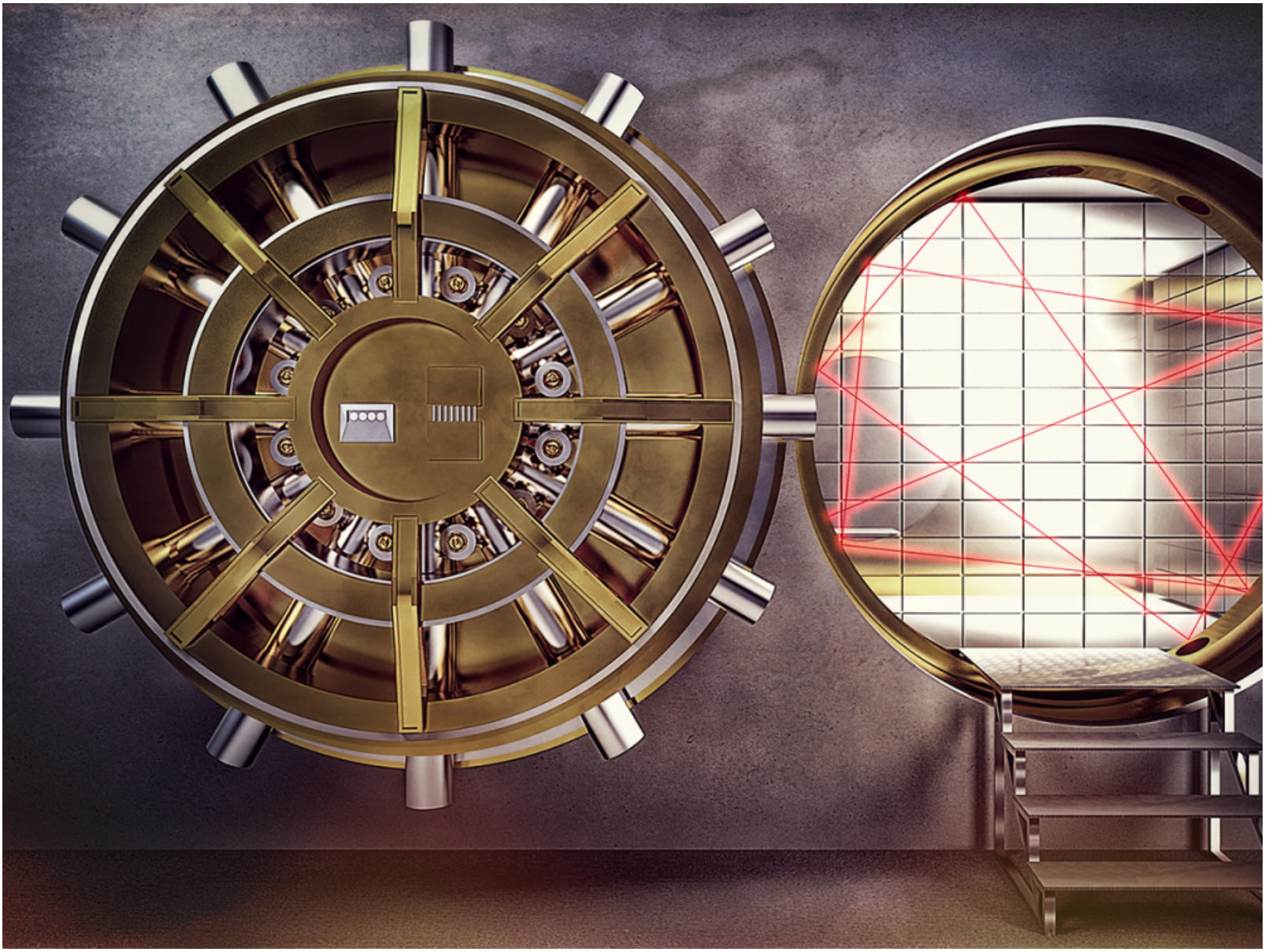
nccgroup



Shutterstock: Royalty-free stock illustration ID: 125355542

Dec 08, 2019 19:02 GMT

Virtual Payment Cards, in scope or out-of-scope for PCI DSS?

With increased demand for virtual card capabilities from Australian businesses, merchants and service providers, we keep being asked by our

customers whether virtual payment cards are subject to Payment Card Industry Data Security Standard (PCI DSS). If they are, what would be the impact and their obligation against the payment standard?

First, let's start with what is a virtual payment card?

When we talk about the virtual cards of course there is no physical plastic card involved, and it is a randomly generated payment card number just like a normal credit or debit card with an expiry date and CVV number under your name or business/merchant name. These cards can be used anywhere online, over the phone or in-store (depending on the virtual card provider). The virtual payment cards can be stored on mobile phones, e-wallets, smart watches and computers.

There are two main types of virtual payment cards, single use (one-use, non-reloadable or disposable) and multi-use (reloadable) virtual cards.

With single use virtual cards, temporary account numbers are used, so if a fraudster obtained the account number, it wouldn't work because the payment number was valid for a single transaction only. Single use non-reloadable virtual cards can be the right payment option when it comes to one-time payments.

With multi-use (reloadable) virtual cards, your personal details aren't attached to the card either, so you can shop securely and in anonymity again and again, as long as you have sufficient funds available on the card. Some reloadable virtual card platforms also give you the ability to freeze or delete a virtual card that has been compromised and instantly replace it with a new one.

By having a quick look at some of the biggest payment data breaches such as; Equifax with ~143 million accounts compromised, Target with ~110 million accounts compromised, and Ashley Madison with ~37 million accounts compromised, we agree that virtual payment cards can add another layer of protection to online endeavours.

Entities who offer virtual payment cards in Australia

In Australia, some of the major banks, financial institutions and service providers offer virtual cards, however there are different services, features and capabilities.

For example, ANZ offer a solution for businesses and corporations called "ANZ Virtual Card". The ANZ Virtual Card is a 16 digit Visa account number that supports payments of strategically managed accounts, allowing multiple employees to purchase on behalf of an organisation without issuing individual plastic cards. It also provides unauthorised transactions insurance.

Westpac has a virtual card solution under its commercial card program. It is

a secure and convenient way to manage the travel and procurement purchases from your suppliers. The Westpac Virtual Card solution is also commonly used as a payment tool lodged at Travel Management Companies (TMCs) to conveniently use for travel related expenses.

Amex, Mastercard and Visa also have virtual prepaid cards which are provided by different gift card platforms in Australia.

While virtual payment cards provide another layer of security, if your bank or financial institute doesn't offer one, there are other security controls that you can consider for your online transactions such as Verified by Visa, MasterCard's Secure code and American Express SafeKey. This extra level of security is called 3-D Secure which is a globally accepted authentication solution designed to make e-Commerce transactions more secure in real-time.

Are the virtual card numbers in scope for PCI DSS?

Since virtual payment cards are becoming more common, merchants and service providers are receiving more virtual card transactions through their systems and environment, that's why it is important to understand your obligation against PCI DSS.

To understand the impact of these cards on PCI DSS scope, the best place to start with is the Payment Card Industry Security Standards Council (PCI SSC) website (Article Number 1285 and 1286), which says:

"PCI DSS applies to all primary account numbers (PANs) that represent a PCI founding payment card brand (American Express, Discover, JCB, MasterCard, or Visa). This includes PANs that are only provided electronically (virtual PANs) as well as PANs that correspond to a physical payment card. Whether a one-time PAN is in scope for PCI DSS will depend on the particular restrictions around their usage as defined by the payment brands. Entities should contact the applicable payment brand to determine how PCI DSS applies."

The above statement puts the onus squarely on the payment brands, so let's see what the card brands' (MasterCard in this case) position is.

What is MasterCard's position on Single Use Virtual Card Numbers and PCI compliance?

MasterCard does not consider Single Use Virtual Card Numbers (SU-VCNs) to be in scope of PCI DSS requirements. The SU-VCN becomes inactive/disabled after only one authorisation; therefore, the virtual PAN data cannot be reused for fraudulent activities within the payment ecosystem. However, it is important to note that even though a SU-VCN may be considered "out of scope" for PCI DSS, it does not mean that the systems and/or entities that are storing, transmitting or processing the SU-VCN are also out of scope. PCI DSS will apply anywhere a multi-use PAN is stored,

transmitted or processed. If the systems storing, transmitting or processing the SU-VCN also store, transmit or process multi-use PANs, those systems will remain in scope of PCI DSS requirements.

The conclusion?

Virtual payment cards are in scope for PCI DSS if a multi-use PAN or multi–use virtual payment card is stored, transmitted or processed.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

NCC Group - Financial Media Enquiries
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750