3D Secure
Frequently Asked Questions

Q: What is 3D Secure and how does it work?
A: 3D Secure, also known as Verified by Visa, MasterCard SecureCode or Amex Safekey, is a method of authentication security, which was developed by the Card Schemes to enhance the security of online transactions for all cardholders. It allows only the cardholder to use the card when shopping online.

The three domains referred to in "3D" Secure consist of the cardholder to issuer domain, the merchant to acquiring bank domain and the interbank domain.

Very simply, the system authenticates the cardholder before any transaction can take place, by diverting the cardholder to the browser of the bank that issued the card. The bank then requests a password or One Time Password/PIN (OTP), from the cardholder, which is typically sent to their mobile phones, which will prove that the person undertaking the online transaction is the authenticated cardholder and therefore entitled to use the card.

Q: How will 3D Secure impact the cardholder experience when paying online?
A: The impact of 3D Secure while making an online payment should be minimal and generally would take less than a minute or two to complete. If a cardholder has already registered or has been registered by the bank, he/she will be prompted with an additional screen requesting an OTP or a PIN/Password. OTPs are sent to the mobile phone number the bank has on record for the cardholder, whilst a PIN or Password is a secret code the cardholder has chosen when he/she registered for 3D Secure or at the time of issuing the card. Simply enter the OTP, PIN or Password in the given space and proceed.

If the cardholder has not registered or been registered for the 3D Secure service, he/she will be prompted with a screen asking him/her to register for 3D Secure. Follow the prompts on the screen to register. Remember, it is in our best interest to be safe.

Q: How much of a problem is online fraud in South Africa?

A: According to the official South African Banking Risk Information Centre (SABRIC), Card Not Present (CNP) fraud consisting of e-commerce (online), m-commerce (mobile) and MOTO (mail order and telephone order) transactions contributed 48.7% of the total credit card fraud losses in 2013. This is in contrast to e-commerce merchants only making up less than 3% of the total merchant base. Therefore, due to the continued growth in e-commerce, it essential that additional measures be put in place to meet this changing environment.

Q: How does PASA foresee this clamping down on online fraud?

A: Whilst there are other industry initiatives happening that would address keeping card data safe, the additional authentication of e-commerce transactions via 3D Secure will reduce instances where card numbers have been compromised and then used by fraudsters for online shopping. Just as EMV compliant chip and PIN technology has been used to counter physical card fraud, so 3D Secure is intended to achieve the same outcome in the online environment.

Q: Will all banks be using the system?

A: Of the 8 issuing banks currently offering traditional e-commerce capability on their cards, the 6 large e-commerce volume banks all use 3D Secure. This accounts for 99% of all e-commerce transactions.

Q: How do cardholders register/activate 3D Secure?

A: Banks have already enrolled all cards capable of doing 3D Secure transactions for the service. Additionally, 87% of all e-commerce cardholders have already been activated to use 3D Secure. In the exceptional case of a first time e-commerce user or a new cardholder who has not been activated, the cardholder will be prompted with an activation screen during its first purchase.

Q: Are all e-commerce enabled cards capable of doing 3D Secure?

A: No, for practical reasons not all e-commerce enabled cards are able to participate in 3D Secure. For example, although corporate credit cards allow for e-commerce functionality, it will not be enrolled for 3D Secure. This will however not impact the functionality of the card.

Q: How does 3D Secure benefit the cardholder?

A: The intention behind the system is that cardholders will have a decreased risk of their cards being fraudulently used on the Internet – in essence this system creates a safer online shopping environment.

Because the issuing bank prompts the cardholder for a password that is known only to the bank and the cardholder, nobody else will be able to use the card to make online payments without also having the cardholder's mobile phone or PIN number. Additionally, since the merchant does not know this password and is not responsible for capturing it; it can be used by the issuing bank as evidence that the purchaser is indeed their cardholder.

Online shopping is already developed with high levels of security and encryption whenever the card is used. The main reason for the current high levels of CNP fraud currently experienced is that card details are fraudulently used to shop online without a prompt for an additional security code/PIN. 3D Secure offers this additional layer of security to protect the cardholder from any unauthorised use of the card.

The 3D Secure process can be compared to entering a PIN at a point-of-sale machine when doing a purchase in the card present environment.

Q: What has PASA's involvement been in 3D Secure?

A: The Payment Association of South Africa (PASA) is appointed by the South African Reserve Bank to ensure the safety and efficiency of the National Payment System and securing the Card Payment System has been a priority for the last two to three years. During February 2013 PASA made the decision to mandate all South African e-commerce merchants to be enrolled and active in the 3D Secure programme by 28 February 2014.

In line with this compliance, PASA has been:

- Encouraging banks and merchants to educate cardholders and increase awareness of 3D Secure and related fraud
- Working with banks and merchants in understanding how to handle cards that are not eligible for, or capable of performing, 3D Secure transactions
- Clarifying the process to enable cardholders to transact using 3D Secure
- Communicating and clarifying technical specifications and standards to ensure compliance

This PASA initiative has also been formally endorsed by the South African Reserve Bank (SARB). In the announcement on 11 March 2014 of new card interchange rates, the SARB has incentivised the adoption of 3D Secure by merchants by allowing a differentiated interchange rate.

Q: When is the implementation deadline?

A: The official implementation deadline for all e-commerce merchants was 28 February 2014. However, many merchants have been using the 3D Secure service for some time already.

Q: Have all merchants moved over to this system?

A: PASA has been working closely with the banks and the e-commerce merchants to ensure implementation of 3D Secure and 91% of South African merchants have put the necessary structures in place to meet the 28th February deadline. PASA and the banks will be working with the remaining merchants to ensure they move over to the safer system as soon as possible.

Q: Are there cost implications for the cardholder?

A: In most instances the registration and activation of 3D Secure happens at no additional cost to the cardholder. Cardholders are encouraged to review their banks' pricing structures or enquire from their banks to be sure of related bank charges, if any.

Q: Some tips for a good 3D Secure experience

A: 3D Secure is not a new system and cardholders should not be anxious or nervous to use it. Many merchants have been using 3D Secure effectively for a number of years and we see thousands of 3D Secure transactions going through the system every month. The deadline of 28 February 2014 will however ensure a more uniform approach to e-commerce security. Some tips for a good experience include:

- Ensure you have the card you wish to pay with ready.
- Ensure you have your mobile phone with you to receive the OTP or you know what your PIN or Password is, depending on what your bank's authentication method is.
- After entering your PIN/Password, the system may take a couple of *seconds* to authenticate your PIN/Password. This is normal – do not close the browser.
- If you receive an error message, be sure to read the message on the screen. You may have entered your PIN/Password incorrectly in which case you will be allowed to retry. Although minimal, there may also be other reasons why the

transaction failed, in which case we recommend that you follow the instructions on the screen or contact your bank for further assistance.

Q: What should a cardholder do if the merchant they wish to purchase from does not support 3D Secure?

A: Where a cardholder feels uncomfortable using a merchant that has not implemented 3D Secure yet, the cardholder can contact the merchant or his/her bank directly.

Q: What about overseas merchants?

A: Only South African merchants are mandated to implement 3D Secure. Whilst some overseas merchants have implemented 3D Secure already, cardholders should be aware that the PASA mandate for 3D Secure only applies to local merchants and that not all overseas merchants participate in 3D Secure.