CLAIMS

1. A method of facilitating a transaction with a payment card of a cardholder, the method comprising:

receiving, by a server system associated with a payment network, a deceptive personal identification number (PIN) comprising a set of characters in which one character is a deceptive character, the deceptive character being different than each of a set of actual characters of an actual PIN of the payment card;

identifying, by the server system, the deceptive character and a position of the deceptive character among the set of characters of the deceptive PIN;

determining, by the server system, a reconstructed PIN by replacing the deceptive character with a corresponding actual character at the position in the deceptive PIN, wherein the actual character is determined based at least on a predefined mathematical expression and a predefined value for the predefined mathematical expression;

authenticating, by the server system, the reconstructed PIN by matching the reconstructed PIN with the actual PIN; and

upon successful authentication, facilitating, by the server system, the transaction.

2. The method as claimed in claim 1, further comprising:

accessing, by the server system, a primary deceptive character and a primary position of the primary deceptive character in a preceding transaction, the preceding transaction being a last transaction immediately prior to the transaction;

checking, by the sever system, if the primary deceptive character and the primary position are same as the deceptive character and the position of the deceptive character, respectively in the transaction; and

upon determining the deceptive character to be same as the primary deceptive character and the position of the deceptive character to be same as the primary position of the primary deceptive character, declining, by the server system, the transaction.

3. The method of claim 1, further comprising:

receiving, by the server system, a registration request for using the deceptive character prior to using the deceptive PIN, the registration request comprising a payment card information of the payment card, the deceptive character, the predefined mathematical expression and the predefined value; and

upon successful verification of the registration request, by the server system, storing the predefined mathematical expression, the predefined value and the deceptive character for the payment card of the cardholder.

4. The method of claim 3, further comprising:

provisioning, by the server system, an option for the cardholder to update the deceptive character, wherein the cardholder initiates the registration request for updating the deceptive character.

5. The method of claim 3, wherein determining the reconstructed PIN comprises:

determining, by the server system, a subset of characters of the set of characters by removing the deceptive character from the set of characters;

defining, by the server system, an intermediate expression based on the subset of characters, the predefined value and the predefined mathematical expression; and

solving, by the server system, the intermediate expression for determining the actual character.

6. The method of claim 1, wherein the payment card comprises an electronic number pad.

7. The method of claim 6, further comprising:

receiving, by the server system, a registration request comprising a pattern and the deceptive character, wherein the pattern and the deceptive character are provided by the cardholder on the electronic number pad prior to using the deceptive PIN.

8. The method of claim 7, wherein the pattern comprises one or more number pad values for registration of the deceptive character.

9. The method of claim 7, further comprising;

receiving, by the server system, a number pad registration request, the number pad registration request comprising a mapping of a first set of positions of keypad inputs in the electronic number pad to a second set of positions in the electronic number pad for providing user defined keypad outputs; and

storing, by the server system, the mapping.

10. The method of claim 9, wherein receiving the deceptive PIN comprises:

receiving, by the server system, a plurality of number pad values of the payment card comprising at least the deceptive character and the deceptive PIN, wherein each number pad value of the plurality of number pad values corresponds to a respective keypad input in the electronic number pad at the second set of positions; and

mapping, by the server system, the plurality of number pad values from the second set of positions to the first set of positions for identifying the deceptive character and the deceptive PIN.

11. A server system for facilitating a transaction with a payment card of a cardholder, the server system comprising:

a memory comprising stored instructions; and

at least one processor configured to execute the stored instructions to cause the server system to perform at least

receiving a deceptive personal identification number (PIN) comprising a set of characters in which one character is a deceptive character, the deceptive character being different than each of a set of actual characters of an actual PIN of the payment card,

identifying the deceptive character and a position of the deceptive character among the set of characters of the deceptive PIN,

determining a reconstructed PIN by replacing the deceptive character with a corresponding actual character at the position in the deceptive PIN, wherein the actual character is determined based at least on a predefined mathematical

expression and a predefined value for the predefined mathematical expression,

authenticating the reconstructed PIN by matching the reconstructed PIN with the actual PIN, and

upon successful authentication, facilitating the transaction.

12. The server system of claim 11, wherein the at least one processor is configured to execute the stored instructions to further cause the server system to perform at least:

accessing a primary deceptive character and a primary position of the primary deceptive character in a preceding transaction, the preceding transaction being a last transaction immediately prior to the transaction;

checking if the primary deceptive character and the primary position are same as the deceptive character and the position of the deceptive character, respectively in the transaction; and

upon determining the deceptive character to be same as the primary deceptive character and the position of the deceptive character to be same as the primary position of the primary deceptive character, declining the transaction.

13. The server system of claim 11, wherein the at least one processor is configured to execute the stored instructions to further cause the server system to perform at least:

receiving a registration request for using the deceptive character prior to using the deceptive PIN, the registration request comprising a payment card information of the payment card, the deceptive character, the predefined mathematical expression and the predefined value; and

upon successful verification of the registration request, storing the predefined mathematical expression, the predefined value and the deceptive character for the payment card of the cardholder.

14. The server system of claim 11, wherein the payment card comprises an electronic number pad.

15. The server system of claim 14, wherein the at least one processor is configured to execute the stored instructions to further cause the server system to perform at least:

receiving a registration request comprising a pattern and the deceptive character, wherein the pattern and the deceptive character are determined and provided by the cardholder on the electronic number pad prior to using the deceptive PIN.

16. The server system of claim 14, wherein the at least one processor is configured to execute the stored instructions to further cause the server system to perform at least:

receiving a number pad registration request, the number pad registration request comprising a mapping of a first set of positions of keypad inputs in the electronic number pad to a second set of positions in the electronic number pad for providing user defined keypad outputs; and

storing the mapping.

17. The server system of claim 16, wherein for receiving the deceptive PIN, the at least one processor is configured to execute the stored instructions to further cause the server system to perform at least:

receiving a plurality of number pad values of the payment card comprising at least the deceptive character and the deceptive PIN, wherein each number pad value of the plurality of number pad values corresponds to a respective keypad input in the electronic number pad at the second set of positions; and

mapping the plurality of number pad values from the second set of positions to the first set of positions for identifying the deceptive character and the deceptive PIN.

18. A method of facilitating a transaction with a payment card of a cardholder, the method comprising:

receiving, by a server system associated with a payment network, a deceptive personal identification number (PIN) for performing the transaction using the payment card of the cardholder, the deceptive PIN comprising a set of characters in which one character is a deceptive character, the deceptive character being different than each of a set of actual characters of an actual PIN of the payment card;

identifying, by the server system, the deceptive character and a position of the deceptive

character among the set of characters of the deceptive PIN;

determining, by the server system, a validity of the transaction by performing at least

accessing, by the server system, a primary deceptive character and a primary position of the primary deceptive character in a preceding transaction, the preceding transaction being a last transaction immediately prior to the transaction,

comparing, by the sever system, the primary deceptive character with the deceptive character and the primary position of the primary deceptive character with the position of the deceptive character, and

upon determining the primary deceptive character to be same as the deceptive character and the primary position of the primary deceptive character to be same as the position of the deceptive character, declining, by the server system, the transaction;

upon determining successful validity of the transaction, determining, by the server system, a reconstructed PIN by replacing the deceptive character with a corresponding actual character at the position in the deceptive PIN, the actual character being determined based on a predefined value, a predefined mathematical expression and a subset of characters of the set of characters;

authenticating, by the server system, the reconstructed PIN by matching the reconstructed PIN with the actual PIN; and

upon successful authentication, facilitating, by the server system, the transaction.

19. The method of claim 18, further comprising:

receiving, by the server system, a registration request for using the deceptive character prior to using the deceptive PIN, the registration request comprising a payment card information of the payment card, the deceptive character, the predefined mathematical expression and the predefined value; and

upon successful verification of the registration request, by the server system, storing the predefined mathematical expression, the predefined value and the deceptive character for the payment card of the cardholder.

20. The method of claim 18, wherein determining the reconstructed PIN comprises:

determining, by the server system, a subset of characters of the set of characters by removing the deceptive character from the set of characters;

defining, by the server system, an intermediate expression based on the subset of characters, the predefined value and the predefined mathematical expression; and

solving, by the server system, the intermediate expression for determining the actual character.