BRIEF DESCRIPTION OF THE INVENTION

[0005] The present disclosure provides a computer-implemented method for correlating identity attributes of a cardholder on a payment card interchange network, the method implemented using a computer device coupled to a memory device, the method comprising:

receiving first personally identifiable information from other than the cardholder; encrypting the received first personally identifiable information; storing at a central store, the encrypted first personally identifiable information, the personally identifiable information encrypted to prevent payment card transaction data from being associated with the personally identifiable information; receiving, from a merchant, second personally identifiable information during a payment card transaction; encrypting the received second personally identifiable information; and comparing the encrypted stored first personally identifiable information to the encrypted received second personally identifiable information to determine a risk of fraud during the payment card transaction. ~~In one embodiment, a method for correlating cardholder identity attributes on a payment card interchange network includes storing at a central store, personally identifiable information from an issuer for a plurality of payment card cardholders, the personally identifiable information encrypted to prevent payment card transaction data from being associated with the personally identifiable information, receiving, from a merchant, personally identifiable information during a payment card transaction, encrypting the received personally identifiable information, and comparing the encrypted stored personally identifiable information to the encrypted received personally identifiable information to determine a risk of fraud during the payment card transaction~~.

[0006] The present disclosure further provides a computer system for processing data, the computer system comprising a memory device and a processor in communication with the memory device, the computer system programmed to:

store at a central store, personally identifiable information from an issuer for a plurality of payment card cardholders, the personally identifiable information encrypted to prevent payment card transaction data from being associated with the personally identifiable information; receive, from a merchant, personally identifiable information during a payment card transaction; encrypt the received personally identifiable information; and compare the encrypted stored personally identifiable information to the encrypted received personally identifiable information to determine a risk of fraud during the payment card

transaction. ~~In another embodiment, a computer system for processing data includes a memory device and a processor in communication with the memory device wherein , the computer system is programmed to store at a central store, personally identifiable information from an issuer for a plurality of payment card cardholders, the personally identifiable information encrypted to prevent payment card transaction data from being associated with the personally identifiable information, receive, from a merchant, personally identifiable information during a payment card transaction, encrypt the received personally identifiable information, and compare the encrypted stored personally identifiable information to the encrypted received personally identifiable information to determine a risk of fraud during the payment card transaction.~~

[0007] The present disclosure also provides one or more non-transitory computer-readable storage media having computer-executable instructions embodied thereon, wherein when executed by at least one processor, the computer-executable instructions cause the processor to:

store at a central store, personally identifiable information from an issuer for a plurality of payment card cardholders, the personally identifiable information encrypted to prevent payment card transaction data from being associated with the personally identifiable information; receive, from a merchant, personally identifiable information during a payment card transaction; encrypt the received personally identifiable information; and compare the encrypted stored personally identifiable information to the encrypted received personally identifiable information to determine a risk of fraud during the payment card transaction. ~~In yet another embodiment, one or more non-transitory computer-readable storage media has computer-executable instructions embodied thereon, wherein when executed by at least one processor, the computer-executable instructions cause the processor to store at a central store, personally identifiable information from an issuer for a plurality of payment card cardholders, the personally identifiable information encrypted to prevent payment card transaction data from being associated with the personally identifiable information, receive, from a merchant, personally identifiable information during a payment card transaction, encrypt the received personally identifiable information, and compare the encrypted stored personally identifiable information to the encrypted received personally identifiable information to determine a risk of fraud during the payment card transaction.~~

CLAIMS

1. A computer-implemented method for correlating identity attributes of a cardholder on a payment card interchange network, the method implemented using a computer device coupled to a memory device, the method comprising:

receiving first personally identifiable information from other than the cardholder;

encrypting the received first personally identifiable information;

storing at a central store, the encrypted first personally identifiable information, the personally identifiable information encrypted to prevent payment card transaction data from being associated with the personally identifiable information;

receiving, from a merchant, second personally identifiable information during a payment card transaction;

encrypting the received second personally identifiable information; and

comparing the encrypted stored first personally identifiable information to the encrypted received second personally identifiable information to determine a risk of fraud during the payment card transaction.

2. The computer-based method of Claim 1, wherein encrypting the received second personally identifiable information comprises encrypting the received second personally identifiable information using a one-way hash.

3. The computer-based method of Claim 1, wherein storing at a central store comprises storing at a central store located at the payment card interchange.

4. The computer-based method of Claim 1, wherein storing at a central store comprises storing at a central store located at a third party service provider.

5. The computer-based method of Claim 1, wherein storing at a central store, personally identifiable information comprises storing at a central store, personally identifiable information from the issuer includes personally identifiable information of the cardholder received during initiation of the cardholder account.

6. The computer-based method of Claim 1, wherein storing at a central store, the encrypted first personally identifiable information comprises storing at a central store, the encrypted first personally identifiable information from the issuer includes personally identifiable information of the cardholder received during a payment card transaction conducted between the cardholder and the merchant.

7. The computer-based method of Claim 1, wherein comparing the encrypted stored first personally identifiable information to the encrypted received second personally identifiable information comprises comparing the encrypted stored first personally identifiable information to the encrypted received second personally identifiable information contemporaneously with an associated payment card transaction.

8. A computer system for processing data, the computer system comprising a memory device and a processor in communication with the memory device, the computer system programmed to:

store at a central store, personally identifiable information from an issuer for a plurality of payment card cardholders, the personally identifiable information encrypted to prevent payment card transaction data from being associated with the personally identifiable information;

receive, from a merchant, personally identifiable information during a payment card transaction;

encrypt the received personally identifiable information; and

compare the encrypted stored personally identifiable information to the encrypted received personally identifiable information to determine a risk of fraud during the payment card transaction.

9. The computer system of Claim 8, wherein said computer system is programmed to encrypt the received personally identifiable information using a one-way hash.

10. The computer system of Claim 8, wherein said computer system is programmed to store at a central store located at the payment card interchange.

11. The computer system of Claim 8, wherein said computer system is programmed to store at a central store located at a third party service provider.

12. The computer system of Claim 8, wherein said computer system is programmed to store at a central store, personally identifiable information from the issuer includes personally identifiable information of the cardholder received during initiation of the cardholder account.

13. The computer system of Claim 8, wherein said computer system is programmed to store at a central store, personally identifiable information from the issuer includes personally identifiable information of the cardholder received during a payment card transaction conducted between the cardholder and the merchant.

14. The computer system of Claim 8, wherein said computer system is programmed to compare the encrypted stored personally identifiable information to the encrypted received personally identifiable information contemporaneously with an associated payment card transaction.

15. One or more non-transitory computer-readable storage media having computer-executable instructions embodied thereon, wherein when executed by at least one processor, the computer-executable instructions cause the processor to:

store at a central store, personally identifiable information from an issuer for a plurality of payment card cardholders, the personally identifiable information encrypted to prevent payment card transaction data from being associated with the personally identifiable information;

receive, from a merchant, personally identifiable information during a payment card transaction;

encrypt the received personally identifiable information; and

compare the encrypted stored personally identifiable information to the encrypted received personally identifiable information to determine a risk of fraud during the payment card transaction.

16. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to encrypt the received personally identifiable information using a one-way hash.

17. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to store at a central store located at the payment card interchange.

18. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to store at a central store located at a third party service provider.

19. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to store at a central store, personally identifiable information from the issuer includes personally identifiable information of the cardholder received during initiation of the cardholder account.

20. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to store at a central store, personally identifiable information from the issuer includes personally identifiable information of the cardholder received during a payment card transaction conducted between the cardholder and the merchant.

CLAIMS

1. A computer-implemented method for correlating cardholder identity attributes on a payment card interchange network, the method implemented using a computer device coupled to a memory device, the method comprising:

storing at a central store, personally identifiable information from an issuer for a plurality of payment card cardholders, the personally identifiable information encrypted to prevent payment card transaction data from being associated with the personally identifiable information;

receiving, from a merchant, personally identifiable information during a payment card transaction;

encrypting the received personally identifiable information; and

comparing the encrypted stored personally identifiable information to the encrypted received personally identifiable information to determine a risk of fraud during the payment card transaction.

2. The computer-based method of Claim 1, wherein encrypting the received personally identifiable information comprises encrypting the received personally identifiable information using a one-way hash.

3. The computer-based method of Claim 1, wherein storing at a central store comprises storing at a central store located at the payment card interchange.

4. The computer-based method of Claim 1, wherein storing at a central store comprises storing at a central store located at a third party service provider.

5. The computer-based method of Claim 1, wherein storing at a central store, personally identifiable information comprises storing at a central store, personally identifiable information from the issuer includes personally identifiable information of the cardholder received during initiation of the cardholder account.

6. The computer-based method of Claim 1, wherein storing at a central store, personally identifiable information comprises storing at a central store, personally identifiable information from the issuer includes personally identifiable information of the cardholder received during a payment card transaction conducted between the cardholder and the merchant.

7. The computer-based method of Claim 1, wherein comparing the encrypted stored personally identifiable information to the encrypted received personally identifiable information comprises comparing the encrypted stored personally identifiable information to the encrypted received personally identifiable information contemporaneously with an associated payment card transaction.

8. A computer system for processing data, the computer system comprising a memory device and a processor in communication with the memory device, the computer system programmed to:

store at a central store, personally identifiable information from an issuer for a plurality of payment card cardholders, the personally identifiable information encrypted to prevent payment card transaction data from being associated with the personally identifiable information;

receive, from a merchant, personally identifiable information during a payment card transaction;

encrypt the received personally identifiable information; and

compare the encrypted stored personally identifiable information to the encrypted received personally identifiable information to determine a risk of fraud during the payment card transaction.

9. The computer system of Claim 8, wherein said computer system is programmed to encrypt the received personally identifiable information using a one-way hash.

10. The computer system of Claim 8, wherein said computer system is programmed to store at a central store located at the payment card interchange.

11. The computer system of Claim 8, wherein said computer system is programmed to store at a central store located at a third party service provider.

12. The computer system of Claim 8, wherein said computer system is programmed to store at a central store, personally identifiable information from the issuer includes personally identifiable information of the cardholder received during initiation of the cardholder account.

13. The computer system of Claim 8, wherein said computer system is programmed to store at a central store, personally identifiable information from the issuer includes personally identifiable information of the cardholder received during a payment card transaction conducted between the cardholder and the merchant.

14. The computer system of Claim 8, wherein said computer system is programmed to compare the encrypted stored personally identifiable information to the encrypted received personally identifiable information contemporaneously with an associated payment card transaction.

15. One or more non-transitory computer-readable storage media having computer-executable instructions embodied thereon, wherein when executed by at least one processor, the computer-executable instructions cause the processor to:

store at a central store, personally identifiable information from an issuer for a plurality of payment card cardholders, the personally identifiable information encrypted to prevent payment card transaction data from being associated with the personally identifiable information;

receive, from a merchant, personally identifiable information during a payment card transaction;

encrypt the received personally identifiable information; and

compare the encrypted stored personally identifiable information to the encrypted received personally identifiable information to determine a risk of fraud during the payment card transaction.

16. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to encrypt the received personally identifiable information using a one-way hash.

17. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to store at a central store located at the payment card interchange.

18. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to store at a central store located at a third party service provider.

19. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to store at a central store, personally identifiable information from the issuer includes personally identifiable information of the cardholder received during initiation of the cardholder account.

20. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to store at a central store, personally identifiable information from the issuer includes personally identifiable information of the cardholder received during a payment card transaction conducted between the cardholder and the merchant.