

Why invest in Fraud Management?

Investing in fraud management is essential for success in the digital economy.



The digital economy is dramatically changing how consumers shop and interact with businesses.

They expect a fast, convenient and highly secure digital experience.

“ Consumers are in the power position, as 2017 is a golden age of choice [and] convenience.⁴

PWC Total Retail report, 2017



With the average company lifespan decreasing rapidly,¹ merchants have to operate as a true digital enterprise to stay competitive and to stay in business.²

Payment and fraud management is no longer a back-office utility. It is a prime differentiator, critical to achieving competitive advantage, improving customer experience and reducing risk.

Digital transformation is not simply a market buzz word. It is real. And those who don't embrace it are in a position to lose.

By 2020, eCommerce sales as a percentage of retail sales are forecast to be 12.4% compared to 8.0% in 2016, according to eMarketer. And engaging customers digitally across channels remains a top digital initiative.³

While there are several drivers of growth in the digital economy, none are more significant than the force of mobile and cloud technologies.

Innovations like these are also contributing to an environment that poses new security challenges. Whilst helping you to capitalise on sales opportunities, if not managed closely they can quickly undermine your business integrity and threaten your customers' confidence.

Overall, the growth in digital channels is increasingly enabling delivery of integrated consumer experiences across multiple touchpoints.

These capabilities lay the foundation platform for an invisible/frictionless payment experience and create a common payment experience across channels of interaction.

¹ <https://www.imperial.ac.uk/business-school/executive-education/resources/articles/why-companies-die/>

² Mckinsey.com - Six secrets to true originality. <http://www.mckinsey.com/business-functions/organization/our-insights/six-building-blocks-for-creating-a-high-performing-digital-enterprise>

³ eMarketer's Updated Forecast and New Mcommerce Estimates for 2016-2021, <http://totalaccess.emarketer.com/reports/viewer.aspx?r=2002182>

⁴ <https://www.pwc.com/gx/en/industries/assets/total-retail-2017.pdf>



Success in the digital economy relies on three areas of focus:



The Customer Experience

Businesses must focus on creating value, delivering this in a way that is seamless – and that can be engaged anytime, anywhere.



Trust / Security

The digital environment introduces new, omnipresent risk. To maintain customer engagement, businesses need to protect customers and their own organisation from harm.



Operational Agility

The pace of change demands fast response to opportunities and threats. Your ability to get atomised services to adapt and execute quickly is crucial.

Merchants who operate successfully in the digital economy are thinking differently about fraud management.

They no longer treat it as purely a cost of doing business. They understand that a committed fraud management investment can be directly linked to success in the digital economy through improved customer satisfaction and engagement, increased revenue, a positive brand reputation – and an overall reduction in operational costs.

The mobile phone has changed human engagement and consumer expectations

It has transformed eCommerce from intent to action anytime – to anytime, anywhere.

Mobile devices have become virtually ubiquitous. The number of connected devices in the world actually overtook the number of people back in 2014. And devices are multiplying faster than we are too.⁵

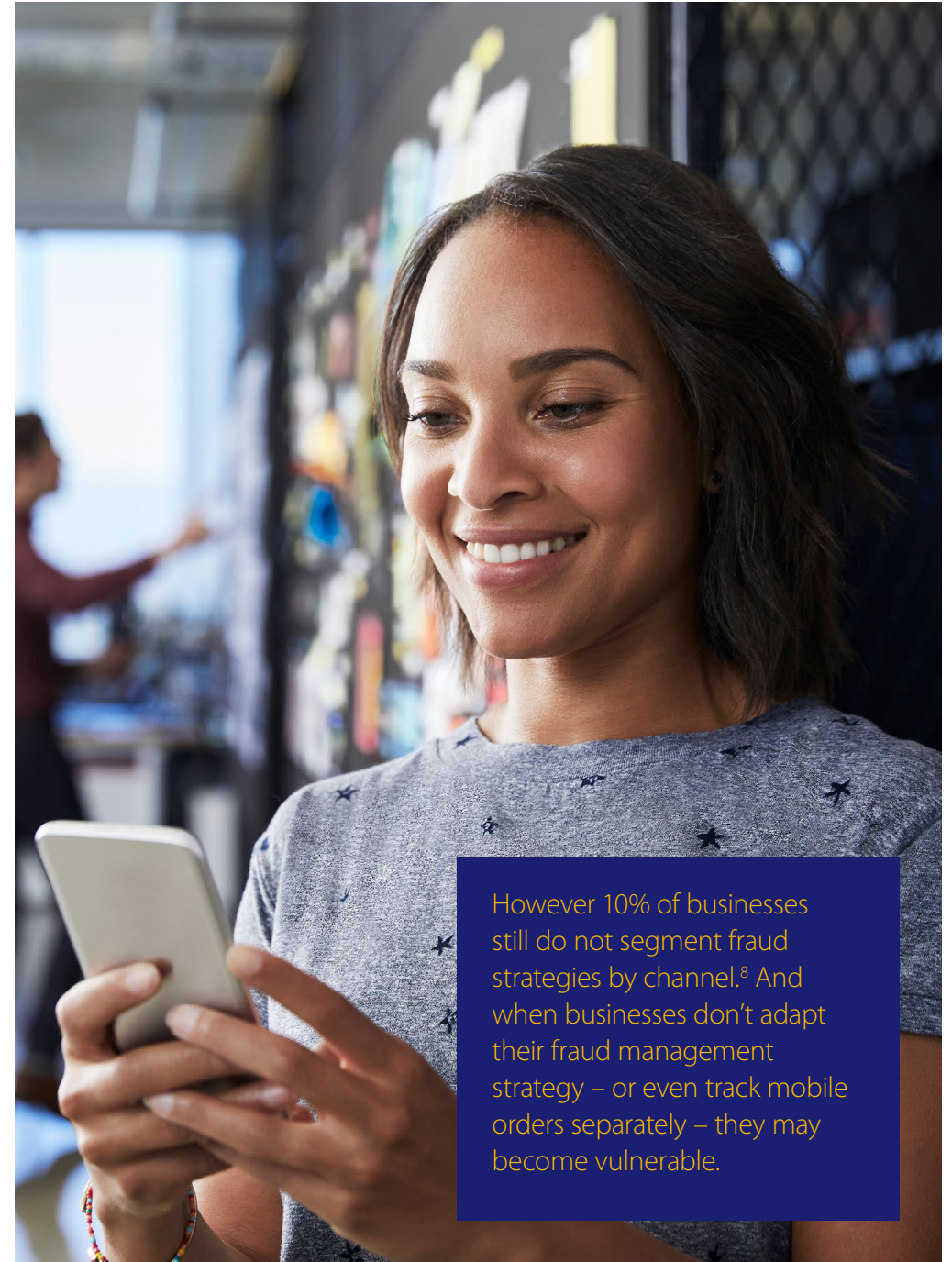
In addition, mobile devices dominate the total minutes we spend online.⁶ So, it's little surprise that mCommerce is growing.⁷

Fraudsters are aware that businesses can be slow to adapt to a new channel and waste no time in taking advantage. For example, they may notice before you, that your existing fraud rules aren't fully suited to the mobile channel and quickly exploit the differences to slip through your defences.

While it may seem intuitive that fraud in mobile would be similar to eCommerce fraud – it isn't. And you are inherently limiting your use of other data sets to determine good transactions from bad transactions.

Further to this, the inability to segment fraud strategies by relationship, channel, and solution category becomes an impediment to a company's ability to deploy new, highly tailored experiences – since fraud management works hand-in-hand with acceptance.

For this reason, the key to success is keeping your best customers by creating value to your service – delivering this seamlessly and protecting them from cybercriminals.



However 10% of businesses still do not segment fraud strategies by channel.⁸ And when businesses don't adapt their fraud management strategy – or even track mobile orders separately – they may become vulnerable.

⁵<http://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html>

⁶<https://qz.com/1116469/we-now-spend-70-of-time-online-on-our-phones/>

⁷<https://www.mckinsey.com/industries/retail/our-insights/doubling-your-companys-growth-in-a-volatile-region>

⁸% of 198 respondents, CyberSource 2016 UK Fraud Report

Your customers expect you to recognise them instantly, understand their individual habits and requirements...

...and deliver a highly-personalised and totally secure experience every time – at any time.

Digital payment types and storing card and account on file can lift checkout completion by up to 50%, because consumers now engage with expectations of seamless checkout.⁹

Millennials want the ability to make payment quickly, in very few steps, whilst being able to pay for anything, anywhere – with personal information being protected.¹⁰

By offering the latest in digital payments – and by storing their payment information on file – your customers are trusting you with their highly personal information.

Increasingly, merchants are being targeted as their security protocols are perceived to be far less strict than banks. Fraudsters are developing different ways to take over your customers' online accounts and use stolen payment information to make fraudulent purchases.

As a nation, we earn around £5.7 billion a year from loyalty schemes. And 86% of us save up our points.¹¹ So, it's no wonder fraudsters find this so appealing.

Monitoring for suspicious activity right from the customers' initial account creation is essential. If, that is, businesses are to defend this highly-lucrative weak point in so many companies' customer data security and loyalty programmes from savvy cybercriminals.

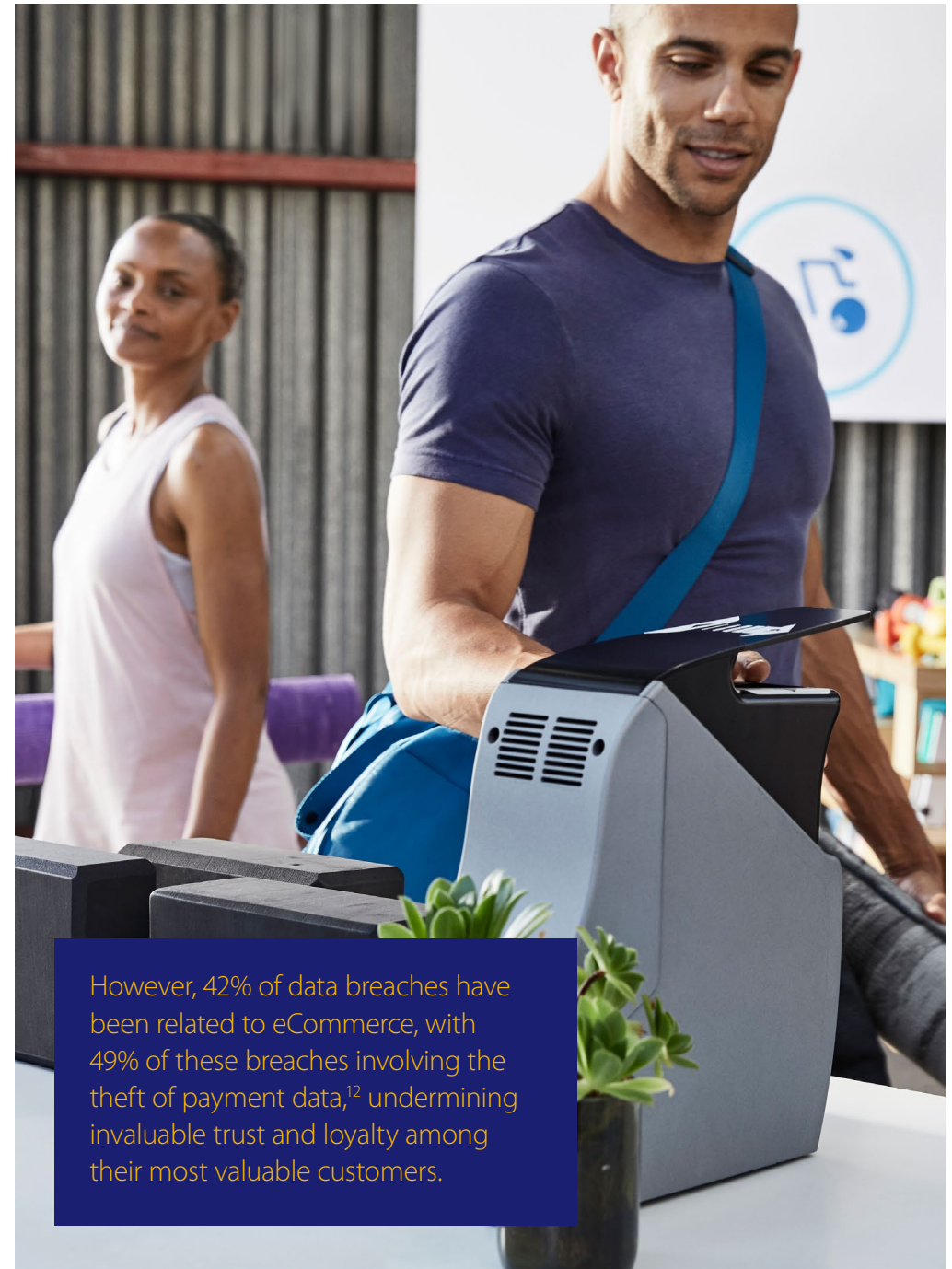
In terms of success factors, trust, security and customer engagement have never been more crucial in today's digital economy.

⁹Business Insider Intelligence 2016

¹⁰Visa 2015 Future of Payments Qualitative Research

¹¹<http://www.mirror.co.uk/money/you-sitting-thousands-loyalty-points-10482757>

¹²Trustwave 2015 Security Report



However, 42% of data breaches have been related to eCommerce, with 49% of these breaches involving the theft of payment data,¹² undermining invaluable trust and loyalty among their most valuable customers.

The digital economy is becoming borderless. Opportunities arrive from all corners of the world.

Connecting to consumers from countries – each with their own distinct characteristics – requires a flexible payment and fraud management approach to enable you to deliver to every customer, on every order, everywhere.

However 62% of UK merchants serving foreign markets experience a higher fraud rate on cross border orders.¹⁵

Cross-border commerce is growing. A Forrester report predicts it will reach \$630 billion by 2022.¹³

Over half of millennials have shopped cross border in the last 12 months and generally feel comfortable buying from an online store in another country.¹⁴

The challenge of distinguishing between fraudulent and genuine customers can be amplified when serving foreign markets. This is because a lack of experience in a new market usually means a lack of knowledge and data about local patterns of fraud and what constitutes normal consumer behaviour.

In the digital economy, fraud is technologically sophisticated, increasingly hard to detect – and is a truly global operation.

To accommodate a growing global and domestic customer base and capture the profitable growth that new markets offer, international expansion must be achieved in a manner that enhances the brand and doesn't degrade it – therefore delivering a seamless customer experience is a critical factor if you are to succeed.



¹³Forrester Data Report: Online Cross-Border Retail Forecast, 2017 To 2022 (Global), April 2017

¹⁴<https://www.internetretailer.com/commentary/2016/03/12/opportunity-selling-online-millennials-around-world>

¹⁵% of respondents serving foreign markets, CyberSource 2016UK Fraud Report

Fraud is a dynamic problem that requires constant rule re-evaluation and the ability to quickly adapt to fraud threats wherever they come from.



On average it takes 3 months to see the impact of a change in fraud strategy.

Executing effective fraud strategies regardless of the channel or country.

Fraud costs the UK up to £193 billion each year.¹⁶

Traditionally, when fine-tuning rules to improve the efficiency and effectiveness of fraud management, 'agile' is not a word you would use to describe the process, if changes are needed.

Three months is required to gather enough cumulative chargeback information, fully assess the impact of new rules and evaluate it properly.

Or a laborious 18 months of time-consuming sequential comparison to hone in on rules if a positive impact is to be made. Months more to test a further iteration – or a different strategy.

As long as future implementation is relied on to assess the effects of fraud management strategies, there will be limitations on how quickly meaningful change can be delivered – whether live, or through passive mode testing.

For this reason, it is crucial that your business is able to make hindsight your insight. To have the ability to undertake 'what if' analysis, and see the results of multiple risk strategies – instantly.

This enables the most effective strategy to be chosen for implementation. And, crucially, it provides the essential operational agility required for success in the digital economy – without impacting operational costs.

Whether on mobile or other innovative devices, card and account on file, or crossing borders into new markets, agility – the ability to adapt to fraud threats at speed – is a key success factor.

¹⁶<http://www.ft.com/cms/s/0/fbb5c2e8-21ad-11e6-9d4dc11776a5124d.html?siteedition=uk#axzz4LMwBr9gM>



Traditional fraud management solutions are often inadequate to address today's threats.

Point solutions, which focus on a single threat or capability, fail to protect against the full range of fraudulent activity.

Many traditional solutions have a single-minded focus on minimising the direct losses caused by fraud. They do not address the need to balance fraud risk with operational costs – and the customer experience.

A holistic approach to fraud management can directly impact the customer experience, trust and security and operational agility – all of which are success factors in the digital economy.

Businesses need a holistic approach. One that begins by reducing the threat of fraud when the customer first establishes an account, and continues all the way through to the moment an online transaction is approved. By implementing an end-to-end approach to fraud management, your business can maximise the effectiveness of fraud prevention, whilst controlling costs and delivering a seamless customer experience.

Find out more about our Multi-Phased Fraud Management Platform

For more information on how our Multi-Phased Fraud Management Platform can detect fraud and protect your business and customers – from customer account creation through to order evaluation, visit

www.cybersource.co.uk/strengthenyournumbers



Account Takeover Protection

Identify suspicious behaviour and help keep your customer accounts secure.



Loyalty Fraud Management

Monitor for suspicious activity and create a secure loyalty programme.

1



Decision Manager

Spot more fraudulent orders faster and maintain a positive customer experience.



Decision Manager Replay

Instantly see the impact of fraud strategies and ensure a successful implementation.

2



Rules-based Payer Authentication

Determine who you authenticate, challenge or accept – and protect against cart abandonment.

3



Managed Risk Services

Recognise fraud trends and patterns and reduce operational costs.

4

Why CyberSource?

- Our platform is built on a secure Visa infrastructure with the benefits and insights of a \$427 billion global processing network.
- We offer payment acceptance in 190+ countries – and accept 137 currencies.
- We have 100 acquirer processor connections and this is increasing by 20+ each year.

In 2017 we:

- Managed 277 billion payments
- Served 450,000 customers worldwide
- Prevented \$11.952B in potential fraud via Decision Manager¹⁶

¹⁶Represents the value of transactions rejected as fraudulent using Decision Manager in 2017

Contact us

Email. europe@cybersource.com www.cybersource.co.uk

CyberSource is a global, modular payment management platform built on secure Visa infrastructure with the benefits and insights of a vast \$427 billion global processing network. This solution helps businesses operate with agility and reach their digital commerce goals by enhancing customer experience, growing revenues and mitigating risk. For acquirer partners, CyberSource provides a technology platform, payments expertise and support services that help them grow and manage their merchant portfolio to fulfill their brand promise. For more information, please visit www.cybersource.com

© 2018 CyberSource Corporation. All rights reserved.