[0019] Clause 5: The method of any of clauses 1-4, further comprising calculating a confidence score indicative of a confidence that the name verification response is accurate.

[0020] Clause 6: The method of any of clauses 1-5, further comprising counting a number of identified records which include the at least one cardholder name that sufficiently matches the submitted cardholder name included in the cardholder name verification request, wherein calculating the confidence score is based at least partially on the number of identified records.

[0021] Clause 7: The method of any of clauses 1-6, wherein receiving the cardholder name verification request, querying the database to identify the one or more records, comparing the cardholder name, determining whether or not there is a sufficient match, and generating the name verification response are performed by at least one processor of the name verification server.

[0022] Clause 8: A system for verifying a cardholder name associated with a payment device used in connection with a card-not-present transaction, the system comprising: a database including a plurality of records pertaining to historically processed transactions, each record including an indication of a primary account number of a payment device and a cardholder name used to conduct a transaction to which the record pertains; and a name verification server comprising at least one processor, the name verification server programmed or configured to: receive a cardholder name verification request sent over a data communications network from a merchant server, the cardholder name verification request including a submitted primary account number of a payment device and a submitted cardholder name; query the database to identify one or more records that include an indication of a primary account number that matches the submitted primary account number included in the cardholder name verification request; compare at least one cardholder name in the identified one or more records to the submitted cardholder name included in the cardholder name verification request; make a determination whether or not there is a sufficient match resulting from the comparison; generate a name verification response, wherein a content of the name verification response is established at least partially based on the determination; and send the name verification response to the merchant server over the data communications network.

[0023] Clause 9: The system of clause 8, wherein the name verification server is further programmed or configured to update the database with an additional record,

[0060] With additional reference now to Fig. 3, there is shown an exemplary process by which (the NVS server 50, for example) generates the hash_ID from the received PAN, e.g., the process by which step 200 is carried out. More specifically, at sub-step 202 the PAN received in the request 42 is input into a suitable hash algorithm. At sub-step 204, a hash key 62 (see Fig. 1A) is retrieved from a secure cryptographic device 60 (see Fig. 1A). At sub-step 206, using the retrieved hash key 62, the hash algorithm is repeatedly applied a number of times, with the input PAN being this initial value to which the hash is applied and subsequent inputs being the preceding output of the algorithm. At sub-step 208, after the hash algorithm has been run for the given number of cycles, the final output is returned as the corresponding hash_ID for the initially input PAN.

[0061] Note, that while the present specification refers to a hash_ID and a particular exemplary process for producing the same, it is to be appreciated that in practice other methods and/or techniques may be used to obscure the PAN and/or generate a PAN "alias," e.g., in accordance with the Payment Card Industry (PCI) Security Standards promulgated by the PCI Security Standards Council and/or other such guidelines. Alternatively, in suitable circumstances (e.g., where data security is not a sufficient consideration and/or other suitably sufficient data security measures are enacted), the PAN itself may be employed unobscured.

[0062] Returning attention to Fig. 2, at step 400, the NVS server 50 conducts a search of the DB 52 for a hash_ID which matches the generated hash_ID corresponding to the PAN received in the request 42 being processed. If no suitable match is found, the NVS server 50 returns an appropriate response 44 to the merchant server 20 indicating, e.g., that the PAN is unrecognized or unknown. That is to say, the response 44 in this case indicates the NVS server 50 has not previously encountered the PAN in question.

[0063] If a suitable match is found in step 400, processing continues to step 500. At step 500, the cardholder name from the record with the matching hash_ID in the DB 52 and the cardholder name received in the request 42 being processed are compared to one another. Provided an identical match and/or sufficiently similar match is found with respect to the compared cardholder names, the NVS server 50 returns an appropriate response 44 to the merchant server 20 indicating, e.g., that the cardholder name in the request 42 is an exact or sufficiently similar match to the

recent transactions in the DB 52 may be given a relatively greater weight than relatively older transactions when the score is calculated.

[0066] In either case, at step 510, a final score generated by the scoring algorithm is output and delivered, e.g., to the merchant's server 20 along with the response 44. Suitably, the score may also be logged into a score warehouse or other data storage device for future reference and/or use. Optionally, the scores may be stored in the DB 52, e.g., along with the record for which the score was generated.

[0067] Returning attention now to Fig. 2, if at step 500 there is no exact match or no sufficiently similar match (e.g., between the cardholder name associated with the matching hash_ID in the DB 52 found in step 400 and the cardholder name received in the request 42 being processed), then the process continues to step 600. At step 600, it is determined if the cardholder name (while not sufficiently similar for an exact match) is still similar enough to warrant further processing. For example, if the cardholder name in the request 42 is "John Doe", while the name obtained from the DB 52 is "Jon G. Doe", it might be considered that there is not a sufficiently similarity to warrant a so-called "exact" or "sufficiently similar" designation in the response 44. However, there is still enough similarity to warrant further processing. That is to say, in the case of the middle initial, it was simply omitted in the one instance, and in the case of the first name, it was simply a typographical error.

[0068] In the case that the result of a comparison between the respective cardholder names in step 600 results in a determination that the names are too dissimilar to warrant further processing, the process branches to step 800. Otherwise, if it results in a determination that the compared cardholder names are still similar enough to warrant further processing, the process continues to step 700.

[0069] At step 700, alternate information and/or data is optionally compared and/or checked for sufficient matches. For example, such alternate information may include, without limitation: email addresses, telephone numbers, delivery or ship-to addresses and/or billing addresses, and/or other order fulfillment information which may have optionally been submitted along with the request 42 to the NVS server 50 from the merchant server 20. Likewise, in connection with previously processed requests, the aforementioned alternate data and/or information may have also likewise been supplied to the NVS server 50 and stored in the DB 52 along with the records created for previous transactions.

an indication of the submitted primary account number of a payment device included in the cardholder name verification request;

the submitted cardholder name included in the cardholder name verification request; and

the name verification response generated in reply to the name verification request.

4. The method of claim 1, wherein the name verification response indicates that the submitted cardholder name is valid when the determination is made that there is a sufficient match resulting from the comparing, otherwise the name verification response indicates that the submitted cardholder name is invalid when the determination is made that there is not a sufficient match resulting from the comparing.

5. The method of claim 1, further comprising:

calculating a confidence score indicative of a confidence that the name verification response is accurate.

6. The method of claim 5, further comprising:

counting a number of identified records which include the at least one cardholder name that sufficiently matches the submitted cardholder name included in the cardholder name verification request, wherein calculating the confidence score is based at least partially on the number of identified records.

7. The method of claim 1, wherein receiving the cardholder name verification request, querying the database to identify the one or more records, comparing the cardholder name, determining whether or not there is a sufficient match, and generating the name verification response are performed by at least one processor of the name verification server.

8. A system for verifying a cardholder name associated with a payment device used in connection with a card-not-present transaction, the system comprising:

a database including a plurality of records pertaining to historically processed transactions, each record including an indication of a primary account