BIZCOMMUNITY

Securing the future of payments: What businesses need to know about payment security

Issued by Ecentric Payment Systems

14 Nov 2023

The only way to combat the increasing cost of cyberattacks, and the reputational threat that comes with them, is to have solid, internationally accredited, security measures in place as well as going above and beyond these requirements, writes Bernard van Der Merwe, Information Security Officer at Ecentric Payment Systems.

Depending on who you believe, there are anywhere between 2,000 and 4,000 cyberattacks each day across the globe. Breaches are not only costly, but also put your reputation at risk. In the payments industry, ensuring integrity and security of consumer data is a critical factor for South African businesses. International accreditation is key to keeping your data and payments safe ahead of the retail shopping season.

Thankfully, there are improved security standards that will help keep consumers' money secure, if payment solution providers adhere to them. A Verizon survey, the Payment Security Report from last year, found that only 27.9% of those companies surveyed were in full compliance with an international payment security standard that is mandatory for the payments industry.

The Payment Card Industry (PCI) Security Standards Council (PCI SSC) has released what is being seen as the biggest update to DSS compliance since DSS was released 18 years ago: Version 4.0. It's a tough ask to comply though, and companies that transfer money in the payments space need to have it implemented by March next year. Version 4.0 adds another 63 obligations for accreditation to the current requirements than under the current 3.2.1.

Simply put, without these standards and yearly accreditation, there is a level of risk when transacting. We go through a PCI audit once a year to ensure that we remain qualified so we stay ahead of cyberattacks as much as possible. This is important when processing 20% of card transactions in South Africa and providing offerings to 65% of the JSE-listed

retailers, serving their in-store, online, mobile and omnichannel payment requirements. Given that we operate in 17 African countries, we have also developed bank-specific as well as business-to-business security measures.

Peer-to-peer payment growth

However, where there is a weak link is when it comes to peer-to-peer (P2P) payments.

Precedence Research states the P2P payment market was worth $2.21tn globally and is expected to reach $11.62tn by 2032, growing at 10.12% on a compound annual growth rate. With any advancement comes increased risk. A huge differentiator in trust comes in when banks, for example, can offer this decryption offering, an area in which we specialise.

Driven by the increasing uptake in smartphones and increased broadband penetration, more people are sending money to each other, especially across South Africa's borders to their families at home. However, these transactions cannot easily be reversed, meaning that once money has gone to a fraudster, it's gone.

Yet, not many companies can currently boast P2P security measures, which are absolutely vital considering that this service, allowing people to transfer money to each other, such as via eWallets, is growing rapidly. A good example is when people buy leather belts or fake rugby jerseys from the side of the road.

This is an area in which inhouse software, such as what we have developed, can close the gap.

A costly event

Failure to protect information when money is transferred is not only a reputational risk, but also comes with a fine, if those affected are not notified.

In terms of the Protection of Information Act, companies need to tell those who have been affected by a data breach that their information – specifying the type of data – has been stolen. While the level of detail varies on a case-by-case basis and is also informed by the measures the company needs to take as well as any action by law enforcement, failure to tell customers means a R10m fine.

There is a large amount of due diligence to be done when it comes to choosing a payment solution or gateway provider. Most may look at the system's ability to integrate with that of the client, which doesn't go nearly deep enough. The most important aspect is the level of security, international accreditations, and in-house security developments that are tracking ahead of the rest of the industry.

In the build up to Black Friday and the peak of South Africa's retail season, ensure that security is top of mind when implementing any system, or using one to transfer one, especially one that affects people's money in a tough socio-economic environment.

- **Top payment trends for 2024** 31 Jan 2024
- **Retailers need to be on the ball this Black Friday and Cyber Monday** 27 Nov 2023
- **Securing the future of payments: What businesses need to know about payment security** 14 Nov 2023
- **Ecentric Payment Systems announces acquisition of IP of payment industry innovator Thumbzup** 26 Oct 2023
- **Tier One South African retailer uses Ecentric's ReconAssist to proactively combat retail fraud** 5 Oct 2023