New ways to pay protect consumers against card fraud

Submitted by: PR Artistry Limited
Thursday, 12 December 2019

With card fraud and identify theft continuing to hit the headlines, Jason Roos, CEO of technology company Cirrus, discusses why it pays to know about payment standards when using your credit or debit card online or on the phone.

In today's increasingly cashless society, we all rely on using cards for payments. We happily relay our account and credit card details on the phone without a second thought, trusting that the company that we are dealing with will manage our card data securely. But how safe are our details?

Major card fraud losses recorded in 2018
According to UK Finance(i), the theft of personal and financial details through social scams and data breaches was a major contributor to fraud losses in 2018. In fact, data breaches involving just three well-known brands are reported to have resulted in the attempted compromise of around 6.3 million payment card details.

The finance industry cannot tackle fraud alone, which means that it is the responsibility of all companies in the chain to take preventative measures and secure card data. So how can we be sure that our details are safe?

We've identified three key areas to be aware of:

1.Making your payments secure – PCI DSS Standards

PCI DSS is a worldwide Payment Card Industry Data Security Standard that was set up the by the five big card providers(ii, the UK Cards Association (now UK Finance), to help businesses process card payments securely and reduce card fraud.

Being compliant with PCI DSS means that a company is doing its best to keep customers valuable information safe and secure. If a business loses a customer's card data i.e. suffers a data breach and is not PCI DSS compliant, they could incur fines for the data loss and be liable for the fraud costs incurred against these cards, not to mention the reputational and brand damage.

2.Your phone payments – no longer the weakest link

The same PCI DSS guidelines also set out requirements for call centres when taking payments. The need for many contact centres to record calls, for security and training purposes, makes protecting the data more difficult. But by complying with the PCI DSS standards, companies can achieve the security levels required.

However, this can be a complex and costly technical process to follow and there are companies that do not comply. To reduce costs and comply with the standards, some organisations choose to minimize (often called 'de-scoping') or eliminate altogether the customer card data that they hold in their systems, reducing fraud risk.

For example, they may offer ‘stop-start’ recording on your call or have ‘clean rooms’ (with no paperwork and nothing is written) and dedicated payment teams. Some use Interactive Voice Response (IVR) Payments, particularly large contact centres, which take your card details and cut the agent risk out of the loop entirely. However, data still resides in the call centre, so IVR alone does not ensure PCI compliance.

3.New ways to pay with SMS and email are ringing the changes

Such is the pace of new technology that there are now new, secure, easier ways to pay. As an example, Cirrus’ new LinkPay+ service (a partnership with Semafone) sends you a secure payment link, via SMS or email, while you are on the phone or webchat to a call centre.

With LinkPay+ you can enter your card details on a secure website page with confidence.

You can complete your purchase during the call or chat, saving you the hassle of ringing a different number or revisiting the original website. It’s more convenient than entering card details over the phone and help is at hand if you need it.

There are plans in the future for this technology to tie up with Apple Pay and Google Pay, which will make it even easier for customers to pay securely.

While companies are making leaps and bounds to protect card payments and identify theft, it will always be a challenge, as fraudsters are constantly looking to find new ways to exploit technology weaknesses.

The Take Five to Stop Fraud(iii)is a national campaign that offers advice to help everyone protect themselves from preventable financial fraud. Whilst you probably already follow the advice as second nature, it’s worth a read.

Jason Roos is CEO of Cirrus (http://www.cirrusresponse.com)

- Ends -

About Cirrus

Cirrus solutions combine best in class video, voice, voice, email, chat and social media. With a cloud infrastructure, Cirrus operates on a real-time basis with unlimited scalability and the highest level of resilience and security. Cirrus solutions activate the workforce, empower businesses and call centres and inform business leaders, driving exceptional business results and customer experiences.

Cirrus deployments typically range from 5 – 1,000 users and customers benefit from the ability to unify resource across separate geographic locations (including homeworkers), leverage omni-channel capability and move to a single view of the customer.

Cirrus provides a range of automation and managed solutions including on-the-fly translation for voice

calls, and managed Conversational AI (CAI) that support 24/7 operations while keeping costs low.
Cirrus has a broad range of experience across both the public and the private sector.
High profile clients include Virgin Trains, NHS, Clarks, FCA, CAA, Cafcass and InsureTheBox.
For more information please visit: Cirrus (http://www.cirrusresponse.com)

Follow us: Twitter (https://twitter.com/CirrusResponse)
Linkedin (https://www.linkedin.com/company/cirrus-response/)

Editors Contacts

Andreina West
PR Artistry
01491 845553
andreina@pra-ltd.co.uk

(i) The collective voice for the UK banking and finance industry representing more than 250 firms across the industry UK Finance (http://www.ukfinance.org.uk)

(ii)VISA, MasterCard, American Express, Discover and JCB International

(ii0)Take Five Stop Fraud (http://www.takefive-stopfraud.org.uk)