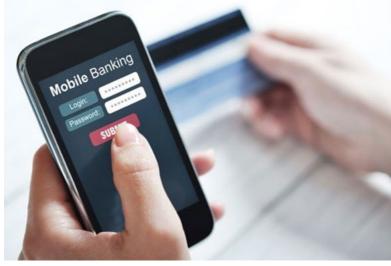# 'Back of the card' puts mobile security front of mind

By Leigh Andrews   24 Mar 2015

Fears of 'card not present' fraud (hello, online and mobile shopping) may soon be a thing of the past, thanks to Gemalto's dynamic CVV code display...

Mobile payment safety is a hot topic at the moment. The Cards & Payment Africa 2015 event took place on 10 and 11 March at the Sandton Convention Centre, with a strong focus on mobile as the next frontier for commerce on the continent.

© Tetiana Vitsenko – 123RF.com

This is important because while purchasing things has become easier, faster and more convenient over the years, the payment methods that come with online shopping also make easier for fraudulent activities to take place. So much so that the number of data breaches in South Africa increased by 33% in 2014 compared to 2013.

That's why companies like Gemalto are coming up with innovative ways around this, such as offering a dynamic CVV code display on the back of the latest banking cards. This helps secure online transactions and 'card not present' transactions.

But this isn't the standard printed three-digit code you're likely to have seen before - the CVV technology dynamically generates the code and displays it on a small ePaper screen on the back of the card, so it automatically changes over time, without cardholder intervention, meaning there's no need for buttons, keys or any type of user input.

What increased security means for merchants and customers alike...

Paul Opie, Banking Field Marketing Manager for Africa at Gemalto, says from an e-commerce perspective, PASA is mandating all local merchants to implement 3D Secure. This effectively makes the consumer check out process more complex.

And the reason? Well, by breaching data security measures, hackers can use card details in CNP fraud transactions.

That's partly why the back of the banking card is taking innovative security technology to a new level.

Opie explains that the temporary CVV/CVC number displayed on the back of the card is only valid for a limited time frame. This means if the card's details are compromised in anyway, they can't actually be used for card-not-present (CNP) fraud outside of the short time frame the number appears.

This translates into online security, with the need for 'secure online' and cards not present for transactions, as it ensures that only the card holder with the card can read and use the CVV to perform a purchase. In addition, there are no impacts on the merchant, and the card can be used on any site globally.

Opie confirmed that this is the only convenient payment solution out there that doesn't impact on the merchant impact and has instant global reach.

Important as Anton Vukic, Channel Director at Phoenix Software, says many consumers do not trust mobile payment methods, believing them to be fraught with vulnerabilities.

Click here and here for more measures against mobile retail fraud.

Paul Opie

ABOUT LEIGH ANDREWS

Leigh Andrews AKA the #MilkshakeQueen, is former Editor-in-Chief: Marketing & Media at Bizcommunity.com, with a passion for issues of diversity, inclusion and equality, and of course, gourmet food and drinks! She can be reached on Twitter at @Leigh_Andrews.
- #Loeries2020: Behavioural economics as creativity, but not as we know it... - 24 Nov 2020
- #DI2020: Ignite your inner activist - representation through illustration - 27 Feb 2020
- #DI2020: How Sho Madjozi brought traditional Tsonga *xibelani* into 2020 - 27 Feb 2020
- #DI2020: Silver jubilee shines with Department of Audacious Projects launch - 26 Feb 2020
- #BehindtheSelfie with... Qingqile 'WingWing' Mdlulwa, CCO at The Whole Idea - 26 Feb 2020

View my profile and articles...

For more, visit: https://www.bizcommunity.com