ELSEVIER

computer
FRAUD & SECURITY

ISSN 1361-3723 January 2016 www.computerfraudandsecurity.com

Featured in this issue:

Think locally, fight globally

Organised criminals operate at a global level to clone cards, hack payment systems, phish for card details and disrupt commerce. Yet while the Internet has created a truly global economy, markets are still diverse.

Each market has different patterns and regulations for fraud. There are fraud hotspots, there are particular security issues associated with each region and there are different methods of payments in different territories. Taking a global view of what's going on provides insight into the regional trends that impact upon global payment security, as Christoph Tutsch of ONPEX explains.

Full story on page 5…

The eagle has landed – what happens next?

Understanding the behaviour of attackers after they have penetrated your systems is not about preventing attacks but rather focusing on what happens once they have access to your networks.

In this second part of a two-part article, Tracey Caldwell looks at how organisations can classify and counter developing threats. Sharing intelligence is crucial, but it's important to strike a balance between the benefit of information sharing and the risk of tipping off attackers that the organisation is on to them.

Full story on page 8…

How technology can mitigate and counteract cyber-stalking and online grooming

Cyber-stalking and online bullying can have devastating effects on individuals, but it's affecting the workplace too. In response, relevant technology could be used to counteract and mitigate the damage caused by online perpetrators.

Haider M al-Khateeb and Gregory Epiphaniou of the University of Bedfordshire approach this issue using an incident response methodology and discuss the role of machine learning to identify and classify such attacks. They also examine how digital forensic investigations can be carried out in order to analyse the nature of the offence and preserve evidence.

Full story on page 14…

Verizon warns of health data vulnerabilities, while Hello Kitty & US voters among breach victims

Personally identifiable medical information is being leaked at a serious rate, and not just by the healthcare industry, according to new research by Verizon. And nearly a fifth of the data breaches are taking years to discover.

These conclusions are contained in a special report that comes from the same sources as Verizon's renowned annual Data Breach Investigations Report (DBIR). The '2015 Protected Health

Continued on page 3...

Contents

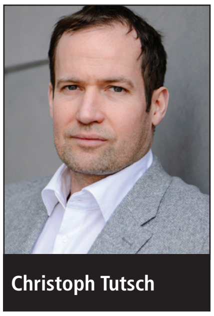
NEWS

FEATURES

REGULARS

Think locally, fight globally

Christoph Tutsch, ONPEX



Christoph Tutsch

Payment fraud knows no national boundaries. Organised criminals operate at a global level to clone cards, hack payment systems, phish for card details and disrupt commerce, all at the cost of billions of pounds per year. Yet while the Internet and ecommerce have connected business and trade in a way unheard of even 20 years ago, bringing a truly global economy, markets are still diverse. From Germany to Ghana, from China to Canada, each market has different patterns and regulations for fraud. There are fraud hotspots, there are particular security issues associated with particular regions and there are different methods of payments in different territories.

Taking a global view of what's going on provides insight into the regional trends that impact upon global payment security. For this article, we will concentrate on four key regions, each with their own particular trends and problems. By doing so, we hope to be able to paint a picture of a diverse world of fraud and security risk but with a number of consistent themes throughout.

Europe

When it comes to payment card security, Europe has led the way. This is predominantly down to the fact that Europe has had an almost universal adoption of EMV (Europay MasterCard Visa) protocols for payment cards. EMV protocols are the technical standard for encrypted payment cards. In essence, it is the gold chip seen on credit and debit cards.

Prior to this, card details were held on the magnetic strip on the rear of the card, above the signature strip. This strip was based on technology first invented during the Second World War and was easy to hack and counterfeit. Allied to this critical flaw was the fact that the method of authentication was the card holder signature. Again, for an experienced, or even inexperienced criminal, this can be easy to copy. Put simply, payment cards were not secure and fraud losses were in the billions. So, the industry took action.

January 2005 saw the MasterCard liability shift in the EU – that is, if a merchant is defrauded and is not using EMV protocols, he or she will be liable for that fraud, not the card issuer or bank. This was followed in January 2006 by Visa. In February of that year, Chip and PIN was rolled out across the UK.

Chip and PIN was, at the time, a radical leap forward in card and authentication security. Information on cards was made far more secure by the addition of the encryption chip, and the use of a four-digit PIN to authenticate card holders was far more secure than a signature. Across Europe, EMV has made payment cards far more secure. A comparison of UK fraud figures from 2004 and 2014 demonstrates the extent of this (Table 1).[1]

Other avenues

The UK has seen a 58% drop in card-present crime since EMV protocols were introduced and this has been the case throughout Europe. Yet this does not mean that card fraud has disappeared from Europe. Far from it. Fraudsters have simply turned their attention to other avenues, specifically card-not-present (CNP) fraud.

CNP fraud is when a fraudster has access to sufficient details (card number, addresses and so on) to be able to make a fraudulent transaction on a payment card. At the same time as EMV protocols started to stamp out card-present fraud, the exponential rise of e-commerce opened a new avenue for fraudsters. European Central Bank (ECB) figures from 2013, the most recent available, show that CNP fraud cost the EU €958m, 66% of the total fraud figure.[2]

> ***"Getting authentication right will prove vital. Given that so many aspects of our lives are online for all to see these days, and our seeming inability to choose secure passwords, we are making life too easy for fraudsters"***

Taking the UK example once more, in 2014, CNP fraud cost £331.5m, of which £217.4m was online related. This CNP fraud figure represents an increase of 120% from the 2004 figure of £150.8m. Total card fraud figures may have fallen from £504.8m in 2004

Fraud type	2004	2014	Percentage Decrease
Counterfeit	£129.7m	£47.9m	63%
Lost or stolen	£114.4m	£59.7m	49%
Card ID theft	£36.9m	£29.9m	19%
Card non-receipt	£72.9m	£10.1m	86%
Total	£353.9m	£147.6m	58%

UK Fraud figures in 2004 and 2014. Source: Financial Fraud Action UK.

to £479m in 2014, but the continued growth of CNP fraud continues to challenge the benefits of EMV adoption.

Fighting CNP fraud continues to be the key priority for the industry in Europe with issuers, banks and merchants pushing for improvements in the storage and transmission of payment data and in customer authentication. Getting authentication right will prove vital. Given that so many aspects of our lives are online for all to see these days, and our seeming inability to choose secure passwords, we are making life too easy for fraudsters.

So, multifactor authentication, bringing together passwords, biometrics and other methods of ID verification will clearly be the way forward. Right now, though, the industry is still struggling to decide upon the way forward with countless companies, all with secure and easy authentication methods, fighting to be the next standard. Until this standard is found and agreed upon, CNP fraud will continue to be the dominant payment fraud trend in Europe.

The US

While Europe has blazed a trail in EMV adoption, the US is a decade behind. While just over a quarter of the world's credit card transactions originate in the US, that country accounts for almost half of the world's fraudulent transactions and this has been down to the delay in the US adopting EMV.[3]

> ***"International retailers and mobile commerce merchants took the heaviest blows, with 1.56% and 1.68% of revenue lost, respectively"***

October 2015 saw the US finally adopting EMV protocols, with card schemes introducing a liability shift, and it has taken a number of high-profile security breaches, such as Target, Michaels and Home Depot, for US banks and issuers to decide that the costs of fraud outweigh the costs of implementing EMV (estimated at $8.65bn).[4] And these fraud costs are, to be blunt, huge. The LexisNexis True Cost of Fraud 2015 study found that retail fraud cost accounted for 1.32% of total revenue in 2015, which represents a 94% increase over 2014. In particular, international retailers and mobile commerce merchants took the heaviest blows, with 1.56% and 1.68% of revenue lost, respectively.[5]

The question, then, is what impact this will have on fraud in the US. In the short-term, there are two interlinked trends that can be predicted:

- **Smaller retailers will be hit hardest**: US retail giants such as Wal-Mart and Walgreens have the resources to implement EMV, but for smaller retailers, costs are proving a headache. Research by Javelin Strategy and Research suggests that the costs of proving 15 million EMV-compliant POS devices in the US will be $6.75bn, which works out at $450 per device installed into existing payment systems. This is indicative of the costs merchants face when they are looking to install new payments technology. For big US retailers these are costs that can be easily absorbed. For smaller merchants, it is more of a challenge. As the US got closer towards the liability shift date, more and more merchants were understandably complaining about the costs involved. In a recent Fox News article, the owner of a chain of restaurants in New Orleans quoted a cost of $25,000 to become EMV compliant.[6] The company isn't willing to increase prices to absorb costs so, instead, is choosing to delay the adoption of new security cameras. A result of these costs could be that smaller retailers could delay implementation, leaving them exposed to risk.
- **A final peak in card-present fraud:** Fraudsters will be alert to the fact that their window of opportunity is shortly to close. And they will also be alert to the fact that some retailers will be slow to switch to EMV, as will some issuers. So there could be a short-term peak in card-present fraud as fraudsters take advantage of opportunity for the final time.

Longer-term predictions

Regarding longer team predictions, again there are two that can be made with reasonable confidence:

- **Card present fraud won't drop as it did in Europe:** While the US is adopting the chip part of Chip and PIN, it isn't adopting the PIN section. Research from Forrester suggests that it could be until 2020 until US consumers authenticate themselves via PIN for in-store purchases.[7] Until this time, consumers will still use signatures. So, rather than chip and PIN, it will be chip and pen. This means that while counterfeit card crime should drop, due to the data encryption afforded by the chip, lost or stolen card crime will not as the added security of PIN is not present.
- **CNP fraud will rise:** Just like in Europe 10 years ago, US fraudsters will not simply give up. Instead, they will use other channels – specifically, CNP fraud. And, much like in Europe, until there is a standard for authentication for online and other remote purchases, the war against CNP fraud will be far from won.

Of these two predicted consequences, it is CNP fraud that has the most implications on the global stage. While lost or stolen card fraud will continue to hit US banks, issuers and merchants, aside from the economic damage done, there will be little impact globally. Yet online fraud knows no national boundaries and if US criminals turn to it in ever greater numbers, this could have a dramatic effect on global payment security.

China

China has around 600 million online consumers with a market value of €14.5bn.[8] This huge market is being driven by mobile. China has around 1.29 billion registered mobile phone users and this explosion of mobile commerce has seen the market boom.[9] Mobile commerce makes digital retail accessible to the world. Consumers don't need an expensive laptop or desktop computer, nor do they need Internet. With 70% of the world's population having access to 3G or better, all that is needed is an increasingly affordable smartphone to start carrying out online transactions.[10]

"China is still a country with significant areas of poverty. And this gives fraudsters a ready supply of people desperate enough to become engaged in criminal activity"

Yet with this opportunity comes challenge. Mobile platforms are, by their nature, less secure than computers, and criminals in China are quick to take advantage of this. While the growing wealth and economic power of China is reported on a regular basis, it is still a country with significant areas of poverty. And this gives fraudsters a ready supply of people desperate enough to become engaged in criminal activity. Mobile fraud is part of the wider CNP trend and, as previously noted, has no national boundaries. Chinese fraudsters are exploiting the developing nature of the Chinese and wider Asian ecommerce market to commit fraud on mobiles.

Across Asia, mobile payments account for 14% of transactions but make a disproportionate 21% of total fraud cases.[11] Dealing with this is proving a challenge for Chinese authorities. For example, over 130 million SIM cards in China are unregistered and a number of them have been utilised by criminals to conduct telecom fraud. To combat this, the Ministry of Industry launched a campaign to implement a real-name registration system for phone users.[12]

So China has a long way to go before any sort of crack down on mobile payment fraud can begin in earnest.

India

In some respects India is similar to China. Again it is a new market, again ecommerce is booming, again this is driven by an explosion in mobile and, again, online crime is a serious problem. It cost India $870m in 2013, the most recently available figures.[13] Yet while these frauds are taking place on cutting edge platforms they are coming from the traditional cons of confidence tricks.

Banking fraud is a particular problem in India. Local fraud expert, cybercrime expert Anshul Abhang told *The Times of India* that most net banking frauds happen because users respond to phishing emails sent from fake email addresses. "The sender of email asks the account holder to update his credentials by clicking on a link, which then takes him to a fake website," he said.

"While India is embracing online commerce, it is coming to it later than Western Europe and the US. As a consequence, the same scams that Western consumers fell for 15 years ago (and still sometimes do) are working"

Much like in China, criminals take advantage of poverty and unemployment. One government official explained: "Unemployed youths are soft targets who fall for lucrative job offers. In case of card holders, fraudsters call posing as bank manager and tell the person that his ATM card has expired and seek his confidential details. Many end up revealing the information."

Much of this can be attributed to the fact that while India is embracing online commerce, it is coming to it later than Western Europe and the US. As a consequence, the same scams that Western consumers fell for 15 years ago (and still sometimes do) are working on the relatively un-savvy Indian consumers.

However, this won't last. Authorities are educating and Indian consumers are rapidly learning. Yet fraudsters will only get more sophisticated and different types of fraud will arise, requiring new ways of fighting them.

Conclusions

There are three main conclusions we can draw from this overview.

Fraudsters are opportunistic: Fraudsters will look for the path of least resistance. In Europe, that means CNP fraud. In the US, it's counterfeit and lost or stolen card fraud (although this is likely to change soon). In China, the dominance of mobile means that is where fraudsters attack and the relative lack of security awareness of the Indian consumer makes that the ideal avenue for fraudsters. Closing down one avenue can mean that fraudsters will seek other ones. However, with the EMV shift in the US, for example, this time the banks, issuers and merchants should be ready and not let the CNP spike happen a second time. That will, however, require a concerted effort towards a global standard for online authentication.

User error is the easiest path in: Of all the various fraud types identified in the territories we have examined, the common denominator is user error. What causes CNP fraud? Hackable passwords, consumers not taking care of personal details and not having sufficient security on their mobile devices and laptops. Counterfeit card and lost or stolen card fraud are driven by carelessness with cards and personal effects. Mobile fraud is driven by carelessness and the scams in India are driven by people being duped. Consumer education can, and should, be an answer to this. Equally, though, banks and issuers have a responsibility to make security easier to comply with.

Local knowledge is everything: Commerce is global. Fraud is local. Despite the common denominators identified, each of the regions we have studied have their own particular trends, even quirks. Any merchant wanting to have a global reach wants to have a presence in

Europe, the US, China and India. We examined them because they are such fertile markets. Yet knowing what fraud is most likely in each area is the first step to building a global payment structure that can handle fraud at all levels.

About the author

Christoph Tutsch is the founder and CEO of ONPEX. He set up and funded the business in 2010 to provide businesses with a way of handling online payments. He is responsible for the overall direction of the business and its continuing growth around the world. A lifelong entrepreneur, Tutsch was previously co-founder and director of several companies in the telecoms and marketing industries.

References

1. 'Fraud The Facts'. Financial Fraud Action UK. Accessed Dec 2015. www.financialfraudaction.org.uk/Fraud-the-Facts-2015.asp.
2. 'Card fraud rises across Europe – ECB'. Finextra, 30 Dec 2015. Accessed Dec 2015. www.finextra.com/news/fullstory.aspx?newsitemid=27626.
3. Laliberte, Scott. 'EMV's the 15% Solution for Card Fraud'. PaymentsSource, 18 Sep 2015. Accessed Dec 2015. www.paymentssource.com/news/paythink/emv-fifteen-percent-solution-for-card-fraud-3022346-1.html.
4. 'Will Retailers be Ready for EMV by Oct 2015?'. Payments Leader, 16 Oct 2013. Accessed Dec 2015. www.paymentsleader.com/will-retailers-be-ready-for-emv-by-oct-2015/.
5. 'Retail Fraud Revenue Losses Up 94% From 2014'. PYMNTS.com, 17 Sep 2015. Accessed Dec 2015. www.pymnts.com/news/2015/retail-fraud-revenue-losses-up-94-percent-from-2014/.
6. 'New chip cards squeezing small businesses, forcing them to pay thousands for new equipment'. Fox Business, 17 Jun 2015. Accessed Dec 2015. www.foxbusiness.com/technology/2015/06/17/new-chip-cards-squeezing-small-businesses-forcing-them-to-pay-thousands-for-new/.
7. Norton, Steven. 'Chip-and-PIN Security for Payment Cards Won't Happen Until 2020: Forrester'. Wall Street Journal, 29 Apr 2015. Accessed Dec 2015. http://blogs.wsj.com/cio/2015/04/29/broad-emv-adoption-for-plastic-cards-wont-happen-until-2020-forrester/.
8. Burbank, John. 'Consumers without borders: Chinese shoppers present a key growth opportunity for the US market this holiday season'. Nielsen, 3 Dec 2014. Accessed Dec 2015. www.nielsen.com/us/en/insights/news/2014/consumers-without-borders – chinese-shoppers-present-a-key-growth.html.
9. 'Number of mobile cell phone subscribers in China from September 2014 to September 2015 (in millions)'. Statistica. Accessed Dec 2015. www.statista.com/statistics/278204/china-mobile-users-by-month/.
10. Voltornist, Andrey. 'Mobile broadband reach expanding globally'. GSMA Intelligence, 18 Dec 2014. Accessed Dec 2015. https://gsmaintelligence.com/research/2014/12/mobile-broadband-reach-expanding-globally/453/.
11. 'Mobile commerce fraud is on the rise in Asia'. Mobile Commerce Press, 10 Sep 2015. Accessed Dec 2015. www.mobilecommercepress.com/mobile-commerce-fraud-is-on-the-rise-in-asia/8518642/.
12. Lee, Cyrus. 'Chinese telcos impose harsh rules to push real-name SIM registration'. ZDNet, 17 Sep 2015. Accessed Dec 2015. www.zdnet.com/article/chinese-telcos-impose-harsh-rules-to-push-real-name-sim-registration/.
13. 'India's new Internet users are a target for fraud'. BBC News, 24 April 2015. Accessed Dec 2015. www.bbc.com/news/business-32446198.

The eagle has landed – what happens next?

Tracey Caldwell, freelance journalist

Tracey Caldwell

Understanding the behaviour of attackers once the 'eagle has landed' – after they have penetrated your systems – is not about preventing attacks but rather focusing on what happens once hackers gain access to your networks. In the first part of this two-part article we started by reviewing the changing threat vectors and objectives. Now we look at how organisations can classify and counter these developing threats.

Hacker motives and techniques have changed greatly in the past 15 years, according to Gavin Millard, technical director for EMEA at Tenable Network Security. "We've seen a huge shift in attacks from simple vandalism towards data collection and profit," he says. "One of the major changes observed over the last few years is the move to leverage known and trusted tools against the target organisation, making it even more difficult to spot an intruder."