PRESS RELEASE
22 November 2021

Gearing up for 2022: PCI Pal® Releases Top-Level Insights to Prepare Businesses for a New Year of Cyber Crime

Geoff Forsyth, Chief Information Security Officer of PCI Pal, (LON:PCIP) – the global provider of cloud-based secure payment solutions – highlights key trends and predictions on how to navigate the security challenges in 2022.

"If there is one word that has been cemented into our heads over the course of the pandemic, it has been "unprecedented." And while we saw a lot of new challenges pop up, they don't seem to be going away anytime soon and will likely grow in number and complexity. With WFH still the norm for many companies, 2021 should've been the year that businesses cemented their digital practices, ensuring that security was woven into each process given the consistent news around data breaches.

"It's clear however that there's a lot more work to be done and as we enter 2022 and the unprecedented situation continues, the expectations are set. Consumers want businesses to ensure their payments are safe, and businesses need to have a concrete game plan in motion to make consumers feel secure."

Geoff Forsyth's predictions and considerations for the new year:

1. "**Stop fearing the unknown and focus on existing threats.** Next year, we shouldn't be focused on seeking out new forms of fraud, but rather focus on the shift and re-emergence of existing iterations. As card-present payments fall farther behind card-not-present, payment webpages are more likely to be compromised by good old fashioned third-party scripts or attacks. 2021 had an abundance of new payment processes emerge, but across these new vendors we saw an obvious lack of security expertise, which allowed fraudsters to use old tricks to attack vulnerable shoppers. As more and more payments go online, the wider the landscape is for scammers to attack.
2. **Businesses need to reset and re-evaluate their security strategies in 2022**. Security in industries like IT and finance need to be reviewed on a consistent basis, to ensure that the company's bases are covered. During the early months of 2021, infrastructure suddenly became a

visible and critical focus for businesses as teams raced to enforce old practices under new restrictions, uncovering new challenges and threats along the way. As society keeps progressing digitally and the urgency to meet security needs continues to grow, businesses need to reset and reorganize. Companies were racing to restructure their old strategies but, in their rush, security precautions could have fallen by the wayside.

3. **The primary security risk for payments lies in the varying types of payments that merchants choose to accept from their customers**. While there will always be new patches, protocols and plans for addressing security, the overarching issue largely remains unchanged. So instead of addressing new concerns with new solutions, companies must first implement the tried and true security basics that can still protect against many vulnerabilities and attack vectors. One measure of security risk worth careful consideration by all businesses is the OWASP Top Ten.

4. **Cryptocurrencies will always be an appealing and exciting option for some businesses and brands, but it will not endear them to governments**. Whilst it is easy for companies to overlook the implications of the consumed processing resources and decentralization of currency, governments have yet to get on board - many are even soft-banning cryptocurrencies in various types of transactions.

You can look at financial fraud like garden weeds: Weeds grow slowly over time, stripping away the life from smaller, less-resilient plants until they grow too large and noticeable. Even if the roots of that weed are fully destroyed, the seeds of other invasive or parasitic species remain and the garden remains a paradise of nutrients to steal. Akin to weeds, fraud will always be present, and though attacks by governments on major criminal rings can scatter or shut down a large volume of fraud, they don't make the issue disappear. In 2022, it's time to get serious about cybersecurity - there's no longer an excuse."

For more information on PCI Pal visit www.pcipal.com, call +44 207 030 3770 to arrange a demonstration or follow PCI Pal on Twitter.

ends

Notes to Editors:

About PCI Pal

PCI Pal is a leading provider of SaaS solutions that empower companies to take payments securely, adhere to strict industry governance, and remove their business from the significant risks posed by non-compliance and data loss. PCI Pal's mission is to safeguard reputation and trust by providing customers with secure payment solutions for any business communications environment including voice, chat, social, email, and contact centre.

PCI Pal is integrated to, and resold by, some of the worlds' leading business communications vendors, as well as major payment service providers.

The entirety of the product-base is available from PCI Pal's global cloud platform hosted in Amazon Web Services ("AWS"), with regional instances across EMEA, North America, and ANZ. PCI Pal products can be used by any size organisation globally, and it is proud to work with some of the largest and most respected brands in the world.

For more information visit www.pcipal.com or LinkedIn: https://www.linkedin.com/company/pci-pal/.

Editor's Contact:
Peppa Sheridan, Peptalk Communications
+ 44 (0)7725 121189 // peppa@peptalkpr.co.uk