ISSUE 6 / NOVEMBER 2014

blackfoot

BLACKFOOT QUARTERLY

WELCOME TO THE WINTER 2014 BLACKFOOT NEWSLETTER.

2014 has been a busy year for the bad guys, but also for the standards writers and regulators. We look back on some of this year's key trends, and look forward to what 2015 may have in store.

The growth of cybercrime

The pace of data breach news seems to be hitting like an incoming tide. Vodafone Germany, JP Morgan and what seems like most of US high street retail have reported data compromises this year. We are even seeing 'breach weariness' as consumers and the IT security industry sigh when the next victim is announced. But this is serious stuff because it's the shape of things to come.

See our articles on **weaponisation** in the cybercrime arms race and **what makes a good pen test?** on the commoditisation of some aspects of cybercrime and information security. We also have an upcoming **webinar** about the key cybercrime threats, threat vectors and the case for security, so register now to participate or download the recording afterwards.

The growth of regulation

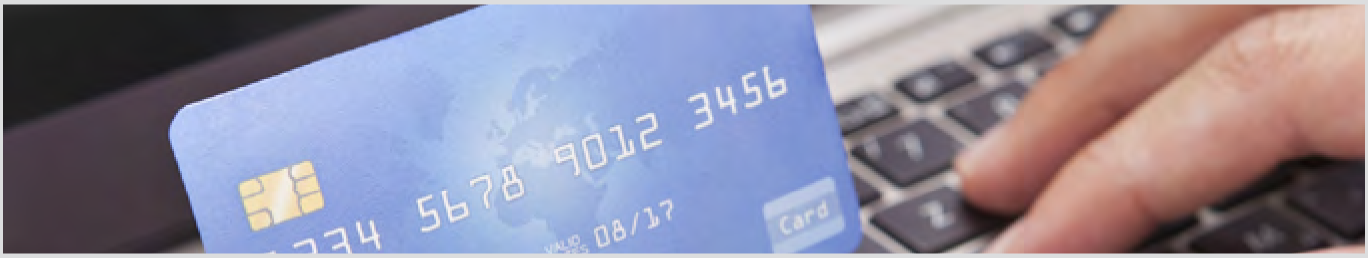
PCI DSS version 3.0 comes into force in 2015 with increased control requirements for hosted website providers, and more delineated responsibilities with third parties. In Brussels, the regulators are examining card interchange payments, which could well lead to the most **significant shake-up of card interchange fees** in 20 years. And closer to home, the new UK Payment Systems Regulator will be operational from April 2015.

More is expected on both the PSD2 (Payment Services Directive 2) and data privacy in 2015. We have a **webinar on data privacy** planned in January 2015, which will consider the various requirements, their intent and the risks, among other things.

So here's to a great festive season and needless to say Blackfoot will be here for you throughout 2015 — the year information security comes of age.

Matthew Tyler
CEO, Blackfoot UK

IN THIS ISSUE



HUGE SHAKE-UP OF CARD INTERCHANGE FEES EXPECTED

Potential cost savings for UK Retail plc, but there'll be winners as well as losers...

Interchange calculations on card payments in Europe will change significantly next year, impacting merchant costs but also acquirer profitability. While there are opportunities for both parties, particularly around cross-border acquiring, there are also dangers of increased costs and complexity.

Blackfoot retail customers are advised to speak to their current and prospective acquirers about the impact of the proposals, and to keep a watching brief on developments.

What's changing?

In July 2013 the European Commission published proposals to regulate interchange fees on card payments in Europe. The Council of the European Union is currently debating proposals to cap debit card fees at 0.2% and credit card fees at 0.3% of the transaction value.

Meanwhile, Visa Europe has already committed to reducing interchange rates for cross-border consumer payments to 0.2% for debit cards and 0.3% for credit cards in 2015. This has stimulated renewed interest in cross-border acquiring.

Acquirers are able to offer these reduced cross-border rates to merchants domiciled in a different European country (to their acquirer). In countries where domestic interchange rates are higher (e.g. in the UK), merchants could potentially make huge savings in the short-term by contracting with an European cross-border acquirer. But is it that simple?

Unsurprisingly, it's not.

What's the impact?

The commitments above currently apply only to Visa Europe cross-border consumer payments, not to other card payments or those from other card schemes, although further rate changes are expected later in 2015. Local acquirers are investigating various offshoring options to retain existing merchants, and reviewing their pricing schedules. In the meantime, some merchants could pay less for card acceptance services, whilst others could well pay more, depending on their pricing plan and how their customers choose to pay.

Blackfoot recommendations

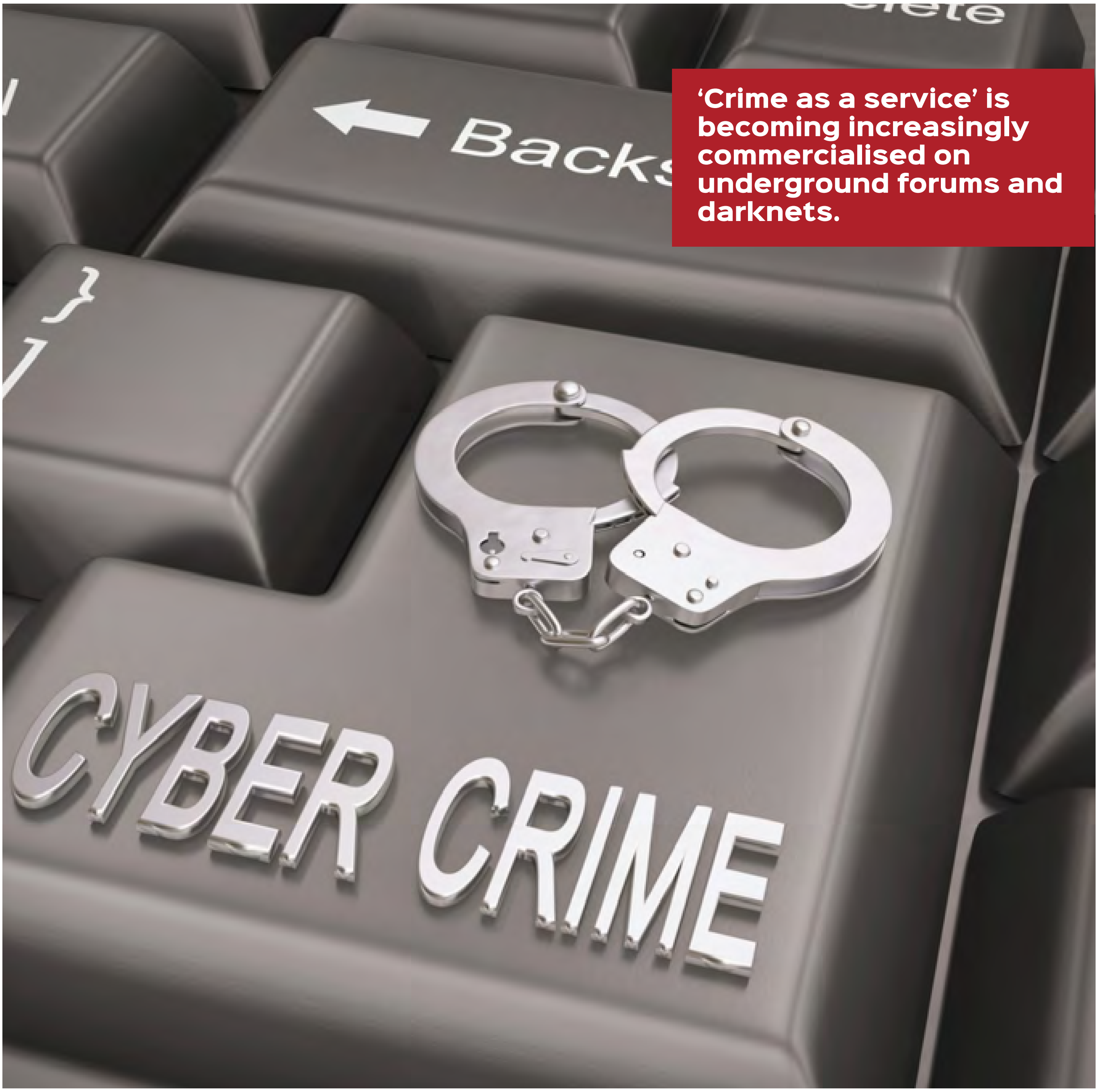
We recommend our retail customers to speak to their current and prospective acquirers about the impact of the interchange proposals, if they haven't already done so. Bear in mind, however, that just as with information security and compliance, answers to questions about interchange and switching acquirers always begin "It depends…" So before agreeing new terms or switching acquirers, perform a cost-benefit analysis.

Some things to consider include: your current card acceptance arrangements (price plan, level of service, contractual terms etc.), the net benefit of changes to your MSC (will your acquirer pass on any interchange rates cuts and/or will costs be structured in a different way?), your business goals and the payment habits of your customers now and in the future, the implications of switching (cost, service, lead times, resource).

What is interchange?

Interchange is a fee paid between two banks each time a payment card is used. In the case of card payments made with Visa and MasterCard, which operate four-party models, the fee for a typical purchase transaction is paid by the merchant's bank (the acquirer) to the cardholder's bank (the issuer). The precise fee depends on a number of factors, including type of card used, security of the transaction, countries where the parties are domiciled and so on. Generally the more secure the transaction (EMV chip or 3D secure), the lower the interchange.

Acquirers usually pass on the cost of interchange to their merchants as part of the merchant service charge (MSC) levied for card acquiring services. Other components of the MSC include card scheme fees, optional acquirer service fees and acquirer margin. Broadly, the MSC a merchant pays as well as the transparency over the break-down of this cost depends on the pricing plan and contract negotiated with their acquirer.



‘Crime as a service’ is becoming increasingly commercialised on underground forums and darknets.

WEAPONISATION WARNING

Barriers to entry for cybercrime newbies fall as ‘weaponisation’ rises

‘Weaponisation’ in the cybersecurity arms race was one of the major themes to emerge from this year’s Black Hat security conference in Las Vegas.

Criminals are increasingly packaging their services into off-the-shelf or ‘crime as a service’ kits. The prices for these malware, ransomware and wifi intercept kits are falling on underground forums and darknets. Consequently, barriers to entry for cybercriminals without specialised knowledge or technical skills are falling, too.

These trends are also reflected in the legitimate information security industry. A portable device designed to assist auditing and penetration testing of man-in-the-middle attacks on wifi networks retails for around US$100. An open source Bluetooth test tool able to detect all clear-text traffic on Bluetooth connections retails for around US$120.

Blackfoot customers are advised to be alert to the growing trend towards ‘weaponisation’ among cybercriminals, and consider the implications for information security within their own organisations.

WHAT MAKES A GOOD PEN TEST?

As penetration testing becomes more commoditised, we consider what makes a good test

How many times have you been cold-called by a vendor this month, trying to sell you a vulnerability assessment or penetration testing solution? Those working in information security, IT or internal audit will know from their own experience that more and more off-the-shelf, automated penetration testing tools are available.

Penetration and security testing remains a strong component of the Blackfoot service offering. So, as penetration testing becomes more commoditised, we consider what makes a good test.

Define the purpose

Firstly, consider not so much the mechanics of the test, but your reasons for doing it. This may sound like common sense, but in our experience not all customers are certain as to the purpose of a test.

It can be tempting to regard penetration testing as a means to satisfy an upcoming certification or compliance requirement. However seen in this light, any testing risks becoming a perfunctory, tick-box exercise, which adds little to the long-term security of your business.

Every business has its constraints, whether as a result of budget, time or resource — and we understand this. We can help you determine the aims and objectives of any testing. Naturally if you do have a certification or compliance action looming, we can offer pragmatic advice on the scope and the approach of any testing. This will help you to make considered investments in the context of your short and longer term business goals.

It's tempting to see penetration testing as simply a means to satisfy an upcoming certification or compliance requirement. However this risks making it a tick-box exercise, which adds little to the long-term security of your business.

Define the scope

Next, consider the scope of any testing. We'd advise you to identify, assess and evaluate the areas of your business or systems that are most at risk. What sensitive data do you hold, and where? If the worst were to happen, what would hurt your business the most if it were stolen or exploited?

Trying to test your whole infrastructure would simply be too cost-, time- and labour-intensive. It may not make your business any more secure either. Our consultants have plenty of experience in defining the scope of testing projects. They are used to gathering requirements, talking to business owners, identifying the data of value, possible risks, and so on.

Plan the test

Once you have defined the purpose and scope of any test, it's a matter of planning the various tests. If you use off-the-shelf testing tools, it may be possible to select the tests you wish to run and the systems to be tested. This may be sufficient in some cases. However, when we work with customers, we tailor the testing according to the purpose, scope and requirements of your particular business.

Execute the test

It is possible to automate pen testing with various tools, or outsource this to junior associates or abroad. At Blackfoot we always use a mix of automated and manual assessment methods, however we don't believe that there's any substitute for knowledge, experience and the human touch.

We always deploy testers with experience and skills pertinent to your test. We draw on specialists in card payment data security, web and mobile applications, wireless security, social engineering and so on when executing a pen test. Our testers think and act as if they were hackers. This means probing the relevant attack vectors, but also bringing creativity, tenacity and thoroughness to the task.

Learn from the test

Once the test is complete, use the output to make improvements. This sounds simple enough, but feedback from customers tells us that this is where you particularly value the expertise of Blackfoot consultants.

We help you learn from the experience. We also help you learn from other people's experience. We prepare a report with the findings as well as insights and recommendations as to how to put things right. We don't believe in over-complicating things and spending £1,000 to protect £1. As such, you can rely on recommendations that are solid, future-proofed and rooted in real-world pragmatism.

For more information

If you are interested in commissioning penetration or other testing, or would like our opinion on a testing tool or approach, please contact your Blackfoot sales representative.

WEBINARS

New series of free, lunchtime webinars on key industry topics

A new series of our popular lunchtime webinars will start in December 2014. Led by Blackfoot CEO, Matthew Tyler, these 45-minute webinars will bring you up to speed on topics of interest, such as the implications of organised cybercrime, data privacy regulation and cloud computing.

Register on the links below to participate in these free webinars, or to download the recording after transmission. Please also feel free to pass these links on to anyone else in your organisation who may benefit.

INTERNET ORGANISED CRIME AND THE CASE FOR SECURITY

Monday 01 December 2014, 12.00-12.45 (GMT)

A new Europol report confirms what many within the security industry had already suspected: cybercrime is becoming more commercialised thus reducing barriers to entry for would-be criminals.

The 2014 iOCTA (Internet Organised Crime Threat Assessment) report aims to help decision-makers prioritise cybercrime and the emerging threats, such as cyber attacks, online exploitation and payment fraud.

Matthew Tyler will share the key findings, explain how threats and threat vectors are evolving, and discuss the imperative for collective management by governments, businesses and citizens alike.

The presentation will also briefly introduce new data security and privacy regulations coming into effect in 2015.

> **https://www.eventbrite.co.uk/e/internet-organised-crime-and-the-case-for-security-tickets-14020773511**

WEBINARS

DATA PRIVACY

Monday 19 January 2015, 12.00-12.45 (GMT)

Hardly a day goes by without another information security or privacy standard being announced, or so it seems. This begs the question, are the standards joined up? Moreover, who do they serve, how does an organisation balance the needs of the business, customers and regulators, and what will this cost?

Matthew Tyler will demystify the main requirements of the new standards, their intent and risks. He will also explore whether regulation, and more regulation, is the answer.

> **https://www.eventbrite.co.uk/e/data-privacy-web-seminar-tickets-14020063387**

SECURITY IN THE CLOUD: A SHARED RESPONSIBILITY?

Monday 09 February 2015, 12.00-12.45 (GMT)

Changes in technology and working practices are heralding a new era of BYOD (bring your own device) as well as WOAD (work on any device) made possible by cloud computing. Growing numbers of organisations are meeting these challenges through secure managed service and infrastructure providers. But are roles and responsibilities adequately defined, and do they comply with emerging regulation?

Matthew Tyler will examine the drivers for change, the impact of evolving data privacy and governance regulations on security, and how your business can position itself for success.

> **https://www.eventbrite.co.uk/e/security-in-the-cloud-a-shared-responsibility-tickets-14021182735**

blackfoot

Blackfoot UK Limited
Tel: 0845 805 2409
E-mail: info@blackfootuk.com
Web: www.blackfootuk.com

ADVISE >
ASSESS >
ASSURE >

This material is for information purposes only and does not take into consideration the particular circumstances or objectives of your business. Whilst every reasonable effort has been made to ensure the accuracy of the information in this document, Blackfoot UK Limited shall not be held liable for any errors or omissions.