References

1. 'Password Guidance: Simplifying Your Approach'. National Cyber-security Centre, 7 Jan 2016. Accessed Jan 2017. www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach.
2. Morris, R; Thompson, K. 'Password Security: A Case History'. Communications of the ACM, 1979, vol 22, no.11, pp.594-597.
3. 'Worst Passwords of 2015'. SplashData, 19 Jan 2016. Accessed Jan 2017. www.teamsid.com/worst-passwords-2015/.
4. Holak, Brian. 'Dropbox hack and the password security conundrum'. TechTarget, 2 Sep 2016. Accessed Jan 2017. http://searchcio.techtarget.com/news/450303697/Dropbox-hack-and-the-password-security-conundrum.
5. Warkentin, M; Davis, K; Bekkering, E. 'Introducing the Check-Off Password System (COPS): An Advancement in User Authentication Methods and Information Security'. Journal of Organisational and End User Computing, Vol.16, No.3, Jul-Sep 2004, pp.41-58.
6. Furnell, S. 'Password practices on leading websites – revisited'. Computer Fraud & Security, Dec 2014, pp.5-11. Accessed Jan 2017. www.sciencedirect.com/science/article/pii/S136137231470555X.
7. Klein, D. 'Foiling the Cracker: A Survey of, and Improvements to, Password Security'. In Proceedings of the Second USENIX Security Workshop, Portland, Oregon, August 1990, pp.5-14.
8. Furnell, S; Bär, N. 'Essential Lessons Still not Learned? Examining the Password Practices of End-users and Service Providers'. In Proceedings of HCI International 2013, Las Vegas, Nevada, 21-26 July 2013.
9. Ur, B; Kelley, PG; Komanduri, S; Lee, J; Maass, M; Mazurek, ML; Passaro, T; Shay, R; Vidas, T; Bauer, L; Christin, N; Cranor, LF. 'How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation'. Proceedings of the 21st USENIX conference on Security symposium, USENIX Association Berkeley, CA, 2012.
10. Mattord, HJ; Levy, Y; Furnell, S. 'Factors for Measuring Password-Based Authentication Practices'. Journal of Information Privacy and Security, 2014, vol.10, no.2, pp.71-94.
11. Mohamed, K. 'Password meter tutorial'. GitHub,19 Sep 2014. Accessed Jan 2017. https://github.com/lifeentity/password-meter-tutorial.
12. Walker, James. 'Researchers have developed a new password system that uses emoji'. Business Insider, 29 Dec 2015. Accessed Jan 2017. www.businessinsider.com/researchers-developed-new-emoji-password-system-2015-12.
13. Bonneau, J. 'The science of guessing: analysing an anonymized corpus of 70 million passwords'. Proceedings of the IEEE Symposium on Security and Privacy, San Francisco, CA, 20-23 May 2012.
14. Felt, AP; Reeder, RW; Ainslie, A; Harris, H; Walker, M; Thompson, C; Acer, ME; Morant, E; Consolvo, S. 'Rethinking Connection Security Indicators'. Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), 22-24 June 2016, Denver, CO, US. ISBN 978-1-931971-31-7.

The worst of both worlds – the problems with the EMV shift in the US

Don Bush

Don Bush, Kount

On 1 Oct 2015 we saw the anticipated and arguably long overdue EMV liability shift in the US. Some 10 years after Western Europe, and 20 years after the technology was developed, EMV cards (ie, payment cards with a chip to encrypt the information held on cards) were finally to become the norm for US consumers.

The liability shift meant that if merchants suffered card fraud and they did not have EMV-enabled card readers then they would be liable for the costs of that fraud. It was hoped that this would encourage merchants to make the necessary investment in the machinery needed to accept EMV cards.

Prior to the liability shift, the majority of payment cards in the US used the magstrip to store the card information. Magstrip technology has its roots in the Second World War. This venerable, obsolete technology is easy to hack and easy to clone. It is very much an analogue technology in a digital world. And yet it took the US a surprisingly long time to ditch the magstrip and adopt the chip. EMVCo figures from the first quarter of 2014 showed that while 96.33% of all card transactions in Europe Zone 1 (all of Europe save countries in the former Yugoslavia and former Soviet Union) were made using encrypted cards – in the US, this figure was a minuscule .03%.[1]

What, then, was the tipping point that led to the US adopting EMV? In 2014, there was a significant number of high-profile breaches in leading US retailers. Household names such as Target, Michael's and Home Depot all suffered damaging data breaches, with millions of card holders finding their personal details compromised. Out of the 1,500 reported breaches in 2014, 1,164 were in North America, almost 78% of the total number.[2] North America truly was the epicentre of the card fraud storm.

It was estimated, prior to the liability shift, that the total costs of making the US EMV compliant would be $8.65bn, a considerable sum of money.[3] The 2014 breaches clearly convinced US card issuers that this was, finally, a sum worth paying. And so in October 2015 the long-awaited liability shift happened. What has happened since? Has there been a drop in fraud? Has it been a success?

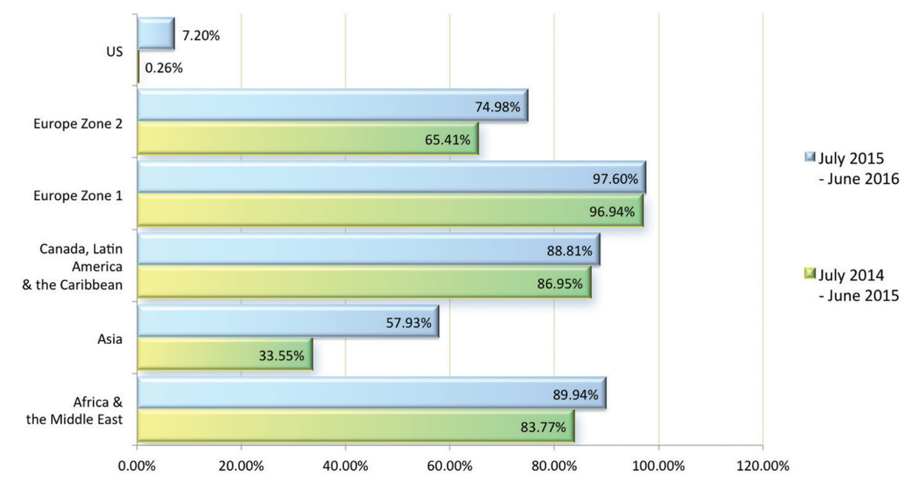
Card-present fraud

MasterCard has recently reported a strong uptake in EMV chip-enabled cards, stating that as of June 2016, nine in 10 of its cards in circulation in the US have EMV chips.[4] It also announced that one in three US merchants now have EMV terminals.

In terms of fraud, MasterCard has released data that show a 54% decrease in counterfeit fraud costs between April 2015 and April 2016.[5] This is good news from MasterCard and is surely indicative that the roll-out has been a success. But not entirely.

Only one third of merchants have EMV terminals and the 54% decrease in counterfeit card fraud is only for merchants who have EMV-enabled payment devices in-store. For larger merchants who have yet to adopt this technology, there has been a rise of 77% in counterfeit card fraud.

What, then, could be causing this? Where there is a window of opportunity fraudsters will take it. And in this situation the opportunity exists to continue to carry out counterfeit card fraud. While MasterCard might be proud of the one in three merchants who have adopted EMV payment technology, the fact remains that two in three do not. This means that the majority of US merchants are still open to the same old frauds as before.



Percentage of card-present transactions that are EMV. Source: EMVCo.

Chip and PIN

In Europe, chip-encrypted payment cards are given a further layer of security by cardholders having to enter their PIN on the payment device at the point of sale. In the US, though, this is still far from the norm. For the most part, the authentication of the card holder is still being done via the signature.

While the addition of the EMV chip in cards might help prevent the cloning of card, by not using the PIN it is doing nothing to stop stolen card fraud. A signature is easy to forge and, as US shoppers will testify, isn't always checked as rigorously as it could be (if at all). So this takes away much of the power of the technology.

Provided that the PIN is kept secure and not shared with anyone, it is a very secure and simple method of in-store authentication. Without this critical part of the EMV equation, payment cards are still far less secure than they could or should be.

There is also a significant amount of anecdotal evidence that where EMV payment devices are installed they are still not being used. This could be down to a lack of training for staff and a lack of education for consumers, but it is symptomatic of the fact that the launch of EMV in the US has been, at best, half-hearted.

It is to be expected that the PIN part of the Chip and PIN process will come into play in the US but this will require more education both for retail workers and consumers.

CNP fraud

In the run-up to the EMV liability shift in the US, fraud experts expected a rise in card-not-present (CNP) fraud. Drawing on the example of the UK – where in the 10 years between 2004 (when EMV was first introduced in the UK) and 2014, CNP fraud increased by 120% – something similar was predicted for the US.[6]

While figures for the past 12 months are as yet unavailable, there is some evidence to suggest that the predictions are sadly coming true. Figures from the end of Q2 2015 to Q1 2016 (which takes in six months of post-EMV activity) suggest that there has been a 137% rise in CNP fraud in the US.[7] To understand what this figure really means, compare it to the UK where, between 2014 and 2015, there was a 20% rise in CNP fraud.[8] Of course, EMV protocols are well established in the UK.

This triple digit rise in fraud seems to suggest that, as predicted, fraudsters in the US are now turning to online fraud in large numbers as the counterfeit card channel is closed off. As more figures are released from industry and law enforcement bodies, we can confidently expect to see this trend continue.

We can expect this growth to be global, too. CNP fraud knows no boundaries and fraudsters who turn now to online and CNP fraud will find that they can use fraudulently obtained card details around the world. It would be surprising, to say the least, if the 2016 global fraud figures did not show a significant spike that could be directly attributed to the sudden grown in US-based CNP fraud.

Worst of both worlds

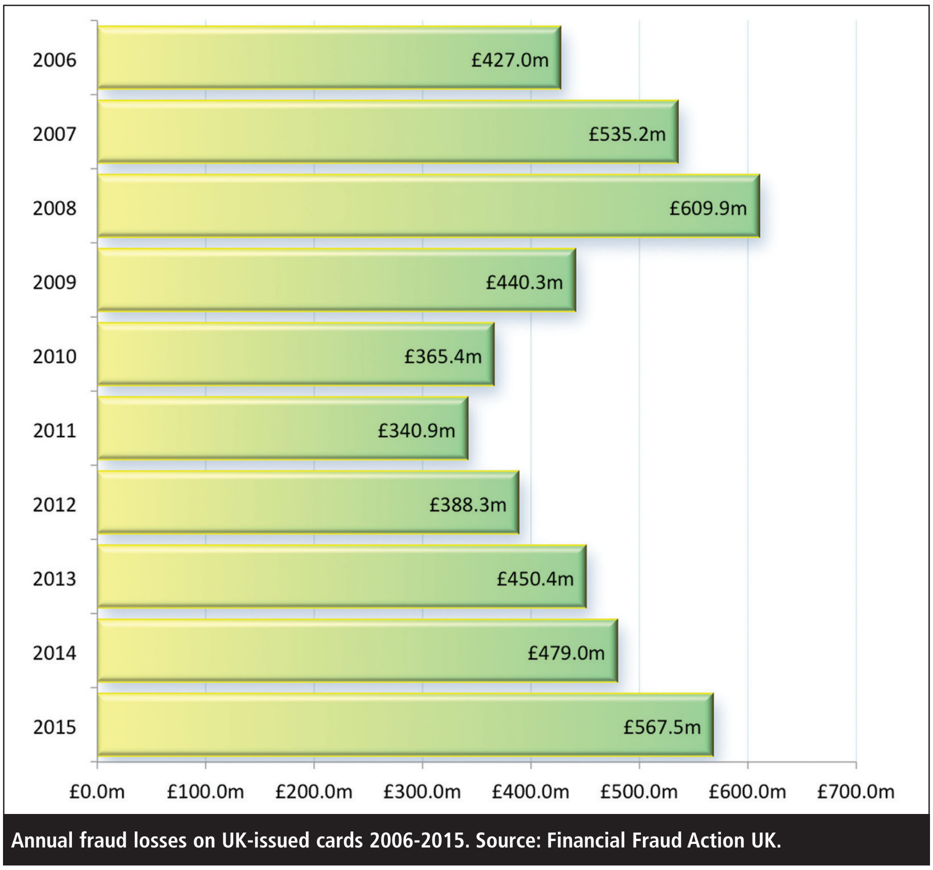
What we have seen with the EMV roll-out in the US is, in essence, the worst of both worlds. In Europe, while there was a considerable increase in card-not-present fraud (which was also driven by the fact that online commerce truly took off at the same time), this was mitigated by a drop by card-present fraud.

In the US, this is not the case. While fraud where merchants have EMV-enabled payment devices has dropped, it is rising where merchants do not have them. And given that this, a year after the liability shift, still represents two-thirds of all US merchants, this is a deeply concerning trend.

It is the worst of both worlds because the EMV shift is incomplete and will remain incomplete for some time to come. There isn't so much a gap left for fraudsters as a gaping door. Coupled with the fact that the PIN is still not commonplace as a method of authenticating face-to-face sales, we are left with a situation where card-present fraud is still rising. Couple this with the sudden spike in CNP fraud and the outlook for fraud in the US and, indeed, worldwide, is looking concerning.

No window of opportunity

What, then, is the answer? In the first instance, the EMV roll-out should be completed and completed properly, with no windows of opportunity left open to fraudsters. This means that every merchant should have EMV-enabled payment devices and authentication should come via something more robust than signatures. Whether this is PIN, biometrics or something else is for another discussion, though.



Annual fraud losses on UK-issued cards 2006-2015. Source: Financial Fraud Action UK.

Second, there has to be a cross-industry drive towards tightening up online security. Banks, issuers, merchants, consumers and law-enforcement agencies must work together to stop fraudsters getting access to personal details and using them.

If we know that we can expect a significant rise in CNP coming from the US then non-US based merchants should pay special attention to transactions coming from the US. This doesn't mean, of course, that all of them should be declined. But merchants, certainly, should be aware of where transactions are coming from and make their decision to decline or accept with this information in mind.

This isn't Armageddon and we don't wish to be hyperbolic about the threat of fraud coming from the US. It will take a concerted and cross-industry effort to fight it. Yet with the right tools and the right attitude, this is far from impossible.

About the author

Donald Bush is the VP of marketing at Kount, having joined the company as director of marketing in October 2010. He attended Brigham Young University, studying business administration and marketing. Prior to joining Kount, Bush was director of marketing at CradlePoint, a manufacturer of wireless routing solutions in the mobile broadband industry. He has worked in several management roles within the technology sector for over 20 years with both hardware and software manufacturers and as a partner in two top technology marketing agencies. He has led product launches and marketing programmes for dozens of companies around the world such as Citi, HP, IBM, Kodak, Motorola and Weyerhaeuser and co-authored the seminar series 'Common Launch Disasters and How to Avoid Them'.

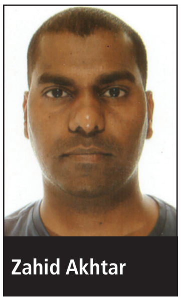
References

1. 'Worldwide EMV deployment statistics'. EMVCo. Accessed Jan 2017. www.emvco.com/about_emvco.aspx?id=202.

2. Reisinger, Don. 'In shift, hackers want your identity, not just your credit card'. CNET, 12 Feb 2015. Accessed Jan 2017. www.cnet.com/uk/news/in-shift-hackers-want-your-identity-not-just-your-credit-card/.
3. 'Will retailers be ready for EMV by Oct 2015?'. FIS Payments Leader, 16 Oct 2013. Accessed Jan 2017. www.paymentsleader.com/will-retailers-be-ready-for-emv-by-oct-2015.
4. 'Mastercard reports strong US EMV uptake'. NFC World, 13 Sep 2016. Accessed Jan 2017. www.nfcworld.com/2016/09/13/347237/mastercard-reports-strong-us-emv-uptake.
5. 'Mastercard says fraud costs dropped 54% since (EMV) October 2015'. PYMNTS.com, 13 Sep 2016. Accessed Jan 2017. http://www.pymnts.com/news/emv/2016/mastercard-fraud-costs-emv-impact/.
6. 'Card fraud figures'. The UK Cards Associations. Accessed Jan 2017. www.theukcardsassociation.org.uk/plastic_fraud_figures/.
7. Card Not Present, news home page. Accessed Jan 2017. https://cardnotpresent.com/news/.
8. 'Fraud the Facts 2016'. Financial Fraud Action UK, 2016. Accessed Jan 2017. https://www.financialfraudaction.org.uk/wp-content/uploads/2016/07/Fraud-the-Facts-A5-final.pdf.

Biometrics vs passwords: a modern version of the tortoise and the hare

Kamran Siddique



Zahid Akhtar

Yangwoo Kim

Kamran Siddique, Dongguk University, South Korea; Zahid Akhtar, INRS-EMT, University of Quebec, Montreal; and Yangwoo Kim, Dongguk University

A popular misconception that biometrics represent the ultimate in authentication and that passwords are dead is causing a significant setback in digital security. For more than a decade, people (and, unfortunately, some vendors) have been promoting this trend with the claim of impregnable digital security. However, this claim is not only unjustified but has also suppressed core password research.

Alas, no technology is a magic bullet for digital security in all situations. Each security technology has strengths and weaknesses and there is a need to recognise the factors that make them better or more suitable for specific application scenarios, including being used alone or in conjunction with other methods. An analysis of widely adopted security technologies suggests that the case for password displacement requires revisiting, to weigh logical factors over convenience and commercial interests.

Slow and steady

Since ancient times, we have been declaring the tortoise (or the turtle) as the winner against the hare (or the rabbit), with the moral 'slow and steady wins the race'. Recently, a modern version of the story has been launched with another perspective – ie, teamwork, where winning a race depends on overcoming weaknesses, identifying individual competencies and exploiting their efficiencies and optimal utilisation to beat the odds.[1] Although it took several decades to think differently and bring efficiency into practice, it is still much better than never doing so. Similarly, the competition between biometrics and passwords deserves analytical treatment in order to achieve efficiency rather than encouraging misplaced attempts to dislodge passwords spanning decades.

News of a death in a society is generally treated as sad news, but interestingly it always brings excitement in the digital world, particularly when associated with passwords. For example, a recent survey showed that 84% of respondents supported the elimination of passwords, with 76% preferring alternative authentication solutions, and 59% preferring fingerprint scanning over passwords.[2]

Thus, a vital question arises: despite countless attempts to displace passwords and overwhelming hatred from the users, how has password security continuously cheated death till now? This phenomenon is causing a significant setback in security that needs to be assessed and rectified pragmatically. In particular, extensive experiments are not always needed to understand such phenomena and alter the future course to avoid failure.[3] However, a careful formal analysis and reasoned arguments supported by facts are crucial.

View ahead

Unproven claims about the elimination of passwords and promoting biometrics