

Claims

I claim:

1. A method of securing a Payment Card transaction conducted, at least in part, over a telecommunication network among a cardholder, an issuing bank, and a merchant, wherein the method comprises:
 - transmitting sufficient information to the issuing bank over the telecommunication network to identify a cardholder;
 - generating a one time data code;
 - transmitting the one time data code to the cardholder over the telecommunication network;
 - conveying the one time data code from the cardholder to the merchant;
 - transmitting the one time data code from the merchant to the issuing bank over the telecommunication network;
 - checking if the one time data code transmitted to the issuing bank by the merchant matches the generated one time data code; and
 - declining to authorize the transaction unless the one time data code transmitted to the issuing bank by the merchant matches the generated one time data code.
2. The method of securing a Payment Card transaction according to claim 1 wherein the one time data code is generated using a random number generator.
3. The method of securing a Payment Card transaction according to claim 2 wherein the issuing bank generates the one time data code.
4. The method of securing a Payment Card transaction according to claim 2 wherein the one time data code is generated after the cardholder initiates the transaction with the merchant.

5. The method of securing a Payment Card transaction according to claim 2 wherein the one time data code is encrypted prior to transmitting the one time data code to the cardholder.
6. The method of securing a Payment Card transaction according to claim 5 wherein the one time data code is transmitted to the cardholder by transmitting the one time data code over the telecommunication network to a mobile device associated with the cardholder.
7. The method of securing a Payment Card transaction according to claim 6 wherein the one time data code is transmitted to the cardholder over the telecommunication network via a communication method selected from the group consisting of email, text message, telephone call, push notification, and combinations thereof.
8. The method of securing a Payment Card transaction according to claim 6 further comprising requiring a security key to be provided to the mobile device before the one time data code is released to the cardholder.
9. The method of securing a Payment Card transaction according to claim 8 wherein the security key is selected from the group consisting of a password and a biometric key and combinations thereof.
10. The method of securing a Payment Card transaction according to claim 9 wherein the biometric key is selected from the group consisting of a match from a fingerprint reader, a match from facial recognition software, a match from iris recognition software, a match from voice recognition software or combinations thereof.
11. The method of securing a Payment Card transaction according to claim 6 wherein the mobile device decrypts the one time data code.
12. The method of securing a Payment Card transaction according to claim 1 further comprising

checking if the one time data code has been used in connection with a previous transaction by the cardholder and, if it has, discarding the one time data code and generating a second one time data code.

13. The method of securing a Payment Card transaction according to claim 1 wherein the
5 merchant comprises an ATM.

14. The method of securing a Payment Card transaction according to claim 6 wherein the mobile device is configured to function as a contactless Payment Card.