

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

WIPO Patent Application Publication No. 2006/087503 (“Waters”) was filed on February 15, 2005, published on August 24, 2006, and therefore qualifies as prior art under at least 35 U.S.C. § 102 as to the asserted claims of U.S. Pat. No. 11,770,756 (“the ’756 Patent”). Waters, including any material incorporated by reference into Waters, anticipates claims 1-18 (“the Asserted Claims”) of the ’756 Patent under 35 U.S.C. § 102. Waters also renders obvious the Asserted Claims under 35 U.S.C. § 103, alone based on the state of the art and/or in combination with one or more references identified in Samsung’s accompanying disclosure for the ’756 Patent.¹

To the extent Plaintiff alleges that the Waters does not disclose any particular limitation of the Asserted Claims of the ’756 Patent, either expressly or inherently, it would have been obvious to a person of ordinary skill in the art as of the priority date of the ’756 Patent to modify the Waters reference and/or to combine the teachings of the Waters reference with other prior art references, including but not limited to the present prior art references found in Exhibit 756-B and the corresponding section(s) of charts for other prior art references for the ’756 Patent in a manner that would have rendered the Asserted Claims invalid as obvious.

With respect to the obviousness of the Asserted Claims under 35 U.S.C. § 103, one or more of the principles enumerated by the United States Supreme Court in *KSR v. Teleflex*, 550 U.S. 398 (2007) apply, including: (a) combining various claimed elements known in the prior art according to known methods to yield a predictable result; and/or (b) making a simple substitution of one or more known elements for another to obtain a predictable result; and/or (c) using a known technique to improve a similar device or method in the same way; and/or (d) applying a known technique to a known device or method ready for improvement to yield a predictable result; and/or (e) choosing from a finite number of identified, predictable solutions with a reasonable expectation of success or, in other words, the solution was one which was “obvious to try”; and/or (f) a known work in one field of endeavor prompting variations of it for use either in the same field or a different field based on given design incentives or other market forces in which the variations were predictable to one of ordinary skill in the art; and/or (g) a teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine the teachings of various prior art references to arrive at the claimed invention. It therefore would have been obvious to one of ordinary skill in the art to combine the disclosures of these references in accordance with the principles and rationales set forth above.

The citations to portions of any reference in this chart are exemplary only. For example, a citation that refers to or discusses a figure or figure item should be understood to also incorporate by reference that figure and any additional descriptions of that figure as if set

¹ Samsung notes that Plaintiff appears in many instances to be pursuing overly broad constructions of various limitations of the asserted claims of the ’756 Patent in an effort to piece together an infringement claim where none exists and to accuse a product that does not practice the claims. This claim chart may take into account Plaintiff’s overly broad constructions of the claim limitations. Any assertion that a particular limitation is disclosed by a prior art reference may be based on Plaintiff’s apparent constructions and is not intended to be, and is not, an admission that such constructions are supportable or proper.

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

forth fully therein. Samsung reserves the right to rely on the entirety of the references cited in this chart to show that the Asserted Claims are invalid. Citations presented for one claim limitation are expressly incorporated by reference into all other limitations for that claim as well as all limitations of all claims on which that claim depends. Samsung also reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in Plaintiff's infringement contentions, and/or information obtained during discovery as the case progresses.

Claim	U.S. Patent No. 11,770,756	Exemplary Disclosure in Waters
[1.1]	A method of operating a device, the method comprising:	To the extent the preamble is limiting, Waters discloses “a method of operating a device, the method comprising:” See e.g.: A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] According to another aspect of the present invention, there is provided a method of controlling use of a near field communication device, including associating smart card means with a mobile telecommunications network for authenticating the smart card means with the network, transmitting to the smart card means from the mobile telecommunications network data for controlling use of the near field communication device and selectively enabling the near field communication device in dependence upon the data. Waters at [Page 03]

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	The times at which, and the circumstances in which, the OTA messages are sent by the mobile telecommunications network 3 to the user's SIM card 15 may be set by the user of the mobile terminal 1. For example, the user of the mobile terminal 1 may initiate a communication session (such as a SIP communication session) with the mobile telecommunications network 1 to configure the times or places in which the RF tag 41 should be enabled. This updating process may require entry of a password, or employ some other security mechanism, to prevent unauthorised persons from reconfiguring the times and/or locations at which the near field tag is rendered operable or inoperable. Alternatively, the user may configure the times and/or locations at which the OTA messages are sent by some other mechanism - for example, by providing verbal instructions to the operator of mobile telecommunications network 3 by a mobile or PSTN telephone call, or by visiting the website of the mobile telecommunications network operator (whether using the mobile terminal or independently thereof using a PC connected to the Internet). Waters at [Page 12] Rather than the user of the mobile terminal 1 determining when/where the RF tag 41 is activated, this may be determined by the mobile telecommunications network 3 or some other entity. For example, a school child's parent may set the times during which the school child is able to use their RF tag to make payments, in the example given above relating to paying for a school lunch. In the example given above relating to payment for public transport, the public transportation authority may alternatively or additionally be able to control when OTA messages are sent so that, if it is notified that the mobile terminal 1 incorporating the near field tag 41 has been stolen, that authority can permanently or temporarily deactivate the near field tag 41. Waters at [Page 12] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[1.2]	sensing by the device, using a device-based sensor, a parameter that is associated with the device, an environment of the device and/or a user of the device;	Waters discloses “sensing by the device, using a device-based sensor, a parameter that is associated with the device, an environment of the device and/or a user of the device;” See e.g.: A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] The apparatus of claim 7, wherein the security data entry means is operable to detect biometric data from a user. Waters at [Claim 11] Biometric data entry - the mobile terminal 1 may incorporate a fingerprint reader 45. The fingerprint reader 45 scans the fingerprint of the user when the user's finger is placed on the reader 45 and compares it to the user's fingerprint stored in the memory of the mobile terminal 1 or the SIM 15. If the fingerprints are determined to match, the message is sent from the SIM 15, via link 43, to the RF tag 41. As an alternative to a fingerprint, other biometric data could be used - for example, voice recognition (using the mobile terminal's built-in microphone and

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		a voice recognition algorithm within the mobile terminal 1 or SIM card 15) or retinal scanning (using the mobile terminal's built-in camera). Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. Waters at [Page 14] Figure 5 shows a smart card 100 with an in-built near field tag including an inductive antenna 200, and a biometric system 120 for reading a finger print. The print is ideally compared to a previously taken print stored in the memory 130 of the smart card 100 or may just be judged as having the characteristics of a non-specific fingerprint. Waters at [Page 21] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[1.3]	determining by the device a value of the parameter that is sensed; and	Waters discloses “determining by the device a value of the parameter that is sensed; and” See e.g.: A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] The apparatus of claim 7, wherein the security data entry means is operable to detect biometric data from a user. Waters at [Claim 11] The following arrangements are useful if the near field tag 41 is to be enabled and disabled for fairly long periods of time: (1) Personal identification number (PIN) entry - the keypad 37 of the mobile terminal 1 is used to enter a PIN (or other secret password) to enable the near field tag 41. The user's PIN may be stored in a secure location in the mobile terminal 1 or in the SIM 15. When the user enters their PIN using the keypad 37, the entered PIN is compared with the stored PIN. If the PINs match, the SIM transmits a message, via link 43, to the near field tag 41 to activate the near field tag. Waters at [Page 14] (2) Biometric data entry - the mobile terminal 1 may incorporate a fingerprint reader 45. The fingerprint reader 45 scans the fingerprint of the user when the user's finger is placed on the reader 45 and compares it to the user's fingerprint stored in the memory of the mobile terminal 1 or the SIM 15. If the fingerprints are determined to match, the message is sent from the SIM 15, via link 43, to the
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	RF tag 41. As an alternative to a fingerprint, other biometric data could be used - for example, voice recognition (using the mobile terminal's built-in microphone and a voice recognition algorithm within the mobile terminal 1 or SIM card 15) or retinal scanning (using the mobile terminal's built-in camera). Waters at [Page 14] Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 14] Figure 5 shows a smart card 100 with an in-built near field tag including an inductive antenna 200, and a biometric system 120 for reading a finger print. The print is ideally compared to a previously taken print stored in the memory 130 of the smart card 100 or may just be judged as having the characteristics of a non-specific fingerprint. Waters at [Page 21] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

[1.4]	responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device and disabling by the device a function of the device;	Waters discloses “responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device and disabling by the device a function of the device;” See e.g.: A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] The near field tag 41 may operate in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards. The tag 41 includes an inbuilt inductive antenna that allows the card to exchange information with a tag reader when the two are brought into close proximity, as described above. The reader may emit an RF signal to supply power to the tag to communicate with it if the tag is "passive". If the tag is "active" it will have a power supply and its operation is independently of the reader. The near field tag 41 may transmit selected information, such as an ID number (GU ID). Waters at [Page 09] In order to improve the security of the near field tag, in the present embodiment it is proposed to use the SIM 15 of mobile terminal 1 to control to some extent the operation of the near field tag 41. The authentication process of a SIM 15 with a
--------------	---	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	mobile telecommunications network, using the network's authentication processor 17 is considered to be highly secure. In this embodiment, this authentication of the SIM 15 is used to protect data held by the memory of the near field tag 41 from unauthorised access. Waters at [Page 09] Conveniently, the SIM 15 is provided with data which controls operation of the near field tag 41 by receiving an OTA message, which is sent to the mobile terminal 1 from the mobile telecommunications network 3 (via the OTA gateway 30 and SMSC 32). As described above, the OTA update message is received by the mobile terminal 1 and it is determined that this is an updating OTA update message rather than a conventional SMS message. The message is then passed to the SIM 15 for processing. Upon processing of the message, commands contained within that message are executed, causing the desired control of the RF tag 41 via the link 43. Waters at [Page 10] In a first example, it is desired to only enable the near field tag 41 to communicate with the reader when it is in the vicinity of the user's office (where entry is obtained using the near field tag 41). The SMSC 32 may send an OTA update message to the node B 5 associated with the cell or group of cells in which the user's office is located. When the mobile terminal 1 enters a cell in the group, the node B transmits the OTA message to the mobile terminal 1. The procedure described above is applied, and the OTA message is passed to the SIM 15 and the instructions therein are processed. A command is sent to the near field tag 41 via link 43 to activate the near field tag (for example, by allowing its antenna to communicate with the reader). When the mobile terminal 1 moves to a different cell, a command is sent from the SIM 15, via the link 43, to disable the near field tag 41. This command may be issued in response to a further OTA message being received from the network 3 when the mobile terminal 1 moves to a different cell, or movement to a different cell may be detected automatically by the SIM (or the mobile terminal 1) and used to generate an appropriate command for sending to the near field tag 41.
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	Waters at [Page 10] In the second example, a user wishes to use the near field tag 41 of the mobile terminal 1 to pay for travel by public transport (for example on the London Underground), where entry barriers are equipped with a suitable near field tag reader. Because the commuter travels at particular, consistent times of day, it is desirable to enable the near field tag 41 only at those times, in order to provide improved security. When so configured, if the mobile terminal 1 incorporating the near field tag 41 were stolen, the thief would not be able to pay for use of public transport using the near field tag 41 outside the times specified. Waters at [Page 11] The mobile telecommunications network 3 is configured to transmit an OTA message to the mobile terminal 1 at the beginning of the time period during which the commuter begins their normal journey. As before, this message is received and interpreted by the SIM, which sends an instruction to enable the near field tag 41 via the link 43. The near field tag 41 is then able to communicate with readers to allow use of public transport. At the end of the time period during which the commuter completes their usual journey, a second OTA message is sent by the network 3 to the mobile terminal 1. This OTA message is received and interpreted by the SIM 15, and sends an appropriate deactivation instruction to the RF tag 41 via the link 43. The near field tag 41 is thereafter not able to allow the user to obtain access to public transport. Waters at [Page 11] A similar arrangement could be used, for example, to enable a school child to pay for their lunch using the near field tag 41. OTA messages would be sent at the beginning and the end of the school lunch time so that the near field tag 41 could only be used to make a payment during the appropriate time. Waters at [Page 11] The times at which, and the circumstances in which, the OTA messages are sent by the mobile telecommunications network 3 to the user's SIM card 15 may be
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	set by the user of the mobile terminal 1. For example, the user of the mobile terminal 1 may initiate a communication session (such as a SIP communication session) with the mobile telecommunications network 1 to configure the times or places in which the RF tag 41 should be enabled. This updating process may require entry of a password, or employ some other security mechanism, to prevent unauthorised persons from reconfiguring the times and/or locations at which the near field tag is rendered operable or inoperable. Alternatively, the user may configure the times and/or locations at which the OTA messages are sent by some other mechanism - for example, by providing verbal instructions to the operator of mobile telecommunications network 3 by a mobile or PSTN telephone call, or by visiting the website of the mobile telecommunications network operator (whether using the mobile terminal or independently thereof using a PC connected to the Internet). Waters at [Page 12] The following arrangements are useful if the near field tag 41 is to be enabled and disabled for fairly long periods of time: (1) Personal identification number (PIN) entry - the keypad 37 of the mobile terminal 1 is used to enter a PIN (or other secret password) to enable the near field tag 41. The user's PIN may be stored in a secure location in the mobile terminal 1 or in the SIM 15. When the user enters their PIN using the keypad 37, the entered PIN is compared with the stored PIN. If the PINs match, the SIM transmits a message, via link 43, to the near field tag 41 to activate the near field tag. Waters at [Page 14] (2) Biometric data entry - the mobile terminal 1 may incorporate a fingerprint reader 45. The fingerprint reader 45 scans the fingerprint of the user when the user's finger is placed on the reader 45 and compares it to the user's fingerprint stored in the memory of the mobile terminal 1 or the SIM 15. If the fingerprints are determined to match, the message is sent from the SIM 15, via link 43, to the RF tag 41. As an alternative to a fingerprint, other biometric data could be used - for example, voice recognition (using the mobile terminal's built-in microphone
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		and a voice recognition algorithm within the mobile terminal 1 or SIM card 15) or retinal scanning (using the mobile terminal's built-in camera). Waters at [Page 14] Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 14] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[1.5]	wherein the parameter that is sensed using the device-based sensor, comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and	Waters discloses “wherein the parameter that is sensed using the device-based sensor, comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and” See e.g.: A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network and is authenticated with that network using the SIM (15). The mobile terminal

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	(1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] The near field tag 41 may be selectively enabled and disabled in order to reduce the opportunity to obtain information from the near field tag 41 by an unauthorised reader. Waters at [Page 13] The following arrangements are useful if the near field tag 41 is to be enabled and disabled for fairly long periods of time: Waters at [Page 14] (1) Personal identification number (PESf) entry - the keypad 37 of the mobile terminal 1 is used to enter a PIN (or other secret password) to enable the near field tag 41. The user's PIN may be stored in a secure location in the mobile terminal 1 or in the SIM 15. When the user enters their PIN using the keypad 37, the entered PIN is compared with the stored PIN. If the PINs match, the SIM transmits a message, via link 43, to the near field tag 41 to activate the near field tag. Waters at [Page 14] (2) Biometric data entry - the mobile terminal 1 may incorporate a fingerprint reader 45. The fingerprint reader 45 scans the fingerprint of the user when the user's finger is placed on the reader 45 and compares it to the user's fingerprint
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	stored in the memory of the mobile terminal 1 or the SIM 15. If the fingerprints are determined to match, the message is sent from the SIM 15, via link 43, to the RF tag 41. As an alternative to a fingerprint, other biometric data could be used - for example, voice recognition (using the mobile terminal's built-in microphone and a voice recognition algorithm within the mobile terminal 1 or SIM card 15) or retinal scanning (using the mobile terminal's built-in camera). Waters at [Page 14] Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 14] Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 15]
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		(1) Light sensor - for example a photodiode (a sensor that modifies an electric current when exposed to a light source) could be built into the casing of the mobile terminal 1 and act as a switch to activate or deactivate the RF tag 41. The RF tag 41 is controlled by the photo diode so that the RF tag 41 is only enabled when the mobile terminal 1 is exposed to light. Therefore, when the mobile terminal 1 was in an opaque case or the user's pocket, the RF tag 41 will be disabled. The photodiode may be sensitive to a particular frequency range - for example visible light, infra red or ultra violet. The tag reader may be provided with a light emitter that emits light at this frequency, in order to activate the tag. Waters at [Page 15] (2) Pressure sensor - a pressure sensor on the casing of mobile terminal 1 acts as a switch. The RF tag 41 is only enabled when the user physically presses the pressure sensor. Therefore, when the mobile terminal is in a case or the user's pocket, the pressure sensor is disabled. The pressure sensor may itself be deactivated by the user, for example, when a function of the mobile terminal 1 is selected such that the keypad 37 is inoperative. The pressure sensor may be combined with the fingerprint scanner 45. The combined sensor detects, not only that pressure is applied, but also that an authorised person is pressing the sensor. Alternatively, the pressure sensor could be combined with an electrical resistance meter and used to detect that it is a human hand pressing the pressure sensor, rather than some other object. Waters at [Page 15] (3) Heat sensors - such sensors incorporated in an appropriate position on the casing of the mobile terminal 1 could be configured to detect that the mobile terminal is in a user's hand by detecting the heat from the hand, and only enabling the near field tag 41 when heat from the hand is so detected. Waters at [Page 15] (4) Skin resistance sensor - a skin resistance sensor may be provided on the casing of the mobile terminal 1 in dependence of the presence of the pressure sensor described above. The near field tag 41 will only be operated when an
--	--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	appropriate resistance, capacitance or inductance is detected, indicating that the user's hand is touching the sensor. Waters at [Page 15] (5) Inertial sensors. An inertial sensor incorporated in the mobile terminal can be used to detect that the user is moving the terminal (and tag 41) around at a sufficient speed to indicate that it is to be used. Inertial sensors may be based on micro-accelerators, which are commonly used in motion detectors - for example in gaming and virtual reality/remote control systems. Waters at [Page 15] A mobile terminal 1 may have any of the above arrangements implemented in any combination. For example, a manual entry system and an automatic entry system may be provided, respectively, to enable the card for short and long periods of use. Alternatively, the arrangements may work in parallel, and the near field tag 41 would be enabled only if the light sensor was activated and the correct PIN was entered (for example). Further, the arrangements may work in series - for example, the near field tag 41 would be enabled if the light sensor was activated and the correct PIN was subsequently entered. Waters at [Page 17] The housing 52 may further optionally provide a display 58 for prompting the user to enter their PIN number and/or for displaying the PIN number as it is entered, if desired. On entry of the PIN number using the push buttons 56, the entered PIN number is compared to the PIN number stored on the SIM. If the PINs are found to match, communication between the SIM and the PC is permitted to authenticate one or more transactions. The comparison between the entered PIN number and the PIN number stored on the SIM 15 is performed within the dongle 50, and neither the entered PIN number nor the PIN number stored on the SIM is communicated to the PC. This prevents or reduces the likelihood that the PINs will become compromised by disclosure to an authorised party. Waters at [Page 18]
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		Figure 5 shows a smart card 100 with an in-built near field tag including an inductive antenna 200, and a biometric system 120 for reading a finger print. The print is ideally compared to a previously taken print stored in the memory 130 of the smart card 100 or may just be judged as having the characteristics of a non-specific fingerprint. Waters at [Page 20] The apparatus of claim 7, 8 or 9, wherein the security data comprises a Personal Identification Number (PIN) and the apparatus includes means for comparing the PIN obtained by the security data entry means with a PIN stored on the apparatus and only enables operation of the near field device when the respective PINs match. [Claim 10] The apparatus of claim 7, wherein the security data entry means is operable to detect biometric data from a user. [Claim 11]
--	--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

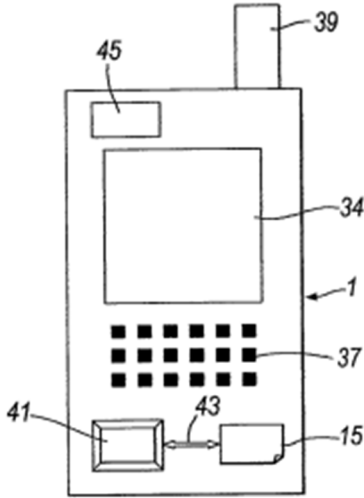
		 Fig.2 [Fig.2] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[1.6]	wherein the device comprises a smartphone.	Waters discloses “wherein the device comprises a smartphone.” See e.g.: As shown in Figure 2, mobile terminal 1 in accordance with the embodiment includes, in addition to SIM 15, a display 34, keypad 37 and an antenna 39 for

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	communicating wirelessly with the mobile communications network 3. Further, the mobile terminal 1 includes a near field or RFID tag 41. The near field tag 41 operates in the unregulated RF band of 13.56 MHz in this embodiment although other frequencies could be used. No licences are required for the use of the near field devices in this RF band. However, each country imposes certain limitations on the electromagnetic emissions in this RF band. Limitations mean that in practice the distance at which the near field tag 41 can communicate with another device is typically less than 20 centimeters. Often the range of communication is such that the RF tag 41 must touch or almost touch the device with which it is to communicate. Communication may be using the Near Field Communication Interface and Protocol (NFCIP-I). Waters at [Page 08] The near field tag 41 may operate in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards. The tag 41 includes an inbuilt inductive antenna that allows the card to exchange information with a tag reader when the two are brought into close proximity, as described above. The reader may emit an RF signal to supply power to the tag to communicate with it if the tag is "passive". If the tag is "active" it will have a power supply and its operation is independently of the reader. The near field tag 41 may transmit selected information, such as an ID number (GU ID). Waters at [Page 09] In order to improve the security of the near field tag, in the present embodiment it is proposed to use the SIM 15 of mobile terminal 1 to control to some extent the operation of the near field tag 41. The authentication process of a SIM 15 with a mobile telecommunications network, using the network's authentication processor 17 is considered to be highly secure. In this embodiment, this
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	authentication of the SIM 15 is used to protect data held by the memory of the near field tag 41 from unauthorized access. Waters at [Page 09] According to an important feature of this embodiment, the near field tag 41 is selectively enabled or disabled for communication with the reader under control of the SIM 15, by means of communication link 43. By means of the link 43, the SIM can enable or disable the near field tag 41 by, for example, rendering its antenna inoperative. In the disabled state, a reader is not able to obtain any information from the near field tag 41, even when brought into close proximity thereto (within a range that, in normal circumstances, near field communication would be possible). Waters at [Page 09] In the second example, a user wishes to use the near field tag 41 of the mobile terminal 1 to pay for travel by public transport (for example on the London Underground), where entry barriers are equipped with a suitable near field tag reader. Because the commuter travels at particular, consistent times of day, it is desirable to enable the near field tag 41 only at those times, in order to provide improved security. When so configured, if the mobile terminal 1 incorporating the near field tag 41 were stolen, the thief would not be able to pay for use of public transport using the near field tag 41 outside the times specified. Waters at [Page 11] The mobile telecommunications network 3 is configured to transmit an OTA message to the mobile terminal 1 at the beginning of the time period during which the commuter begins their normal journey. As before, this message is received and interpreted by the SIM, which sends an instruction to enable the
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

near field tag 41 via the link 43. The near field tag 41 is then able to communicate with readers to allow use of public transport. At the end of the time period during which the commuter completes their usual journey, a second OTA message is sent by the network 3 to the mobile terminal 1. This OTA message is received and interpreted by the SIM 15, and sends an appropriate deactivation instruction to the RF tag 41 via the link 43. The near field tag 41 is thereafter not able to allow the user to obtain access to public transport.

Waters at [Page 11]

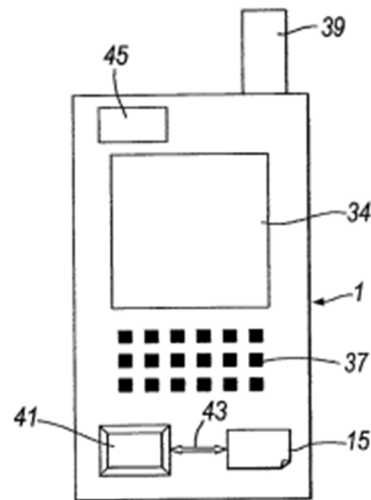


Fig.2

[Fig.2]

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[2.1]	The method of claim 1, wherein said enabling by the device a number of functions of the device comprises enabling by the device a number of functions of the device that is greater than or equal to one.	Waters discloses “The method of claim 1, wherein said enabling by the device a number of functions of the device comprises enabling by the device a number of functions of the device that is greater than or equal to one.” See e.g.: Claim 1, supra. Conveniently, the SIM 15 is provided with data which controls operation of the near field tag 41 by receiving an OTA message, which is sent to the mobile terminal 1 from the mobile telecommunications network 3 (via the OTA gateway 30 and SMSC 32). As described above, the OTA update message is received by the mobile terminal 1 and it is determined that this is an updating OTA update message rather than a conventional SMS message. The message is then passed to the SIM 15 for processing. Upon processing of the message, commands contained within that message are executed, causing the desired control of the RF tag 41 via the link 43. Waters at [Page 10] In a first example, it is desired to only enable the near field tag 41 to communicate with the reader when it is in the vicinity of the user's office (where entry is obtained using the near field tag 41). The SMSC 32 may send an OTA update message to the node B 5 associated with the cell or group of cells in which the user's office is located. When the mobile terminal 1 enters a cell in the group, the node B transmits the OTA message to the mobile terminal 1. The procedure described above is applied, and the OTA message is passed to the SIM 15 and the instructions therein are processed. A command is sent to the near field tag 41 via link 43 to activate the near field tag (for example, by allowing its antenna to

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	communicate with the reader). When the mobile terminal 1 moves to a different cell, a command is sent from the SIM 15, via the link 43, to disable the near field tag 41. This command may be issued in response to a further OTA message being received from the network 3 when the mobile terminal 1 moves to a different cell, or movement to a different cell may be detected automatically by the SIM (or the mobile terminal 1) and used to generate an appropriate command for sending to the near field tag 41. Waters at [Page 10] In the second example, a user wishes to use the near field tag 41 of the mobile terminal 1 to pay for travel by public transport (for example on the London Underground), where entry barriers are equipped with a suitable near field tag reader. Because the commuter travels at particular, consistent times of day, it is desirable to enable the near field tag 41 only at those times, in order to provide improved security. When so configured, if the mobile terminal 1 incorporating the near field tag 41 were stolen, the thief would not be able to pay for use of public transport using the near field tag 41 outside the times specified. Waters at [Page 11] The mobile telecommunications network 3 is configured to transmit an OTA message to the mobile terminal 1 at the beginning of the time period during which the commuter begins their normal journey. As before, this message is received and interpreted by the SIM, which sends an instruction to enable the near field tag 41 via the link 43. The near field tag 41 is then able to communicate with readers to allow use of public transport. At the end of the time period during which the commuter completes their usual journey, a second OTA message is sent by the network 3 to the mobile terminal 1. This OTA message is received and interpreted by the SIM 15, and sends an appropriate deactivation instruction to the RF tag 41 via the link 43. The near field tag 41 is thereafter not able to allow the user to obtain access to public transport. Waters at [Page 11]
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	A similar arrangement could be used, for example, to enable a school child to pay for their lunch using the near field tag 41. OTA messages would be sent at the beginning and the end of the school lunch time so that the near field tag 41 could only be used to make a payment during the appropriate time. Waters at [Page 11] The times at which, and the circumstances in which, the OTA messages are sent by the mobile telecommunications network 3 to the user's SIM card 15 may be set by the user of the mobile terminal 1. For example, the user of the mobile terminal 1 may initiate a communication session (such as a SIP communication session) with the mobile telecommunications network 1 to configure the times or places in which the RF tag 41 should be enabled. This updating process may require entry of a password, or employ some other security mechanism, to prevent unauthorised persons from reconfiguring the times and/or locations at which the near field tag is rendered operable or inoperable. Alternatively, the user may configure the times and/or locations at which the OTA messages are sent by some other mechanism - for example, by providing verbal instructions to the operator of mobile telecommunications network 3 by a mobile or PSTN telephone call, or by visiting the website of the mobile telecommunications network operator (whether using the mobile terminal or independently thereof using a PC connected to the Internet). Waters at [Page 12] The following arrangements are useful if the near field tag 41 is to be enabled and disabled for fairly long periods of time: (1) Personal identification number (PIN) entry - the keypad 37 of the mobile terminal 1 is used to enter a PIN (or other secret password) to enable the near field tag 41. The user's PIN may be stored in a secure location in the mobile terminal 1 or in the SIM 15. When the user enters their PIN using the keypad 37, the entered PIN is compared with the stored PIN. If the PINs match, the SIM transmits a message, via link 43, to the near field tag 41 to activate the near field tag.
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	Waters at [Page 14] (2) Biometric data entry - the mobile terminal 1 may incorporate a fingerprint reader 45. The fingerprint reader 45 scans the fingerprint of the user when the user's finger is placed on the reader 45 and compares it to the user's fingerprint stored in the memory of the mobile terminal 1 or the SIM 15. If the fingerprints are determined to match, the message is sent from the SIM 15, via link 43, to the RF tag 41. As an alternative to a fingerprint, other biometric data could be used - for example, voice recognition (using the mobile terminal's built-in microphone and a voice recognition algorithm within the mobile terminal 1 or SIM card 15) or retinal scanning (using the mobile terminal's built-in camera). Waters at [Page 14] Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 14] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

[3.1]	The method of claim 1, further comprising:	To the extent the preamble is limiting, Waters discloses “The method of claim 1, further comprising:” See e.g.: Claim 1, <i>supra</i>.
[3.2]	while said number of functions is enabled by having sensed by the device the parameter and by having determined by the device that the value of the parameter that is sensed satisfies the threshold criterion, requesting by the device from a second device an authorization to enable a function for conducting a financial transaction by the device;	Waters discloses “while said number of functions is enabled by having sensed by the device the parameter and by having determined by the device that the value of the parameter that is sensed satisfies the threshold criterion, requesting by the device from a second device an authorization to enable a function for conducting a financial transaction by the device;” See e.g.: A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] According to a first aspect of the present invention, there is provided apparatus for controlling use of a near field communication device, including smart card means associable with a mobile telecommunications network for authenticating the smart card means with the network, wherein the smart card means is operable to receive from the mobile telecommunications network data for controlling use of the near field communication device and is operable to selectively enable the near field communication device in dependence upon the data.

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	Waters at [Page 02] Each of the mobile terminals 1,11 and 13 is provided with a respective smart card or subscriber identity module (SIM) 15. During the manufacturing process of each SIM, authentication information is stored thereon under the control of the mobile telecommunications network 3. The mobile telecommunications network 3 itself stores details of each of the SIMs issued under its control. In operation of the mobile telecommunications network 3, a terminal 1, 11, 13 is authenticated (for example, when the user activates the terminal in the network with a view to making or receiving calls) by the network sending a challenge to the terminal 1,11,13 incorporating a SIM 15, in response to which the SIM 15 calculates a reply (dependent on the predetermined information held on the SIM - typically an authentication algorithm and a unique key Ki) and transmits it back to the mobile telecommunications network 3. The mobile telecommunications network 3 includes an authentication processor 17 which generates the challenge and which receives the reply from the terminal 1,11,13. Using information pre- stored concerning the content of the relevant SIM 15, the authentication processor calculates the expected value of the reply from the mobile terminal 1,11,13. If the reply received matches the expected calculated reply, the SIM 15 and the associated mobile terminal are considered to be authenticated. It should be understood that such an authentication process can be performed for any terminal provided with a SIM 15 under control of the mobile telecommunications network 3. In the embodiment the terminal communicates wirelessly with the mobile telecommunications network 3 via the network's radio access network, although this is not essential. For example, the terminal may communicate with the network via the fixed telephone network (PSTN), via a UMA "access point" and/or via the Internet. The PC 23 and the PDA 25 may also be provided with a SIM 15 under the control of the network. Waters at [Page 05] As shown in Figure 2, mobile terminal 1 in accordance with the embodiment includes, in addition to SIM 15, a display 34, keypad 37 and an antenna 39 for communicating wirelessly with the mobile communications network 3. Further,
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	the mobile terminal 1 includes a near field or RFID tag 41. The near field tag 41 operates in the unregulated RF band of 13.56 MHz in this embodiment although other frequencies could be used. No licences are required for the use of the near field devices in this RF band. However, each country imposes certain limitations on the electromagnetic emissions in this RF band. Limitations mean that in practice the distance at which the near field tag 41 can communicate with another device is typically less than 20 centimeters. Often the range of communication is such that the RF tag 41 must touch or almost touch the device with which it is to communicate. Communication may be using the Near Field Communication Interface and Protocol (NFCIP-I). Waters at [Page 08] The near field tag 41 may operate in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards. The tag 41 includes an inbuilt inductive antenna that allows the card to exchange information with a tag reader when the two are brought into close proximity, as described above. The reader may emit an RF signal to supply power to the tag to communicate with it if the tag is "passive". If the tag is "active" it will have a power supply and its operation is independently of the reader. The near field tag 41 may transmit selected information, such as an ID number (GU ID). Waters at [Page 09] In order to improve the security of the near field tag, in the present embodiment it is proposed to use the SIM 15 of mobile terminal 1 to control to some extent the operation of the near field tag 41. The authentication process of a SIM 15 with a mobile telecommunications network, using the network's authentication processor 17 is considered to be highly secure. In this embodiment, this authentication of the SIM 15 is used to protect data held by the memory of the near field tag 41 from unauthorised access. Waters at [Page 09] According to an important feature of this embodiment, the near field tag 41 is selectively enabled or disabled for communication with the reader under control
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	of the SIM 15, by means of communication link 43. By means of the link 43, the SIM can enable or disable the near field tag 41 by, for example, rendering its antenna inoperative. In the disabled state, a reader is not able to obtain any information from the near field tag 41, even when brought into close proximity thereto (within a range that, in normal circumstances, near field communication would be possible). Waters at [Page 09] In the second example, a user wishes to use the near field tag 41 of the mobile terminal 1 to pay for travel by public transport (for example on the London Underground), where entry barriers are equipped with a suitable near field tag reader. Because the commuter travels at particular, consistent times of day, it is desirable to enable the near field tag 41 only at those times, in order to provide improved security. When so configured, if the mobile terminal 1 incorporating the near field tag 41 were stolen, the thief would not be able to pay for use of public transport using the near field tag 41 outside the times specified. Waters at [Page 11] The mobile telecommunications network 3 is configured to transmit an OTA message to the mobile terminal 1 at the beginning of the time period during which the commuter begins their normal journey. As before, this message is received and interpreted by the SIM, which sends an instruction to enable the near field tag 41 via the link 43. The near field tag 41 is then able to communicate with readers to allow use of public transport. At the end of the time period during which the commuter completes their usual journey, a second OTA message is sent by the network 3 to the mobile terminal 1. This OTA message is received and interpreted by the SIM 15, and sends an appropriate deactivation instruction to the RF tag 41 via the link 43. The near field tag 41 is thereafter not able to allow the user to obtain access to public transport. Waters at [Page 11] A similar arrangement could be used, for example, to enable a school child to pay for their lunch using the near field tag 41. OTA messages would be sent at the
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	beginning and the end of the school lunch time so that the near field tag 41 could only be used to make a payment during the appropriate time. Waters at [Page 11] The times at which, and the circumstances in which, the OTA messages are sent by the mobile telecommunications network 3 to the user's SIM card 15 may be set by the user of the mobile terminal 1. For example, the user of the mobile terminal 1 may initiate a communication session (such as a SIP communication session) with the mobile telecommunications network 1 to configure the times or places in which the RF tag 41 should be enabled. This updating process may require entry of a password, or employ some other security mechanism, to prevent unauthorised persons from reconfiguring the times and/or locations at which the near field tag is rendered operable or inoperable. Alternatively, the user may configure the times and/or locations at which the OTA messages are sent by some other mechanism - for example, by providing verbal instructions to the operator of mobile telecommunications network 3 by a mobile or PSTN telephone call, or by visiting the website of the mobile telecommunications network operator (whether using the mobile terminal or independently thereof using a PC connected to the Internet). Waters at [Page 12] Rather than the user of the mobile terminal 1 determining when/where the RF tag 41 is activated, this may be determined by the mobile telecommunications network 3 or some other entity. For example, a school child's parent may set the times during which the school child is able to use their RF tag to make payments, in the example given above relating to paying for a school lunch. In the example given above relating to payment for public transport, the public transportation authority may alternatively or additionally be able to control when OTA messages are sent so that, if it is notified that the mobile terminal 1 incorporating the near field tag 41 has been stolen, that authority can permanently or temporarily deactivate the near field tag 41. Waters at [Page 12]
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	In an alternative embodiment, the SIM 15 activates and deactivates the tag in dependence upon whether the SIM is authenticated with the mobile Waters at [Page 12] In another embodiment of the invention, the mobile terminal and/or near field tag 41 is provided with means for disabling the tag 41 without requiring communication between the mobile terminal 1 and the mobile telecommunications network 3 (and therefore without requiring receipt of an OTA message). Waters at [Page 13] The near field tag 41 may be selectively enabled and disabled in order to reduce the opportunity to obtain information from the near field tag 41 by an unauthorised reader. Waters at [Page 13] The following arrangements are useful if the near field tag 41 is to be enabled and disabled for fairly long periods of time: Waters at [Page 14] (1) Personal identification number (PESf) entry - the keypad 37 of the mobile terminal 1 is used to enter a PIN (or other secret password) to enable the near field tag 41. The user's PIN may be stored in a secure location in the mobile terminal 1 or in the SIM 15. When the user enters their PIN using the keypad 37, the entered PIN is compared with the stored PIN. If the PINs match, the SIM transmits a message, via link 43, to the near field tag 41 to activate the near field tag. Waters at [Page 14] (2) Biometric data entry - the mobile terminal 1 may incorporate a fingerprint reader 45. The fingerprint reader 45 scans the fingerprint of the user when the user's finger is placed on the reader 45 and compares it to the user's fingerprint stored in the memory of the mobile terminal 1 or the SIM 15. If the fingerprints
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	are determined to match, the message is sent from the SIM 15, via link 43, to the RF tag 41. As an alternative to a fingerprint, other biometric data could be used - for example, voice recognition (using the mobile terminal's built-in microphone and a voice recognition algorithm within the mobile terminal 1 or SIM card 15) or retinal scanning (using the mobile terminal's built-in camera). Waters at [Page 14] Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 14] A mobile terminal 1 may have any of the above arrangements implemented in any combination. For example, a manual entry system and an automatic entry system may be provided, respectively, to enable the card for short and long periods of use. Alternatively, the arrangements may work in parallel, and the near field tag 41 would be enabled only if the light sensor was activated and the correct PIN was entered (for example). Further, the arrangements may work in series - for example, the near field tag 41 would be enabled if the light sensor was activated and the correct PIN was subsequently entered. Waters at [Page 17] The housing 52 may further optionally provide a display 58 for prompting the user to enter their PIN number and/or for displaying the PIN number as it is entered, if desired. On entry of the PIN number using the push buttons 56, the entered PIN number is compared to the PIN number stored on the SIM. If the
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	PINs are found to match, communication between the SIM and the PC is permitted to authenticate one or more transactions. The comparison between the entered PIN number and the PIN number stored on the SIM 15 is performed within the dongle 50, and neither the entered PIN number nor the PIN number stored on the SIM is communicated to the PC. This prevents or reduces the likelihood that the PINs will become compromised by disclosure to an authorised party. Waters at [Page 18] Figure 5 shows a smart card 100 with an in-built near field tag including an inductive antenna 200, and a biometric system 120 for reading a finger print. The print is ideally compared to a previously taken print stored in the memory 130 of the smart card 100 or may just be judged as having the characteristics of a non-specific fingerprint. Waters at [Page 20] Apparatus for controlling use of a near field communication device, including smart card means associable with a mobile telecommunications network for authenticating the smart card means with the network, wherein the smart card means is operable to receive from the mobile telecommunications network data for controlling use of the near field communication device and is operable to selectively enable the near field communication device in dependence upon the data. [Claim 1] 2. The apparatus of claim 1, wherein the smart card means is operable to selectively enable the near field communication device by selectively enabling the near field communication device to be read by a reader [Claim 2] The apparatus of claim 7, 8 or 9, wherein the security data comprises a Personal Identification Number (PIN) and the apparatus includes means for comparing the PIN obtained by the security data entry means with a PIN stored on the apparatus
--	---

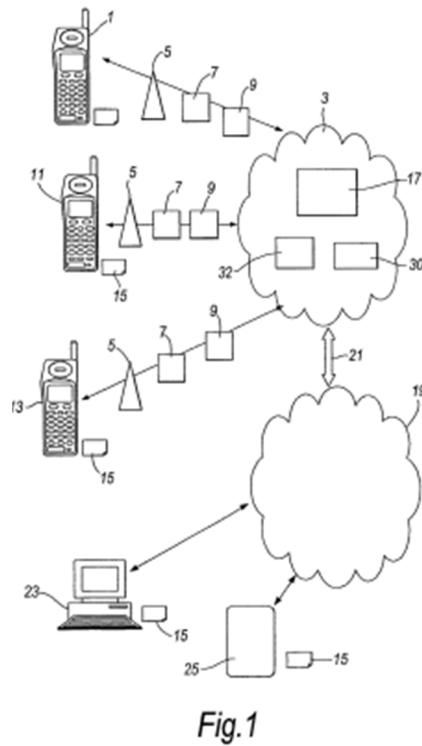
Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

and only enables operation of the near field device when the respective PINs match.

[Claim 10]

The apparatus of claim 7, wherein the security data entry means is operable to detect biometric data from a user.

[Claim 11]



[Fig.1]

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[3.3]	responsive to the requesting, receiving by the device from the second device the authorization to enable the function for conducting the financial transaction; and	Waters discloses “responsive to the requesting, receiving by the device from the second device the authorization to enable the function for conducting the financial transaction; and” See e.g.: A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] Conveniently, the SIM 15 is provided with data which controls operation of the near field tag 41 by receiving an OTA message, which is sent to the mobile terminal 1 from the mobile telecommunications network 3 (via the OTA gateway 30 and SMSC 32). As described above, the OTA update message is received by the mobile terminal 1 and it is determined that this is an updating OTA update message rather than a conventional SMS message. The message is then passed to the SIM 15 for processing. Upon processing of the message, commands

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		contained within that message are executed, causing the desired control of the RF tag 41 via the link 43. Waters at [Page 10] In a first example, it is desired to only enable the near field tag 41 to communicate with the reader when it is in the vicinity of the user's office (where entry is obtained using the near field tag 41). The SMSC 32 may send an OTA update message to the node B 5 associated with the cell or group of cells in which the user's office is located. When the mobile terminal 1 enters a cell in the group, the node B transmits the OTA message to the mobile terminal 1. The procedure described above is applied, and the OTA message is passed to the SIM 15 and the instructions therein are processed. A command is sent to the near field tag 41 via link 43 to activate the near field tag (for example, by allowing its antenna to communicate with the reader). When the mobile terminal 1 moves to a different cell, a command is sent from the SIM 15, via the link 43, to disable the near field tag 41. This command may be issued in response to a further OTA message being received from the network 3 when the mobile terminal 1 moves to a different cell, or movement to a different cell may be detected automatically by the SIM (or the mobile terminal 1) and used to generate an appropriate command for sending to the near field tag 41. Waters at [Page 10] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[3.4]	responsive to receiving the authorization, enabling at the device	Waters discloses “responsive to receiving the authorization, enabling at the device the function for conducting the financial transaction.” See e.g.:

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	the function for conducting the financial transaction.	A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] Conveniently, the SIM 15 is provided with data which controls operation of the near field tag 41 by receiving an OTA message, which is sent to the mobile terminal 1 from the mobile telecommunications network 3 (via the OTA gateway 30 and SMSC 32). As described above, the OTA update message is received by the mobile terminal 1 and it is determined that this is an updating OTA update message rather than a conventional SMS message. The message is then passed to the SIM 15 for processing. Upon processing of the message, commands contained within that message are executed, causing the desired control of the RF tag 41 via the link 43. Waters at [Page 10] In a first example, it is desired to only enable the near field tag 41 to communicate with the reader when it is in the vicinity of the user's office (where entry is obtained using the near field tag 41). The SMSC 32 may send an OTA update message to the node B 5 associated with the cell or group of cells in which the user's office is located. When the mobile terminal 1 enters a cell in the group, the node B transmits the OTA message to the mobile terminal 1. The procedure described above is applied, and the OTA message is passed to the SIM 15 and the
--	---	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		instructions therein are processed. A command is sent to the near field tag 41 via link 43 to activate the near field tag (for example, by allowing its antenna to communicate with the reader). When the mobile terminal 1 moves to a different cell, a command is sent from the SIM 15, via the link 43, to disable the near field tag 41. This command may be issued in response to a further OTA message being received from the network 3 when the mobile terminal 1 moves to a different cell, or movement to a different cell may be detected automatically by the SIM (or the mobile terminal 1) and used to generate an appropriate command for sending to the near field tag 41. Waters at [Page 10] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[4.1]	The method of claim 3, further comprising:	To the extent the preamble is limiting, Waters discloses “The method of claim 3, further comprising:” See e.g.: Claim 3, <i>supra</i>.
[4.2]	responsive to the device satisfying a proximity condition relative to an entity and responsive to the device sensing the parameter and determining the value that is associated with parameter that is sensed satisfies the threshold criterion, using by the device the function for conducting the financial transaction and conducting	Waters discloses “responsive to the device satisfying a proximity condition relative to an entity and responsive to the device sensing the parameter and determining the value that is associated with parameter that is sensed satisfies the threshold criterion, using by the device the function for conducting the financial transaction and conducting by the device the financial transaction by paying for a product.” See e.g.: A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network and is authenticated with that network using the SIM (15). The mobile terminal

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	by the device the financial transaction by paying for a product.	(1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] As shown in Figure 2, mobile terminal 1 in accordance with the embodiment includes, in addition to SIM 15, a display 34, keypad 37 and an antenna 39 for communicating wirelessly with the mobile communications network 3. Further, the mobile terminal 1 includes a near field or RFID tag 41. The near field tag 41 operates in the unregulated RF band of 13.56 MHz in this embodiment although other frequencies could be used. No licences are required for the use of the near field devices in this RF band. However, each country imposes certain limitations on the electromagnetic emissions in this RF band. Limitations mean that in practice the distance at which the near field tag 41 can communicate with another device is typically less than 20 centimeters. Often the range of communication is such that the RF tag 41 must touch or almost touch the device with which it is to communicate. Communication may be using the Near Field Communication Interface and Protocol (NFCIP-I). Waters at [Page 08] The near field tag 41 may operate in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards. The tag 41 includes an inbuilt inductive antenna that allows the card to exchange information with a tag reader when the two are brought into close proximity, as described above. The reader may emit an RF signal to supply power to the tag to communicate with it if the tag is "passive". If the tag is "active" it will have a power supply and its operation is independently of the
--	---	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	reader. The near field tag 41 may transmit selected information, such as an ID number (GU ID). Waters at [Page 09] In order to improve the security of the near field tag, in the present embodiment it is proposed to use the SIM 15 of mobile terminal 1 to control to some extent the operation of the near field tag 41. The authentication process of a SIM 15 with a mobile telecommunications network, using the network's authentication processor 17 is considered to be highly secure. In this embodiment, this authentication of the SIM 15 is used to protect data held by the memory of the near field tag 41 from unauthorised access. Waters at [Page 09] According to an important feature of this embodiment, the near field tag 41 is selectively enabled or disabled for communication with the reader under control of the SIM 15, by means of communication link 43. By means of the link 43, the SIM can enable or disable the near field tag 41 by, for example, rendering its antenna inoperative. In the disabled state, a reader is not able to obtain any information from the near field tag 41, even when brought into close proximity thereto (within a range that, in normal circumstances, near field communication would be possible). Waters at [Page 09] In the second example, a user wishes to use the near field tag 41 of the mobile terminal 1 to pay for travel by public transport (for example on the London Underground), where entry barriers are equipped with a suitable near field tag reader. Because the commuter travels at particular, consistent times of day, it is desirable to enable the near field tag 41 only at those times, in order to provide improved security. When so configured, if the mobile terminal 1 incorporating the near field tag 41 were stolen, the thief would not be able to pay for use of public transport using the near field tag 41 outside the times specified. Waters at [Page 11]
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	The mobile telecommunications network 3 is configured to transmit an OTA message to the mobile terminal 1 at the beginning of the time period during which the commuter begins their normal journey. As before, this message is received and interpreted by the SIM, which sends an instruction to enable the near field tag 41 via the link 43. The near field tag 41 is then able to communicate with readers to allow use of public transport. At the end of the time period during which the commuter completes their usual journey, a second OTA message is sent by the network 3 to the mobile terminal 1. This OTA message is received and interpreted by the SIM 15, and sends an appropriate deactivation instruction to the RF tag 41 via the link 43. The near field tag 41 is thereafter not able to allow the user to obtain access to public transport. Waters at [Page 11] A similar arrangement could be used, for example, to enable a school child to pay for their lunch using the near field tag 41. OTA messages would be sent at the beginning and the end of the school lunch time so that the near field tag 41 could only be used to make a payment during the appropriate time. Waters at [Page 11] The times at which, and the circumstances in which, the OTA messages are sent by the mobile telecommunications network 3 to the user's SIM card 15 may be set by the user of the mobile terminal 1. For example, the user of the mobile terminal 1 may initiate a communication session (such as a SIP communication session) with the mobile telecommunications network 1 to configure the times or places in which the RF tag 41 should be enabled. This updating process may require entry of a password, or employ some other security mechanism, to prevent unauthorised persons from reconfiguring the times and/or locations at which the near field tag is rendered operable or inoperable. Alternatively, the user may configure the times and/or locations at which the OTA messages are sent by some other mechanism - for example, by providing verbal instructions to the operator of mobile telecommunications network 3 by a mobile or PSTN telephone call, or by visiting the website of the mobile telecommunications
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	network operator (whether using the mobile terminal or independently thereof using a PC connected to the Internet). Waters at [Page 12] Rather than the user of the mobile terminal 1 determining when/where the RF tag 41 is activated, this may be determined by the mobile telecommunications network 3 or some other entity. For example, a school child's parent may set the times during which the school child is able to use their RF tag to make payments, in the example given above relating to paying for a school lunch. In the example given above relating to payment for public transport, the public transportation authority may alternatively or additionally be able to control when OTA messages are sent so that, if it is notified that the mobile terminal 1 incorporating the near field tag 41 has been stolen, that authority can permanently or temporarily deactivate the near field tag 41. Waters at [Page 12] In an alternative embodiment, the SIM 15 activates and deactivates the tag in dependence upon whether the SIM is authenticated with the mobile Waters at [Page 12] In another embodiment of the invention, the mobile terminal and/or near field tag 41 is provided with means for disabling the tag 41 without requiring communication between the mobile terminal 1 and the mobile telecommunications network 3 (and therefore without requiring receipt of an OTA message). Waters at [Page 13] The near field tag 41 may be selectively enabled and disabled in order to reduce the opportunity to obtain information from the near field tag 41 by an unauthorised reader. Waters at [Page 13] The following arrangements are useful if the near field tag 41 is to be enabled and disabled for fairly long periods of time:
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	Waters at [Page 14] (1) Personal identification number (PESf) entry - the keypad 37 of the mobile terminal 1 is used to enter a PIN (or other secret password) to enable the near field tag 41. The user's PIN may be stored in a secure location in the mobile terminal 1 or in the SIM 15. When the user enters their PIN using the keypad 37, the entered PIN is compared with the stored PIN. If the PINs match, the SIM transmits a message, via link 43, to the near field tag 41 to activate the near field tag. Waters at [Page 14] (2) Biometric data entry - the mobile terminal 1 may incorporate a fingerprint reader 45. The fingerprint reader 45 scans the fingerprint of the user when the user's finger is placed on the reader 45 and compares it to the user's fingerprint stored in the memory of the mobile terminal 1 or the SIM 15. If the fingerprints are determined to match, the message is sent from the SIM 15, via link 43, to the RF tag 41. As an alternative to a fingerprint, other biometric data could be used - for example, voice recognition (using the mobile terminal's built-in microphone and a voice recognition algorithm within the mobile terminal 1 or SIM card 15) or retinal scanning (using the mobile terminal's built-in camera). Waters at [Page 14] Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 14]
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 15] (1) Light sensor - for example a photodiode (a sensor that modifies an electric current when exposed to a light source) could be built into the casing of the mobile terminal 1 and act as a switch to activate or deactivate the RF tag 41. The RF tag 41 is controlled by the photo diode so that the RF tag 41 is only enabled when the mobile terminal 1 is exposed to light. Therefore, when the mobile terminal 1 was in an opaque case or the user's pocket, the RF tag 41 will be disabled. The photodiode may be sensitive to a particular frequency range - for example visible light, infra red or ultra violet. The tag reader may be provided with a light emitter that emits light at this frequency, in order to activate the tag. Waters at [Page 15] (2) Pressure sensor - a pressure sensor on the casing of mobile terminal 1 acts as a switch. The RF tag 41 is only enabled when the user physically presses the pressure sensor. Therefore, when the mobile terminal is in a case or the user's pocket, the pressure sensor is disabled. The pressure sensor may itself be deactivated by the user, for example, when a function of the mobile terminal 1 is selected such that the keypad 37 is inoperative. The pressure sensor may be combined with the fingerprint scanner 45. The combined sensor detects, not only that pressure is applied, but also that an authorised person is pressing the sensor. Alternatively, the pressure sensor could be combined with an electrical resistance
--	--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	meter and used to detect that it is a human hand pressing the pressure sensor, rather than some other object. Waters at [Page 15] (3) Heat sensors - such sensors incorporated in an appropriate position on the casing of the mobile terminal 1 could be configured to detect that the mobile terminal is in a user's hand by detecting the heat from the hand, and only enabling the near field tag 41 when heat from the hand is so detected. Waters at [Page 15] (4) Skin resistance sensor - a skin resistance sensor may be provided on the casing of the mobile terminal 1 in dependence of the presence of the pressure sensor described above. The near field tag 41 will only be operated when an appropriate resistance, capacitance or inductance is detected, indicating that the user's hand is touching the sensor. Waters at [Page 15] (5) Inertial sensors. An inertial sensor incorporated in the mobile terminal can be used to detect that the user is moving the terminal (and tag 41) around at a sufficient speed to indicate that it is to be used. Inertial sensors may be based on micro-accelerators, which are commonly used in motion detectors - for example in gaming and virtual reality/remote control systems. Waters at [Page 15] A mobile terminal 1 may have any of the above arrangements implemented in any combination. For example, a manual entry system and an automatic entry system may be provided, respectively, to enable the card for short and long periods of use. Alternatively, the arrangements may work in parallel, and the near field tag 41 would be enabled only if the light sensor was activated and the correct PIN was entered (for example). Further, the arrangements may work in series - for example, the near field tag 41 would be enabled if the light sensor was activated and the correct PIN was subsequently entered. Waters at [Page 17]
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	The housing 52 may further optionally provide a display 58 for prompting the user to enter their PIN number and/or for displaying the PIN number as it is entered, if desired. On entry of the PIN number using the push buttons 56, the entered PIN number is compared to the PIN number stored on the SIM. If the PINs are found to match, communication between the SIM and the PC is permitted to authenticate one or more transactions. The comparison between the entered PIN number and the PIN number stored on the SIM 15 is performed within the dongle 50, and neither the entered PIN number nor the PIN number stored on the SIM is communicated to the PC. This prevents or reduces the likelihood that the PINs will become compromised by disclosure to an authorised party. Waters at [Page 18] Figure 5 shows a smart card 100 with an in-built near field tag including an inductive antenna 200, and a biometric system 120 for reading a finger print. The print is ideally compared to a previously taken print stored in the memory 130 of the smart card 100 or may just be judged as having the characteristics of a non-specific fingerprint. Waters at [Page 20] Apparatus for controlling use of a near field communication device, including smart card means associable with a mobile telecommunications network for authenticating the smart card means with the network, wherein the smart card means is operable to receive from the mobile telecommunications network data for controlling use of the near field communication device and is operable to selectively enable the near field communication device in dependence upon the data. [Claim 1] 2. The apparatus of claim 1, wherein the smart card means is operable to selectively enable the near field communication device by selectively enabling the near field communication device to be read by a reader
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

[Claim 2]

The apparatus of claim 7, 8 or 9, wherein the security data comprises a Personal Identification Number (PIN) and the apparatus includes means for comparing the PIN obtained by the security data entry means with a PIN stored on the apparatus and only enables operation of the near field device when the respective PINs match.

[Claim 10]

The apparatus of claim 7, wherein the security data entry means is operable to detect biometric data from a user.

[Claim 11]

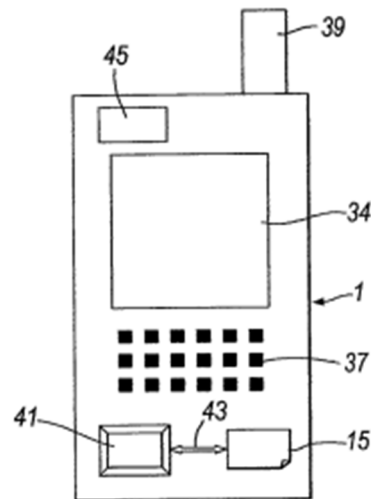


Fig.2

[Fig.2]

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[5.1]	The method of claim 3, further comprising:	To the extent the preamble is limiting, Waters discloses “The method of claim 3, further comprising:” See e.g.: Claim 3, supra.
[5.2]	enabling at the second device a function for conducting the financial transaction.	Waters discloses “enabling at the second device a function for conducting the financial transaction.” See e.g.: Claim 1, supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[6.1]	A device that is configured to perform operations comprising:	Waters discloses “A device that is configured to perform operations comprising:” See e.g.: [1.1], supra. A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] According to another aspect of the present invention, there is provided a method of controlling use of a near field communication device, including associating smart card means with a mobile telecommunications network for authenticating the smart card means with the network, transmitting to the smart card means from the mobile telecommunications network data for controlling use of the near field communication device and selectively enabling the near field communication device in dependence upon the data. Waters at [Page 03] The times at which, and the circumstances in which, the OTA messages are sent by the mobile telecommunications network 3 to the user's SIM card 15 may be set by the user of the mobile terminal 1. For example, the user of the mobile terminal 1 may initiate a communication session (such as a SIP communication session) with the mobile telecommunications network 1 to configure the times or places in which the RF tag 41 should be enabled. This updating process may require entry of a password, or employ some other security mechanism, to
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	prevent unauthorised persons from reconfiguring the times and/or locations at which the near field tag is rendered operable or inoperable. Alternatively, the user may configure the times and/or locations at which the OTA messages are sent by some other mechanism - for example, by providing verbal instructions to the operator of mobile telecommunications network 3 by a mobile or PSTN telephone call, or by visiting the website of the mobile telecommunications network operator (whether using the mobile terminal or independently thereof using a PC connected to the Internet). Waters at [Page 12] Rather than the user of the mobile terminal 1 determining when/where the RF tag 41 is activated, this may be determined by the mobile telecommunications network 3 or some other entity. For example, a school child's parent may set the times during which the school child is able to use their RF tag to make payments, in the example given above relating to paying for a school lunch. In the example given above relating to payment for public transport, the public transportation authority may alternatively or additionally be able to control when OTA messages are sent so that, if it is notified that the mobile terminal 1 incorporating the near field tag 41 has been stolen, that authority can permanently or temporarily deactivate the near field tag 41. Waters at [Page 12] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[6.2]	sensing by the device, using a device-based sensor, a parameter that is associated with the device, an environment of the device and/or a user of the device;	Waters discloses “sensing by the device, using a device-based sensor, a parameter that is associated with the device, an environment of the device and/or a user of the device;” See e.g.: [1.2], supra. A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] The apparatus of claim 7, wherein the security data entry means is operable to detect biometric data from a user. Waters at [Claim 11] Biometric data entry - the mobile terminal 1 may incorporate a fingerprint reader 45. The fingerprint reader 45 scans the fingerprint of the user when the user's finger is placed on the reader 45 and compares it to the user's fingerprint stored in the memory of the mobile terminal 1 or the SIM 15. If the fingerprints are determined to match, the message is sent from the SIM 15, via link 43, to the RF tag 41. As an alternative to a fingerprint, other biometric data could be used - for example, voice recognition (using the mobile terminal's built-in microphone and

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		a voice recognition algorithm within the mobile terminal 1 or SIM card 15) or retinal scanning (using the mobile terminal's built-in camera). Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. Waters at [Page 14] Figure 5 shows a smart card 100 with an in-built near field tag including an inductive antenna 200, and a biometric system 120 for reading a finger print. The print is ideally compared to a previously taken print stored in the memory 130 of the smart card 100 or may just be judged as having the characteristics of a non-specific fingerprint. Waters at [Page 21] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[6.3]	determining by the device a value of the parameter that is sensed; and	Waters discloses “determining by the device a value of the parameter that is sensed; and” See e.g.: [1.3], supra.

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[6.4]	responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device and disabling by the device a function of the device;	Waters discloses “responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device and disabling by the device a function of the device;” See e.g.: [1.4], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[6.5]	wherein the parameter that is sensed using the device-based sensor, comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and	Waters discloses “wherein the parameter that is sensed using the device-based sensor, comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and” See e.g.: [1.5], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[6.6]	wherein the device comprises a smartphone.	Waters discloses “wherein the device comprises a smartphone.” See e.g.: [1.6], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[7.1]	The device of claim 6, wherein said enabling by the device a number of functions of the device comprises enabling by the device a number of functions of the device that is greater than or equal to one.	To the extent the preamble is limiting, Waters discloses “the device of claim 6, wherein said enabling by the device a number of functions of the device comprises enabling by the device a number of functions of the device that is greater than or equal to one.” See e.g.: Claim 6, supra. [2.1], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[8.1]	The device of claim 6, wherein the operations further comprise:	To the extent the preamble is limiting, Waters discloses “the device of claim 6, wherein the operations further comprise:” See e.g.: Claim 6, supra.

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[8.2]	while said number of functions is enabled by having sensed the parameter and by having determined by the device that the value of the parameter that is sensed satisfies the threshold criterion, requesting by the device from a second device an authorization to enable a function for conducting a financial transaction by the device;	Waters discloses “while said number of functions is enabled by having sensed the parameter and by having determined by the device that the value of the parameter that is sensed satisfies the threshold criterion, requesting by the device from a second device an authorization to enable a function for conducting a financial transaction by the device;” See e.g.: [3.2], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[8.3]	responsive to the requesting, receiving from the second device the authorization to enable the function for conducting the financial transaction; and	Waters discloses “responsive to the requesting, receiving from the second device the authorization to enable the function for conducting the financial transaction; and” See e.g.: [3.3], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[8.4]	responsive to receiving the authorization, enabling the function for conducting the financial transaction.	Waters discloses “responsive to receiving the authorization, enabling the function for conducting the financial transaction.” See e.g.: [3.4], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[9.1]	The device of claim 8, wherein the operations further comprise:	To the extent the preamble is limiting, Waters discloses “the device of claim 8, wherein the operations further comprise:” See e.g.: Claim 8, supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[9.2]	detecting by the device that a proximity condition has been satisfied between the device and an entity;	Waters discloses “detecting by the device that a proximity condition has been satisfied between the device and an entity;” See e.g.: [4.2], supra.

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[9.3]	sensing by the device the parameter and determining by the device the value that is associated with the parameter that is sensed satisfies the threshold criterion; and	Waters discloses “sensing by the device the parameter and determining by the device the value that is associated with the parameter that is sensed satisfies the threshold criterion; and” See e.g.: [1.2], [1.3], [1.4], [4.2] supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[9.4]	responsive to the value that is associated with the parameter that is sensed satisfying the threshold criterion, using by the device the function for conducting the financial transaction and conducting by the device the financial transaction by paying for a product.	Waters discloses “responsive to the value that is associated with the parameter that is sensed satisfying the threshold criterion, using by the device the function for conducting the financial transaction and conducting by the device the financial transaction by paying for a product.” See e.g.: [1.4], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[10.1]	The device of claim 8, wherein the operations further comprise:	To the extent the preamble is limiting, Waters discloses “the device of claim 8, wherein the operations further comprise:” See e.g.: Claim 8, <i>supra</i>. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[10.2]	causing a function for conducting the financial transaction to be enabled at the second device.	Waters discloses “causing a function for conducting the financial transaction to be enabled at the second device.” See e.g.: [5.2], <i>supra</i>. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[11.1]	A method of operating a wireless device, the method comprising:	To the extent the preamble is limiting, Waters discloses “a method of operating a wireless device, the method comprising:” See e.g.: [1.1] and [1.6], <i>supra</i>. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[11.2]	sensing by the wireless device, using a sensor of the wireless device, a parameter that is associated with the wireless device, an environment of the wireless device and/or a user of the wireless device;	Waters discloses “sensing by the wireless device, using a sensor of the wireless device, a parameter that is associated with the wireless device, an environment of the wireless device and/or a user of the wireless device;” See e.g.: [1.2], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[11.3]	determining by the wireless device a value of the parameter that is sensed and determining by the wireless device whether or not the value that is sensed satisfies a threshold criterion;	Waters discloses “determining by the wireless device a value of the parameter that is sensed and determining by the wireless device whether or not the value that is sensed satisfies a threshold criterion;” See e.g.: [1.3] and [1.4], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

[11.4]	responsive to the value that is sensed satisfying the threshold criterion, enabling a number of functions of the wireless device and disabling a function of the wireless device;	Waters discloses “responsive to the value that is sensed satisfying the threshold criterion, enabling a number of functions of the wireless device and disabling a function of the wireless device;” See e.g.: [1.4], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[11.5]	requesting by the wireless device from a second device an authorization to enable a function for conducting a financial transaction;	Waters discloses “requesting by the wireless device from a second device an authorization to enable a function for conducting a financial transaction;” See e.g.: [3.2], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[11.6]	responsive to the requesting, receiving by the wireless device from the second device the authorization to enable the function for conducting the financial transaction;	Waters discloses “responsive to the requesting, receiving by the wireless device from the second device the authorization to enable the function for conducting the financial transaction;” See e.g.: [3.3], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[11.7]	responsive to receiving the authorization, enabling at the wireless device the function for conducting the financial transaction; and	Waters discloses “responsive to receiving the authorization, enabling at the wireless device the function for conducting the financial transaction; and” See e.g.: [3.4], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[11.8]	responsive to the wireless device satisfying a proximity condition relative to an entity and responsive to the wireless device sensing the parameter and determining that the value sensed satisfies the threshold criterion, using the function for conducting the financial transaction and conducting the financial transaction by paying for a product;	Waters discloses “responsive to the wireless device satisfying a proximity condition relative to an entity and responsive to the wireless device sensing the parameter and determining that the value sensed satisfies the threshold criterion, using the function for conducting the financial transaction and conducting the financial transaction by paying for a product;” See e.g.: [4.2], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

[11.9]	wherein the parameter that is sensed, using the sensor of the wireless device, comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and	Waters discloses “wherein the parameter that is sensed, using the sensor of the wireless device, comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and” See e.g.: [1.5], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[11.10]	wherein the wireless device comprises a smartphone.	Waters discloses “wherein the wireless device comprises a smartphone.” See e.g.: [1.6], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[12.1]	The method of claim 11, wherein said enabling a number of functions of the wireless device comprises enabling a number of functions of the wireless device that is greater than or equal to one.	To the extent the preamble is limiting, Waters discloses “the method of claim 11, wherein said enabling a number of functions of the wireless device comprises enabling a number of functions of the wireless device that is greater than or equal to one.” See e.g.: Claim 11, supra. 2.1, supra.

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[13.1]	The method of claim 11, further comprising:	To the extent the preamble is limiting, Waters discloses “the method of claim 11, further comprising:” See e.g.: Claim 11, supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[13.2]	enabling at the second device a function for conducting the financial transaction.	Waters discloses “enabling at the second device a function for conducting the financial transaction.” See e.g.: [5.2], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

[14.1]	A wireless device that is configured to perform operations comprising:	To the extent the preamble is limiting, Waters discloses “a wireless device that is configured to perform operations comprising:” See e.g.: [11.1] and [6.1], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[14.2]	using a sensor of the wireless device and sensing a parameter that is associated with the wireless device, an environment of the wireless device and/or a user of the wireless device;	Waters discloses “using a sensor of the wireless device and sensing a parameter that is associated with the wireless device, an environment of the wireless device and/or a user of the wireless device;” See e.g.: [1.2], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[14.3]	determining a value that is associated with the parameter that is sensed and determining whether or not the value satisfies a threshold criterion;	Waters discloses “determining a value that is associated with the parameter that is sensed and determining whether or not the value satisfies a threshold criterion;” See e.g.: [1.3] and [1.4], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[14.4]	responsive to the value satisfying the threshold criterion, enabling a number of functions of the wireless device and disabling a function of the wireless device;	Waters discloses “responsive to the value satisfying the threshold criterion, enabling a number of functions of the wireless device and disabling a function of the wireless device;” See e.g.: [1.4], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[14.5]	requesting from a second device an authorization to enable a function for conducting a financial transaction;	Waters discloses “requesting from a second device an authorization to enable a function for conducting a financial transaction;” See e.g.: [3.2], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[14.6]	responsive to the requesting, receiving from the second device the authorization to enable the	Waters discloses “responsive to the requesting, receiving from the second device the authorization to enable the function for conducting the financial transaction;” See e.g.:

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	function for conducting the financial transaction;	[3.3], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[14.7]	responsive to receiving the authorization, enabling the function for conducting the financial transaction; and	Waters discloses “responsive to receiving the authorization, enabling the function for conducting the financial transaction; and” See e.g.: [3.4], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[14.8]	responsive to the wireless device satisfying a proximity condition relative to an entity and responsive to the wireless device sensing the parameter and determining that the value of the parameter sensed satisfies the threshold criterion, using the function for conducting the financial transaction and conducting the financial transaction by paying for a product;	Waters discloses “responsive to the wireless device satisfying a proximity condition relative to an entity and responsive to the wireless device sensing the parameter and determining that the value of the parameter sensed satisfies the threshold criterion, using the function for conducting the financial transaction and conducting the financial transaction by paying for a product;” See e.g.: [4.2], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[14.9]	wherein the parameter that is sensed comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and	Waters discloses “wherein the parameter that is sensed comprises a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state; and” See e.g.: [1.5], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[14.10]	wherein the wireless device comprises a smartphone.	Waters discloses “wherein the wireless device comprises a smartphone.” See e.g.: [1.6], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[15.1]	The wireless device of claim 14, wherein said enabling a number of functions of the wireless device comprises enabling a number of	Waters discloses “the wireless device of claim 14, wherein said enabling a number of functions of the wireless device comprises enabling a number of functions of the wireless device that is greater than or equal to one.” See e.g.:

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	functions of the wireless device that is greater than or equal to one.	Claim 14, supra. [2.1], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[16.1]	The wireless device of claim 14, wherein the operations further comprise:	To the extent the preamble is limiting, Waters discloses “the wireless device of claim 14, wherein the operations further comprise:” See e.g.: Claim 14, supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[16.2]	causing a function for conducting the financial transaction to be enabled at the second device.	Waters discloses “causing a function for conducting the financial transaction to be enabled at the second device.” See e.g.: [5.2], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[17.1]	The wireless device of claim 14, wherein said conducting the financial transaction by paying for a product comprises:	To the extent the preamble is limiting, Waters discloses “the wireless device of claim 14, wherein said conducting the financial transaction by paying for a product comprises:” See e.g.: Claim 14, supra. A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] As shown in Figure 2, mobile terminal 1 in accordance with the embodiment includes, in addition to SIM 15, a display 34, keypad 37 and an antenna 39 for communicating wirelessly with the mobile communications network 3. Further, the mobile terminal 1 includes a near field or RFID tag 41. The near field tag 41 operates in the unregulated RF band of 13.56 MHz in this embodiment although other frequencies could be used. No licences are required for the use of the near field devices in this RF band. However, each country imposes certain limitations on the electromagnetic emissions in this RF band. Limitations mean that in practice the distance at which the near field tag 41 can communicate with another device is typically less than 20 centimeters. Often the range of communication is such that the RF tag 41 must touch or almost touch the device with which it is to

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	communicate. Communication may be using the Near Field Communication Interface and Protocol (NFCIP-I). Waters at [Page 08] The near field tag 41 may operate in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards. The tag 41 includes an inbuilt inductive antenna that allows the card to exchange information with a tag reader when the two are brought into close proximity, as described above. The reader may emit an RF signal to supply power to the tag to communicate with it if the tag is "passive". If the tag is "active" it will have a power supply and its operation is independently of the reader. The near field tag 41 may transmit selected information, such as an ID number (GU ID). Waters at [Page 09] In order to improve the security of the near field tag, in the present embodiment it is proposed to use the SIM 15 of mobile terminal 1 to control to some extent the operation of the near field tag 41. The authentication process of a SIM 15 with a mobile telecommunications network, using the network's authentication processor 17 is considered to be highly secure. In this embodiment, this authentication of the SIM 15 is used to protect data held by the memory of the near field tag 41 from unauthorised access. Waters at [Page 09] According to an important feature of this embodiment, the near field tag 41 is selectively enabled or disabled for communication with the reader under control of the SIM 15, by means of communication link 43. By means of the link 43, the SIM can enable or disable the near field tag 41 by, for example, rendering its antenna inoperative. In the disabled state, a reader is not able to obtain any information from the near field tag 41, even when brought into close proximity thereto (within a range that, in normal circumstances, near field communication would be possible). Waters at [Page 09]
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	In the second example, a user wishes to use the near field tag 41 of the mobile terminal 1 to pay for travel by public transport (for example on the London Underground), where entry barriers are equipped with a suitable near field tag reader. Because the commuter travels at particular, consistent times of day, it is desirable to enable the near field tag 41 only at those times, in order to provide improved security. When so configured, if the mobile terminal 1 incorporating the near field tag 41 were stolen, the thief would not be able to pay for use of public transport using the near field tag 41 outside the times specified. Waters at [Page 11] The mobile telecommunications network 3 is configured to transmit an OTA message to the mobile terminal 1 at the beginning of the time period during which the commuter begins their normal journey. As before, this message is received and interpreted by the SIM, which sends an instruction to enable the near field tag 41 via the link 43. The near field tag 41 is then able to communicate with readers to allow use of public transport. At the end of the time period during which the commuter completes their usual journey, a second OTA message is sent by the network 3 to the mobile terminal 1. This OTA message is received and interpreted by the SIM 15, and sends an appropriate deactivation instruction to the RF tag 41 via the link 43. The near field tag 41 is thereafter not able to allow the user to obtain access to public transport. Waters at [Page 11] A similar arrangement could be used, for example, to enable a school child to pay for their lunch using the near field tag 41. OTA messages would be sent at the beginning and the end of the school lunch time so that the near field tag 41 could only be used to make a payment during the appropriate time. Waters at [Page 11] The times at which, and the circumstances in which, the OTA messages are sent by the mobile telecommunications network 3 to the user's SIM card 15 may be set by the user of the mobile terminal 1. For example, the user of the mobile terminal 1 may initiate a communication session (such as a SIP communication
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	session) with the mobile telecommunications network 1 to configure the times or places in which the RF tag 41 should be enabled. This updating process may require entry of a password, or employ some other security mechanism, to prevent unauthorised persons from reconfiguring the times and/or locations at which the near field tag is rendered operable or inoperable. Alternatively, the user may configure the times and/or locations at which the OTA messages are sent by some other mechanism - for example, by providing verbal instructions to the operator of mobile telecommunications network 3 by a mobile or PSTN telephone call, or by visiting the website of the mobile telecommunications network operator (whether using the mobile terminal or independently thereof using a PC connected to the Internet). Waters at [Page 12] Rather than the user of the mobile terminal 1 determining when/where the RF tag 41 is activated, this may be determined by the mobile telecommunications network 3 or some other entity. For example, a school child's parent may set the times during which the school child is able to use their RF tag to make payments, in the example given above relating to paying for a school lunch. In the example given above relating to payment for public transport, the public transportation authority may alternatively or additionally be able to control when OTA messages are sent so that, if it is notified that the mobile terminal 1 incorporating the near field tag 41 has been stolen, that authority can permanently or temporarily deactivate the near field tag 41. Waters at [Page 12] In an alternative embodiment, the SIM 15 activates and deactivates the tag in dependence upon whether the SIM is authenticated with the mobile Waters at [Page 12] A mobile terminal 1 may have any of the above arrangements implemented in any combination. For example, a manual entry system and an automatic entry system may be provided, respectively, to enable the card for short and long periods of use. Alternatively, the arrangements may work in parallel, and the near
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		field tag 41 would be enabled only if the light sensor was activated and the correct PIN was entered (for example). Further, the arrangements may work in series - for example, the near field tag 41 would be enabled if the light sensor was activated and the correct PIN was subsequently entered. Waters at [Page 17] The housing 52 may further optionally provide a display 58 for prompting the user to enter their PIN number and/or for displaying the PIN number as it is entered, if desired. On entry of the PIN number using the push buttons 56, the entered PIN number is compared to the PIN number stored on the SIM. If the PINs are found to match, communication between the SIM and the PC is permitted to authenticate one or more transactions. The comparison between the entered PIN number and the PIN number stored on the SIM 15 is performed within the dongle 50, and neither the entered PIN number nor the PIN number stored on the SIM is communicated to the PC. This prevents or reduces the likelihood that the PINs will become compromised by disclosure to an authorised party. Waters at [Page 18] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[17.2]	establishing by the wireless device a short-range wireless link with the entity;	Waters discloses “establishing by the wireless device a short-range wireless link with the entity;” See e.g.: A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] As shown in Figure 2, mobile terminal 1 in accordance with the embodiment includes, in addition to SIM 15, a display 34, keypad 37 and an antenna 39 for communicating wirelessly with the mobile communications network 3. Further, the mobile terminal 1 includes a near field or RFID tag 41. The near field tag 41 operates in the unregulated RF band of 13.56 MHz in this embodiment although other frequencies could be used. No licences are required for the use of the near field devices in this RF band. However, each country imposes certain limitations on the electromagnetic emissions in this RF band. Limitations mean that in practice the distance at which the near field tag 41 can communicate with another device is typically less than 20 centimetres. Often the range of communication is such that the RF tag 41 must touch or almost touch the device with which it is to communicate. Communication may be using the Near Field Communication Interface and Protocol (NFCIP-1). Waters at [Page 9] The near field tag 41 may operate in accordance with ISO-IEC 14443 and ISOIEC 15693 standards. The tag 41 includes an inbuilt inductive antenna that allows the card to exchange information with a tag reader when the two are brought into close proximity, as described above. The reader may emit an RF signal to supply power to the tag to communicate with it if the tag is "passive". If
--	--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	the tag is "active" it will have a power supply and its operation is independently of the reader. The near field tag 41 may transmit selected information, such as an ID number (GU ID). Waters at [Page 10] Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Waters at [Page 15] Biometric data entry - the mobile terminal 1 may incorporate a fingerprint reader 45. The fingerprint reader 45 scans the fingerprint of the user when the user's finger is placed on the reader 45 and compares it to the user's fingerprint stored in the memory of the mobile terminal 1 or the SIM 15. If the fingerprints are determined to match, the message is sent from the SIM 15, via link 43, to the RF tag 41. As an alternative to a fingerprint, other biometric data could be used - for example, voice recognition (using the mobile terminal's built-in microphone and a voice recognition algorithm within the mobile terminal 1 or SIM card 15) or retinal scanning (using the mobile terminal's built-in camera). Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently.
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		Waters at [Page 15] The invention is applicable to any device that uses RF communication and relies on close proximity of a reader for its operation. Waters at [Page 23] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[17.3]	wirelessly transmitting information to the entity using unlicensed frequencies; and	Waters discloses “wirelessly transmitting information to the entity using unlicensed frequencies; and” See e.g.: A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] As shown in Figure 2, mobile terminal 1 in accordance with the embodiment includes, in addition to SIM 15, a display 34, keypad 37 and an antenna 39 for communicating wirelessly with the mobile communications network 3. Further,

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	the mobile terminal 1 includes a near field or RFID tag 41. The near field tag 41 operates in the unregulated RF band of 13.56 MHz in this embodiment although other frequencies could be used. No licences are required for the use of the near field devices in this RF band. However, each country imposes certain limitations on the electromagnetic emissions in this RF band. Limitations mean that in practice the distance at which the near field tag 41 can communicate with another device is typically less than 20 centimeters. Often the range of communication is such that the RF tag 41 must touch or almost touch the device with which it is to communicate. Communication may be using the Near Field Communication Interface and Protocol (NFCIP-I). Waters at [Page 08] The near field tag 41 may operate in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards. The tag 41 includes an inbuilt inductive antenna that allows the card to exchange information with a tag reader when the two are brought into close proximity, as described above. The reader may emit an RF signal to supply power to the tag to communicate with it if the tag is "passive". If the tag is "active" it will have a power supply and its operation is independently of the reader. The near field tag 41 may transmit selected information, such as an ID number (GU ID). Waters at [Page 09] In order to improve the security of the near field tag, in the present embodiment it is proposed to use the SIM 15 of mobile terminal 1 to control to some extent the operation of the near field tag 41. The authentication process of a SIM 15 with a mobile telecommunications network, using the network's authentication processor 17 is considered to be highly secure. In this embodiment, this authentication of the SIM 15 is used to protect data held by the memory of the near field tag 41 from unauthorised access. Waters at [Page 09] According to an important feature of this embodiment, the near field tag 41 is selectively enabled or disabled for communication with the reader under control
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	of the SIM 15, by means of communication link 43. By means of the link 43, the SIM can enable or disable the near field tag 41 by, for example, rendering its antenna inoperative. In the disabled state, a reader is not able to obtain any information from the near field tag 41, even when brought into close proximity thereto (within a range that, in normal circumstances, near field communication would be possible). Waters at [Page 09] In the second example, a user wishes to use the near field tag 41 of the mobile terminal 1 to pay for travel by public transport (for example on the London Underground), where entry barriers are equipped with a suitable near field tag reader. Because the commuter travels at particular, consistent times of day, it is desirable to enable the near field tag 41 only at those times, in order to provide improved security. When so configured, if the mobile terminal 1 incorporating the near field tag 41 were stolen, the thief would not be able to pay for use of public transport using the near field tag 41 outside the times specified. Waters at [Page 11] The mobile telecommunications network 3 is configured to transmit an OTA message to the mobile terminal 1 at the beginning of the time period during which the commuter begins their normal journey. As before, this message is received and interpreted by the SIM, which sends an instruction to enable the near field tag 41 via the link 43. The near field tag 41 is then able to communicate with readers to allow use of public transport. At the end of the time period during which the commuter completes their usual journey, a second OTA message is sent by the network 3 to the mobile terminal 1. This OTA message is received and interpreted by the SIM 15, and sends an appropriate deactivation instruction to the RF tag 41 via the link 43. The near field tag 41 is thereafter not able to allow the user to obtain access to public transport. Waters at [Page 11] A similar arrangement could be used, for example, to enable a school child to pay for their lunch using the near field tag 41. OTA messages would be sent at the
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	beginning and the end of the school lunch time so that the near field tag 41 could only be used to make a payment during the appropriate time. Waters at [Page 11] The times at which, and the circumstances in which, the OTA messages are sent by the mobile telecommunications network 3 to the user's SIM card 15 may be set by the user of the mobile terminal 1. For example, the user of the mobile terminal 1 may initiate a communication session (such as a SIP communication session) with the mobile telecommunications network 1 to configure the times or places in which the RF tag 41 should be enabled. This updating process may require entry of a password, or employ some other security mechanism, to prevent unauthorised persons from reconfiguring the times and/or locations at which the near field tag is rendered operable or inoperable. Alternatively, the user may configure the times and/or locations at which the OTA messages are sent by some other mechanism - for example, by providing verbal instructions to the operator of mobile telecommunications network 3 by a mobile or PSTN telephone call, or by visiting the website of the mobile telecommunications network operator (whether using the mobile terminal or independently thereof using a PC connected to the Internet). Waters at [Page 12] Rather than the user of the mobile terminal 1 determining when/where the RF tag 41 is activated, this may be determined by the mobile telecommunications network 3 or some other entity. For example, a school child's parent may set the times during which the school child is able to use their RF tag to make payments, in the example given above relating to paying for a school lunch. In the example given above relating to payment for public transport, the public transportation authority may alternatively or additionally be able to control when OTA messages are sent so that, if it is notified that the mobile terminal 1 incorporating the near field tag 41 has been stolen, that authority can permanently or temporarily deactivate the near field tag 41. Waters at [Page 12]
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	In an alternative embodiment, the SIM 15 activates and deactivates the tag in dependence upon whether the SIM is authenticated with the mobile Waters at [Page 12] In another embodiment of the invention, the mobile terminal and/or near field tag 41 is provided with means for disabling the tag 41 without requiring communication between the mobile terminal 1 and the mobile telecommunications network 3 (and therefore without requiring receipt of an OTA message). Waters at [Page 13] The near field tag 41 may be selectively enabled and disabled in order to reduce the opportunity to obtain information from the near field tag 41 by an unauthorised reader. Waters at [Page 13] The following arrangements are useful if the near field tag 41 is to be enabled and disabled for fairly long periods of time: Waters at [Page 14] (1) Personal identification number (PESf) entry - the keypad 37 of the mobile terminal 1 is used to enter a PIN (or other secret password) to enable the near field tag 41. The user's PIN may be stored in a secure location in the mobile terminal 1 or in the SIM 15. When the user enters their PIN using the keypad 37, the entered PIN is compared with the stored PIN. If the PINs match, the SIM transmits a message, via link 43, to the near field tag 41 to activate the near field tag. Waters at [Page 14] (2) Biometric data entry - the mobile terminal 1 may incorporate a fingerprint reader 45. The fingerprint reader 45 scans the fingerprint of the user when the user's finger is placed on the reader 45 and compares it to the user's fingerprint stored in the memory of the mobile terminal 1 or the SIM 15. If the fingerprints
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	are determined to match, the message is sent from the SIM 15, via link 43, to the RF tag 41. As an alternative to a fingerprint, other biometric data could be used - for example, voice recognition (using the mobile terminal's built-in microphone and a voice recognition algorithm within the mobile terminal 1 or SIM card 15) or retinal scanning (using the mobile terminal's built-in camera). Waters at [Page 14] Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 15] A mobile terminal 1 may have any of the above arrangements implemented in any combination. For example, a manual entry system and an automatic entry system may be provided, respectively, to enable the card for short and long periods of use. Alternatively, the arrangements may work in parallel, and the near field tag 41 would be enabled only if the light sensor was activated and the correct PIN was entered (for example). Further, the arrangements may work in series - for example, the near field tag 41 would be enabled if the light sensor was activated and the correct PIN was subsequently entered. Waters at [Page 17] The housing 52 may further optionally provide a display 58 for prompting the user to enter their PIN number and/or for displaying the PIN number as it is entered, if desired. On entry of the PIN number using the push buttons 56, the entered PIN number is compared to the PIN number stored on the SIM. If the
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	PINs are found to match, communication between the SIM and the PC is permitted to authenticate one or more transactions. The comparison between the entered PIN number and the PIN number stored on the SIM 15 is performed within the dongle 50, and neither the entered PIN number nor the PIN number stored on the SIM is communicated to the PC. This prevents or reduces the likelihood that the PINs will become compromised by disclosure to an authorised party. Waters at [Page 18] Figure 5 shows a smart card 100 with an in-built near field tag including an inductive antenna 200, and a biometric system 120 for reading a finger print. The print is ideally compared to a previously taken print stored in the memory 130 of the smart card 100 or may just be judged as having the characteristics of a non-specific fingerprint. Waters at [Page 20] Apparatus for controlling use of a near field communication device, including smart card means associable with a mobile telecommunications network for authenticating the smart card means with the network, wherein the smart card means is operable to receive from the mobile telecommunications network data for controlling use of the near field communication device and is operable to selectively enable the near field communication device in dependence upon the data. [Claim 1] 2. The apparatus of claim 1, wherein the smart card means is operable to selectively enable the near field communication device by selectively enabling the near field communication device to be read by a reader [Claim 2] The apparatus of claim 7, 8 or 9, wherein the security data comprises a Personal Identification Number (PIN) and the apparatus includes means for comparing the PIN obtained by the security data entry means with a PIN stored on the apparatus
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

and only enables operation of the near field device when the respective PINs match.

[Claim 10]

The apparatus of claim 7, wherein the security data entry means is operable to detect biometric data from a user.

[Claim 11]

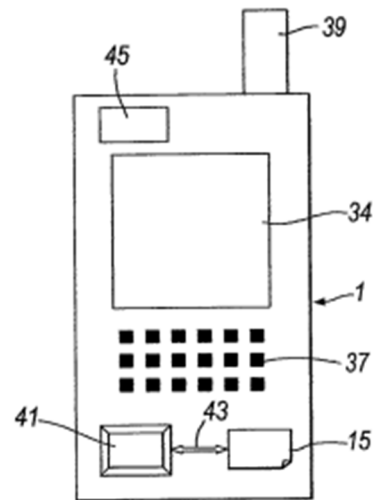


Fig.2

[Fig.2]

Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[17.4]	wirelessly receiving information from the entity using unlicensed frequencies;	Waters discloses “wirelessly receiving information from the entity using unlicensed frequencies;” See e.g.: A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] As shown in Figure 2, mobile terminal 1 in accordance with the embodiment includes, in addition to SIM 15, a display 34, keypad 37 and an antenna 39 for communicating wirelessly with the mobile communications network 3. Further, the mobile terminal 1 includes a near field or RFID tag 41. The near field tag 41 operates in the unregulated RF band of 13.56 MHz in this embodiment although other frequencies could be used. No licences are required for the use of the near field devices in this RF band. However, each country imposes certain limitations on the electromagnetic emissions in this RF band. Limitations mean that in practice the distance at which the near field tag 41 can communicate with another device is typically less than 20 centimeters. Often the range of communication is such that the RF tag 41 must touch or almost touch the device with which it is to communicate. Communication may be using the Near Field Communication Interface and Protocol (NFCIP-I).

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	Waters at [Page 08] The near field tag 41 may operate in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards. The tag 41 includes an inbuilt inductive antenna that allows the card to exchange information with a tag reader when the two are brought into close proximity, as described above. The reader may emit an RF signal to supply power to the tag to communicate with it if the tag is "passive". If the tag is "active" it will have a power supply and its operation is independently of the reader. The near field tag 41 may transmit selected information, such as an ID number (GU ID). Waters at [Page 09] In order to improve the security of the near field tag, in the present embodiment it is proposed to use the SIM 15 of mobile terminal 1 to control to some extent the operation of the near field tag 41. The authentication process of a SIM 15 with a mobile telecommunications network, using the network's authentication processor 17 is considered to be highly secure. In this embodiment, this authentication of the SIM 15 is used to protect data held by the memory of the near field tag 41 from unauthorised access. Waters at [Page 09] According to an important feature of this embodiment, the near field tag 41 is selectively enabled or disabled for communication with the reader under control of the SIM 15, by means of communication link 43. By means of the link 43, the SIM can enable or disable the near field tag 41 by, for example, rendering its antenna inoperative. In the disabled state, a reader is not able to obtain any information from the near field tag 41, even when brought into close proximity thereto (within a range that, in normal circumstances, near field communication would be possible). Waters at [Page 09] In the second example, a user wishes to use the near field tag 41 of the mobile terminal 1 to pay for travel by public transport (for example on the London
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	Underground), where entry barriers are equipped with a suitable near field tag reader. Because the commuter travels at particular, consistent times of day, it is desirable to enable the near field tag 41 only at those times, in order to provide improved security. When so configured, if the mobile terminal 1 incorporating the near field tag 41 were stolen, the thief would not be able to pay for use of public transport using the near field tag 41 outside the times specified. Waters at [Page 11] The mobile telecommunications network 3 is configured to transmit an OTA message to the mobile terminal 1 at the beginning of the time period during which the commuter begins their normal journey. As before, this message is received and interpreted by the SIM, which sends an instruction to enable the near field tag 41 via the link 43. The near field tag 41 is then able to communicate with readers to allow use of public transport. At the end of the time period during which the commuter completes their usual journey, a second OTA message is sent by the network 3 to the mobile terminal 1. This OTA message is received and interpreted by the SIM 15, and sends an appropriate deactivation instruction to the RF tag 41 via the link 43. The near field tag 41 is thereafter not able to allow the user to obtain access to public transport. Waters at [Page 11] A similar arrangement could be used, for example, to enable a school child to pay for their lunch using the near field tag 41. OTA messages would be sent at the beginning and the end of the school lunch time so that the near field tag 41 could only be used to make a payment during the appropriate time. Waters at [Page 11] The times at which, and the circumstances in which, the OTA messages are sent by the mobile telecommunications network 3 to the user's SIM card 15 may be set by the user of the mobile terminal 1. For example, the user of the mobile terminal 1 may initiate a communication session (such as a SIP communication session) with the mobile telecommunications network 1 to configure the times or places in which the RF tag 41 should be enabled. This updating process may
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	require entry of a password, or employ some other security mechanism, to prevent unauthorised persons from reconfiguring the times and/or locations at which the near field tag is rendered operable or inoperable. Alternatively, the user may configure the times and/or locations at which the OTA messages are sent by some other mechanism - for example, by providing verbal instructions to the operator of mobile telecommunications network 3 by a mobile or PSTN telephone call, or by visiting the website of the mobile telecommunications network operator (whether using the mobile terminal or independently thereof using a PC connected to the Internet). Waters at [Page 12] Rather than the user of the mobile terminal 1 determining when/where the RF tag 41 is activated, this may be determined by the mobile telecommunications network 3 or some other entity. For example, a school child's parent may set the times during which the school child is able to use their RF tag to make payments, in the example given above relating to paying for a school lunch. In the example given above relating to payment for public transport, the public transportation authority may alternatively or additionally be able to control when OTA messages are sent so that, if it is notified that the mobile terminal 1 incorporating the near field tag 41 has been stolen, that authority can permanently or temporarily deactivate the near field tag 41. Waters at [Page 12] In an alternative embodiment, the SIM 15 activates and deactivates the tag in dependence upon whether the SIM is authenticated with the mobile Waters at [Page 12] In another embodiment of the invention, the mobile terminal and/or near field tag 41 is provided with means for disabling the tag 41 without requiring communication between the mobile terminal 1 and the mobile telecommunications network 3 (and therefore without requiring receipt of an OTA message). Waters at [Page 13]
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	The near field tag 41 may be selectively enabled and disabled in order to reduce the opportunity to obtain information from the near field tag 41 by an unauthorised reader. Waters at [Page 13] The following arrangements are useful if the near field tag 41 is to be enabled and disabled for fairly long periods of time: Waters at [Page 14] (1) Personal identification number (PESf) entry - the keypad 37 of the mobile terminal 1 is used to enter a PIN (or other secret password) to enable the near field tag 41. The user's PIN may be stored in a secure location in the mobile terminal 1 or in the SIM 15. When the user enters their PIN using the keypad 37, the entered PIN is compared with the stored PIN. If the PINs match, the SIM transmits a message, via link 43, to the near field tag 41 to activate the near field tag. Waters at [Page 14] (2) Biometric data entry - the mobile terminal 1 may incorporate a fingerprint reader 45. The fingerprint reader 45 scans the fingerprint of the user when the user's finger is placed on the reader 45 and compares it to the user's fingerprint stored in the memory of the mobile terminal 1 or the SIM 15. If the fingerprints are determined to match, the message is sent from the SIM 15, via link 43, to the RF tag 41. As an alternative to a fingerprint, other biometric data could be used - for example, voice recognition (using the mobile terminal's built-in microphone and a voice recognition algorithm within the mobile terminal 1 or SIM card 15) or retinal scanning (using the mobile terminal's built-in camera). Waters at [Page 14] Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 15] A mobile terminal 1 may have any of the above arrangements implemented in any combination. For example, a manual entry system and an automatic entry system may be provided, respectively, to enable the card for short and long periods of use. Alternatively, the arrangements may work in parallel, and the near field tag 41 would be enabled only if the light sensor was activated and the correct PIN was entered (for example). Further, the arrangements may work in series - for example, the near field tag 41 would be enabled if the light sensor was activated and the correct PIN was subsequently entered. Waters at [Page 17] The housing 52 may further optionally provide a display 58 for prompting the user to enter their PIN number and/or for displaying the PIN number as it is entered, if desired. On entry of the PIN number using the push buttons 56, the entered PIN number is compared to the PIN number stored on the SIM. If the PINs are found to match, communication between the SIM and the PC is permitted to authenticate one or more transactions. The comparison between the entered PIN number and the PIN number stored on the SIM 15 is performed within the dongle 50, and neither the entered PIN number nor the PIN number stored on the SIM is communicated to the PC. This prevents or reduces the likelihood that the PINs will become compromised by disclosure to an authorised party. Waters at [Page 18] Figure 5 shows a smart card 100 with an in-built near field tag including an inductive antenna 200, and a biometric system 120 for reading a finger print. The
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	print is ideally compared to a previously taken print stored in the memory 130 of the smart card 100 or may just be judged as having the characteristics of a non-specific fingerprint. Waters at [Page 20] Apparatus for controlling use of a near field communication device, including smart card means associable with a mobile telecommunications network for authenticating the smart card means with the network, wherein the smart card means is operable to receive from the mobile telecommunications network data for controlling use of the near field communication device and is operable to selectively enable the near field communication device in dependence upon the data. [Claim 1] 2. The apparatus of claim 1, wherein the smart card means is operable to selectively enable the near field communication device by selectively enabling the near field communication device to be read by a reader [Claim 2] The apparatus of claim 7, 8 or 9, wherein the security data comprises a Personal Identification Number (PIN) and the apparatus includes means for comparing the PIN obtained by the security data entry means with a PIN stored on the apparatus and only enables operation of the near field device when the respective PINs match. [Claim 10] The apparatus of claim 7, wherein the security data entry means is operable to detect biometric data from a user. [Claim 11]
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

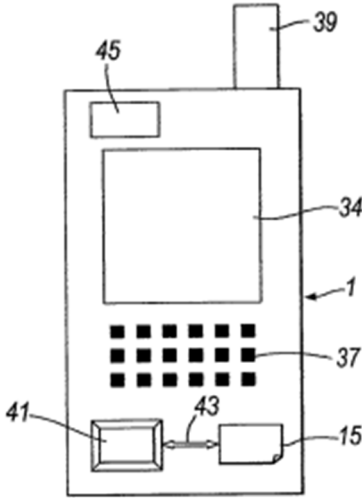
		 Fig.2 [Fig.2] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[17.5]	wherein said wirelessly transmitting and said wirelessly receiving comprises using a time domain duplex protocol; and	Waters discloses “wherein said wirelessly transmitting and said wirelessly receiving comprises using a time domain duplex protocol; and” See e.g.: A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] As shown in Figure 2, mobile terminal 1 in accordance with the embodiment includes, in addition to SIM 15, a display 34, keypad 37 and an antenna 39 for communicating wirelessly with the mobile communications network 3. Further, the mobile terminal 1 includes a near field or RFID tag 41. The near field tag 41 operates in the unregulated RF band of 13.56 MHz in this embodiment although other frequencies could be used. No licences are required for the use of the near field devices in this RF band. However, each country imposes certain limitations on the electromagnetic emissions in this RF band. Limitations mean that in practice the distance at which the near field tag 41 can communicate with another device is typically less than 20 centimeters. Often the range of communication is such that the RF tag 41 must touch or almost touch the device with which it is to communicate. Communication may be using the Near Field Communication Interface and Protocol (NFCIP-I). Waters at [Page 08] The near field tag 41 may operate in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards. The tag 41 includes an inbuilt inductive antenna that allows the card to exchange information with a tag reader when the two are brought into close proximity, as described above. The reader may emit an RF signal to supply power to the tag to communicate with it if the tag is "passive". If the tag is
--	--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	"active" it will have a power supply and its operation is independently of the reader. The near field tag 41 may transmit selected information, such as an ID number (GU ID). Waters at [Page 09] In order to improve the security of the near field tag, in the present embodiment it is proposed to use the SIM 15 of mobile terminal 1 to control to some extent the operation of the near field tag 41. The authentication process of a SIM 15 with a mobile telecommunications network, using the network's authentication processor 17 is considered to be highly secure. In this embodiment, this authentication of the SIM 15 is used to protect data held by the memory of the near field tag 41 from unauthorised access. Waters at [Page 09] According to an important feature of this embodiment, the near field tag 41 is selectively enabled or disabled for communication with the reader under control of the SIM 15, by means of communication link 43. By means of the link 43, the SIM can enable or disable the near field tag 41 by, for example, rendering its antenna inoperative. In the disabled state, a reader is not able to obtain any information from the near field tag 41, even when brought into close proximity thereto (within a range that, in normal circumstances, near field communication would be possible). Waters at [Page 09] In the second example, a user wishes to use the near field tag 41 of the mobile terminal 1 to pay for travel by public transport (for example on the London Underground), where entry barriers are equipped with a suitable near field tag reader. Because the commuter travels at particular, consistent times of day, it is desirable to enable the near field tag 41 only at those times, in order to provide improved security. When so configured, if the mobile terminal 1 incorporating the near field tag 41 were stolen, the thief would not be able to pay for use of public transport using the near field tag 41 outside the times specified. Waters at [Page 11]
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	The mobile telecommunications network 3 is configured to transmit an OTA message to the mobile terminal 1 at the beginning of the time period during which the commuter begins their normal journey. As before, this message is received and interpreted by the SIM, which sends an instruction to enable the near field tag 41 via the link 43. The near field tag 41 is then able to communicate with readers to allow use of public transport. At the end of the time period during which the commuter completes their usual journey, a second OTA message is sent by the network 3 to the mobile terminal 1. This OTA message is received and interpreted by the SIM 15, and sends an appropriate deactivation instruction to the RF tag 41 via the link 43. The near field tag 41 is thereafter not able to allow the user to obtain access to public transport. Waters at [Page 11] A similar arrangement could be used, for example, to enable a school child to pay for their lunch using the near field tag 41. OTA messages would be sent at the beginning and the end of the school lunch time so that the near field tag 41 could only be used to make a payment during the appropriate time. Waters at [Page 11] The times at which, and the circumstances in which, the OTA messages are sent by the mobile telecommunications network 3 to the user's SIM card 15 may be set by the user of the mobile terminal 1. For example, the user of the mobile terminal 1 may initiate a communication session (such as a SIP communication session) with the mobile telecommunications network 1 to configure the times or places in which the RF tag 41 should be enabled. This updating process may require entry of a password, or employ some other security mechanism, to prevent unauthorised persons from reconfiguring the times and/or locations at which the near field tag is rendered operable or inoperable. Alternatively, the user may configure the times and/or locations at which the OTA messages are sent by some other mechanism - for example, by providing verbal instructions to the operator of mobile telecommunications network 3 by a mobile or PSTN telephone call, or by visiting the website of the mobile telecommunications
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	network operator (whether using the mobile terminal or independently thereof using a PC connected to the Internet). Waters at [Page 12] Rather than the user of the mobile terminal 1 determining when/where the RF tag 41 is activated, this may be determined by the mobile telecommunications network 3 or some other entity. For example, a school child's parent may set the times during which the school child is able to use their RF tag to make payments, in the example given above relating to paying for a school lunch. In the example given above relating to payment for public transport, the public transportation authority may alternatively or additionally be able to control when OTA messages are sent so that, if it is notified that the mobile terminal 1 incorporating the near field tag 41 has been stolen, that authority can permanently or temporarily deactivate the near field tag 41. Waters at [Page 12] In an alternative embodiment, the SIM 15 activates and deactivates the tag in dependence upon whether the SIM is authenticated with the mobile Waters at [Page 12] In another embodiment of the invention, the mobile terminal and/or near field tag 41 is provided with means for disabling the tag 41 without requiring communication between the mobile terminal 1 and the mobile telecommunications network 3 (and therefore without requiring receipt of an OTA message). Waters at [Page 13] The near field tag 41 may be selectively enabled and disabled in order to reduce the opportunity to obtain information from the near field tag 41 by an unauthorised reader. Waters at [Page 13] The following arrangements are useful if the near field tag 41 is to be enabled and disabled for fairly long periods of time:
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	Waters at [Page 14] (1) Personal identification number (PESf) entry - the keypad 37 of the mobile terminal 1 is used to enter a PIN (or other secret password) to enable the near field tag 41. The user's PIN may be stored in a secure location in the mobile terminal 1 or in the SIM 15. When the user enters their PIN using the keypad 37, the entered PIN is compared with the stored PIN. If the PINs match, the SIM transmits a message, via link 43, to the near field tag 41 to activate the near field tag. Waters at [Page 14] (2) Biometric data entry - the mobile terminal 1 may incorporate a fingerprint reader 45. The fingerprint reader 45 scans the fingerprint of the user when the user's finger is placed on the reader 45 and compares it to the user's fingerprint stored in the memory of the mobile terminal 1 or the SIM 15. If the fingerprints are determined to match, the message is sent from the SIM 15, via link 43, to the RF tag 41. As an alternative to a fingerprint, other biometric data could be used - for example, voice recognition (using the mobile terminal's built-in microphone and a voice recognition algorithm within the mobile terminal 1 or SIM card 15) or retinal scanning (using the mobile terminal's built-in camera). Waters at [Page 14] Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 15]
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	A mobile terminal 1 may have any of the above arrangements implemented in any combination. For example, a manual entry system and an automatic entry system may be provided, respectively, to enable the card for short and long periods of use. Alternatively, the arrangements may work in parallel, and the near field tag 41 would be enabled only if the light sensor was activated and the correct PIN was entered (for example). Further, the arrangements may work in series - for example, the near field tag 41 would be enabled if the light sensor was activated and the correct PIN was subsequently entered. Waters at [Page 17] The housing 52 may further optionally provide a display 58 for prompting the user to enter their PIN number and/or for displaying the PIN number as it is entered, if desired. On entry of the PIN number using the push buttons 56, the entered PIN number is compared to the PIN number stored on the SIM. If the PINs are found to match, communication between the SIM and the PC is permitted to authenticate one or more transactions. The comparison between the entered PIN number and the PIN number stored on the SIM 15 is performed within the dongle 50, and neither the entered PIN number nor the PIN number stored on the SIM is communicated to the PC. This prevents or reduces the likelihood that the PINs will become compromised by disclosure to an authorised party. Waters at [Page 18] Figure 5 shows a smart card 100 with an in-built near field tag including an inductive antenna 200, and a biometric system 120 for reading a finger print. The print is ideally compared to a previously taken print stored in the memory 130 of the smart card 100 or may just be judged as having the characteristics of a non-specific fingerprint. Waters at [Page 20] Apparatus for controlling use of a near field communication device, including smart card means associable with a mobile telecommunications network for authenticating the smart card means with the network, wherein the smart card
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		means is operable to receive from the mobile telecommunications network data for controlling use of the near field communication device and is operable to selectively enable the near field communication device in dependence upon the data. [Claim 1] 2. The apparatus of claim 1, wherein the smart card means is operable to selectively enable the near field communication device by selectively enabling the near field communication device to be read by a reader [Claim 2] The apparatus of claim 7, 8 or 9, wherein the security data comprises a Personal Identification Number (PIN) and the apparatus includes means for comparing the PIN obtained by the security data entry means with a PIN stored on the apparatus and only enables operation of the near field device when the respective PINs match. [Claim 10] The apparatus of claim 7, wherein the security data entry means is operable to detect biometric data from a user. [Claim 11]
--	--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

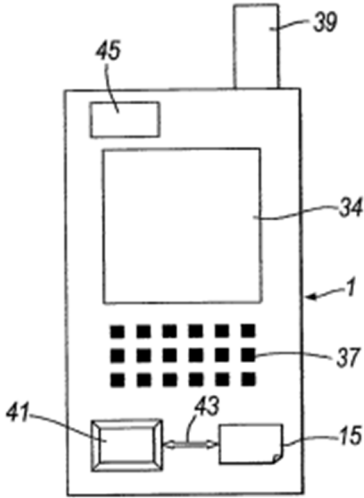
		 Fig.2 [Fig.2] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[17.6]	wherein said establishing by the wireless device a short-range wireless link with the entity comprises establishing the short-range wireless link with the entity responsive to the wireless device	Waters discloses “wherein said establishing by the wireless device a short-range wireless link with the entity comprises establishing the short-range wireless link with the entity responsive to the wireless device satisfying the proximity condition relative to the entity and responsive to the wireless device sensing the parameter and determining that the value associated therewith satisfies the threshold criterion.” See e.g.:

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	satisfying the proximity condition relative to the entity and responsive to the wireless device sensing the parameter and determining that the value associated therewith satisfies the threshold criterion.	[4.2], supra. Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[18.1]	The wireless device of claim 14, wherein said requesting from a second device an authorization to enable a function for conducting a financial transaction and/or said receiving from the second device the authorization to enable the function for conducting the financial transaction comprises:	To the extent the preamble is limiting, Waters discloses “the wireless device of claim 14, wherein said requesting from a second device an authorization to enable a function for conducting a financial transaction and/or said receiving from the second device the authorization to enable the function for conducting the financial transaction comprises:” See e.g.: Claim 14, supra. The procedure described above is applied, and the OTA message is passed to the SIM 15 and the instructions therein are processed. A command is sent to the near field tag 41 via link 43 to activate the near field tag (for example, by allowing its antenna to communicate with the reader). When the mobile terminal 1 moves to a different cell, a command is sent from the SIM 15, via the link 43, to disable the near field tag 41. This command may be issued in response to a further OTA message being received from the network 3 when the mobile terminal 1 moves to a different cell, or movement to a different cell may be detected automatically by the SIM (or the mobile terminal 1) and used to generate an appropriate command for sending to the near field tag 41. Waters at [Page 11] The mobile telecommunications network 3 is configured to transmit an OTA message to the mobile terminal 1 at the beginning of the time period during which the commuter begins their normal journey. As before, this message is received and interpreted by the SIM, which sends an instruction to enable the

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	near field tag 41 via the link 43. The near field tag 41 is then able to communicate with readers to allow use of public transport. At the end of the time period during which the commuter completes their usual journey, a second OTA message is sent by the network 3 to the mobile terminal 1. This OTA message is received and interpreted by the SIM 15, and sends an appropriate deactivation instruction to the RF tag 41 via the link 43. The near field tag 41 is thereafter not able to allow the user to obtain access to public transport. Waters at [Page 12] The times at which, and the circumstances in which, the OTA messages are sent by the mobile telecommunications network 3 to the user's SIM card 15 may be set by the user of the mobile terminal 1. For example, the user of the mobile terminal 1 may initiate a communication session (such as a SIP communication session) with the mobile telecommunications network 1 to configure the times or places in which the RF tag 41 should be enabled. This updating process may require entry of a password, or employ some other security mechanism, to prevent unauthorised persons from reconfiguring the times and/or locations at which the near field tag is rendered operable or inoperable. Alternatively, the user may configure the times and/or locations at which the OTA messages are sent by some other mechanism - for example, by providing verbal instructions to the operator of mobile telecommunications network 3 by a mobile or PSTN telephone call, or by visiting the website of the mobile telecommunications network operator (whether using the mobile terminal or independently thereof using a PC connected to the Internet). Waters at [Page 13] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[18.2]	establishing by the wireless device a link with the second device, comprising a wireless link that comprises a distance that is greater than a distance associated with the proximity condition;	Waters discloses “establishing by the wireless device a link with the second device, comprising a wireless link that comprises a distance that is greater than a distance associated with the proximity condition;” See e.g.: [3.2], supra. A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] As shown in Figure 2, mobile terminal 1 in accordance with the embodiment includes, in addition to SIM 15, a display 34, keypad 37 and an antenna 39 for communicating wirelessly with the mobile communications network 3. Further, the mobile terminal 1 includes a near field or RFID tag 41. The near field tag 41 operates in the unregulated RF band of 13.56 MHz in this embodiment although other frequencies could be used. No licences are required for the use of the near field devices in this RF band. However, each country imposes certain limitations on the electromagnetic emissions in this RF band. Limitations mean that in practice the distance at which the near field tag 41 can communicate with another device is typically less than 20 centimeters. Often the range of communication is

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	such that the RF tag 41 must touch or almost touch the device with which it is to communicate. Communication may be using the Near Field Communication Interface and Protocol (NFCIP-I). Waters at [Page 08] The near field tag 41 may operate in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards. The tag 41 includes an inbuilt inductive antenna that allows the card to exchange information with a tag reader when the two are brought into close proximity, as described above. The reader may emit an RF signal to supply power to the tag to communicate with it if the tag is "passive". If the tag is "active" it will have a power supply and its operation is independently of the reader. The near field tag 41 may transmit selected information, such as an ID number (GU ID). Waters at [Page 09] In order to improve the security of the near field tag, in the present embodiment it is proposed to use the SIM 15 of mobile terminal 1 to control to some extent the operation of the near field tag 41. The authentication process of a SIM 15 with a mobile telecommunications network, using the network's authentication processor 17 is considered to be highly secure. In this embodiment, this authentication of the SIM 15 is used to protect data held by the memory of the near field tag 41 from unauthorised access. Waters at [Page 09] According to an important feature of this embodiment, the near field tag 41 is selectively enabled or disabled for communication with the reader under control of the SIM 15, by means of communication link 43. By means of the link 43, the SIM can enable or disable the near field tag 41 by, for example, rendering its antenna inoperative. In the disabled state, a reader is not able to obtain any information from the near field tag 41, even when brought into close proximity thereto (within a range that, in normal circumstances, near field communication would be possible). Waters at [Page 09]
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	In the second example, a user wishes to use the near field tag 41 of the mobile terminal 1 to pay for travel by public transport (for example on the London Underground), where entry barriers are equipped with a suitable near field tag reader. Because the commuter travels at particular, consistent times of day, it is desirable to enable the near field tag 41 only at those times, in order to provide improved security. When so configured, if the mobile terminal 1 incorporating the near field tag 41 were stolen, the thief would not be able to pay for use of public transport using the near field tag 41 outside the times specified. Waters at [Page 11] The mobile telecommunications network 3 is configured to transmit an OTA message to the mobile terminal 1 at the beginning of the time period during which the commuter begins their normal journey. As before, this message is received and interpreted by the SIM, which sends an instruction to enable the near field tag 41 via the link 43. The near field tag 41 is then able to communicate with readers to allow use of public transport. At the end of the time period during which the commuter completes their usual journey, a second OTA message is sent by the network 3 to the mobile terminal 1. This OTA message is received and interpreted by the SIM 15, and sends an appropriate deactivation instruction to the RF tag 41 via the link 43. The near field tag 41 is thereafter not able to allow the user to obtain access to public transport. Waters at [Page 11] A similar arrangement could be used, for example, to enable a school child to pay for their lunch using the near field tag 41. OTA messages would be sent at the beginning and the end of the school lunch time so that the near field tag 41 could only be used to make a payment during the appropriate time. Waters at [Page 11] The times at which, and the circumstances in which, the OTA messages are sent by the mobile telecommunications network 3 to the user's SIM card 15 may be set by the user of the mobile terminal 1. For example, the user of the mobile terminal 1 may initiate a communication session (such as a SIP communication
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	session) with the mobile telecommunications network 1 to configure the times or places in which the RF tag 41 should be enabled. This updating process may require entry of a password, or employ some other security mechanism, to prevent unauthorised persons from reconfiguring the times and/or locations at which the near field tag is rendered operable or inoperable. Alternatively, the user may configure the times and/or locations at which the OTA messages are sent by some other mechanism - for example, by providing verbal instructions to the operator of mobile telecommunications network 3 by a mobile or PSTN telephone call, or by visiting the website of the mobile telecommunications network operator (whether using the mobile terminal or independently thereof using a PC connected to the Internet). Waters at [Page 12] Rather than the user of the mobile terminal 1 determining when/where the RF tag 41 is activated, this may be determined by the mobile telecommunications network 3 or some other entity. For example, a school child's parent may set the times during which the school child is able to use their RF tag to make payments, in the example given above relating to paying for a school lunch. In the example given above relating to payment for public transport, the public transportation authority may alternatively or additionally be able to control when OTA messages are sent so that, if it is notified that the mobile terminal 1 incorporating the near field tag 41 has been stolen, that authority can permanently or temporarily deactivate the near field tag 41. Waters at [Page 12] In an alternative embodiment, the SIM 15 activates and deactivates the tag in dependence upon whether the SIM is authenticated with the mobile Waters at [Page 12] In another embodiment of the invention, the mobile terminal and/or near field tag 41 is provided with means for disabling the tag 41 without requiring communication between the mobile terminal 1 and the mobile
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	telecommunications network 3 (and therefore without requiring receipt of an OTA message). Waters at [Page 13] The near field tag 41 may be selectively enabled and disabled in order to reduce the opportunity to obtain information from the near field tag 41 by an unauthorised reader. Waters at [Page 13] The following arrangements are useful if the near field tag 41 is to be enabled and disabled for fairly long periods of time: Waters at [Page 14] (1) Personal identification number (PESf) entry - the keypad 37 of the mobile terminal 1 is used to enter a PIN (or other secret password) to enable the near field tag 41. The user's PIN may be stored in a secure location in the mobile terminal 1 or in the SIM 15. When the user enters their PIN using the keypad 37, the entered PIN is compared with the stored PIN. If the PINs match, the SIM transmits a message, via link 43, to the near field tag 41 to activate the near field tag. Waters at [Page 14] (2) Biometric data entry - the mobile terminal 1 may incorporate a fingerprint reader 45. The fingerprint reader 45 scans the fingerprint of the user when the user's finger is placed on the reader 45 and compares it to the user's fingerprint stored in the memory of the mobile terminal 1 or the SIM 15. If the fingerprints are determined to match, the message is sent from the SIM 15, via link 43, to the RF tag 41. As an alternative to a fingerprint, other biometric data could be used - for example, voice recognition (using the mobile terminal's built-in microphone and a voice recognition algorithm within the mobile terminal 1 or SIM card 15) or retinal scanning (using the mobile terminal's built-in camera). Waters at [Page 14]
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 14] Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 15] (1) Light sensor - for example a photodiode (a sensor that modifies an electric current when exposed to a light source) could be built into the casing of the mobile terminal 1 and act as a switch to activate or deactivate the RF tag 41. The RF tag 41 is controlled by the photo diode so that the RF tag 41 is only enabled when the mobile terminal 1 is exposed to light. Therefore, when the mobile terminal 1 was in an opaque case or the user's pocket, the RF tag 41 will be disabled. The photodiode may be sensitive to a particular frequency range - for example visible light, infra red or ultra violet. The tag reader may be provided with a light emitter that emits light at this frequency, in order to activate the tag.
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	Waters at [Page 15] (2) Pressure sensor - a pressure sensor on the casing of mobile terminal 1 acts as a switch. The RF tag 41 is only enabled when the user physically presses the pressure sensor. Therefore, when the mobile terminal is in a case or the user's pocket, the pressure sensor is disabled. The pressure sensor may itself be deactivated by the user, for example, when a function of the mobile terminal 1 is selected such that the keypad 37 is inoperative. The pressure sensor may be combined with the fingerprint scanner 45. The combined sensor detects, not only that pressure is applied, but also that an authorised person is pressing the sensor. Alternatively, the pressure sensor could be combined with an electrical resistance meter and used to detect that it is a human hand pressing the pressure sensor, rather than some other object. Waters at [Page 15] (3) Heat sensors - such sensors incorporated in an appropriate position on the casing of the mobile terminal 1 could be configured to detect that the mobile terminal is in a user's hand by detecting the heat from the hand, and only enabling the near field tag 41 when heat from the hand is so detected. Waters at [Page 15] (4) Skin resistance sensor - a skin resistance sensor may be provided on the casing of the mobile terminal 1 in dependence of the presence of the pressure sensor described above. The near field tag 41 will only be operated when an appropriate resistance, capacitance or inductance is detected, indicating that the user's hand is touching the sensor. Waters at [Page 15] (5) Inertial sensors. An inertial sensor incorporated in the mobile terminal can be used to detect that the user is moving the terminal (and tag 41) around at a sufficient speed to indicate that it is to be used. Inertial sensors may be based on micro-accelerators, which are commonly used in motion detectors - for example in gaming and virtual reality/remote control systems.
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		Waters at [Page 15] A mobile terminal 1 may have any of the above arrangements implemented in any combination. For example, a manual entry system and an automatic entry system may be provided, respectively, to enable the card for short and long periods of use. Alternatively, the arrangements may work in parallel, and the near field tag 41 would be enabled only if the light sensor was activated and the correct PIN was entered (for example). Further, the arrangements may work in series - for example, the near field tag 41 would be enabled if the light sensor was activated and the correct PIN was subsequently entered. Waters at [Page 17] The housing 52 may further optionally provide a display 58 for prompting the user to enter their PIN number and/or for displaying the PIN number as it is entered, if desired. On entry of the PIN number using the push buttons 56, the entered PIN number is compared to the PIN number stored on the SIM. If the PINs are found to match, communication between the SIM and the PC is permitted to authenticate one or more transactions. The comparison between the entered PIN number and the PIN number stored on the SIM 15 is performed within the dongle 50, and neither the entered PIN number nor the PIN number stored on the SIM is communicated to the PC. This prevents or reduces the likelihood that the PINs will become compromised by disclosure to an authorised party. Waters at [Page 18] Figure 5 shows a smart card 100 with an in-built near field tag including an inductive antenna 200, and a biometric system 120 for reading a finger print. The print is ideally compared to a previously taken print stored in the memory 130 of the smart card 100 or may just be judged as having the characteristics of a non-specific fingerprint. Waters at [Page 20]
--	--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		Apparatus for controlling use of a near field communication device, including smart card means associable with a mobile telecommunications network for authenticating the smart card means with the network, wherein the smart card means is operable to receive from the mobile telecommunications network data for controlling use of the near field communication device and is operable to selectively enable the near field communication device in dependence upon the data. [Claim 1] 2. The apparatus of claim 1, wherein the smart card means is operable to selectively enable the near field communication device by selectively enabling the near field communication device to be read by a reader [Claim 2] The apparatus of claim 7, 8 or 9, wherein the security data comprises a Personal Identification Number (PIN) and the apparatus includes means for comparing the PIN obtained by the security data entry means with a PIN stored on the apparatus and only enables operation of the near field device when the respective PINs match. [Claim 10] The apparatus of claim 7, wherein the security data entry means is operable to detect biometric data from a user. [Claim 11]
--	--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

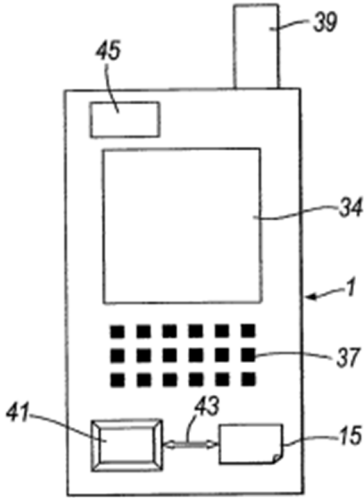
		 Fig.2 [Fig.2] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[18.3]	wirelessly transmitting information to the second device over said wireless link using unlicensed and/or licensed frequencies; and	Waters discloses “wirelessly transmitting information to the second device over said wireless link using unlicensed and/or licensed frequencies; and” See e.g.: A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] As shown in Figure 2, mobile terminal 1 in accordance with the embodiment includes, in addition to SIM 15, a display 34, keypad 37 and an antenna 39 for communicating wirelessly with the mobile communications network 3. Further, the mobile terminal 1 includes a near field or RFID tag 41. The near field tag 41 operates in the unregulated RF band of 13.56 MHz in this embodiment although other frequencies could be used. No licences are required for the use of the near field devices in this RF band. However, each country imposes certain limitations on the electromagnetic emissions in this RF band. Limitations mean that in practice the distance at which the near field tag 41 can communicate with another device is typically less than 20 centimeters. Often the range of communication is such that the RF tag 41 must touch or almost touch the device with which it is to communicate. Communication may be using the Near Field Communication Interface and Protocol (NFCIP-I). Waters at [Page 08] The near field tag 41 may operate in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards. The tag 41 includes an inbuilt inductive antenna that allows the card to exchange information with a tag reader when the two are brought into close proximity, as described above. The reader may emit an RF signal to supply power to the tag to communicate with it if the tag is "passive". If the tag is
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	"active" it will have a power supply and its operation is independently of the reader. The near field tag 41 may transmit selected information, such as an ID number (GU ID). Waters at [Page 09] In order to improve the security of the near field tag, in the present embodiment it is proposed to use the SIM 15 of mobile terminal 1 to control to some extent the operation of the near field tag 41. The authentication process of a SIM 15 with a mobile telecommunications network, using the network's authentication processor 17 is considered to be highly secure. In this embodiment, this authentication of the SIM 15 is used to protect data held by the memory of the near field tag 41 from unauthorised access. Waters at [Page 09] According to an important feature of this embodiment, the near field tag 41 is selectively enabled or disabled for communication with the reader under control of the SIM 15, by means of communication link 43. By means of the link 43, the SIM can enable or disable the near field tag 41 by, for example, rendering its antenna inoperative. In the disabled state, a reader is not able to obtain any information from the near field tag 41, even when brought into close proximity thereto (within a range that, in normal circumstances, near field communication would be possible). Waters at [Page 09] In the second example, a user wishes to use the near field tag 41 of the mobile terminal 1 to pay for travel by public transport (for example on the London Underground), where entry barriers are equipped with a suitable near field tag reader. Because the commuter travels at particular, consistent times of day, it is desirable to enable the near field tag 41 only at those times, in order to provide improved security. When so configured, if the mobile terminal 1 incorporating the near field tag 41 were stolen, the thief would not be able to pay for use of public transport using the near field tag 41 outside the times specified. Waters at [Page 11]
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	The mobile telecommunications network 3 is configured to transmit an OTA message to the mobile terminal 1 at the beginning of the time period during which the commuter begins their normal journey. As before, this message is received and interpreted by the SIM, which sends an instruction to enable the near field tag 41 via the link 43. The near field tag 41 is then able to communicate with readers to allow use of public transport. At the end of the time period during which the commuter completes their usual journey, a second OTA message is sent by the network 3 to the mobile terminal 1. This OTA message is received and interpreted by the SIM 15, and sends an appropriate deactivation instruction to the RF tag 41 via the link 43. The near field tag 41 is thereafter not able to allow the user to obtain access to public transport. Waters at [Page 11] A similar arrangement could be used, for example, to enable a school child to pay for their lunch using the near field tag 41. OTA messages would be sent at the beginning and the end of the school lunch time so that the near field tag 41 could only be used to make a payment during the appropriate time. Waters at [Page 11] The times at which, and the circumstances in which, the OTA messages are sent by the mobile telecommunications network 3 to the user's SIM card 15 may be set by the user of the mobile terminal 1. For example, the user of the mobile terminal 1 may initiate a communication session (such as a SIP communication session) with the mobile telecommunications network 1 to configure the times or places in which the RF tag 41 should be enabled. This updating process may require entry of a password, or employ some other security mechanism, to prevent unauthorised persons from reconfiguring the times and/or locations at which the near field tag is rendered operable or inoperable. Alternatively, the user may configure the times and/or locations at which the OTA messages are sent by some other mechanism - for example, by providing verbal instructions to the operator of mobile telecommunications network 3 by a mobile or PSTN telephone call, or by visiting the website of the mobile telecommunications
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	network operator (whether using the mobile terminal or independently thereof using a PC connected to the Internet). Waters at [Page 12] Rather than the user of the mobile terminal 1 determining when/where the RF tag 41 is activated, this may be determined by the mobile telecommunications network 3 or some other entity. For example, a school child's parent may set the times during which the school child is able to use their RF tag to make payments, in the example given above relating to paying for a school lunch. In the example given above relating to payment for public transport, the public transportation authority may alternatively or additionally be able to control when OTA messages are sent so that, if it is notified that the mobile terminal 1 incorporating the near field tag 41 has been stolen, that authority can permanently or temporarily deactivate the near field tag 41. Waters at [Page 12] In an alternative embodiment, the SIM 15 activates and deactivates the tag in dependence upon whether the SIM is authenticated with the mobile Waters at [Page 12] In another embodiment of the invention, the mobile terminal and/or near field tag 41 is provided with means for disabling the tag 41 without requiring communication between the mobile terminal 1 and the mobile telecommunications network 3 (and therefore without requiring receipt of an OTA message). Waters at [Page 13] The near field tag 41 may be selectively enabled and disabled in order to reduce the opportunity to obtain information from the near field tag 41 by an unauthorised reader. Waters at [Page 13] The following arrangements are useful if the near field tag 41 is to be enabled and disabled for fairly long periods of time:
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	Waters at [Page 14] (1) Personal identification number (PESf) entry - the keypad 37 of the mobile terminal 1 is used to enter a PIN (or other secret password) to enable the near field tag 41. The user's PIN may be stored in a secure location in the mobile terminal 1 or in the SIM 15. When the user enters their PIN using the keypad 37, the entered PIN is compared with the stored PIN. If the PINs match, the SIM transmits a message, via link 43, to the near field tag 41 to activate the near field tag. Waters at [Page 14] (2) Biometric data entry - the mobile terminal 1 may incorporate a fingerprint reader 45. The fingerprint reader 45 scans the fingerprint of the user when the user's finger is placed on the reader 45 and compares it to the user's fingerprint stored in the memory of the mobile terminal 1 or the SIM 15. If the fingerprints are determined to match, the message is sent from the SIM 15, via link 43, to the RF tag 41. As an alternative to a fingerprint, other biometric data could be used - for example, voice recognition (using the mobile terminal's built-in microphone and a voice recognition algorithm within the mobile terminal 1 or SIM card 15) or retinal scanning (using the mobile terminal's built-in camera). Waters at [Page 14] Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 14]
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 15] (1) Light sensor - for example a photodiode (a sensor that modifies an electric current when exposed to a light source) could be built into the casing of the mobile terminal 1 and act as a switch to activate or deactivate the RF tag 41. The RF tag 41 is controlled by the photo diode so that the RF tag 41 is only enabled when the mobile terminal 1 is exposed to light. Therefore, when the mobile terminal 1 was in an opaque case or the user's pocket, the RF tag 41 will be disabled. The photodiode may be sensitive to a particular frequency range - for example visible light, infra red or ultra violet. The tag reader may be provided with a light emitter that emits light at this frequency, in order to activate the tag. Waters at [Page 15] (2) Pressure sensor - a pressure sensor on the casing of mobile terminal 1 acts as a switch. The RF tag 41 is only enabled when the user physically presses the pressure sensor. Therefore, when the mobile terminal is in a case or the user's pocket, the pressure sensor is disabled. The pressure sensor may itself be deactivated by the user, for example, when a function of the mobile terminal 1 is selected such that the keypad 37 is inoperative. The pressure sensor may be combined with the fingerprint scanner 45. The combined sensor detects, not only that pressure is applied, but also that an authorised person is pressing the sensor. Alternatively, the pressure sensor could be combined with an electrical resistance
--	--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	meter and used to detect that it is a human hand pressing the pressure sensor, rather than some other object. Waters at [Page 15] (3) Heat sensors - such sensors incorporated in an appropriate position on the casing of the mobile terminal 1 could be configured to detect that the mobile terminal is in a user's hand by detecting the heat from the hand, and only enabling the near field tag 41 when heat from the hand is so detected. Waters at [Page 15] (4) Skin resistance sensor - a skin resistance sensor may be provided on the casing of the mobile terminal 1 in dependence of the presence of the pressure sensor described above. The near field tag 41 will only be operated when an appropriate resistance, capacitance or inductance is detected, indicating that the user's hand is touching the sensor. Waters at [Page 15] (5) Inertial sensors. An inertial sensor incorporated in the mobile terminal can be used to detect that the user is moving the terminal (and tag 41) around at a sufficient speed to indicate that it is to be used. Inertial sensors may be based on micro-accelerators, which are commonly used in motion detectors - for example in gaming and virtual reality/remote control systems. Waters at [Page 15] A mobile terminal 1 may have any of the above arrangements implemented in any combination. For example, a manual entry system and an automatic entry system may be provided, respectively, to enable the card for short and long periods of use. Alternatively, the arrangements may work in parallel, and the near field tag 41 would be enabled only if the light sensor was activated and the correct PIN was entered (for example). Further, the arrangements may work in series - for example, the near field tag 41 would be enabled if the light sensor was activated and the correct PIN was subsequently entered. Waters at [Page 17]
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	The housing 52 may further optionally provide a display 58 for prompting the user to enter their PIN number and/or for displaying the PIN number as it is entered, if desired. On entry of the PIN number using the push buttons 56, the entered PIN number is compared to the PIN number stored on the SIM. If the PINs are found to match, communication between the SIM and the PC is permitted to authenticate one or more transactions. The comparison between the entered PIN number and the PIN number stored on the SIM 15 is performed within the dongle 50, and neither the entered PIN number nor the PIN number stored on the SIM is communicated to the PC. This prevents or reduces the likelihood that the PINs will become compromised by disclosure to an authorised party. Waters at [Page 18] Figure 5 shows a smart card 100 with an in-built near field tag including an inductive antenna 200, and a biometric system 120 for reading a finger print. The print is ideally compared to a previously taken print stored in the memory 130 of the smart card 100 or may just be judged as having the characteristics of a non-specific fingerprint. Waters at [Page 20] Apparatus for controlling use of a near field communication device, including smart card means associable with a mobile telecommunications network for authenticating the smart card means with the network, wherein the smart card means is operable to receive from the mobile telecommunications network data for controlling use of the near field communication device and is operable to selectively enable the near field communication device in dependence upon the data. [Claim 1] 2. The apparatus of claim 1, wherein the smart card means is operable to selectively enable the near field communication device by selectively enabling the near field communication device to be read by a reader
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

[Claim 2]

The apparatus of claim 7, 8 or 9, wherein the security data comprises a Personal Identification Number (PIN) and the apparatus includes means for comparing the PIN obtained by the security data entry means with a PIN stored on the apparatus and only enables operation of the near field device when the respective PINs match.

[Claim 10]

The apparatus of claim 7, wherein the security data entry means is operable to detect biometric data from a user.

[Claim 11]

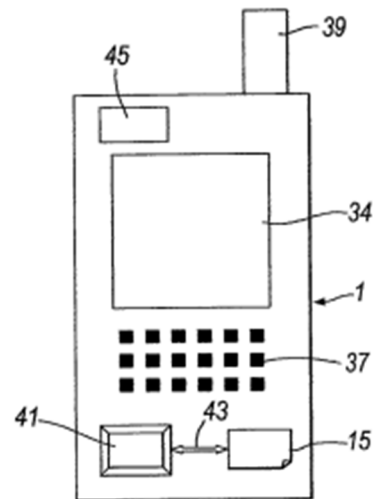


Fig.2

[Fig.2]

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[18.4]	wirelessly receiving information from the second device over said wireless link using unlicensed and/or licensed frequencies;	Waters discloses “wirelessly receiving information from the second device over said wireless link using unlicensed and/or licensed frequencies;” See e.g.: A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] As shown in Figure 2, mobile terminal 1 in accordance with the embodiment includes, in addition to SIM 15, a display 34, keypad 37 and an antenna 39 for communicating wirelessly with the mobile communications network 3. Further, the mobile terminal 1 includes a near field or RFID tag 41. The near field tag 41 operates in the unregulated RF band of 13.56 MHz in this embodiment although other frequencies could be used. No licences are required for the use of the near field devices in this RF band. However, each country imposes certain limitations on the electromagnetic emissions in this RF band. Limitations mean that in

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	practice the distance at which the near field tag 41 can communicate with another device is typically less than 20 centimeters. Often the range of communication is such that the RF tag 41 must touch or almost touch the device with which it is to communicate. Communication may be using the Near Field Communication Interface and Protocol (NFCIP-I). Waters at [Page 08] The near field tag 41 may operate in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards. The tag 41 includes an inbuilt inductive antenna that allows the card to exchange information with a tag reader when the two are brought into close proximity, as described above. The reader may emit an RF signal to supply power to the tag to communicate with it if the tag is "passive". If the tag is "active" it will have a power supply and its operation is independently of the reader. The near field tag 41 may transmit selected information, such as an ID number (GU ID). Waters at [Page 09] In order to improve the security of the near field tag, in the present embodiment it is proposed to use the SIM 15 of mobile terminal 1 to control to some extent the operation of the near field tag 41. The authentication process of a SIM 15 with a mobile telecommunications network, using the network's authentication processor 17 is considered to be highly secure. In this embodiment, this authentication of the SIM 15 is used to protect data held by the memory of the near field tag 41 from unauthorised access. Waters at [Page 09] According to an important feature of this embodiment, the near field tag 41 is selectively enabled or disabled for communication with the reader under control of the SIM 15, by means of communication link 43. By means of the link 43, the SIM can enable or disable the near field tag 41 by, for example, rendering its antenna inoperative. In the disabled state, a reader is not able to obtain any information from the near field tag 41, even when brought into close proximity
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	thereto (within a range that, in normal circumstances, near field communication would be possible). Waters at [Page 09] In the second example, a user wishes to use the near field tag 41 of the mobile terminal 1 to pay for travel by public transport (for example on the London Underground), where entry barriers are equipped with a suitable near field tag reader. Because the commuter travels at particular, consistent times of day, it is desirable to enable the near field tag 41 only at those times, in order to provide improved security. When so configured, if the mobile terminal 1 incorporating the near field tag 41 were stolen, the thief would not be able to pay for use of public transport using the near field tag 41 outside the times specified. Waters at [Page 11] The mobile telecommunications network 3 is configured to transmit an OTA message to the mobile terminal 1 at the beginning of the time period during which the commuter begins their normal journey. As before, this message is received and interpreted by the SIM, which sends an instruction to enable the near field tag 41 via the link 43. The near field tag 41 is then able to communicate with readers to allow use of public transport. At the end of the time period during which the commuter completes their usual journey, a second OTA message is sent by the network 3 to the mobile terminal 1. This OTA message is received and interpreted by the SIM 15, and sends an appropriate deactivation instruction to the RF tag 41 via the link 43. The near field tag 41 is thereafter not able to allow the user to obtain access to public transport. Waters at [Page 11] A similar arrangement could be used, for example, to enable a school child to pay for their lunch using the near field tag 41. OTA messages would be sent at the beginning and the end of the school lunch time so that the near field tag 41 could only be used to make a payment during the appropriate time. Waters at [Page 11]
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	The times at which, and the circumstances in which, the OTA messages are sent by the mobile telecommunications network 3 to the user's SIM card 15 may be set by the user of the mobile terminal 1. For example, the user of the mobile terminal 1 may initiate a communication session (such as a SIP communication session) with the mobile telecommunications network 1 to configure the times or places in which the RF tag 41 should be enabled. This updating process may require entry of a password, or employ some other security mechanism, to prevent unauthorised persons from reconfiguring the times and/or locations at which the near field tag is rendered operable or inoperable. Alternatively, the user may configure the times and/or locations at which the OTA messages are sent by some other mechanism - for example, by providing verbal instructions to the operator of mobile telecommunications network 3 by a mobile or PSTN telephone call, or by visiting the website of the mobile telecommunications network operator (whether using the mobile terminal or independently thereof using a PC connected to the Internet). Waters at [Page 12] Rather than the user of the mobile terminal 1 determining when/where the RF tag 41 is activated, this may be determined by the mobile telecommunications network 3 or some other entity. For example, a school child's parent may set the times during which the school child is able to use their RF tag to make payments, in the example given above relating to paying for a school lunch. In the example given above relating to payment for public transport, the public transportation authority may alternatively or additionally be able to control when OTA messages are sent so that, if it is notified that the mobile terminal 1 incorporating the near field tag 41 has been stolen, that authority can permanently or temporarily deactivate the near field tag 41. Waters at [Page 12] In an alternative embodiment, the SIM 15 activates and deactivates the tag in dependence upon whether the SIM is authenticated with the mobile Waters at [Page 12]
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	In another embodiment of the invention, the mobile terminal and/or near field tag 41 is provided with means for disabling the tag 41 without requiring communication between the mobile terminal 1 and the mobile telecommunications network 3 (and therefore without requiring receipt of an OTA message). Waters at [Page 13] The near field tag 41 may be selectively enabled and disabled in order to reduce the opportunity to obtain information from the near field tag 41 by an unauthorised reader. Waters at [Page 13] The following arrangements are useful if the near field tag 41 is to be enabled and disabled for fairly long periods of time: Waters at [Page 14] (1) Personal identification number (PESf) entry - the keypad 37 of the mobile terminal 1 is used to enter a PIN (or other secret password) to enable the near field tag 41. The user's PIN may be stored in a secure location in the mobile terminal 1 or in the SIM 15. When the user enters their PIN using the keypad 37, the entered PIN is compared with the stored PIN. If the PINs match, the SIM transmits a message, via link 43, to the near field tag 41 to activate the near field tag. Waters at [Page 14] (2) Biometric data entry - the mobile terminal 1 may incorporate a fingerprint reader 45. The fingerprint reader 45 scans the fingerprint of the user when the user's finger is placed on the reader 45 and compares it to the user's fingerprint stored in the memory of the mobile terminal 1 or the SIM 15. If the fingerprints are determined to match, the message is sent from the SIM 15, via link 43, to the RF tag 41. As an alternative to a fingerprint, other biometric data could be used - for example, voice recognition (using the mobile terminal's built-in microphone
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	and a voice recognition algorithm within the mobile terminal 1 or SIM card 15) or retinal scanning (using the mobile terminal's built-in camera). Waters at [Page 14] Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 14] Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 15] (1) Light sensor - for example a photodiode (a sensor that modifies an electric current when exposed to a light source) could be built into the casing of the mobile terminal 1 and act as a switch to activate or deactivate the RF tag 41. The RF tag 41 is controlled by the photo diode so that the RF tag 41 is only enabled when the mobile terminal 1 is exposed to light. Therefore, when the mobile
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	terminal 1 was in an opaque case or the user's pocket, the RF tag 41 will be disabled. The photodiode may be sensitive to a particular frequency range - for example visible light, infra red or ultra violet. The tag reader may be provided with a light emitter that emits light at this frequency, in order to activate the tag. Waters at [Page 15] (2) Pressure sensor - a pressure sensor on the casing of mobile terminal 1 acts as a switch. The RF tag 41 is only enabled when the user physically presses the pressure sensor. Therefore, when the mobile terminal is in a case or the user's pocket, the pressure sensor is disabled. The pressure sensor may itself be deactivated by the user, for example, when a function of the mobile terminal 1 is selected such that the keypad 37 is inoperative. The pressure sensor may be combined with the fingerprint scanner 45. The combined sensor detects, not only that pressure is applied, but also that an authorised person is pressing the sensor. Alternatively, the pressure sensor could be combined with an electrical resistance meter and used to detect that it is a human hand pressing the pressure sensor, rather than some other object. Waters at [Page 15] (3) Heat sensors - such sensors incorporated in an appropriate position on the casing of the mobile terminal 1 could be configured to detect that the mobile terminal is in a user's hand by detecting the heat from the hand, and only enabling the near field tag 41 when heat from the hand is so detected. Waters at [Page 15] (4) Skin resistance sensor - a skin resistance sensor may be provided on the casing of the mobile terminal 1 in dependence of the presence of the pressure sensor described above. The near field tag 41 will only be operated when an appropriate resistance, capacitance or inductance is detected, indicating that the user's hand is touching the sensor. Waters at [Page 15]
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	(5) Inertial sensors. An inertial sensor incorporated in the mobile terminal can be used to detect that the user is moving the terminal (and tag 41) around at a sufficient speed to indicate that it is to be used. Inertial sensors may be based on micro-accelerators, which are commonly used in motion detectors - for example in gaming and virtual reality/remote control systems. Waters at [Page 15] A mobile terminal 1 may have any of the above arrangements implemented in any combination. For example, a manual entry system and an automatic entry system may be provided, respectively, to enable the card for short and long periods of use. Alternatively, the arrangements may work in parallel, and the near field tag 41 would be enabled only if the light sensor was activated and the correct PIN was entered (for example). Further, the arrangements may work in series - for example, the near field tag 41 would be enabled if the light sensor was activated and the correct PIN was subsequently entered. Waters at [Page 17] The housing 52 may further optionally provide a display 58 for prompting the user to enter their PIN number and/or for displaying the PIN number as it is entered, if desired. On entry of the PIN number using the push buttons 56, the entered PIN number is compared to the PIN number stored on the SIM. If the PINs are found to match, communication between the SIM and the PC is permitted to authenticate one or more transactions. The comparison between the entered PIN number and the PIN number stored on the SIM 15 is performed within the dongle 50, and neither the entered PIN number nor the PIN number stored on the SIM is communicated to the PC. This prevents or reduces the likelihood that the PINs will become compromised by disclosure to an authorised party. Waters at [Page 18] Figure 5 shows a smart card 100 with an in-built near field tag including an inductive antenna 200, and a biometric system 120 for reading a finger print. The print is ideally compared to a previously taken print stored in the memory 130 of
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		the smart card 100 or may just be judged as having the characteristics of a non-specific fingerprint. Waters at [Page 20] Apparatus for controlling use of a near field communication device, including smart card means associable with a mobile telecommunications network for authenticating the smart card means with the network, wherein the smart card means is operable to receive from the mobile telecommunications network data for controlling use of the near field communication device and is operable to selectively enable the near field communication device in dependence upon the data. [Claim 1] 2. The apparatus of claim 1, wherein the smart card means is operable to selectively enable the near field communication device by selectively enabling the near field communication device to be read by a reader [Claim 2] The apparatus of claim 7, 8 or 9, wherein the security data comprises a Personal Identification Number (PIN) and the apparatus includes means for comparing the PIN obtained by the security data entry means with a PIN stored on the apparatus and only enables operation of the near field device when the respective PINs match. [Claim 10] The apparatus of claim 7, wherein the security data entry means is operable to detect biometric data from a user. [Claim 11]
--	--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

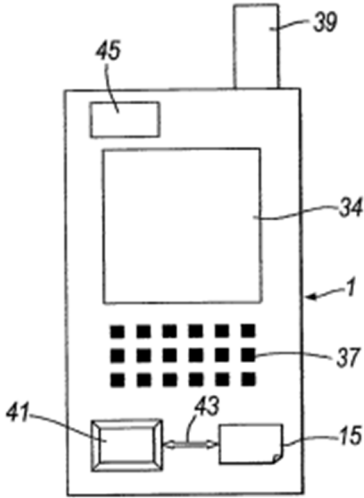
		 Fig.2 [Fig.2] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[18.5]	wherein said wirelessly transmitting and/or said wirelessly receiving comprises using an orthogonal frequency division multiplexing and/or orthogonal frequency	Waters discloses “wherein said wirelessly transmitting and/or said wirelessly receiving comprises using an orthogonal frequency division multiplexing and/or orthogonal frequency division multiple access protocol; and” See e.g.:

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	division multiple access protocol; and	A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract] As shown in Figure 2, mobile terminal 1 in accordance with the embodiment includes, in addition to SIM 15, a display 34, keypad 37 and an antenna 39 for communicating wirelessly with the mobile communications network 3. Further, the mobile terminal 1 includes a near field or RFID tag 41. The near field tag 41 operates in the unregulated RF band of 13.56 MHz in this embodiment although other frequencies could be used. No licences are required for the use of the near field devices in this RF band. However, each country imposes certain limitations on the electromagnetic emissions in this RF band. Limitations mean that in practice the distance at which the near field tag 41 can communicate with another device is typically less than 20 centimeters. Often the range of communication is such that the RF tag 41 must touch or almost touch the device with which it is to communicate. Communication may be using the Near Field Communication Interface and Protocol (NFCIP-I). Waters at [Page 08] The near field tag 41 may operate in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards. The tag 41 includes an inbuilt inductive antenna that allows the card to exchange information with a tag reader when the two are brought into
--	---	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	close proximity, as described above. The reader may emit an RF signal to supply power to the tag to communicate with it if the tag is "passive". If the tag is "active" it will have a power supply and its operation is independently of the reader. The near field tag 41 may transmit selected information, such as an ID number (GU ID). Waters at [Page 09] In order to improve the security of the near field tag, in the present embodiment it is proposed to use the SIM 15 of mobile terminal 1 to control to some extent the operation of the near field tag 41. The authentication process of a SIM 15 with a mobile telecommunications network, using the network's authentication processor 17 is considered to be highly secure. In this embodiment, this authentication of the SIM 15 is used to protect data held by the memory of the near field tag 41 from unauthorized access. Waters at [Page 09] According to an important feature of this embodiment, the near field tag 41 is selectively enabled or disabled for communication with the reader under control of the SIM 15, by means of communication link 43. By means of the link 43, the SIM can enable or disable the near field tag 41 by, for example, rendering its antenna inoperative. In the disabled state, a reader is not able to obtain any information from the near field tag 41, even when brought into close proximity thereto (within a range that, in normal circumstances, near field communication would be possible). Waters at [Page 09] In the second example, a user wishes to use the near field tag 41 of the mobile terminal 1 to pay for travel by public transport (for example on the London Underground), where entry barriers are equipped with a suitable near field tag reader. Because the commuter travels at particular, consistent times of day, it is desirable to enable the near field tag 41 only at those times, in order to provide improved security. When so configured, if the mobile terminal 1 incorporating
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	the near field tag 41 were stolen, the thief would not be able to pay for use of public transport using the near field tag 41 outside the times specified. Waters at [Page 11] The mobile telecommunications network 3 is configured to transmit an OTA message to the mobile terminal 1 at the beginning of the time period during which the commuter begins their normal journey. As before, this message is received and interpreted by the SIM, which sends an instruction to enable the near field tag 41 via the link 43. The near field tag 41 is then able to communicate with readers to allow use of public transport. At the end of the time period during which the commuter completes their usual journey, a second OTA message is sent by the network 3 to the mobile terminal 1. This OTA message is received and interpreted by the SIM 15, and sends an appropriate deactivation instruction to the RF tag 41 via the link 43. The near field tag 41 is thereafter not able to allow the user to obtain access to public transport. Waters at [Page 11] A similar arrangement could be used, for example, to enable a school child to pay for their lunch using the near field tag 41. OTA messages would be sent at the beginning and the end of the school lunch time so that the near field tag 41 could only be used to make a payment during the appropriate time. Waters at [Page 11] The times at which, and the circumstances in which, the OTA messages are sent by the mobile telecommunications network 3 to the user's SIM card 15 may be set by the user of the mobile terminal 1. For example, the user of the mobile terminal 1 may initiate a communication session (such as a SIP communication session) with the mobile telecommunications network 1 to configure the times or places in which the RF tag 41 should be enabled. This updating process may require entry of a password, or employ some other security mechanism, to prevent unauthorized persons from reconfiguring the times and/or locations at which the near field tag is rendered operable or inoperable. Alternatively, the user may configure the times and/or locations at which the OTA messages are sent by
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	some other mechanism - for example, by providing verbal instructions to the operator of mobile telecommunications network 3 by a mobile or PSTN telephone call, or by visiting the website of the mobile telecommunications network operator (whether using the mobile terminal or independently thereof using a PC connected to the Internet). Waters at [Page 12] Rather than the user of the mobile terminal 1 determining when/where the RF tag 41 is activated, this may be determined by the mobile telecommunications network 3 or some other entity. For example, a school child's parent may set the times during which the school child is able to use their RF tag to make payments, in the example given above relating to paying for a school lunch. In the example given above relating to payment for public transport, the public transportation authority may alternatively or additionally be able to control when OTA messages are sent so that, if it is notified that the mobile terminal 1 incorporating the near field tag 41 has been stolen, that authority can permanently or temporarily deactivate the near field tag 41. Waters at [Page 12] In an alternative embodiment, the SIM 15 activates and deactivates the tag in dependence upon whether the SIM is authenticated with the mobile Waters at [Page 12] In another embodiment of the invention, the mobile terminal and/or near field tag 41 is provided with means for disabling the tag 41 without requiring communication between the mobile terminal 1 and the mobile telecommunications network 3 (and therefore without requiring receipt of an OTA message). Waters at [Page 13] The near field tag 41 may be selectively enabled and disabled in order to reduce the opportunity to obtain information from the near field tag 41 by an unauthorized reader.
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	Waters at [Page 13] The following arrangements are useful if the near field tag 41 is to be enabled and disabled for fairly long periods of time: Waters at [Page 14] (1) Personal identification number (PESf) entry - the keypad 37 of the mobile terminal 1 is used to enter a PIN (or other secret password) to enable the near field tag 41. The user's PIN may be stored in a secure location in the mobile terminal 1 or in the SIM 15. When the user enters their PIN using the keypad 37, the entered PIN is compared with the stored PIN. If the PINs match, the SIM transmits a message, via link 43, to the near field tag 41 to activate the near field tag. Waters at [Page 14] (2) Biometric data entry - the mobile terminal 1 may incorporate a fingerprint reader 45. The fingerprint reader 45 scans the fingerprint of the user when the user's finger is placed on the reader 45 and compares it to the user's fingerprint stored in the memory of the mobile terminal 1 or the SIM 15. If the fingerprints are determined to match, the message is sent from the SIM 15, via link 43, to the RF tag 41. As an alternative to a fingerprint, other biometric data could be used - for example, voice recognition (using the mobile terminal's built-in microphone and a voice recognition algorithm within the mobile terminal 1 or SIM card 15) or retinal scanning (using the mobile terminal's built-in camera). Waters at [Page 14] Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 14] Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 15] (1) Light sensor - for example a photodiode (a sensor that modifies an electric current when exposed to a light source) could be built into the casing of the mobile terminal 1 and act as a switch to activate or deactivate the RF tag 41. The RF tag 41 is controlled by the photo diode so that the RF tag 41 is only enabled when the mobile terminal 1 is exposed to light. Therefore, when the mobile terminal 1 was in an opaque case or the user's pocket, the RF tag 41 will be disabled. The photodiode may be sensitive to a particular frequency range - for example visible light, infra-red or ultra violet. The tag reader may be provided with a light emitter that emits light at this frequency, in order to activate the tag. Waters at [Page 15] (2) Pressure sensor - a pressure sensor on the casing of mobile terminal 1 acts as a switch. The RF tag 41 is only enabled when the user physically presses the pressure sensor. Therefore, when the mobile terminal is in a case or the user's pocket, the pressure sensor is disabled. The pressure sensor may itself be deactivated by the user, for example, when a function of the mobile terminal 1 is
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	selected such that the keypad 37 is inoperative. The pressure sensor may be combined with the fingerprint scanner 45. The combined sensor detects, not only that pressure is applied, but also that an authorized person is pressing the sensor. Alternatively, the pressure sensor could be combined with an electrical resistance meter and used to detect that it is a human hand pressing the pressure sensor, rather than some other object. Waters at [Page 15] (3) Heat sensors - such sensors incorporated in an appropriate position on the casing of the mobile terminal 1 could be configured to detect that the mobile terminal is in a user's hand by detecting the heat from the hand, and only enabling the near field tag 41 when heat from the hand is so detected. Waters at [Page 15] (4) Skin resistance sensor - a skin resistance sensor may be provided on the casing of the mobile terminal 1 in dependence of the presence of the pressure sensor described above. The near field tag 41 will only be operated when an appropriate resistance, capacitance or inductance is detected, indicating that the user's hand is touching the sensor. Waters at [Page 15] (5) Inertial sensors. An inertial sensor incorporated in the mobile terminal can be used to detect that the user is moving the terminal (and tag 41) around at a sufficient speed to indicate that it is to be used. Inertial sensors may be based on micro-accelerators, which are commonly used in motion detectors - for example in gaming and virtual reality/remote control systems. Waters at [Page 15] A mobile terminal 1 may have any of the above arrangements implemented in any combination. For example, a manual entry system and an automatic entry system may be provided, respectively, to enable the card for short and long periods of use. Alternatively, the arrangements may work in parallel, and the near field tag 41 would be enabled only if the light sensor was activated and the
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	correct PIN was entered (for example). Further, the arrangements may work in series - for example, the near field tag 41 would be enabled if the light sensor was activated and the correct PIN was subsequently entered. Waters at [Page 17] The housing 52 may further optionally provide a display 58 for prompting the user to enter their PIN number and/or for displaying the PIN number as it is entered, if desired. On entry of the PIN number using the push buttons 56, the entered PIN number is compared to the PIN number stored on the SIM. If the PINs are found to match, communication between the SIM and the PC is permitted to authenticate one or more transactions. The comparison between the entered PIN number and the PIN number stored on the SIM 15 is performed within the dongle 50, and neither the entered PIN number nor the PIN number stored on the SIM is communicated to the PC. This prevents or reduces the likelihood that the PINs will become compromised by disclosure to an authorized party. Waters at [Page 18] Figure 5 shows a smart card 100 with an in-built near field tag including an inductive antenna 200, and a biometric system 120 for reading a finger print. The print is ideally compared to a previously taken print stored in the memory 130 of the smart card 100 or may just be judged as having the characteristics of a non-specific fingerprint. Waters at [Page 20] Apparatus for controlling use of a near field communication device, including smart card means associable with a mobile telecommunications network for authenticating the smart card means with the network, wherein the smart card means is operable to receive from the mobile telecommunications network data for controlling use of the near field communication device and is operable to selectively enable the near field communication device in dependence upon the data. [Claim 1]
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

2. The apparatus of claim 1, wherein the smart card means is operable to selectively enable the near field communication device by selectively enabling the near field communication device to be read by a reader

[Claim 2]

The apparatus of claim 7, 8 or 9, wherein the security data comprises a Personal Identification Number (PIN) and the apparatus includes means for comparing the PIN obtained by the security data entry means with a PIN stored on the apparatus and only enables operation of the near field device when the respective PINs match.

[Claim 10]

The apparatus of claim 7, wherein the security data entry means is operable to detect biometric data from a user.

[Claim 11]

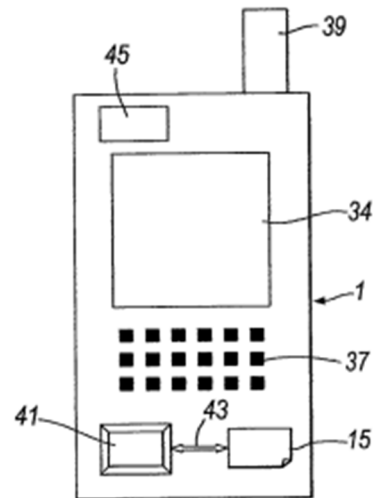


Fig. 2

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		[Fig.2] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
[18.6]	wherein said establishing by the wireless device a link with the second device comprises establishing the link with the second device responsive to the wireless device sensing the parameter and determining that the value sensed satisfies the threshold criterion.	Waters discloses “wherein said establishing by the wireless device a link with the second device comprises establishing the link with the second device responsive to the wireless device sensing the parameter and determining that the value sensed satisfies the threshold criterion.” See e.g.: [4.2], [11.8], [17.6], supra. A mobile terminal is disclosed which includes a near field or RF ID tag (41). The mobile terminal (1) communicates with the mobile telecommunications network and is authenticated with that network using the SIM (15). The mobile terminal (1) is operable to obtain security data from the user thereof, such as a PIN or biometric data, or the mobile terminal (1) incorporates a sensor such as a light sensor, pressure sensor, heat sensor, skin resistant sensor or inertial sensor. The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment or obtain entry to a building (for example). Data from the sensor is passed to the SIM (15), which issues a command enabling the near field tag (41), via link (43). The near field tag (41) may then be read by a reader. The near field tag (41) may be automatically disabled after being read by the reader, after a predetermined time, or when the stimulus to the sensor is no longer present. Waters at [Abstract]

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	The near field tag 41 may operate in accordance with ISO-IEC 14443 and ISO-IEC 15693 standards. The tag 41 includes an inbuilt inductive antenna that allows the card to exchange information with a tag reader when the two are brought into close proximity, as described above. The reader may emit an RF signal to supply power to the tag to communicate with it if the tag is "passive". If the tag is "active" it will have a power supply and its operation is independently of the reader. The near field tag 41 may transmit selected information, such as an ID number (GU ID). Waters at [Page 09] In order to improve the security of the near field tag, in the present embodiment it is proposed to use the SIM 15 of mobile terminal 1 to control to some extent the operation of the near field tag 41. The authentication process of a SIM 15 with a mobile telecommunications network, using the network's authentication processor 17 is considered to be highly secure. In this embodiment, this authentication of the SIM 15 is used to protect data held by the memory of the near field tag 41 from unauthorised access. Waters at [Page 09] Conveniently, the SIM 15 is provided with data which controls operation of the near field tag 41 by receiving an OTA message, which is sent to the mobile terminal 1 from the mobile telecommunications network 3 (via the OTA gateway 30 and SMSC 32). As described above, the OTA update message is received by the mobile terminal 1 and it is determined that this is an updating OTA update message rather than a conventional SMS message. The message is then passed to the SIM 15 for processing. Upon processing of the message, commands contained within that message are executed, causing the desired control of the RF tag 41 via the link 43. Waters at [Page 10] In a first example, it is desired to only enable the near field tag 41 to communicate with the reader when it is in the vicinity of the user's office (where entry is obtained using the near field tag 41). The SMSC 32 may send an OTA
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	update message to the node B 5 associated with the cell or group of cells in which the user's office is located. When the mobile terminal 1 enters a cell in the group, the node B transmits the OTA message to the mobile terminal 1. The procedure described above is applied, and the OTA message is passed to the SIM 15 and the instructions therein are processed. A command is sent to the near field tag 41 via link 43 to activate the near field tag (for example, by allowing its antenna to communicate with the reader). When the mobile terminal 1 moves to a different cell, a command is sent from the SIM 15, via the link 43, to disable the near field tag 41. This command may be issued in response to a further OTA message being received from the network 3 when the mobile terminal 1 moves to a different cell, or movement to a different cell may be detected automatically by the SIM (or the mobile terminal 1) and used to generate an appropriate command for sending to the near field tag 41. Waters at [Page 10] In the second example, a user wishes to use the near field tag 41 of the mobile terminal 1 to pay for travel by public transport (for example on the London Underground), where entry barriers are equipped with a suitable near field tag reader. Because the commuter travels at particular, consistent times of day, it is desirable to enable the near field tag 41 only at those times, in order to provide improved security. When so configured, if the mobile terminal 1 incorporating the near field tag 41 were stolen, the thief would not be able to pay for use of public transport using the near field tag 41 outside the times specified. Waters at [Page 11] The mobile telecommunications network 3 is configured to transmit an OTA message to the mobile terminal 1 at the beginning of the time period during which the commuter begins their normal journey. As before, this message is received and interpreted by the SIM, which sends an instruction to enable the near field tag 41 via the link 43. The near field tag 41 is then able to communicate with readers to allow use of public transport. At the end of the time period during which the commuter completes their usual journey, a second OTA message is sent by the network 3 to the mobile terminal 1. This OTA message is
--	---

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	received and interpreted by the SIM 15, and sends an appropriate deactivation instruction to the RF tag 41 via the link 43. The near field tag 41 is thereafter not able to allow the user to obtain access to public transport. Waters at [Page 11] A similar arrangement could be used, for example, to enable a school child to pay for their lunch using the near field tag 41. OTA messages would be sent at the beginning and the end of the school lunch time so that the near field tag 41 could only be used to make a payment during the appropriate time. Waters at [Page 11] The times at which, and the circumstances in which, the OTA messages are sent by the mobile telecommunications network 3 to the user's SIM card 15 may be set by the user of the mobile terminal 1. For example, the user of the mobile terminal 1 may initiate a communication session (such as a SIP communication session) with the mobile telecommunications network 1 to configure the times or places in which the RF tag 41 should be enabled. This updating process may require entry of a password, or employ some other security mechanism, to prevent unauthorised persons from reconfiguring the times and/or locations at which the near field tag is rendered operable or inoperable. Alternatively, the user may configure the times and/or locations at which the OTA messages are sent by some other mechanism - for example, by providing verbal instructions to the operator of mobile telecommunications network 3 by a mobile or PSTN telephone call, or by visiting the website of the mobile telecommunications network operator (whether using the mobile terminal or independently thereof using a PC connected to the Internet). Waters at [Page 12] The following arrangements are useful if the near field tag 41 is to be enabled and disabled for fairly long periods of time: (1) Personal identification number (PIN) entry - the keypad 37 of the mobile terminal 1 is used to enter a PIN (or other secret password) to enable the near field tag 41. The user's PIN may be stored in a secure location in the mobile
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

	terminal 1 or in the SIM 15. When the user enters their PIN using the keypad 37, the entered PIN is compared with the stored PIN. If the PINs match, the SIM transmits a message, via link 43, to the near field tag 41 to activate the near field tag. Waters at [Page 14] (2) Biometric data entry - the mobile terminal 1 may incorporate a fingerprint reader 45. The fingerprint reader 45 scans the fingerprint of the user when the user's finger is placed on the reader 45 and compares it to the user's fingerprint stored in the memory of the mobile terminal 1 or the SIM 15. If the fingerprints are determined to match, the message is sent from the SIM 15, via link 43, to the RF tag 41. As an alternative to a fingerprint, other biometric data could be used - for example, voice recognition (using the mobile terminal's built-in microphone and a voice recognition algorithm within the mobile terminal 1 or SIM card 15) or retinal scanning (using the mobile terminal's built-in camera). Waters at [Page 14] Arrangements (1) and (2) above may advantageously be combined with an RF tag 41 that automatically deactivates after it has been read by a reader. That is, the user will activate the RF tag by entering their PIN or biometric data prior to bringing the mobile terminal 1 into proximity to the reader. After successful reading of the RF tag 41, the RF tag automatically disables itself so that no further reading can occur without the PIN or biometric data being re-entered. If the mobile terminal 1 is lost or stolen, an unauthorised person cannot use the RF tag 41. Arrangements (1) and (2) above are fairly inconvenient if a user wishes to activate their RF tag 41 fairly frequently. The following arrangements may be more convenient when relatively frequent activation of the RF tag 41 is required: Waters at [Page 14] Furthermore, this claim element is obvious in light of Waters itself, when combined with any of the other references as charted for this claim element in Exs. 756-A01-A23, Ex. 756-B, and/or when combined with the knowledge of one of ordinary skill
--	--

Exhibit 756-A16
Invalidity Chart for U.S. Patent No. 11,770,756 In View of Waters

		in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in the Cover Pleading and Ex. 756-B.
--	--	---