About MYPINPAD

MYPINPAD is a technology company with a goal of delivering economic, scalable solutions to meet our clients’ diverse requirements for authentication and identity management.

The Company is managed by an alliance of leaders from the payments industry with a collective 100+ years’ experience spanning a wide spectrum of banking, security and payment technology.

MYPINPAD is a global leader in payments software solutions. The patented technology creates a trusted and hardened environment to protect sensitive consumer operations on devices such as smartphones and tablets.

Available as an SDK, the solution allows for rapid and simple integration into an Acquirer’s, Issuers or PSP’s existing technology stack, enabling bank grade, multi-factor authentication through the use of card PIN and FIDO Biometric credentials for financial transactions, secure sign-in and consumer on-boarding.
Executive Summary

Allan Syms, COO, MYPINPAD

More than £1.7m a day was lost to financial fraud across payment cards in the UK last year, with losses on card purchases made remotely comprising £1m of this daily figure. This news makes for uncomfortable reading and has inevitably had a negative impact on consumers’ trust in online banking and shopping.

Although financial fraud is high, organisations such as Financial Fraud Action UK have recognised that a considerable volume of attempted fraudulent activity is prevented through the efforts of banks and card companies, with £1.38bn worth of fraudulent activity prevented in 2016.1

There is a strong case to support the view that a lack of trust in online commerce and financial transactions has held back consumer adoption of online payments. More consumers could be making online payments if they had a better understanding of (and greater confidence in) the processes and security measure behind these payments.

To help build consumer trust one of the most innovative developments we can expect to see in the mobile world this year is ability for consumers to enter their card PIN number securely into their mobile devices to authenticate a transaction. We will also see the growth and adoption of strong multi-factor authentication, especially as it becomes a mandatory part of the Second Payment Services Directive (PSD2).

Our own research found that UK consumers have a high degree of confidence in PIN as a method of authentication, with 85% of respondents saying they would like to be notified on their mobile of high value transactions and have the ability to instantly authorise with their card PIN. An even higher percentage (90%) of frequent online shoppers said that if it were available they would use PIN to authorise payment via a mobile device.2

To gain a better understanding of how news of rising online fraud and data breaches have impacted consumers’ use of mobile and online payments, MYPINPAD conducted a survey to ascertain what could be done to boost consumer confidence and trust in online transactions, specifically in terms of security and authentication.

The results are analysed within – we hope you find them insightful.

Guest Foreword

Robert Courtneidge,
Global Head of Cards and Payments
Locke Lord (UK) LLP

PSD2 will reduce the barriers to entry for competitive players trying to join the payments market and therefore stimulate competition and innovation. The European Banking Authority (EBA) has made it clear that the proposed regulatory technical standards on Strong Customer Authentication (SCA) and secure communication are key to promoting innovation and improving the security of payment services across the European Union.

Consumers are increasingly carrying out financial transactions using their mobile devices, for services such as online banking, paying for a taxi or buying goods online. While this has been hugely convenient for consumers - resulting in increased levels of revenue for companies - the industry needs to tread carefully when considering data sharing.

Failure to appropriately safeguard such data could result in greater instances of data breaches and damage the trust consumers have in businesses and banks.

MYPINPAD is already leading the way in digital security by using the cardholder PIN and FIDO Biometric technology for authentication on devices such as smartphones and tablets - combining first class security practice, great user experience and innovative technology to empower the consumer.

We already know that many consumers feel more comfortable conducting financial activities where multi-factor authentication is used. MYPINPAD’s research indicates that the majority of online UK consumers are willing to adopt more rigorous processes to access online banking services and make payments in return for greater security.

Consumers will feel more positive towards brands that proactively seek to protect them, by adding multi-factor, transaction appropriate, security for online transactions.

Authentication solutions act like defences against fraud and like all defensive measures, they work best when used in combination with each other. It is important that authentication solutions such as biometrics are combined with other authentication methods, to offer the greatest levels of protection while maintaining a smooth customer experience.
Background

Recent fraud data underlines the challenge of maintaining customer trust in online transactions.

Financial Fraud Action UK reports that losses due to payment card fraud in 2016 totalled £618m, with losses on card purchases made remotely increasing by 9% to £432.3m; the global figure for card fraud losses now stands at an estimated $21.84bn (£17.07bn). However, the data also shows that banks and issuers are making progress in reducing losses, with £138bn of fraudulent activity prevented in 2016. Nonetheless, fraudsters are constantly trying to break the industry’s security systems.

Increasing consumer confidence in online and mobile commerce is not just about preventing fraudulent transactions though – it is also about boosting the number of successful transactions.

False positives are a major issue for merchants. Security measures often incorrectly flag legitimate transactions, which impacts on the customer experience, causing frustration to those trying to purchase items and results in reduced revenue for merchants.

According to a 2015 Javelin whitepaper, 15% of all legitimate cardholders in the US experienced at least one decline because of suspected fraud over the previous 12 months, resulting in a total of $116bn declined transactions. Nearly 4 in 10 (39%) of declined cardholders reported that they abandoned their shopping cart after being falsely declined.

Javelin also found that the false positive decline rate is more than three times that for known card fraud. Closing that gap will increase merchant’s revenue, which is also beneficial for issuers and acquirers. There is a simple way to reduce false positive declines, particularly for remote transactions, and this is with strong, yet convenient, consumer authentication.

Banks’ ability to invest in authentication solutions is in many cases inhibited by the need to maintain legacy systems and by the overhead of regulatory compliance. However, PIN as an authentication method has been used successfully at ATMs for more than 30 years and consumers are familiar with entering a PIN code to access their bank accounts. Having taken the PIN from ATM to the store, merchants and consumers are now ready to take their PIN into the digital age.

Consumers want to know more about the security of payments and take control of their finances - financial education leads to financial literacy and capability and in turn, to financial wellbeing. The Centre for Economics and Business Research has previously estimated that consumers’ lack of financial know-how costs the UK billions of pounds a year and it is clear that informed consumers are better equipped to enjoy the enhanced financial freedom different payments systems can offer.

Consumers are also becoming more concerned about fraud, and banking institutions and Payments Service Providers (PSP) need to step up their educational efforts to maintain consumer confidence. Merchants with an online and mobile presence will need to remain vigilant and open to a wider variety of fraud prevention solutions.

A 2016 LexisNexis report found that the mobile channel’s share of successful fraud transactions among large remote channel merchants in the US had grown from 26% in 2015 to 35%. As mobile commerce grows, so does mobile fraud. Fighting this trend will require targeted and mobile-optimised fraud prevention solutions.
**Measuring Consumer Trust: Survey Findings**

There needs to be an evolving conversation between banks, retailers and their customers with regards to what makes a consumer safe whilst transacting and banking online. MYPINPAD conducted a survey to ascertain what could be done to boost and retain customer trust, specifically in terms of security and authentication.

*This survey is the second in a series of insightful research conducted by MYPINPAD to understand better the dynamics around consumer trust in digital and online commerce.*

<table>
<thead>
<tr>
<th>Key Findings</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only 2% of respondents believe speed is more important than security when completing an online transaction</td>
<td>2%</td>
</tr>
<tr>
<td>Are concerned about their online shopping and banking security, with almost a quarter of all respondents ‘very concerned’</td>
<td>67%</td>
</tr>
<tr>
<td>Stated that information about data breaches and fraud has impacted their trust of online shopping and banking</td>
<td>61%</td>
</tr>
<tr>
<td>Of respondents have been a victim of online fraud</td>
<td>29%</td>
</tr>
<tr>
<td>Respondents have no idea whether or not they have fallen victim to online fraud</td>
<td>1 IN 10</td>
</tr>
<tr>
<td>Of respondents want to use card PIN as a means of authenticating an online transaction</td>
<td>40%</td>
</tr>
<tr>
<td>Would like the option to use a combination of card PIN and biometrics</td>
<td>50%</td>
</tr>
</tbody>
</table>
The survey also confirmed that just over one in four respondents said they were ‘very concerned’ about online banking and shopping security.

A further 41.5% described themselves as ‘somewhat concerned’. Only 2.7% said they were not at all concerned by the security of online banking and shopping. Similar concerns have been expressed elsewhere; in Mintel’s Consumer Attitudes towards Mobile Payments UK 2016 report, 76% of respondents said they were concerned about the risk that hackers might be able to make fraudulent transactions.

Just under one in three of survey respondents claimed to have been a victim of online fraud; worryingly, more than 9% said they ‘didn’t know’. In excess of 60% said information about data breaches and online fraud had significantly impacted their trust in online shopping and banking.

When asked how this had changed their online shopping behaviour, 11.3% said they shopped less and almost one in 10 said they did not use mobile devices to carry out transactions.

Our survey revealed that security of transactions was more important than speed for 45.7% of respondents, with smaller independent online retailers perceived to be the most vulnerable to online fraud. A disturbingly high number – one in four – felt banks were vulnerable to online fraud risks despite Financial Fraud Action UK reporting a 19% fall in remote banking fraud losses last year compared with 2015.

Encouragingly, more than 57% of respondents expected online commerce security to improve over the next five years.

The use of both card PIN and biometric based authentication was identified by half of the survey respondents as the most significant step online retailers and banks could take to improve consumer trust, whilst just under 40% referred to the use of card PIN based authentication alone as a strong method in which to protect their data.

Implications

Which business types do consumers believe are most at risk from fraud?

<table>
<thead>
<tr>
<th>Business Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smaller independent retailer</td>
<td>65%</td>
</tr>
<tr>
<td>Large online retailers</td>
<td>44%</td>
</tr>
<tr>
<td>Banks</td>
<td>39%</td>
</tr>
<tr>
<td>Travel providers</td>
<td>29%</td>
</tr>
<tr>
<td>Utility companies</td>
<td>17%</td>
</tr>
<tr>
<td>Others: Gaming and other companies</td>
<td>5%</td>
</tr>
</tbody>
</table>

Banks

For banks, card PIN as an authentication tool is tightly integrated within their legal fabric and legacy infrastructure, it is trusted by the consumer and can be swiftly implemented on mobile and other touchscreen devices with minimal change.

There is also a regulatory imperative. The revised EU Second Payments Services Directive (PSD2) requires that all Payment Service Providers adopt ‘Strong Customer Authentication’ (SCA). This means an authentication method based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others and is designed in such a way as to protect the confidentiality of the authentication data.

With Juniper Research forecasting that the number of users accessing retail banking services via smartphones, tablets, PCs and smartwatches will rise by more than half to nearly three billion by 2021, banks will need to focus on providing a more frictionless and secure digital experience for their customers, especially if they are to retain customer trust and remain market leaders.

Payment Service Providers and Online Merchants

With eMarketer valuing UK mCommerce sales at more than £25bn in 201612 – up by more than a quarter compared with 2015 – and forecasting an increased worth of more than £42bn by the end of the decade, and global eCommerce revenue predicted to reach $2.4tn by 201913, the scale of the opportunity for those business which can gain and retain customer trust is clear.

For example, if the respondents to the MYPINPAD survey, who said they have never completed a transaction via their mobile device, could be encouraged to change their behaviour with increased security, the additional revenue generated could significantly improve the bottom line for merchants, issuers and acquirers.

Consumers are changing their behaviour based on the degree of trust they have each eCommerce or mCommerce channel. Merchants of all sizes will need to adopt appropriate levels of security and, innovative and future-proofed authentication methods play a crucial part in this.

As our research has demonstrated, with increased damage to consumer trust, it is a vital time for businesses to ensure they have the best security processes in place.

Authentication methods must be compliant with the upcoming PSD2 regulations and meet the EBA requirements for Strong Customer Authentication (SCA). Currently only 46% of PSPs are prepared to comply.14

If compliance and implementation of scalable security systems is done correctly, PSPs, issuers, acquirers and merchants will have the opportunity to transform the online and mobile industry as we know it; improving the customer experience, enabling greater transaction volumes, and adding to the value of the merchant services they deliver.

How Can Consumer Trust Be Increased?

Consumers appear to have huge concerns about fraud, which has harmed trust and impacted on behaviour. Our survey indicates that consumers do not believe transaction speed is more important than security, and would accept reasonable friction to enhance transaction security.

In order to gain trust, banks, merchants and PSPs should implement multi-factor authentication.

Entering a PIN in to a mobile device facilitates SCA by verifying the identity of a person through something you have (a mobile device) something you know (card PIN) and with the additional layer of something you are (a biometric).

MYPINPAD has a simple and incredibly effective mobile authentication platform. The technology utilises biometrics and card PIN to identify consumers across sectors, devices and channels whilst fully meeting all known best security practices and regulations.

PIN is a universally accepted form of authentication. It is a truly habitual behaviour that has been embedded over decades of education and experience. For the customer, entering their PIN within a familiar and trusted environment provides a level of security they are comfortable with. Combined with biometrics, merchants would not only answer to consumers’ demand for increased transaction security, but incorporate multi-factor authentication to their check out processes. Ultimately providing a secure and friendly environment for legitimate consumers and bridging the gap between rigorous security and smooth customer experience.

The business has developed a number of solutions and technologies that are deployed by issuers and financial institutions onto a consumer’s own mobile device to enable bank grade, multi-factor authentication for online payments, banking, on-boarding and log-ins. The technologies are perfectly positioned for deployment, creating a trusted and hardened environment in which to securely enter and protect sensitive data on devices such as tablets and smartphones.

| 98% | of consumers believe transaction security is more important than speed |
| 50% | would like to use a combination of both PIN and biometrics |
| 40% | of respondents would like to use cardholder PIN as a means of authenticating an online transaction |
Conclusion

The challenges of addressing the concerns highlighted in our survey should not be underestimated. In its final draft, Regulatory Technical Standards (RTS) on strong customer authentication and common and secure communication published in February 2017\(^\text{15}\), the European Banking Authority (EBA) recognises that enhancing security and protecting consumers whilst facilitating customer convenience and innovation and enhancing competition under PSD2 involves trade-offs.

Across all channels, the industry needs appropriate and scalable security and authentication methods. For example, the level of payment security needed to purchase an app does not have to be as stringent as that for a high value item, which the EBA has recognised by increasing the threshold for remote payment transactions from €10 to €30.

Significant growth in the adoption of mobile payments in 2017 and beyond is inevitable. In Europe alone, the number of consumers using a mobile device for payments has tripled from 18% in 2015 to 54% in 2016\(^\text{16}\). As the popularity of online and mobile purchases continues to grow so has the associated fraud; consumer authentication needs to be multi-factor, consistent and convenient.

From acquirers to retailers to systems integrators and payment service providers, drivers of mobile payments have a key role to play in educating consumers of the benefits, security and convenience of mobile payments. Awareness amongst younger consumers is the essential precursor to mass-market adoption,


 Significant growth in the adoption of mobile payments in 2017 and beyond is inevitable. In Europe alone, the number of consumers using a mobile device for payments has tripled from 18% in 2015 to 54% in 2016.

yet there are solutions like PIN that offer a ‘bridge’ to other generations who already trust and are familiar with this method of authentication.

The emergence of card PIN and biometrics authentication supports market demand to enhance online and mobile experiences. Previous MYPINPAD research\(^\text{17}\) has found that the vast majority (85%) of consumers surveyed would be comfortable using PIN to authenticate transactions on a mobile device. Secure PIN entry on smart mobile devices is ready to meet looming regulatory demands and can easily be deployed by traditional and new third-party payment providers.

Conclusion

The challenges of addressing the concerns highlighted in our survey should not be underestimated. In its final draft, Regulatory Technical Standards (RTS) on strong customer authentication and common and secure communication published in February 2017\(^\text{15}\), the European Banking Authority (EBA) recognises that enhancing security and protecting consumers whilst facilitating customer convenience and innovation and enhancing competition under PSD2 involves trade-offs.

Across all channels, the industry needs appropriate and scalable security and authentication methods. For example, the level of payment security needed to purchase an app does not have to be as stringent as that for a high value item, which the EBA has recognised by increasing the threshold for remote payment transactions from €10 to €30.

Significant growth in the adoption of mobile payments in 2017 and beyond is inevitable. In Europe alone, the number of consumers using a mobile device for payments has tripled from 18% in 2015 to 54% in 2016\(^\text{16}\). As the popularity of online and mobile purchases continues to grow so has the associated fraud; consumer authentication needs to be multi-factor, consistent and convenient.

From acquirers to retailers to systems integrators and payment service providers, drivers of mobile payments have a key role to play in educating consumers of the benefits, security and convenience of mobile payments. Awareness amongst younger consumers is the essential precursor to mass-market adoption,
Europe

Level 39
1 Canada Square
Canary Wharf
London, E14 5AB

+44 (0)203 289 6728

info@mypinpad.com
www.mypinpad.com

Asia

21/F Gloucester Tower
The Landmark
15 Queens Road Central
Hong Kong

+6281210298920