Browne Jacobson

Payment Fraud landscape shaped by technology in 2021

Payment systems across Europe are under increased pressure to mitigate fraud risks and defend against persistent attacks from enablers using ever more sophisticated and malicious viruses and malware.

17 December 2021

Payment systems across Europe (as in the UK) are under increased pressure to mitigate risks of fraud and to defend against persistent attacks from enablers using ever more sophisticated and malicious viruses and malware. UK Finance reported fraud losses from bank customers of £754m in the first 6 month of 2021 posed a national security threat.

In its 2021 Fraud Trends Report the European Payments Council (EPC) has carried out an annual survey of the fraud landscape affecting Payment Service Providers (PSPs), as well as merchants, and stakeholders which has identified some interesting trends and offers extensive advice on mitigation techniques.

Although this is a snapshot of experiences in Europe, with the global nature of the payments and banking systems, and jurisdictional challenges posed by fraud threats, its relevance to the UK is no less important. For a UK perspective, UK Finance's Fraud The Facts 2021 provides a detailed analysis of payment industry fraud which includes an Infographic representation of the Covid-19 related lockdown scams likely to have been caused by larger volumes of online activity, and remote working.

The EPC report also provides some historical perspective on the evolution of cyberweapons such as DDoS (Distributed Denial of Service) and Botnet attacks; and how mule accounts are used to monetise the transfers. It also offers a helpful insight into mitigation and risk management both in terms of awareness raising, and technological solutions being pursued by PSPs.

The key takeaways from the report are that the fraudulent schemes in which consumers were once targeted have shifted into the potentially more lucrative business world. The EPC report confirms an evolution in criminal thinking and a change in methodology. SME's, though company directors and employees are being more frequently exploited by social engineering in combination with malware though phishing attacks.

The possibility of human error in individuals or organisations to obtain data, or access to systems rather than vulnerabilities in IT is a gamechanger. It can be used to directly access financial resources or corporate financial business processes to extract payments through authorised push payments (APP fraud) or more seriously can be used as a precursor to encrypting data for extortion through ransomware. Ransomware attacks which do not exclusively require harvesting of user's data and credentials to commit theft cause significant cost and disruption to business activities. It has become the top cyber threat across Europe.

This is particularly concerning when considered in combination with the development of the Advanced Persistent Threats (APTs) which is a targeted attack of companies which repeats and adapts its methods to access through vulnerabilities in IT infrastructure by malware. This access to systems allows criminals to gather information and data to perform unauthorised transactions. The report regarded this as a 'high risk' both for customers and merchants.

Monetisation channels though money mules have reduced and transfers into crypto-assets which offer anonymisation is on the increase. Whilst blockchain offers some visibility, potential obfuscation though new "mixers" make it more difficult to trace crypto-currencies. This places significant burden on PSPs to adopt its AML and SARs tools and policies to detect cashing out by monitoring activities, as well as at the point of payment execution.

Universally acknowledged is that sharing intelligence remains a key mitigation factor. In Europe due to GDPR this is inhibited to a degree. It is hoped that implementation of the EBA fraud reporting guidelines under the 2nd Payment Services Directive due for pan European implementation will permit more accurate fraud assessment figures as well as sharing of prevention measures through members contributions to the Payment Scheme Fraud Prevention Working group (PSFPWG). There remains no mandated fraud reporting save for the SARs regime under AML regulations in the UK but organisations like CIFAS offer data and intelligence collated through its National Fraud database to assist in combatting fraud.

Technological advances have certainly played their part in shaping the fraud landscape in 2021 both in the volume, method and execution of criminal schemes. It remains to be seen whether the evidence of renewed focus on commercial organisations will cause similar levels of engagement and response from the payments sector with its customers; and whether companies will have the foresight to look beyond necessary IT measures and offer regular staff training and seek comprehensive insurance cover for such risks.

Contact

Paul Wainwright

Partner

paul.wainwright@brownejacobson.com

+44 (0)121 237 4577

Related expertise

Counter fraud for insurance

Fraud and asset recovery

Fraud in academy trusts and schools