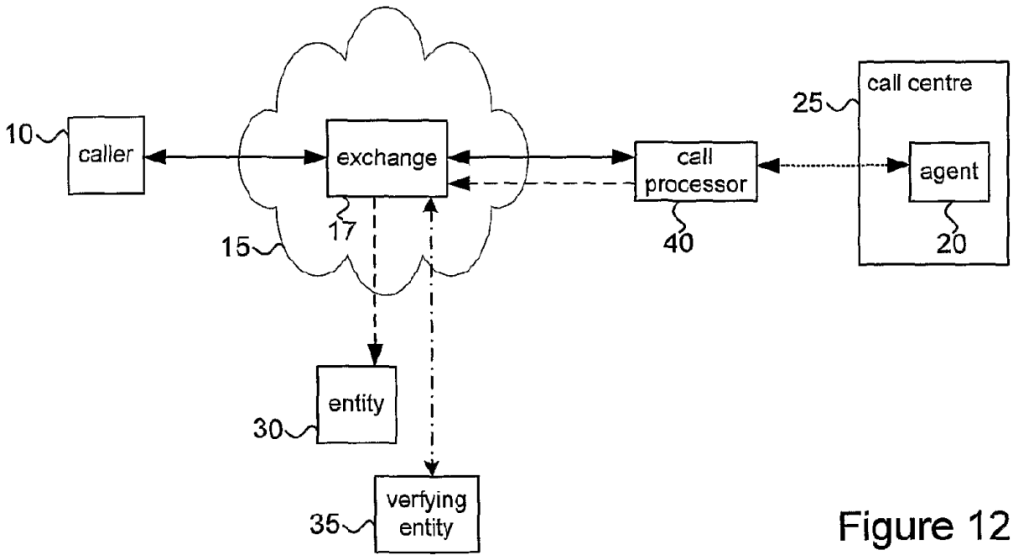

Figure 12

56. Figures 12 and 13 are described at page 27 line 23 to page 29 line 6 as follows:

> "Figure 12 shows another embodiment of the telephone call processing system, wherein an additional verification stage is used. This corresponds to the stage shown in Figure [6], steps 24 and 25, entitled Verification. In this embodiment, before proceeding with the transaction with entity 30, the call processor 40 verifies details provided by the caller 10 with verifying entity 35. Only upon receiving confirmation from the verifying entity 35 does the call processor 40 proceed with the transaction with entity 30. One example of such a verification

> stage will be known to those skilled in the art as 3D Secure system used by certain credit card companies, which is also known as Verified by Visa /Mastercard SecureCode.
>
> ***Hosted payment gateway***
>
> In the embodiments shown in and described with reference to Figures 11 and 12 the call processor 40 effectively acts as a hosted (voice) payment gateway which provides means by which a merchant can ensure compliance with the payment card industry (PCI) data security standard (DSS) through the use of the call processor, effectively allowing the merchant to outsource its responsibilities to a trusted system comprising the call processor 40.
>
> In the hosted model, the call processor 40 (or the telephony card 50 part of the call 40 processor) preferably resides in a telecomm provider's infrastructure. In operation payment card data would be collected from the caller using DTMF as described previously, and call centre 25 associated transaction data (e.g. merchant ID, payment reference, and transaction value) would be sent from the call centre 25. Accordingly, all the data needed to process the transaction is assembled at the call processor 40. This process is illustrated in Figure 13.
>
> Once the data is assembled, the call processor 40 routes the data to a payment handling entity 30/35 for payment processing. The entity 30, 35 provides the appropriate response (authorisation success or failure) back to the call processor 40, which then communicates (via a voice and/or data link) the authorisation success or failure to the call centre agent 20 for appropriate action.
>
> Beneficially, therefore, the payment is completed in a PCI compliant environment and accordingly there are no PCI implications for the call centre 25 as well as all the other benefits (such as keeping payment card details away from call centre agents, improving caller perception etc)."

57. Figure 14(a) is reproduced below.

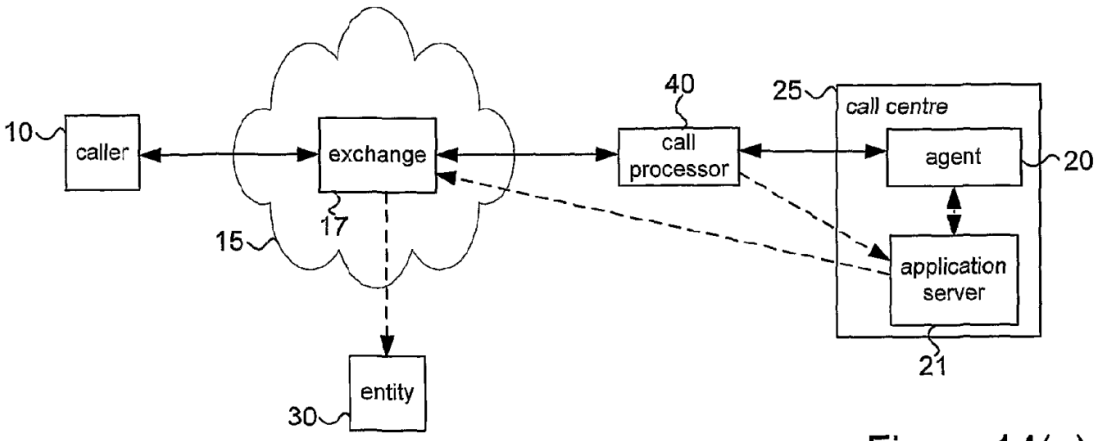

Figure 14(a)

58. At page 29 lines 7-10 the specification states:

> "***System Integration***
>
> Figures 14(a) to 14(c) illustrate different options for simple integration of the call processor 40 into existing systems for acquiring payment information and/or handling transactions at a call centre."

59. Figure 14(a) illustrates "*Option 1 - Full integration with payment engine*". As the specification explains at page 29 lines 12-21:

> "In Figure 14(a) an implementation is shown in which the call processor 40 is located outside the call centre 25, and in which the call processor 40 is adapted to transmit sensitive information, such as card details, collected whilst operating in safe mode (e.g. corresponding to the DTMF ACQUISITION /SAFE MODE stage in Figure [6] - steps 13 to 23) directly to an application server 21 at the call centre, thereby by-passing the agent. The application server 21 is adapted to handle the transaction (including any verification stage) using the sensitive data essentially as if the data had been collected directly by the agent. The application server 21 is further operable to filter the information received from the call processor for display on the agent's desktop to hide or obscure sensitive information whilst allowing the agent to see the progress of the transaction and/or confirm when it is completed successfully."

60. Figure 14(b) illustrates "*Option 2 - Desktop middleware*". In this implementation the agent's computer runs a dedicated application ("middleware") which is "operable to retrieve the sensitive data from the call processor 40 and to pass it to an application server 21 without revealing it to the agent 20" (page 29 lines 33-35).

61. Figure 14(c) illustrates "*Option 3 - Manual Inputs*". In this implementation data is provided to a graphical interface running on desktops of trusted agents over an encrypted connection. As the specification explains at page 30 lines 17-26:

> "Accordingly, interception of the sensitive data (for example by recording DTMF tones) within the call centre, before it reaches the agent, is prevented or at least severely inhibited.
>
> The sensitive data is displayed in the graphical interface on the agent desktop 20' where the agent is able to 'cut and paste' (in the standard manner) it into a transaction handling application on their desktop 21. It will be appreciated that whilst this implementation advantageously takes advantage of the flexibility, provided by the call processor, for secure data communication to a trusted agent, the agent desktop (or applications thereon) could, nevertheless, be adapted such that data displayed is obscured from the agent (or encrypted) whilst still allowing the cut and paste operation."

62. Figure 15 shows part of the sequence of operation for some implementations of the call processor. The specification states at page 30 lines 36-39 that this is "particularly relevant to the implementations described with reference to Figures 14(b) and (c)" but "the principles embodied by this example are more generally applicable to other implementations of the call processor". The description of Figure 15 is followed at page 33 line 19 to page 35 line 36 by a section headed "***Other Features and benefits of the call processor***" which is sub-divided into sections headed "**Voice verification**", "**Voice feedback generation**", "**Two-way interface**", "**Further secure mode**", "**Compatibility with agent systems**", "**Control of third party activity**" and "***Scaling and Resilience***".

63. Figures 16 to 18 are described at page 35 line 37 to page 38 line 22. It is not necessary to describe this part of the disclosure for present purposes.

64. The specification concludes with a section headed "***Overview***" which begins at page 38 lines 24-45 as follows:

> "A system has therefore been described in which a call processor can be used either as a hosted (voice) payment gateway (or as a customer premises or customer-provided equipment (CPE) at a call centre) which allows the collection of payment card data via the telephone keypad using the DTMF protocol (or potentially by voice recognition).
>
> The call processor has the potential to eliminate (or reduce) the collection of card details by live agents by masking the data they receive. This means both the agent and the call recording do not 'hear' the DTMF data, such that pausing the call recording equipment or encrypting the data becomes unnecessary thereby removing a significant point of compromise for stolen card details.
>
> In one implementation, the caller maintains a voice connection with the customer throughout the interaction; there is no transferring of the call to an interactive voice response (IVR) system or other impersonal automated system. The call

> processor effectively 'splits' the call into voice and DTMF channels automatically such that the caller experiences little or no difference in call, other than a beneficial reduction in handling time. A safe (or secure) mode in the call processor is automatically activated when a secure transaction is required. In the safe mode the call processor effectively removes the DTMF Channel from the Call Centre Agent's experience. The configuration of the call processor allows it to be integrated directly with existing call centre (transaction handling) applications to collect and transmit secure data.
>
> Accordingly, aside from the communication of card details, the call between customer and merchant is entirely as normal and indeed the agent and the customer remain in voice contact throughout the call. This means that customer satisfaction levels are maintained and any input errors can be quickly identified and remedied."

65. The first sentence appears to contain a number of typographical errors, but it is not easy to work out how it should read. The most likely reading appears to be as follows:

> "A system has therefore been described in which a call processor can be used either as a hosted (voice) payment gateway or at a customer's premises or as customer-provided equipment (CPE) at a call centre which allows the collection of payment card data via the telephone keypad using the DTMF protocol (or potentially by voice recognition)."

The claims

66. Ignoring two "substantially as described" claims (claims 108 and 109), there are only two independent claims: claim 1, which is an apparatus (or product) claim, and claim 9, which is a method (or process) claim. Claims 2-8 and claims 17-87 are all dependent on claim 1. Claims 10-16 and claims 88-105 are all dependent on claim 9. Claim 106 is a very curious product-by-process claim (which, incidentally, mistakenly purports to be dependent on "any of claims 9 to 15 or 87 to 104").

67. Broken down into integers, claim 9 is as follows:

> "[a] A method of processing telephone calls comprising voice signals and data signals comprising:
>
> [b] receiving voice signals and data signals at a first telephone interface and
>
> [c] transmitting the voice signals and selectively transmitting the data signals received at the first telephone interface via a second telephone interface wherein
>
> [d] if said received data signals include transaction information signals representing information relating to a transaction said

> transaction information signals are blocked from transmission via said second interface;
>
> [e] generating a request based on said transaction information signals;
>
> [f] transmitting said request via a data interface to an external entity;
>
> [g] receiving a message from the entity via the data interface to identify success or failure of the request; and
>
> [h] processing the transaction information signals in dependence on the success or failure of the request."

68. It is common ground that all of the terms used in claim 9 are ordinary English words with no special technical meanings. The judge held that the "information relating to a transaction" referred to in integer (d) included, but was not limited to, payment information. There is no challenge by Sycurio to that conclusion.

The issue on construction

69. The issue raised by the appeal concerns the correct construction of integer (f). Sycurio contends that integer (f) requires the request to be sent directly to the external entity without entering the call centre's data processing environment. PCI-PAL dispute this.

The judge's reasoning

70. The judge rejected Sycurio's construction for the following reasons:

> "109. There is no doubt that integers 9(c)–(f) describe the blocking of the sensitive data signals from the second telephone interface, and the transmission to an external entity of a request based on those data signals. That does not, however, mean that the claim is limited to a method which sends the relevant data signals *directly* to the external entity without passing through any of the other components of the call centre telephony system. Nothing in claim 9 indicates that the method described is so limited. Integer 9(f), in particular, says nothing about the format in which the data is sent or whether it has undergone any processing to get it into an appropriate format for onwards transmission.
>
> 110. Nor is there any basis for reading into claim 9 such a limitation. Mr Silverleaf referred to Figures 11 and 12 of the Patent specification, which are examples of embodiments where the sensitive data are not sent into the call centre. As explained … above, that is one possible arrangement described in the specification, but it is not described as being the only one. On the contrary, … Figures 14(a)–(c) and 15 all provide examples of embodiments of the Patent where the sensitive data are processed within the call centre (albeit that they are not

> accessible to the agent) before being sent to the external entity. These examples are described in the specification as illustrating the second alternative arrangement described … above, the benefit of those examples being that they show ways in which the call processor can be integrated into existing call centre systems for handling transactions. The 'overview' part of the specification also notes that the call processor may be configured so as to be integrated directly with the existing call centre transaction handling applications ….
>
> 111. Mr Silverleaf's response was to contend that although the embodiments illustrated by Figures 14(a)–(c) and 15 are included in the Patent specification, the claims of the Patent abandoned those options because the claims only covered embodiments where the call processing system was outside the boundary of the call centre environment.
>
> 112. There are two problems with that submission. The first is that there is nothing in the Patent to suggest that the claims only cover the situation where the call processor or call processing system lies outside the boundary of the call centre environment, to the exclusion of the arrangements illustrated by (for example) Figures 2 and 5 ….
>
> 113. Secondly, as I have explained above, Mr Silverleaf's contention rested on a misunderstanding of what is described in Figures 14(a)–(c) and 15. Those figures all show arrangements where the call processor is indeed located outside the boundaries of the call centre environment. But they are expressly described as illustrating ways in which the call processor (wherever it is located) can be integrated into existing call centre transaction handling systems. Figure 14(a), for example, shows the sensitive data being sent to an application server within the call centre, bypassing the agent, before being relayed by the application server to the external entity. This is quite clearly an arrangement contemplated as being within the claims of the Patent: it is expressly described in the 'overview' section of the specification, and nothing in the claims of the Patent excludes this arrangement."

The appeal

71. Counsel for Sycurio submitted that the judge's reasoning, in particular at [113], involved a misunderstanding of his argument, which was based on a functional distinction and not a physical one. Although counsel for PCI-PAL disputed this, I am prepared to assume that the judge did not fully understand the argument. What matters, however, is whether the judge arrived at the right answer. I have no doubt that she did. My reasons are as follows.

72. First, standing back from the detail of the Patent, it seems to me that the skilled team would note that claim 9 is drafted in broad and general terms. The skilled team would

conclude that this was deliberate. The skilled team would also note that the specification discloses a wide variety of possible embodiments of the claimed inventions. The skilled team would conclude that the plethora of dependent claims were intended to capture most, although not necessarily all, of those embodiments. That conclusion would reinforce the conclusion that claim 9 was intended to be of broad scope. (The same goes for claim 1.)

73. Secondly, the skilled team would have no reason to think that the inventors intended positively to exclude any particular embodiments from the scope of the claims. There is no express statement to that effect. Nor is it implicit. Counsel for Sycurio argued that the skilled team would note that, in various places, the specification refers to "the invention" whereas in others it uses the phraseology "also described" or "also provided". This contrast in wording can be seen from the first two paragraphs (quoted in paragraph 31 above), but emerges most clearly from the passage containing the two consistory clauses followed by the "also provided" paragraph (paragraph 33 above). Counsel for Sycurio further argued that the skilled team would conclude that the explanation for this was that the claims had been narrowed in prosecution in order to avoid anticipation by Van Volkenburgh (which is one of five cited documents listed in the cover sheet but is not acknowledged in the specification) and that the specification had been amended to make it clear that certain embodiments no longer fell within the claims as a result.

74. I do not accept this argument. I will assume in Sycurio's favour that the skilled team is deemed to be aware that patent claims are often amended during prosecution in order to distance the claimed invention from cited prior art. Even so, there is no evidence that the skilled team would have any reason to focus on Van Volkenburgh and to ask themselves whether, and if so how, the claims had been amended to avoid it. Nor is there any reason to think that the skilled team would notice the relatively subtle linguistic distinction relied upon by counsel for Sycurio, let alone conclude that it was intended to have the effect contended for. The distinction does not assist Sycurio anyway, as I shall explain.

75. Thirdly, the linchpin of Sycurio's case is that the skilled team would appreciate that claim 9 is intended to include embodiments (such as Figure 12) in which the request is sent directly from the call processor to the external entity without entering the call centre and to exclude embodiments (such as Figures 14(a)-(c)) in which the request is sent via the call centre; and that the judge was wrong to conclude otherwise.

76. I disagree. There is nothing in the specification to support the idea that the claims embrace the first group of embodiments but not the second. The message conveyed by the specification is that both groups are intended to be covered. As noted above, the specification distinguishes at page 13 lines 17-36 (paragraph 43 above) between embodiments in which the transactional information is blocked from transmission to the switch and embodiments in which the transactional information is modified so that it is not ordinarily readable by the agent. The same distinction is drawn at page 14 lines 28-46 (paragraph 44 above), where the latter group is described as a "preferred embodiment" and the former as "an alternative, preferred arrangement". It is fair to say that, at this point in the specification, the distinction between the two groups of embodiments is concerned with what happens in integers (c) and (d) of claim 9, and I do not understand there to be any dispute that the word "blocked" in integer (d) should be interpreted as covering both approaches at that stage of the method.

Nevertheless, these passages make it clear that the invention is intended to cover processing of sensitive information within the call centre as well as processing of such information outside the call centre.

77. Next, there is Figure 2, which is the basic embodiment of the invention disclosed in the specification. This shows the call processor 40 within the call centre 25. As the specification makes clear at page 18 lines 12-24 (paragraph 48 above), the call processor modifies characteristics of the call or signal from the caller 10 and routes data to the external entity 30 such that sensitive information from the caller is barred from reaching the agent 10. It follows that in this embodiment the sensitive information is not merely processed within the call centre, but also transmitted from within the call centre to the external entity as shown by the dashed line.

78. Next, the specification makes it clear that the invention includes both embodiments in which the call processor is inside the call centre (such as Figure 2) and embodiments in which the call processor is outside the call centre (such as Figure 11). This is consistent with the statement at page 18 lines 32-33 (paragraph 48 above) that the call processor can be placed at any point along the network between the caller and the agent. Furthermore, the skilled team would understand from the statements at page 19 lines 26-27 and page 19 line 46 to page 20 line 1 (paragraph 49 above) that the components of the call processor may be distributed and communicate with each other by an IP network that these components may be located in different places. All of these points make it clear that the location of the call processor is unimportant, what matters is its functionality.

79. As for Figures 12 and 14(a)-(c), these are both presented as embodiments of the invention at page 17 lines 29-32 (paragraph 46 above). Furthermore, they are both described without differentiation as "exemplary embodiments" at page 23 lines 16-22 (paragraph 51 above). Still further, the passage at page 23 lines 24-27 (paragraph 52 above) again makes it clear that the invention covers both embodiments in which sensitive information is prevented from reaching the agent and embodiments in which it is prevented from reaching the call centre at all.

80. Finally, the "Overview" section (paragraph 64 above) confirms that embodiments involving both masking the DTMF data and splitting the DTMF channel from the voice channel so that it can be removed from the call centre are intended to be covered.

81. Not only are both Figures 12 and 14(a)-(c) presented as embodiments of the invention, but also it would be very odd if claim 9 were intended to be limited to Figure 12 and to exclude Figures 14(a)-(c). This is because Figure 12 shows verification. As the specification explains at page 17 lines 29-32 (paragraph 46 above), page 25 lines 7-21 (paragraph 53 above) and page 27 lines 23-30 (paragraph 56 above), verification is an additional stage of the process. It is conspicuously not required by claim 9. Although Figures 14(a)-(c) are optional ways of integrating the call processor into existing systems for acquiring payment information and/or handling transactions, there is no such additional stage in the process.

82. Counsel for Sycurio pointed out that the specification explains at page 27 lines 32 to page 29 line 6 (paragraph 56 above) that, when the Figure 12 embodiment is used as a hosted payment gateway, one benefit is that compliance with PCI DSS can be

outsourced, whereas no such claim was made in respect of Figures 14(a)-(c). He argued that this benefit was only obtained if the request was sent directly to the external entity without passing through the call centre. As noted above, however, claim 9 is not limited to payment information. It extends to methods in which there is no need for compliance with PCI DSS at all. Thus this is not a reason for thinking that Figure 12 is covered by the claim, but not Figures 14(a)-(c).

83. Counsel for Sycurio did not attempt to apply his general proposition concerning the "also provided" language in the specification to the specific case of the Figure 14(a)-(c) embodiments, but if one attempts the exercise it soon breaks down. There is no "also provided" language in the description of Figures 14(a)-(c) themselves. On the contrary, as I have explained, both Figure 12 and Figures 14(a)-(c) are presented as embodiments of the invention. The skilled team might notice that at least Figure 14(c) appears to correspond to some extent to what is described as "Also provided" under the heading "**System Integration**" at page 7 lines 21-39 (paragraph 39 above); but if so they would notice as great a degree of correspondence between Figure 12 and what is described as "Also provided" under the heading "**Hosted Payment Gateway**" at page 8 lines 17-37 (paragraph 40 above). In neither case does claim 9 read precisely on to what is described.

84. Fourthly, and most importantly, Sycurio's case finds no support in the language of integer (f). All this integer requires is that the request is transmitted via a data interface to an external entity. That language on its face covers both direct and indirect routes of transmission. This reading is reinforced by the fact the specification explicitly contemplates implementation using IP networks, in which individual packets of data are transmitted by different routes.

85. Furthermore, even if the language was confined to direct transmission, Sycurio would still face the difficulty that integer (f) says nothing about where the request is transmitted from. Claim 9 is a method claim expressed in functional terms. Apart from requiring the presence of means for receiving, processing and transmitting voice and data signals, two telephone interfaces and a data interface, the method does not require the presence of a call processor with any specific features. The method could be implemented entirely in software, although the software would obviously need appropriate hardware to run on. (This no doubt explains why Sycurio claimed that PCI-PAL had infringed claim 9, but not claim 1.) Thus there is nothing to exclude the request from being transmitted from within the call centre. This is consistent with the fact that the specification is clear that the call processor may be located inside or outside the call centre.

86. In addition, the skilled team would appreciate that a call centre is just a building. It is doubtless for this reason that counsel for Sycurio referred variously to the request not being sent from the call centre's "communication environment", "processing environment" and "data processing environment". It was on this basis that he submitted that the Figure 2 embodiment was within claim 9 on Sycurio's construction: even though the figure shows the request being transmitted by call processor 40 located within call centre 25, he claimed that the call processor was outside the call centre's communication/processing/data processing environment. Even leaving aside the objections that (i) all of these expressions are indefinite and (ii) the distinction drawn by counsel for Sycurio is nowhere mentioned in the specification, none of this has any basis in the language of the claim.

Conclusion

87. Since the judge correctly construed claim 9, it follows that the challenge to her assessment of obviousness fails. As she held, the Patent is invalid.

Lord Justice Nugee:

88. I agree.

Lord Justice Singh:

89. I also agree. I would add only a brief response to the suggestion by counsel for Sycurio that the judge did not fully understand his argument: see [71] above. In my view, the judge did understand that argument, in particular that the suggested distinction was a functional one, and not a physical one. In my view, this is apparent from her judgment at [112]-[113] and also from [82]: the judge was using the phrase "boundary of the call centre environment" in a functional sense, not a physical one. As those passages make clear, she appreciated that the crucial purpose of the Patent was to bypass "the agent", not necessarily to bypass the call centre.