35. Verifying A Bank Customer's Identity To Permit An ATM Transaction

The following fact pattern and claims are hypothetical. Assume that the claims are presented in a recently filed application that is under examination and thus each claim is given its broadest reasonable interpretation in view of the specification as it would be understood by one of ordinary skill in the art. In this example, the terms in the claim are given their plain meaning in the art because no special definitions have been set forth in the specification. An abbreviated version of the hypothetical specification is provided below. Claim 1 is ineligible, because it is directed to an abstract idea and does not recite additional elements that amount to significantly more. Claims 2 and 3 are directed to the same abstract idea, but are eligible because they have additional elements that amount to significantly more than the abstract idea (i.e., provide an inventive concept) because they implement the abstract idea with specific meaningful limitations. This example was published in December 2016 as part of a set of business method examples.

Background

Financial institutions routinely provide automated teller machines (ATMs) for customers to conduct banking transactions at convenient locations other than brick-and-mortar banks, and without the need to interact with a bank teller. Typical ATMs include a customer interface with a keypad, function key, display, outlet slot for statements or other information, cash dispenser slot, deposit inlet, and often a speaker to provide customer voice guidance and a camera to monitor transactions. A reader is provided for customers to present data bearing records, which can include data corresponding to the customer, financial accounts, or other data, and are commonly embodied as a bank card with a magnetic strip or a contactless card with a radio frequency identification (RFID) tag. Other input devices, such as a biometric reader to receive customer identifying inputs such as fingerprints, iris scans, and face topography data, a camera, or speech recognition device, used to identify a user can be provided as well. The customer interface is coupled to a controller with a processor and memory and a network communicator to enable communication between the controller and a financial institution to exchange information about the transactions. To conduct a transaction, a customer typically inserts a bank card into the appropriate slot in the ATM and inputs a personal identification number (PIN) that verifies that the user is an authorized user for the bank account associated with the bank card. The account data is read from the card using the reader in the ATM and the PIN associated with the card. The network communicator transmits the read data and PIN to a remote computer at the financial institution, which then transmits instructions back to the ATM regarding authorization to carry out the requested transaction.

Due to its speed and convenience, the use of ATMs to conduct banking business has become ubiquitous, but so have problems with theft and fraud. For example, if another person illegally or fraudulently obtains a user's PIN, that person can gain access to funds in the account. Another problem associated with ATMs is "skimming" where a false card reader that appears to be a legitimate reader is affixed to an ATM to obtain an authorized user's account information and PIN. In skimming operations, an authorized user unwittingly presents their bank card to the skimming device on the ATM and enters their PIN, which is then captured and stored for subsequent fraudulent activity.

There have been various solutions attempting to reduce the instance of fraud associated with ATMs and to improve security when verifying an authorized user. For example, some bank cards are provided with chips that interact with a special reader to generate a unique transaction number each time a transaction is conducted to reduce the chance that a user's account information and PIN can be stolen for later use (so-called "chip and pin" cards). Bank cards have also been outfitted with RFID tags or "smart labels" (non-contact transponders) that allow account information to be transmitted to an ATM without inserting the card into the machine, and thus exposing it to theft or skimming.

The smart label can contain various types of customer information, including profile data, preferences, and unique customer identification data. To conduct a transaction using such a contactless card, the customer brings the card into range of an ATM reader, which uses radio frequencies to interrogate the smart label to receive information about the customer. The interrogation can be encrypted to provide additional security. The customer can then start a transaction, *e.g*., by pressing an enter key on the ATM. While such cards can prevent fraud based on skimming, these non-contact cards have given rise to other security issues, such as allowing a malicious person to obtain card information by use of an unauthorized RFID reader.

Applicant has invented a method of ensuring secure transmission of data from a card using a smart label and encryption techniques. The invention leverages the wide-spread use of mobile personal communication devices (smart phones) to facilitate the secure transmission. When a customer is issued a bank card with a smart label, the financial institution also provides a downloadable software application to the customer to install on their mobile communication device. The software application is designed to assist communication with a specially outfitted ATM.

The ATM in accordance with this invention includes a controller that is programmed with a time-variant random code generator. The code generator generates a random code when activated in response to the reader receiving data from the customer's bank card. In other words, when the customer is within a certain range of the ATM with their bank card, the smart label is read from the RFID reader in the ATM, which signals the code generator to generate a time-variant random code, which can be a plurality of digits, numbers and/or letters. The ATM then provides the random code to the customer. In one embodiment, the ATM provides the random code by displaying it. The customer is prompted to enter the displayed code into their mobile device, which already has the institutional software installed. In another embodiment, the random code is transmitted by the ATM to the customer's mobile device, *e.g*., by a near-field communication or Bluetooth link, if the customer has installed the institutional software on their mobile device and registered their mobile device with the institution.

The software provided by the institution generates data in response to the random code, which may be, *e.g*., a customer confirmation code or an encryption that includes the code data and the card's data. The software then causes the mobile device to communicate the responsive data to the ATM. In one embodiment, the mobile device displays the encrypted data as an image on its display screen. The image can be machine readable data in the form of a bar code or an image such as a colored pattern. The customer is prompted to allow the ATM to scan the image displayed by the mobile device. The reader of the ATM reads the encrypted image and verifies that it is authentic by, for example, determining if it is readable, recognizable, or properly formatted. Once verified, the processor in the ATM decrypts the data and confirms that the decrypted code matches the random code that was generated for the current transaction session. In another embodiment, the customer confirmation code is obtained by the ATM (*e.g*., by transmission over near-field communication or Bluetooth link), and the ATM then confirms that the customer confirmation code matches the random code. The outcome of the comparison between the responsive code data (*e.g*., the decrypted code or the customer confirmation code) and the random code is used to control access to the keypad. In particular, if the responsive code data and the generated code match and the elapsed time is within a certain time frame, the transaction is continued in conventional fashion with the customer entering a PIN using the keypad. If the responsive code data and generated code do not match or the elapsed time exceeds the time frame, a signal is sent to lock the keypad so that any attempts at entering a PIN will be futile.

Applicant's method allows the ATM to receive user card data in a more secure and efficient manner. Customer card data entry begins before PIN entry and verification, so if the ATM user is not the authorized customer and does not have the appropriate verification software on their mobile device,

the transaction is concluded before entry of the PIN. This method prevents skimming and other techniques to fraudulently obtain a customer's PIN and even theft of the card since the downloaded software can authenticate the user and likewise authenticate the ATM before the PIN is produced.

Claims

1. A method of conducting a secure automated teller transaction with a financial institution by authenticating a customer's identity, comprising the steps of:

obtaining customer-specific information from a bank card,

comparing, by a processor, the obtained customer-specific information with customer information from the financial institution to verify the customer's identity, and

determining whether the transaction should proceed when a match from the comparison verifies the authenticity of the customer's identity.

2. A method of conducting a secure automated teller transaction with a financial institution by authenticating a customer's identity, comprising the steps of:

obtaining customer-specific information from a bank card,

comparing, by a processor, the obtained customer-specific information with customer information from the financial institution to verify the customer's identity, by

generating a random code and transmitting it to a mobile communication device that is registered to the customer associated with the bank card,

reading, by the automated teller machine, an image from the customer's mobile communication device that is generated in response to receipt of the random code, wherein the image includes encrypted code data,

decrypting the code data from the read image, and

analyzing the decrypted code data from the read image and the generated code to determine if the decrypted code data from the read image matches the generated code data, and

determining whether the transaction should proceed when a match from the analysis verifies the authenticity of the customer's identity.

3. A method of conducting a secure automated teller transaction with a financial institution by authenticating a customer's identity, comprising the steps of:

obtaining customer-specific information from a bank card,

comparing, by a processor, the obtained customer-specific information with customer information from the financial institution to verify the customer's identity, by

generating a random code and visibly displaying it on a customer interface of the automated teller machine,

obtaining, by the automated teller machine, a customer confirmation code from the customer's mobile communication device that is generated in response to the random code, and

determining whether the customer confirmation code matches the random code, and

automatically sending a control signal to an input for the automated teller machine to provide access to a keypad when a match from the analysis verifies the authenticity of the customer's identity, and to deny access to a keypad so that the transaction is terminated when the comparison results in no match.

Analysis

Claim 1: Ineligible

The claim recites a method of conducting a secure automated teller transaction comprising a series of steps. Thus, the claim is directed to a process, which is a statutory category of invention (*Step 1: Yes*).

The claim is then analyzed to determine if the claim is directed to a judicial exception. The claim recites the steps of obtaining customer-specific information, comparing the obtained customer-specific information with customer information from the financial institution to authenticate the customer's identity, and determining whether the transaction should proceed when a match from the comparison verifies the authenticity of the customer's identity. These steps describe a method of fraud prevention by verifying the authenticity of the customer's identity prior to proceeding with a banking transaction, which is a "long prevalent" business practice that bank tellers have used for many years. Fraud prevention by verifying the identity of the customer is as fundamental to business as the economic concepts that were identified as abstract ideas by the Supreme Court, such as intermediated settlement (*Alice Corp.*) and risk hedging (*Bilski*). The claim as a whole is also similar to the claimed invention in *CyberSource*, which the Federal Circuit described as directed to an abstract mental process for detecting fraud by obtaining and comparing intangible data pertinent to business risks. The method of claim 1 similarly recites steps of obtaining and comparing data pertinent to business risks. More particularly, it describes a method of fraud prevention by authenticating a customer's identity. Therefore, claim 1 is directed to an abstract idea (*Step 2A: Yes*).

Next, the claim as a whole is analyzed to determine whether any element, or combination of elements, is sufficient to ensure the claim amounts to significantly more than the abstract idea. In addition to the steps that describe the abstract idea of preventing fraud through verifying a customer's identity, the claim recites the additional limitation of obtaining customer-specific information from a bank card. This additional element taken individually represents a conventional action of an ATM, as evidenced by the discussion of the prior art in the background specification. Further, the step is recited at a high level of generality such that it amounts to insignificant pre-solution activity, *e.g.*, a mere data gathering step necessary to use the abstract idea. The claim also recites the additional element of a processor comparing data. This processor is no more than a generic computer component, and the comparison performed by the processor does not represent any computer function beyond what processors typically perform. Taken individually therefore, the additional elements of claim 1 do not provide significantly more, *i.e.*, an inventive concept, to the claim.

Looking at the combination of elements in claim 1 also fails to show an inventive concept. Unlike the eligible claims in *Diehr* and *Bascom*, in which the elements limiting the exception were individually conventional but taken together provided an inventive concept because they improved a technical field, the claim here does not invoke any of the considerations that courts have identified as providing significantly more than an exception. The combination of elements is no more than the sum of their parts, and provides nothing more than mere automation of verification steps that were in years past performed mentally by tellers when engaging with a bank customer. Mere automation of an economic business practice does not provide significantly more (*i.e.*, provide an inventive concept). For these reasons, claim 1 is ineligible (*Step 2B: No*).

A rejection of claim 1 should identify the abstract idea by pointing to the language of the claim that describes fraud prevention by identity verification (*i.e.*, obtaining customer information, comparing the obtained customer information to customer information from a financial institution, and determining whether the transaction should proceed when a match from the comparison verifies the authenticity of the customer's identity) and explaining that fraud prevention by identity verification is similar to concepts that courts have previously found abstract. The rejection should identify the additional limitations regarding obtaining customer-specific information from a bank card and a processor that compares data, and explain why those limitations are conventional or are only generic computer components performing generic functions and are mere automation of economic business practices.

Claim 2: Eligible

The claim recites a method of conducting a secure automated teller transaction comprising a series of steps. Thus, the claim is directed to a process, which is a statutory category of invention (*Step 1: Yes*).

The claim is then analyzed to determine if the claim is directed to a judicial exception. Claim 2 recites steps of obtaining customer-specific information, comparing the obtained customer-specific information with customer information from the financial institution to authenticate the customer's identity, and determining whether the transaction should proceed when a match from the analysis verifies the authenticity of the customer's identity. Like the steps of obtaining and comparing customer information in claim 1, these steps in claim 2 describe a method of fraud prevention by identity verification before proceeding with a banking transaction, which as explained above is a fundamental business practice and is similar to ideas found abstract by the courts. Therefore, claim 2 is directed to an abstract idea (*Step 2A: Yes*).

Next, the claim as a whole is analyzed to determine whether any element, or combination of elements, is sufficient to ensure the claim amounts to significantly more than the abstract idea. In addition to the steps that describe the abstract idea of preventing fraud through identity verification, the claim recites the additional limitations of obtaining customer-specific information from a bank card, a processor comparing data, generating a random code and transmitting it to the customer's mobile communication device, and the processor reading an image that was generated by the customer's mobile communication device in response to receipt of the random code, where the image includes encrypted code data. The encrypted code data from the image is then used by the processor to verify the customer's identity by decrypting the code data and analyzing the decrypted code data. Considered individually, the steps of obtaining information from a bank card and the comparing data do not provide significantly more for the same reasons as in claim 1. Similarly, the processor and the mobile communication device are recited at a high level of generality and perform programmed functions that represent conventional and generic operations for these devices, including reading data, generating random codes, and analyzing data.

However, the ***combination*** of the steps (*e.g.*, the ATM providing a random code, the mobile communication device's generation of the image having encrypted code data in response to the random code, the ATM's decryption and analysis of the code data, and the subsequent determination of whether the transaction should proceed based on the analysis of the code data) operates in a non-conventional and non-generic way to ensure that the customer's identity is verified in a secure manner that is more than the conventional verification process employed by an ATM alone. In combination, these steps do not represent merely gathering data for comparison or security purposes, but instead set up a sequence of events that address unique problems associated with bank cards and ATMs (*e.g.*, the use of stolen or "skimmed" bank cards and/or customer information to perform unauthorized transactions). Thus, like in *BASCOM*, the claimed combination of additional

elements presents a specific, discrete implementation of the abstract idea. Further, the combination of obtaining information from the mobile communication device (instead of the ATM keypad) and using the image (instead of a PIN) to verify the customer's identity by matching identification information does not merely select information by content or source, in contrast to *Electric Power,* but instead describes a process that differs from the routine and conventional sequence of events normally conducted by ATM verification, such as entering a PIN, similar to the unconventional sequence of events in *DDR*. The additional elements in claim 2 thus represent significantly more (*i.e.,* provide an inventive concept) because they are a practical implementation of the abstract idea of fraud prevention that performs identity verification in a non-conventional and non-generic way, even though the steps use well-known components (a processor and mobile communication device). Claim 2 is eligible (*Step 2B: Yes*).

While an examiner would not be required to provide an explanation of eligibility, the record would be enhanced if clarifying remarks were provided to point to the reason for eligibility. In this instance, clarification could easily be made by simply pointing to the combination of elements used in the non-conventional implementation of identity verification in the method of fraud prevention.

Claim 3: Eligible

The claim recites a method of conducting a secure automated teller transaction comprising a series of steps. Thus, the claim is directed to a process, which is a statutory category of invention (*Step 1: Yes*).

The claim is then analyzed to determine if the claim is directed to a judicial exception. Claim 3 recites steps of obtaining customer-specific information, comparing the obtained customer-specific information with customer information from the financial institution to authenticate the customer's identity, and permitting the transaction to proceed when a match from the analysis verifies the authenticity of the customer's identity, and terminating the transaction when there is no match. Like the steps of obtaining and comparing customer information in claim 1, these steps in claim 3 describe a method of fraud prevention by identity verification before proceeding with a banking transaction, which as explained above is a fundamental business practice and is similar to ideas found abstract by the courts. Therefore, claim 3 is directed to an abstract idea (*Step 2A: Yes*).

Next, the claim as a whole is analyzed to determine whether any element, or combination of elements, is sufficient to ensure the claim amounts to significantly more than the abstract idea. In addition to the steps that describe the abstract idea of preventing fraud through identity verification, the claim recites the additional limitations of obtaining customer-specific information from a bank card, a processor comparing data, the ATM generating a random code and visibly displaying it on a customer interface, and the ATM obtaining a customer confirmation code that was generated by the customer's mobile communication device in response to the random code. The customer confirmation code is then used by the ATM to verify the customer's identity by analyzing the customer confirmation code with respect to the random code, and controlling the transaction by providing or preventing access to a keypad of the ATM based on the analysis of the code data. Considered individually, the ATM obtaining information from a bank card and the processor comparing data do not provide significantly more for the same reasons as in claim 1. Similarly, the ATM and the mobile communication device are recited at a high level of generality and perform programmed functions that represent conventional and generic operations for these devices, including reading data, generating random codes, and analyzing data.

However, the ***combination*** of the steps (*e.g*., the ATM's provision of the random code, the mobile communication device's generation of the customer confirmation code in response to the random code, the ATM's analysis of the customer confirmation code, and the ATM's subsequent sending of a

control signal to provide or prevent access to the keypad of the ATM and thus allow or prevent a transaction based on the analysis of the code data sets) operates in a non-conventional and non-generic way to ensure that the customer's identity is verified in a secure manner that is more than the conventional verification process employed by an ATM alone. In combination, these steps do not represent merely gathering data for comparison or security purposes, but instead set up a sequence of events that address unique problems associated with bank cards and ATMs (*e.g*., the use of stolen or "skimmed" bank cards and/or customer information to perform unauthorized transactions). Thus, like in *BASCOM*, the claimed combination of additional elements presents a specific, discrete implementation of the abstract idea. Further, the combination of obtaining information from the mobile communication device (instead of the ATM keypad) and using the customer confirmation code (instead of a PIN) to verify the customer's identity does not merely select information by content or source, in contrast to *Electric Power,* but instead describes a process that differs from the routine and conventional sequence of events normally conducted by ATM verification, such as entering a PIN, similar to the unconventional sequence of events in *DDR*. The additional elements in claim 3 thus represent significantly more (*i.e.,* provide an inventive concept) because they are a practical implementation of the abstract idea of fraud prevention that performs identity verification in a non-conventional and non-generic way, even though the steps use a combination of well-known components (an ATM and mobile communication device). Claim 3 is eligible (*Step 2B: Yes*).

While an examiner would not be required to provide an explanation of eligibility, the record would be enhanced if clarifying remarks were provided to point to the reason for eligibility. In this instance, clarification could easily be made by simply pointing to the combination of elements used in the non-conventional implementation of identity verification in the method of fraud prevention.